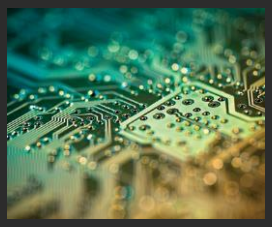
Ciberriesgos 2021:
Un Año en Retrospectiva

pwc

Contenidos



Introducción

El ransomware consolidó su posición como la amenaza de ciberseguridad más prominente a la que se enfrentan las organizaciones en todas las geografías y sectores, con un mayor impulso e impacto a lo largo de 2021.

PwC sirve a más de 200.000 clientes en 156 países. Aprovechamos nuestra posición ventajosa como una de las mayores y más globales redes de servicios profesionales para ofrecer información superior (y crucial) información sobre amenazas a nuestros clientes. Nuestra investigación es la base de todos nuestros servicios de seguridad, y es utilizada por organizaciones del sector público y privado de todo el mundo para proteger las redes, proporcionar conocimiento de la situación e informar sobre la estrategia. Este informe anual documenta las tendencias generales y temáticas que observamos en 2021, y forma parte de nuestra contribución para ayudar a construir una sociedad digital segura.

Los programas de afiliación y los esquemas de Ransomware como Servicio (RaaS) fomentaron un mayor crecimiento de la amenaza de la ciberdelincuencia, y su impacto oculto en las vidas quedó cada vez más al descubierto, ya que las escuelas, las organizaciones benéficas, los servicios públicos y las infraestructuras críticas a menudo sufrieron la peor parte de los ataques indiscriminados. Estas estructuras agilizaban las vías de compromiso para obtener beneficios, proporcionando incentivos financieros, tratos basados en la reputación e incluso proporcionando a los operadores recursos tales como manuales de intrusión paso a paso. Al mismo tiempo, las estructuras de ransomware siguieron reforzando los vínculos mutuos con el ecosistema de ciberdelincuencia que los rodea, incluidos los sistemas de distribución de malware (o programa malicioso) tales como TrickBot, IcedID y QakBot, los foros clandestinos que facilitan el reclutamiento de afiliados al ransomware y los mercados de Acceso como Servicio (AaaS).

Mientras que el año 2020 estuvo dominado por la pandemia COVID-19, su propagación por todo el mundo y su impacto en el ciberespacio, una tendencia importante en 2021 fue la proliferación de las habilidades cibernéticas. Las vulnerabilidades de día cero (cero días para solucionar) volvieron a ser una de las principales preocupaciones que se debatieron en las conversaciones sobre ciberseguridad, con temas relacionadas con su investigación, divulgación y explotación que atraen un mayor escrutinio público. Estas cuestiones surgieron especialmente en relación con los ataques indiscriminados y las cuestiones de seguridad nacional, ya que los agentes de amenaza de todas las motivaciones y habilidades se apresuraron a explotar vulnerabilidades de alto perfil como ProxyLogon y Log4Shell. El abuso de los exploits de día cero también se interrelacionó con otros dos fenómenos: el impacto de los intendentes digitales en el panorama de las ciberamenazas (incluido el de los intendentes comerciales), y la actividad de vigilancia contra blancos civiles.

Las operaciones de recopilación de información, en su mayor parte, se mantuvieron alineadas con los acontecimientos geopolíticos. Sin embargo, en 2021, más que en cualquier otro año hasta ahora, identificamos grupos de actividad nuevos y emergentes que persiguen objetivos alineados con los intereses estratégicos de países específicos, incluyendo agentes de amenazas probablemente basados en países de los que no habíamos observado anteriormente actividad ciberriesgo ofensiva.

El análisis de este informe fue realizado por la práctica de Inteligencia de Amenazas de PwC, que está distribuida en Australia, Italia, Alemania, Países Bajos, Suecia, Reino Unido y Estados Unidos. Se basa en nuestros conjuntos de datos de inteligencia internos sobre ciberataques y objetivos de una amplia variedad de agentes de amenazas, la inteligencia obtenida de los compromisos de respuesta a incidentes de PwC en todo el mundo, y nuestros servicios gestionados de cacería de amenazas, así como la información disponible públicamente.

Una tormenta perfecta: Ataques de día-cero, intendentes, y vigilancia

Año del ataque día-cero

Las vulnerabilidades de los ataques llamados día cero, y en particular su investigación y divulgación, han sido un tema de interés siempre presente en la comunidad de ciber seguridad. En 2021, varios sucesos de alto perfil, incluyendo operaciones altamente focalizadas así como la explotación masiva de vulnerabilidades, llevaron este tema una vez más al primer plano de las discusiones estratégicas y tácticas, y al ojo público.

En lugar de tratar los día cero como una amenaza insuperable, en esta sección proporcionamos el contexto estratégico de este fenómeno.

Un día cero a la vez: una visión estratégica del panorama de los día cero

Los debates sobre los día cero suelen girar en torno a la dificultad de evitarlos, basándose en la percepción de que podría ser aún más difícil defenderse de estos. En 2021, vimos cómo la cobertura de este tema se extendía a la tendencia popular, junto con otros temas de alto perfil como el ataque a la cadena de suministro (tras el incidente de SolarWinds) y el ransomware (tras los ataques a entidades como Colonial Pipeline). El año 2021 también registró el mayor número de estos día cero revelados en un solo año1, casi duplicando las cifras de 2020. Las razones de este aumento son matizadas, y probablemente sean el resultado de una combinación de factores, entre ellos :

- **Un elemento más manifiesto de la seguridad nacional:** Aunque los día cero han sido objeto de abuso durante años, en 2021 se produjeron varias muestras políticas de "diplomacia de los día cero", es decir, debates sobre su uso a nivel de seguridad nacional. Por ejemplo, la coalición alemana recién elegida hizo una declaración política sobre el embargo de la compra de día cero por parte del gobierno, citando su "relación altamente problemática con la seguridad informática y los derechos civiles".[2] La Administración del Ciberespacio de China (CAC) anunció nuevas leyes en torno a la divulgación de vulnerabilidades nacionales.[3] La nueva ley también se aplica a los proveedores, que deben garantizar que cualquier vulnerabilidad se mitigue de manera oportuna y se divulgue rápidamente a los clientes junto con las correcciones, y alienta a las organizaciones privadas a establecer programas de recompensas por errores para incentivar económicamente la investigación de vulnerabilidades.
- **El mercado de los día cero se ha expandido:** En los últimos años, ha habido un número creciente de actores que operan en el espacio de la investigación de vulnerabilidades: desde investigadores de seguridad individuales, hasta corredores de delitos de día cero, hasta empresas privadas de espionaje como Hacking Team, FinFisher, NSO Group y Candiru. Los corredores de exploits y las organizaciones del sector privado, en particular, se encuentran entre los actores más destacados en lo que respecta al desarrollo y el comercio de los ataques de día cero.
- **Más incentivos que nunca:** Ahora existen cada vez más vías para que los investigadores de vulnerabilidades compitan y obtengan recompensas económicas por su trabajo de desarrollo de exploits. Estas pueden ser legítimas, como la Tianfu Cup y Pwn2Own, o ilegítimas, como ha sido el caso de los concursos de investigación ofensiva lanzados en foros de la dark web (o internet oscura) en ruso.[4] Con esta actividad firmemente arraigada en el mundo de la seguridad ofensiva, los defensores han tenido que responder, dedicando recursos a su propio trabajo de desarrollo de exploits con fines de identificación y divulgación, como con el Project Zero de Google.[5]
- **Un enfoque renovado sobre la infección de terceros:** Los agentes de las amenazas, con diversas motivaciones, han comenzado a atacar a las organizaciones que participan en las cadenas de suministro, lo que a menudo permite el acceso a varios objetivos a la vez. Esto ha hecho que se inviertan recursos en la investigación de vulnerabilidades de tecnologías empresariales de uso generalizado, como los servidores de correo electrónico o el software de gestión del conocimiento, como ejemplos clave. Naturalmente, esto ha aumentado la cantidad de los día cero descubiertos y, con su divulgación (incluso cuando es responsable y va acompañada de correcciones y avisos del proveedor), la cantidad de intentos de explotar esas mismas vulnerabilidades.

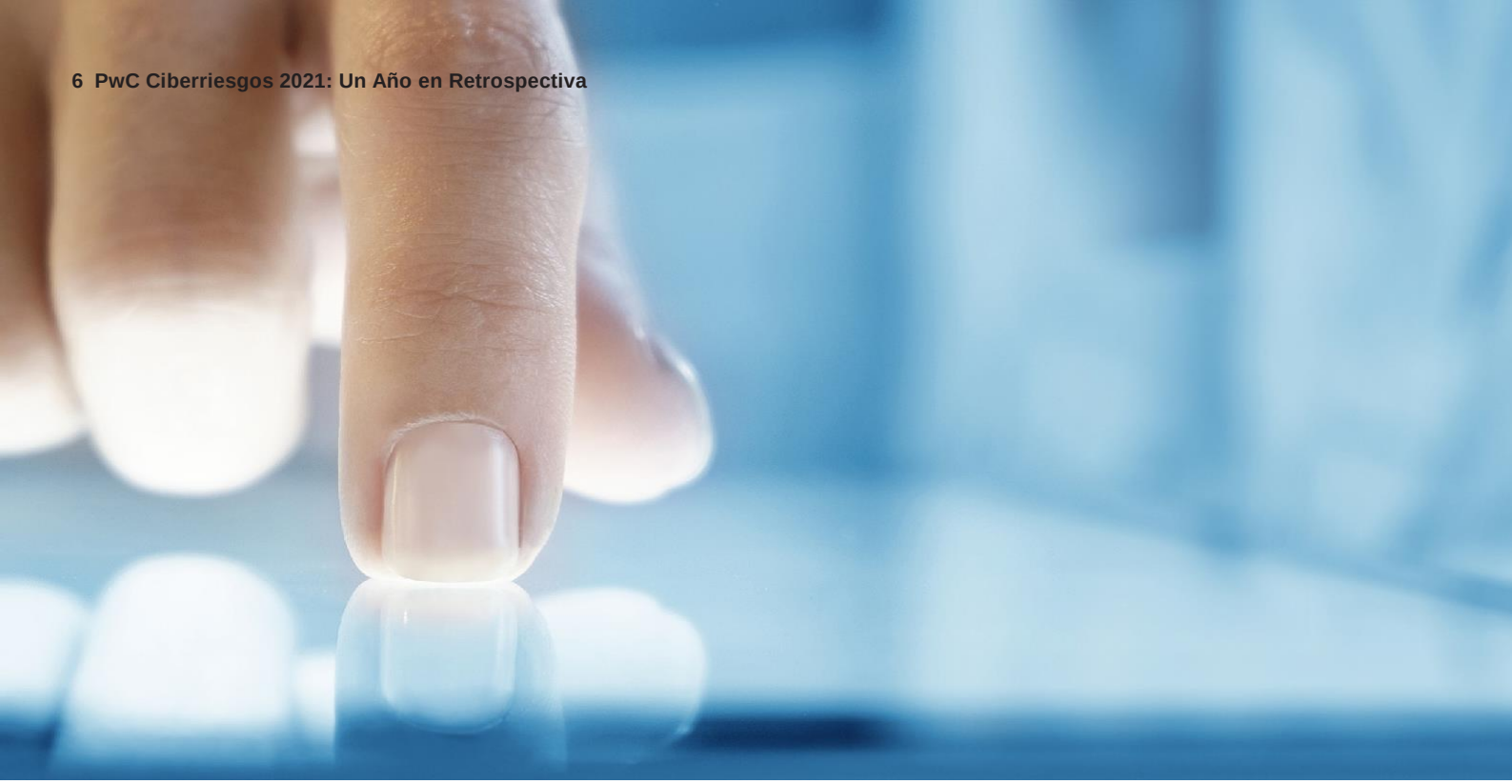
En última instancia, la prevención de los día cero no es una cuestión trivial para los desarrolladores y proveedores de software, y mucho menos para su base de clientes.

Sin embargo, los clientes y los defensores no deberían subestimar las capacidades y medidas que se pueden poner en marcha centrándose en la detección y respuesta a los comportamientos y actividades posteriores a la explotación. Junto con una sólida higiene de seguridad básica, una sólida función de detección y respuesta puede marcar la diferencia en el impacto que los nuevos día cero puedan tener en las organizaciones.

Una visión general de la actividad de intendencia

La forma en que los agentes de las amenazas adquieren y suministran las herramientas puede afectar no sólo a la atribución, sino, lo que es más importante, a sus capacidades y a su habilidad para perseguir nuevos grupos de objetivos. El concepto de intendencia digital no es nuevo en lo que respecta a las operaciones cibernéticas, pero sigue siendo cada vez más relevante. Los intendentes se han asociado tradicionalmente con el suministro de tecnología a las unidades militares. Por lo tanto, los intendentes digitales se consideran más a menudo en el contexto de los agentes de Amenazas Persistentes Avanzadas (APT) que obtienen acceso a las capacidades que sólo comparten un grupo selecto de agentes de amenazas, o que obtienen herramientas de una entidad central encargada de distribuirlas y permitir su uso.

Sin embargo, PwC también define a las empresas que venden soluciones de seguridad ofensivas, como programas espía, exploits de los día cero y capacidades relacionadas, a entidades que luego las explotan que las operan como “Intendentes Comerciales". Mientras que los intendentes tradicionales a menudo sólo proporcionan herramientas a los agentes de amenazas con sede en el propio país del intendente, los clientes de los intendentes comerciales pueden tener su sede en varios países.



Intendentes de APT

Aunque no siempre es posible demostrarlo, no se puede descartar la hipótesis de que varios grupos de Amenaza Persistente Avanzada (APT por sus siglas en ingles) operen bajo el mismo intendente digital, o reciban sus recursos, para varios conjuntos de agentes de amenazas. En 2021, seguimos observando este fenómeno, ya sea a través de observaciones de capacidad compartida (malware, técnicas, exploits, etc.), o a través de solapamientos en la infraestructura (ya sea a través de los mismos patrones observados en los C2, o la reutilización de dominios/IP por otros agentes de la amenaza).

De Sombras y Poderes: Agentes de amenazas con base en China que comparten herramientas

El continuo intercambio de herramientas y técnicas es un tema recurrente entre los agentes de las amenazas basadas en China. Aunque no todos los agentes de amenazas basados en China comparten herramientas entre sí, y no todos tienen acceso a las mismas herramientas, los acuerdos de intendencia (que se tratan con más detalle en una sección posterior) siguen complicando la atribución de la actividad. Por ejemplo, las mismas familias de malware (como PlugX, PoisonIvy, ShadowPad, Quarian y el backdoor Winnti) son utilizadas por múltiples agentes de amenazas con sede en China y, como se ha hecho muy conocido en 2021 con los incidentes de ProxyLogon, algunos agentes de amenazas también comparten exploits.

Aunque no se ha observado que todos estos agentes de amenazas tengan acceso a las herramientas compartidas que se detallan a continuación, se trata de ejemplos destacados de la dinámica descrita en esta sección.

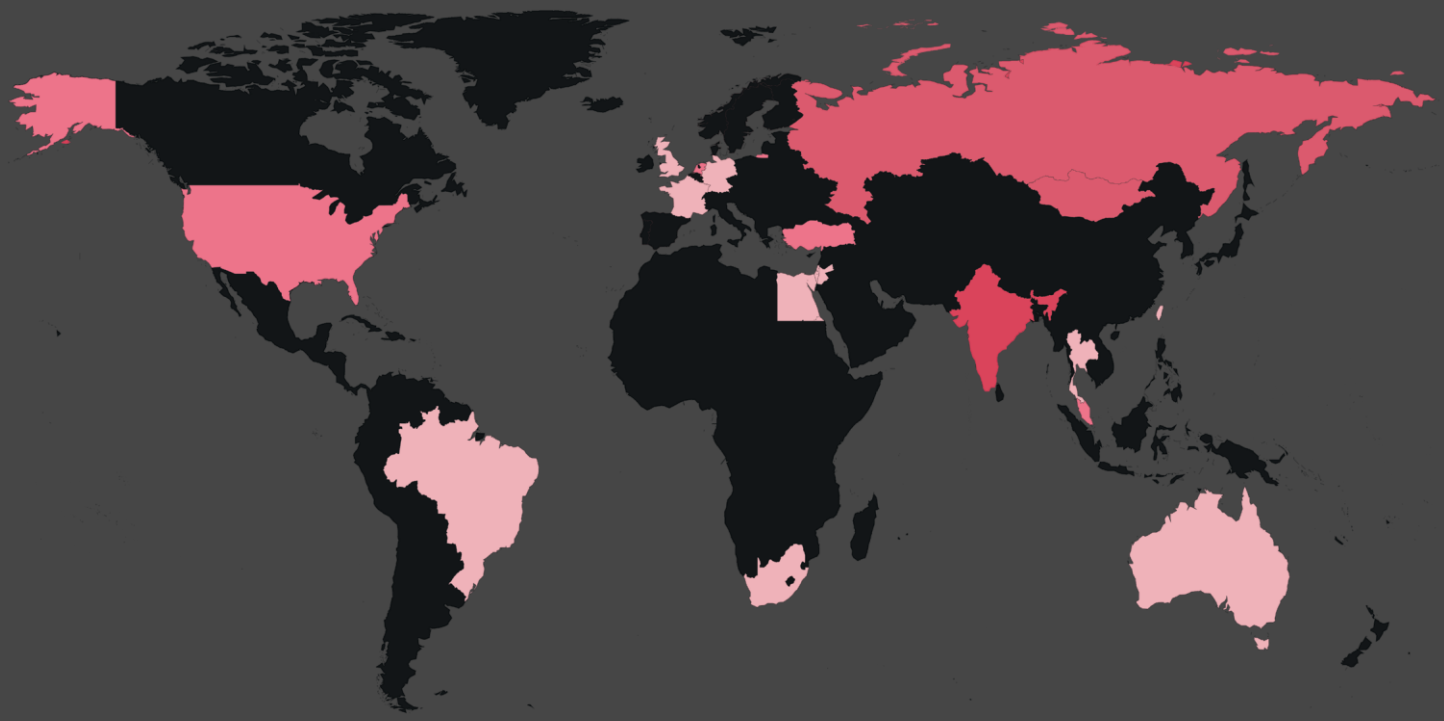
ShadowPad y Scatterbee

ShadowPad es un backdoor modular que permite a un agente de amenazas personalizar la funcionalidad entregada en un implante. Cada muestra de ShadowPad que hemos visto tiene un módulo raíz diseñado para orquestar el siguiente conjunto de módulos, incluyendo un módulo de plugins que puede ser personalizado dependiendo de la funcionalidad que el agente de la amenaza requiera. Los plugins pueden habilitar capacidades que pueden incluir, entre otras, comunicaciones C2 a través de HTTP o TCP, registro de teclas, recopilación de capturas de pantalla, mapeo de puertos y recopilación de información del sistema.[6]

Al rastrear las muestras "estándar" de ShadowPad en 2021, identificamos y analizamos una nueva variante, a la que llamamos ScatterBee: muestras de ShadowPad que habían sido encubiertas usando una técnica personalizada.[7] Probablemente con el fin de minimizar la detección en las redes de las víctimas, el mecanismo de empaque de ScatterBee implementa la ofuscación del flujo de control, la codificación de cadenas, las resoluciones dinámicas de la API, varias técnicas de antianálisis, así como la decodificación/descifrado de shellcode. Evaluamos que uno o más usuarios de ShadowPad tienen acceso a ScatterBee, y es muy probable que hayan entregado algunas de estas payloads (o descargas) maliciosas a través de ataques de watering hole (o de abrevadero) en sitios que se utilizan para entregar archivos de actualización de Adobe Flash. Consideramos que la mayoría de las cargas útiles de ScatterBee pueden vincularse directamente con el agente de la amenaza que rastreamos como Red Dev 10 (también conocido como Earth Lusca), y se han utilizado para atacar a organizaciones de los sectores aeroespacial y de defensa.

Evaluamos que es muy probable que ShadowPad sea utilizado por al menos 11 agentes de amenazas con sede en China.[8] uestro análisis de subconjuntos específicos de la infraestructura de ShadowPad nos permitió identificar un amplio conjunto de víctimas, que van desde entidades con sede en la India en los sectores de las telecomunicaciones y el petróleo y el gas, hasta sucursales de Asia oriental de organizaciones humanitarias internacionales.

Figura 1: Distribución geográfica de las víctimas de ShadowPad observadas hasta diciembre de 2021



Fuente : PwC

"Intercambiando" Intercambio: ProxyLogon

A principios de 2021, Red Dev 13 (también conocido como HAFNIUM) comenzó a explotar vulnerabilidades en Microsoft Exchange, que pasaron a conocerse colectivamente como ProxyLogon.[10, 11] Mientras que la actividad inicial en torno a ProxyLogon estaba asociada exclusivamente a HAFNIUM, a finales de febrero/principios de marzo de 2021 (cerca pero antes del momento de la primera divulgación pública de estas campañas), múltiples agentes de amenazas con base en China comenzaron a explotar las mismas vulnerabilidades, a escala masiva frente a un objetivo preciso.

Como ya hemos destacado, no es raro que estos agentes de la amenaza compartan herramientas. Sin embargo, el rápido intercambio de estos exploits antes del parcheado de las vulnerabilidades de Microsoft Exchange no tiene precedentes.

Creadores en Irán trabajando en múltiples APTs

Los agentes de las amenazas suelen ser identificados por las capacidades, la infraestructura, los objetivos y las TTP generales que muestran. Sin embargo, los desarrolladores u operadores que están detrás de las campañas y que trabajan con múltiples agentes de la amenaza pueden enturbiar el análisis y la atribución.

Este puede ser el caso ocasionalmente de los agentes de amenazas con base en Irán. Por ejemplo, al investigar las campañas de phishing de Yellow Liderc (alias Tortoiseshell, TA456), identificamos un conjunto de documentos PDF maliciosos dirigidos al sector de la educación superior. Este objetivo no se ajustaba normalmente a Yellow Liderc,[12] pero coincide con el de Yellow Garuda (también conocido como Charming Kitten, APT35, PHOSPHORUS, TA453 e ITG18). Anteriormente hemos observado solapamientos de infraestructura entre estos dos agentes de amenazas, lo que plantea la hipótesis de que Yellow Liderc es una rama de Yellow Garuda.[13] Basándonos en varias similitudes entre estos agentes de la amenaza, evaluamos que existe una probabilidad realista de que un operador haya atravesado o cambiado entre ambos en 2021.

Intendentes Commerciales

Los intendentes comerciales difieren de las empresas definidas como hackers por encargo, como CyberRoot y BellTroX.[14] Las empresas de hackeo por encargo se encargan de realizar el hackeo real en nombre de un cliente que paga, mientras que los intendentes comerciales sólo ofrecen herramientas pagadas por el cliente, que luego son utilizadas por el propio cliente para realizar el hackeo. Entre los primeros ejemplos de intendentes comerciales se encuentran Hacking Team y FinFisher, que fueron el centro de una considerable indignación pública y desde entonces han cambiado de marca o han quebrado. A pesar de las consecuencias las actividades de estas empresas', PwC sigue observando que los agentes de las amenazas, en particular los que dirigen operaciones de vigilancia, aprovechan los intendentes comerciales y sus habilidades.[15]

La reciente atención pública que se ha prestado a los intendentes comerciales como NSO Group y Candiru ha permitido conocer una industria relativamente secreta y en crecimiento que tiene implicaciones para los profesionales de la ciberseguridad y las víctimas potenciales, entre ellas:

- dificultad para atribuir a los agentes de la amenaza que, de otro modo, no serían capaces de llevar a cabo operaciones tan sofisticadas;
- la rápida habilitación de un país para atacar tanto al sector privado como al público con malware avanzado, como una empresa, un organismo gubernamental o su personal; y,
- el potencial abuso de estas herramientas para atacar a periodistas, activistas y a la sociedad civil.

Además, las herramientas producidas por los intendentes comerciales se utilizan casi con toda seguridad contra una amplia gama de objetivos, que pueden incluir también a funcionarios del gobierno y ejecutivos del sector privado, lo que justifica la atención de organizaciones que podrían pensar que este tipo de agentes de amenazas no encajan en su perfil de amenaza.

Un ojo siempre vigilante: vigilancia y sociedad civil

La vigilancia de objetivos civiles, ya sea armada por el auge de los proveedores de exploits y de software de vigilancia, reforzada por medidas de intendencia, o llevada a cabo por grupos patrocinados por el Estado, supone una importante amenaza para la consecución de una sociedad digital segura para todos. Las minorías, los activistas de los derechos civiles, los disidentes, los políticos y los periodistas, así como los civiles en general, suelen estar en el punto de mira de estas actividades de espionaje patrocinadas por los Estados. Los objetivos de la sociedad civil suelen incluir también a las ONG, los movimientos sociales, las coaliciones y las organizaciones religiosas que pueden compartir intereses comunes..

Si bien la actividad de vigilancia suele centrarse en una persona de interés, a veces las organizaciones asociadas a esas personas resultan ser víctimas, cuando la organización se considera un peldaño para acceder al objetivo previsto. Este factor es útil para contextualizar las amenazas a la sociedad civil como un problema compartido.

La vigilancia: de los hackers a sueldo a los intendentes comerciales

Candiru

En julio de 2021 Citizen Lab,[16] Microsoft,[17] y Google[18] sacaron a la luz, en mayor o menor medida, un intendente comercial llamado Candiru, al que rastreamos como Grey Mazzikim (alias SOURGUM). Según Microsoft, el software espía del agente se habría desplegado contra más de 100 víctimas. Varios dominios asociados a las campañas que rastreamos en 2021 indicaban un claro objetivo de activistas de derechos humanos y periodistas; otros se alineaban más con los intereses estratégicos de una nación-estado, como las exportaciones de energía u organizaciones de gobierno. El software espía vendido por Grey Mazzikim es muy sofisticado y puede infectar y vigilar iPhones, Androids, Macs, PCs y cuentas en la nube.[19] Una vez que el objetivo está infectado con el software espía, el operador puede filtrar los datos privados de la víctima desde una serie de aplicaciones y cuentas, incluyendo Gmail, Skype, Telegram y Facebook, junto con la captura del historial de navegación y las contraseñas.[20] El agente de la amenaza también podría ser capaz de encender la cámara web y el micrófono del blanco, o tomar capturas de pantalla.

Dado que Candiru es un proveedor de múltiples agentes de amenazas en todo el mundo, la complejidad y la escala de estos ataques es bastante amplia. Con el fin de maximizar la cobertura y la categorización de estas amenazas, PwC rastrea a Candiru como Grey Mazzikim y a sus clientes, que en la actualidad consisten en al menos cuatro agentes de amenazas diferentes, por separado cuando es posible.[21] ay una amplia gama de blancos, pero con un claro enfoque en Europa y Oriente Medio.

NSO Group

NSO Group, que PwC rastrea como Grey Anqa, se fundó en 2010. La empresa es más conocida por su software espía llamado Pegasus, pero también ofrece una gama de otros productos, como software de geolocalización para teléfonos móviles y sistemas de análisis de datos. Sus principales servicios y ofertas de productos se centran en los dispositivos y redes móviles. Pegasus es conocido por infectar las versiones más recientes de los sistemas operativos móviles más populares a través de exploits zero-click y de día cero, incluyendo uno de los exploits más sofisticados jamás documentados, conocido como FORCEDENTRY.[22, 23]

NSO fue noticia en múltiples ocasiones por vender su programa espía Pegasus a Estados-nación que, en última instancia, abusaron de las herramientas para espiar a la sociedad civil.

Las similitudes reconocibles entre Grey Anqa y Grey Mazzikim son muchas: un tipo de empresa similar, que opera desde el mismo país, que recluta de las mismas reservas de talento, con una base de clientes similar. En ambos casos, las capacidades ofensivas fácilmente disponibles para la compra ponen de relieve una industria que permite a un consumidor manejar herramientas sofisticadas de las que también se ha abusado para atacar a la sociedad civil a escala internacional.

Retirada de la circulación: reacción a los intendentes comerciales

2021 ha puesto a los intendentes comerciales de programas espía en el centro de la atención pública y en los tribunales de justicia de varios países. Por ejemplo, varias empresas tecnológicas estadounidenses están presentando demandas contra los proveedores de programas espía comerciales en nombre de su base de clientes, y en algunos casos tratan de restringir el acceso de los demandados al hardware y software de las empresas. En 2021, también observamos la primera acción de alto perfil contra los intendentes comerciales de programas espía a nivel estatal: el Departamento de Comercio de Estados Unidos incluyó a NSO Group y Candiru en su lista de entidades, citando un riesgo significativo de que actuaran "en contra de los intereses de seguridad nacional o de política exterior de Estados Unidos".[24]

Una primera consecuencia de esta acción ha sido, por ejemplo, la medida del gobierno israelí de restringir en dos tercios la lista de países a los que las empresas de seguridad israelíes están autorizadas a vender herramientas de vigilancia y hacking ofensivo. Como se ha destacado anteriormente, observamos que los intendentes comerciales operan en varios países a nivel internacional, con numerosos intermediarios activos en Europa[25, 26] y en Estados Unidos.[27]

La probable existencia duradera de los intendentes comerciales plantea una nueva serie de retos. Es relativamente fácil para un país comprar herramientas ofensivas altamente sofisticadas y a medida que elevan las capacidades del país a de una amenaza persistente avanzada. La alta sofisticación de los intendentes comerciales, junto con sus presupuestos para investigación y desarrollo, también implica su capacidad para reequiparse manteniendo altos estándares de seguridad operativa, lo que permite a los usuarios finales seguir operando incluso después de la exposición pública.

Vigilantes Persistentes Avanzados: Actividad de vigilancia APT

Red Dev Redemption

Red Dev 3 (también conocido como DeepCliff, RedAlpha) es un agente de amenazas activo desde al menos 2015, que fue expuesto por primera vez en código abierto en 2018 por CitizenLab como objetivo de una comunidad específica.[28] A lo largo de 2021 observamos que Red Dev 3 estableció cientos de dominios que alojaban páginas de phishing de credenciales dirigidas a diversos grupos de objetivos a escala internacional.[29]

La convención de nomenclatura de dominios de Red Dev 3 imita a proveedores de servicios de correo populares, y el agente de la amenaza puede falsificar los portales de acceso a los servicios de correo específicos de las organizaciones a las que se dirige.[30]

también atacó o suplantó servicios que incluían medios de comunicación populares entre las comunidades de la diáspora y los disidentes; ONG centradas en los refugiados, así como en los derechos civiles y humanos, como Amnistía Internacional; y grupos de reflexión e institutos políticos.

Desde abril de 2021, hemos observado una ampliación de los objetivos del agente de la amenaza, que han pasado de la sociedad civil a las entidades gubernamentales, incluidos los Ministerios de Asuntos Exteriores de al menos cinco países, así como varias organizaciones gubernamentales y políticas de todo el mundo.[31] Sin embargo, el agente de la amenaza también ha seguido atacando de forma descarada y persistente a ciudadanos individuales y comunidades vulnerables, en relación con temas políticos y sociales delicados.

Las nuevas artimañas de Red Nue

Red Nue, activo desde al menos 2017, es conocido por su uso del backdoor multiplataforma LootRAT, también conocido como ReverseWindow.[32] LootRAT tiene variantes para Windows[33] y Macintosh[34] (reportado en código abierto como Demsty), así como una variante para Android conocida como SpyDealer.[35] Red Nue también ha utilizado otro backdoor para Windows[36] conocido como WinDealer[37] desde al menos 2019, cuando lo desplegó en blancos como parte de una campaña de watering hole en un sitio web de noticias chino para la comunidad de la diáspora china.

En 2021, observamos que el agente de la amenaza siguió iterando sobre LootRAT, desplegando una variante de Linux del backdoor.[38]

La nueva muestra del backdoor tenía la sección de comentarios del binario eliminada, probablemente en un intento de dificultar el análisis y la comprensión del agente de la amenaza. Todas las víctimas que observamos de esta campaña tenían su sede en Asia. en Asia, y entre ellas se encontraba una empresa de tecnología que suministraba software de simulación.

> La alta sofisticación de los intendentes comerciales, junto con sus presupuestos para investigación y desarrollo, también implica su capacidad para reequiparse manteniendo altos estándares de seguridad operativa, lo que permite a los usuarios finales seguir operando incluso después de la exposición pública."

Algunas partes de Asia están muy presentes en la victimología de Red Nue. El agente de la amenaza ha atacado a individuos y universidades con la variante Demsty MacOS de LootRat. Por ejemplo, SpyDealer (la versión para Android de LootRAT) es capaz de robar información de más de 40 aplicaciones de comunicación móvil, como WeChat, Facebook, WhatsApp, Skype, Sina Weibo, Tencent Weibo y Oupeng Browser, muchas de las cuales se utilizan ampliamente en China.

White Dev 75 dirigido a Oriente Medio y el Norte de África

White Dev 75 ha estado activo desde al menos 2015, y PwC ha determinado que este agente de la amenaza está probablemente motivado por el espionaje. Sus víctimas observadas son principalmente miembros de la sociedad civil, que probablemente están siendo atacados en relación con temas políticos. White Dev 75 sigue siendo muy eficaz a la hora de comprometer las cuentas de correo electrónico de periodistas, disidentes y personas implicadas políticamente en todo Oriente Medio y el Norte de África.[39, 40, 41]

Entre al menos abril y octubre de 2021, White Dev 75 registró docenas de nuevos dominios de phishing que se alinean con tácticas y procedimientos anteriores observados en sus campañas, incluyendo uno que suplantaba al Ministerio de Asuntos Exteriores de un país de Oriente Medio. White Dev 75 es especialmente eficaz gracias a su capacidad para eludir la AMF y aprovechar las convincentes técnicas de ingeniería social. Los correos electrónicos de phishing que White Dev 75 suele utilizar son falsas alertas de seguridad sobre comportamientos anormales de inicio de sesión. También se ha observado que el agente de la amenaza abusa de OAuth para eludir la MFA y las contraseñas en conjunto.[42] OAuth es una aplicación común que permite la autenticación de servicios de terceros sin necesidad de compartir contraseñas. Las TTPs observadas de White Dev 75 no son demasiado avanzadas, pero demuestran una persistencia y una astucia en su arte de navegar que le permiten perpetrar estas tácticas contra la sociedad civil.

40+

Aplicaciones de las que SpyDealer (la versión para Android de LootRAT) puede robar información

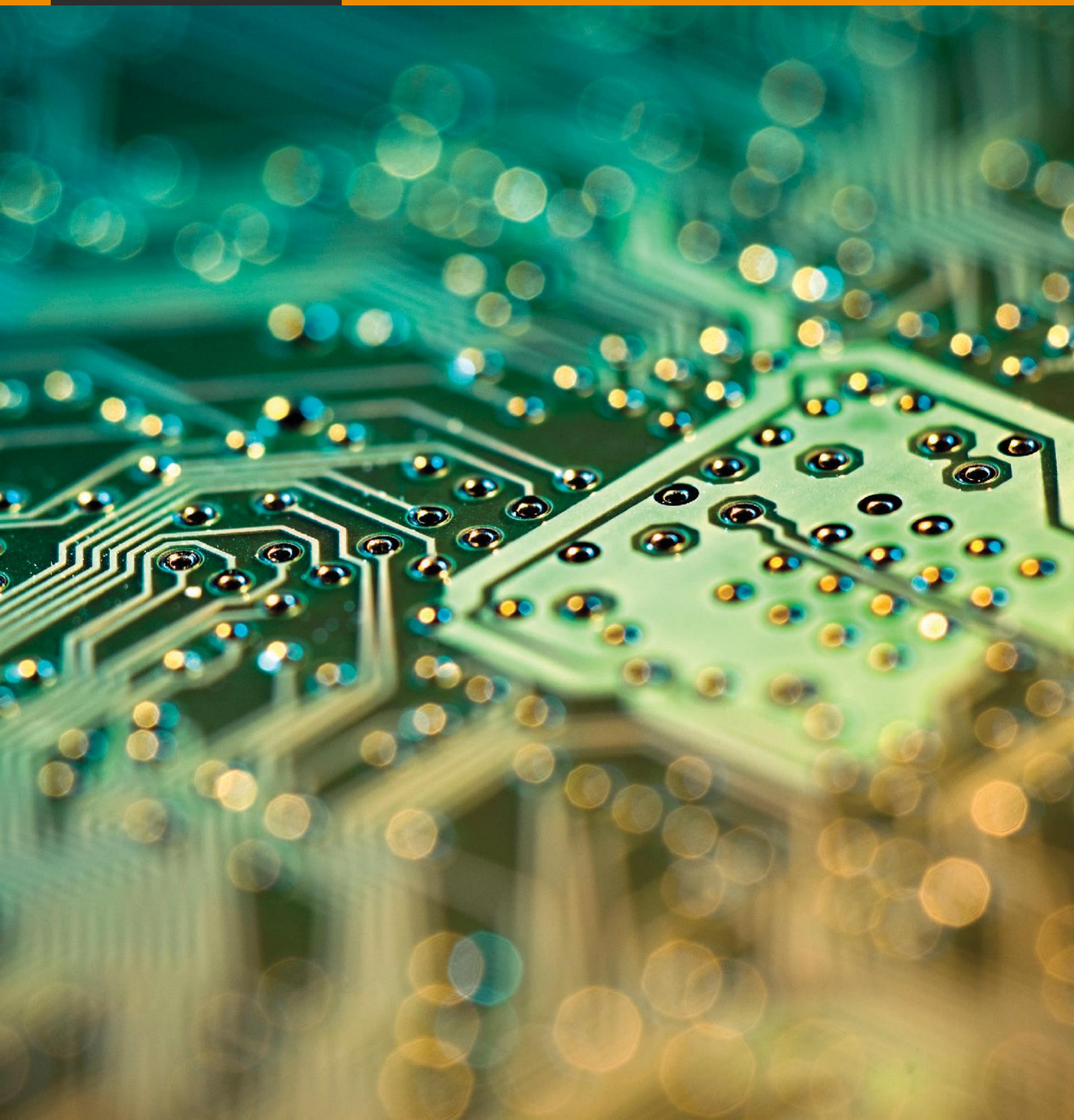
Vigilancia doméstica de Yellow Garuda

Yellow Garuda (alias Charming Kitten, PHOSPHORUS, ITG18) es un versátil agente de amenazas con base en Irán que ha estado activo al menos desde 2012. Estuvo muy activo a lo largo de 2021, llevando a cabo una serie de actividades de vigilancia.

Encontramos pruebas de que Yellow Garuda llevó a cabo una campaña de vigilancia nacional selectiva para extraer datos de la cuenta de Telegram de una víctima.[43] Esto incluía la exfiltración de mensajes, archivos multimedia, detalles de pertenencia a grupos y contactos de la víctima. Entre septiembre y octubre de 2021, el agente de la amenaza comprometió al menos a seis víctimas con sede en Irán, según los datos obtenidos por PwC junto con copias de la herramienta de "capturad" de Telegram hecha a medida por el agente, que se utilizó para exfiltrar los datos de las cuentas de las víctimas. También descubrimos un informe operativo escrito por el propio agente de la amenaza sobre la vigilancia de una séptima víctima nacional; los datos de esta víctima eran más extensos y probablemente el resultado de la exfiltración a través de malware móvil.

La adición de malware para móviles en el conjunto de herramientas de Yellow Garuda se ha reportado en código abierto[44] y se correlaciona con nuestro propio análisis de una muestra de malware para Android con múltiples enlaces a la infraestructura conocida de Yellow Garuda a principios de 2021.[45] Esta muestra se hacía pasar por la aplicación de mensajería WhatsApp e incluía la capacidad de grabar audio y vídeo, tomar fotos, acceder a los contactos, datos de localización y SMS, e iniciar llamadas. Su funcionalidad y su código base eran similares a una muestra más antigua de malware para Android de 2018 que, al parecer, se utilizó para atacar a ciudadanos iraníes, lo que indica que Yellow Garuda probablemente ha tenido esta capacidad durante algún tiempo.

Cibercrimen



Ransomware

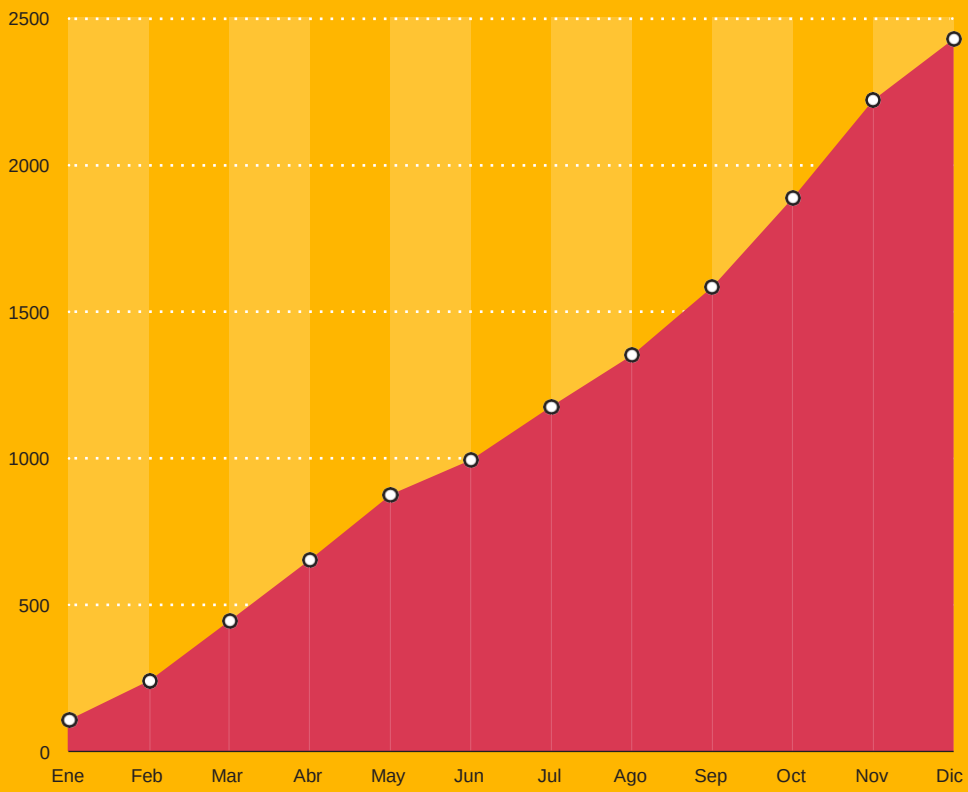
El ransomware siguió siendo la amenaza cibernética más importante a la que se enfrentaron la mayoría de las organizaciones en 2021. Los factores que contribuyen a esta tendencia siguen siendo aplicables, y muchos de ellos se amplificaron con las siguientes observaciones:

- el número de agentes de amenazas involucrados en operaciones de ransomware aumentó, impulsado por el aumento de la prominencia de los acuerdos de ransomware como servicio (RaaS) y los esquemas de afiliación;
- el ritmo y la frecuencia de los ataques denunciados públicamente casi se duplicaron; y,
- la filtración de datos robados, o la amenaza de hacerlo, se convirtió en un procedimiento estándar para la mayoría de los agentes de amenazas de alto perfil, añadiendo riesgos de privacidad, regulatorios y de reputación a la crisis de interrupción del negocio causada por el cifrado de datos.

La abrumadora mayoría de los incidentes de ransomware tuvieron una motivación económica, con un conjunto limitado de ataques que probablemente tuvieron una motivación política y fueron intencionalmente destructivos.

En 2020, aproximadamente 1.300 víctimas de ransomware tuvieron sus datos expuestos en sitios de filtración. Esta cifra casi se duplicó en 2021, con 2.435 víctimas expuestas..

Figura 2: Total de fugas de ransomware en 2021

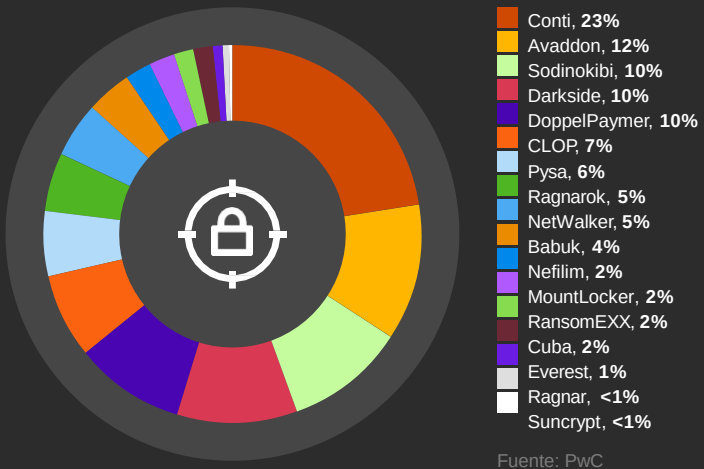


2,435

víctimas fueron expuestas en sitios filtrados, casi el doble del número expuesto en 2020

Fuente: PwC

Figura 3: Incidentes de ransomware - 1er trimestre de 2021

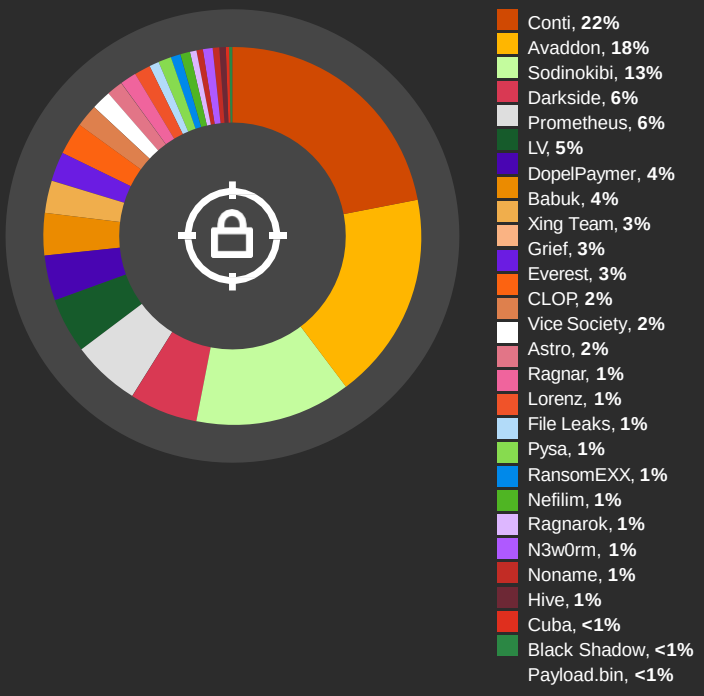


Fuente: PwC

El número de agentes de amenazas involucrados en operaciones de ransomware fluctuó, con agentes de amenazas prominentes que se tomaron descansos, cerraron por completo o resurgieron después de una brecha en la actividad bajo una nueva "marca", como se detalla en secciones posteriores. Por ejemplo, en el primer trimestre de 2021, PwC observó que 17 agentes de amenazas filtraron datos de aproximadamente 440 víctimas, pero el 65% de estos ataques fueron atribuibles a sólo cinco agentes de amenazas:

- White Onibi (aka Conti) - 23%
- White Dev 70 (aka Avaddon) - 12%
- White Apep (aka DarkSide) - 10%
- White Ursia (aka Sodinokibi, REvil) - 10%
- Blue Lelantos (aka DoppelPaymer) - 10%

Figura 4: Incidentes de ransomware - 2do trimestre de 2021



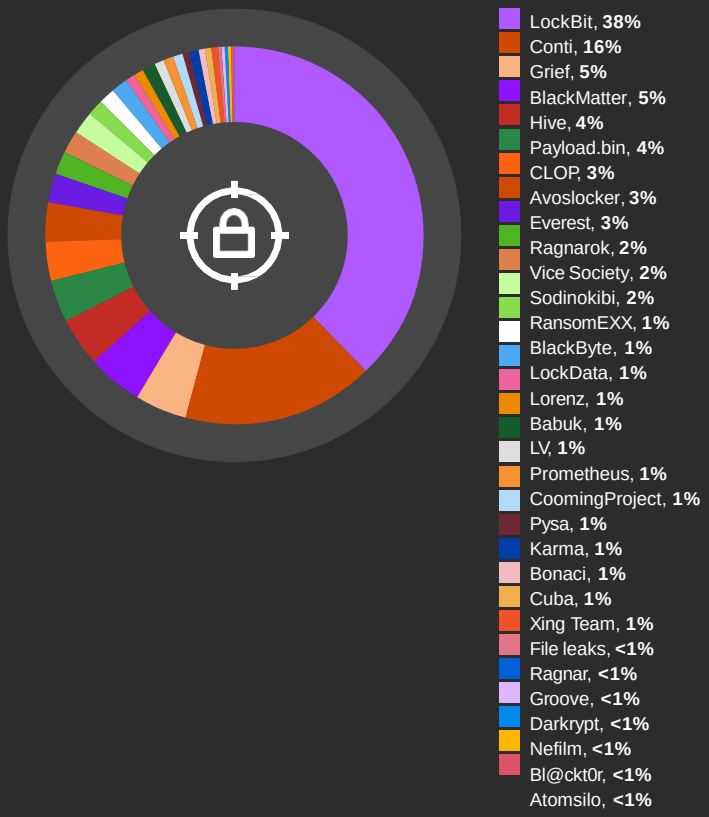
Fuente: PwC

En el segundo trimestre de 2021, el número de agentes de amenazas observados que realizaban operaciones de ransomware aumentó a 27, y el correspondiente número de víctimas fue superior a 500.
Sin embargo, la actividad estuvo de nuevo dominada por un pequeño número de familias de ransomware, con aproximadamente el 60% de los incidentes atribuibles a solo cuatro operaciones:

- Conti - 22%
- Avaddon - 18%
- REvil - 13%
- DarkSide - 6%

Determinamos que la notable reducción de las operaciones de DoppelPaymer en el segundo trimestre de 2021 se debió probablemente a que el agente de la amenaza cambió la marca de sus operaciones, antes de introducir la variante de ransomware conocida como "Grief".

Figura 5: Incidentes de ransomware - 3er trimestre de 2021

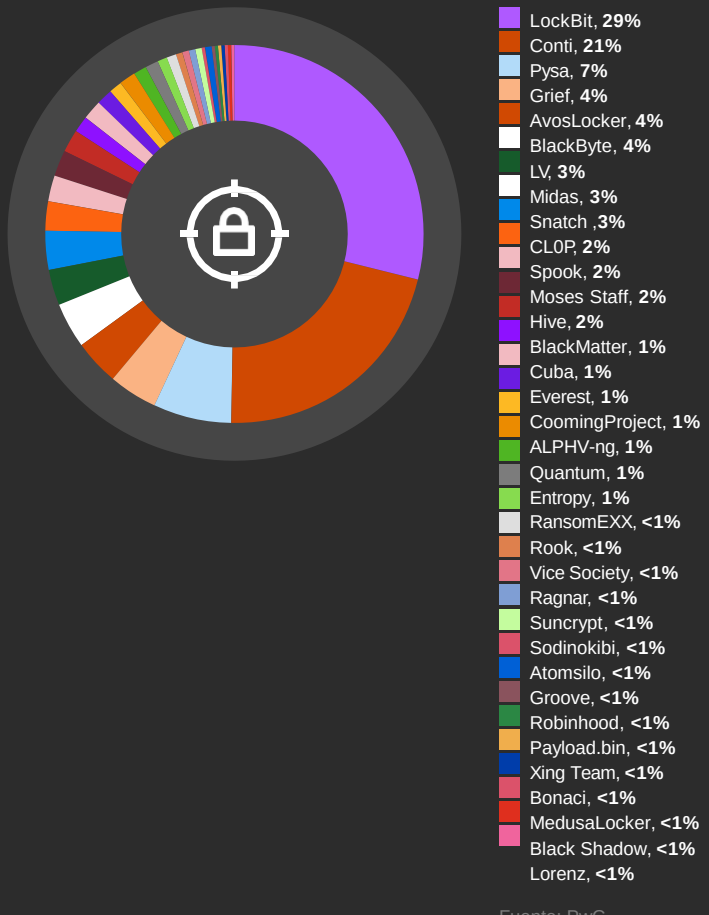


Fuente: PwC

Para el tercer trimestre de 2021, empezaron a producirse cambios significativos en el mercado del ransomware. Estos fueron causados por la expulsión de los programas de afiliados de sus principales sitios de captación, y la disolución voluntaria de algunas operaciones tras ataques de alto perfil. Sin embargo, el acontecimiento más significativo que afectó al mercado del ransomware durante este periodo fue la reaparición de White Janus (también conocido como LockBit) como LockBit 2.0 en julio de 2021. El programa de afiliados original de LockBit estuvo inactivo desde finales de 2020 y no reapareció hasta julio de 2021, en el foro delictivo RAMP, mientras White Janus retocaba su ransomware.[46] El agente de la amenaza estableció rápidamente una operación de alto ritmo, siendo responsable de casi el 40% de los incidentes observados en el tercer trimestre. Esto fue probablemente el resultado de atraer a los afiliados de otros esquemas de ransomware que cerraron a finales del segundo trimestre o a principios del tercero. En total, en el tercer trimestre, hubo 32 agentes de amenazas que filtraron datos, lo que supuso casi 600 víctimas, y el 64% de los incidentes se atribuyeron de nuevo a sólo cuatro operaciones de ransomware:

- LockBit - 38%
- Conti - 16%
- BlackMatter - 5%
- Grief - 5%

Figura 6: Incidentes de ransomware - 4to trimestre de 2021



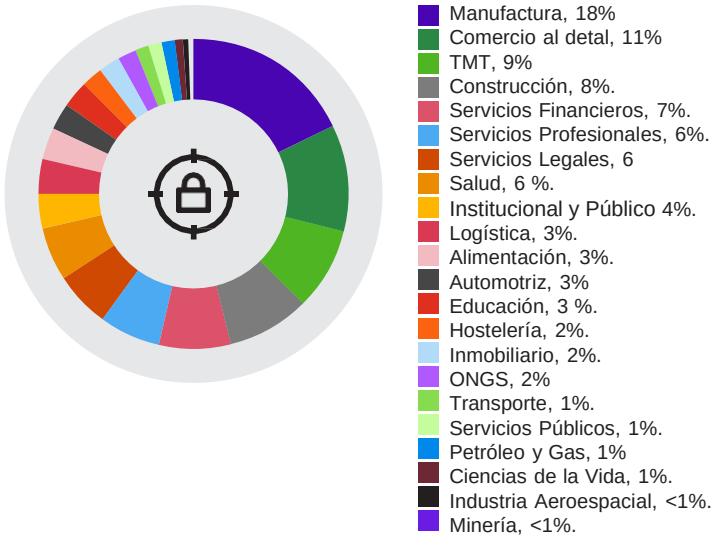
Fuente: PwC

En el cuarto trimestre de 2021, el ritmo de los ataques aumentó, con aproximadamente 850 víctimas añadidas al recuento de incidentes observados. Al igual que en el trimestre anterior, el número de agentes de amenazas que filtran
datos creció una vez más, con 35 sitios de filtración activos durante el período. LockBit y Conti siguieron dominando y el 64% de los incidentes observados se atribuyeron a solo cinco agentes:

- LockBit - 29%
- Conti - 21%
- White Thalia (aka Pysa) - 6%
- Grief - 4%; and,
- White Caerus (aka AvosLocker) - 4%

Un pico en la actividad observada por Pysa fue el resultado de una afluencia de filtraciones de datos el 10 de noviembre, que fue más bien el resultado de la actualización por parte del agente de la amenaza de su sitio de filtraciones, a menudo descuidado, en lugar de un aumento en las operaciones de Pysa de ese período en particular.

Figura 7: Incidentes de ransomware por sector 2021



Fuente: PwC

Desglose por sectores

Las operaciones de ransomware son, en gran medida, indiferentes al sector económico de las organizaciones, aunque desde que la pandemia se instaló, muchos agentes de amenazas han hecho declaraciones públicas -que no han cumplido del todo- de que evitarían dirigirse a hospitales u otros centros sanitarios. En los casos en los que los agentes de las amenazas han especificado sus objetivos, se han centrado exclusivamente en el tamaño de la organización (número de puntos finales), su ubicación geográfica (con énfasis en Canadá, la UE, EE.UU. y el Reino Unido) y sus ingresos.[47] Al igual que en 2020, pocos sectores fueron inmunes a los ataques, pero algunos sectores experimentaron ataques con más frecuencia que otros, siendo los seis principales sectores los que representaron el 60% de todos los incidentes observados:

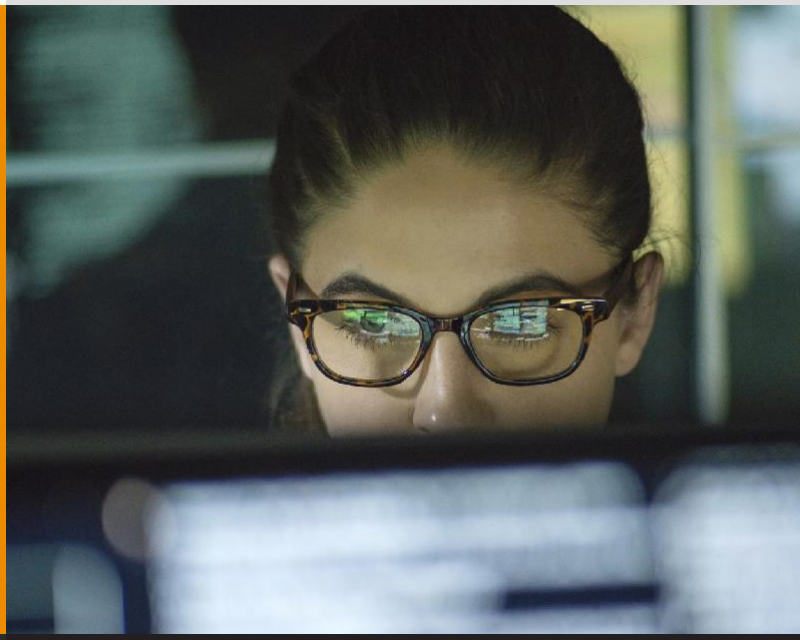
- Manufactura - 18%
- Venta al detal y consumo: 11%.
- Tecnología - 9 %
- Construcción - 8
- Servicios Financieros - 7 %
- Servicios Profesionales - 6%.

Los mismos seis sectores principales representaron el 66% de los incidentes de ransomware en 2020.

No hemos visto pruebas de que estos sectores sean el objetivo específico de los agentes de las amenazas. Sin embargo, si no se incluye el sector sanitario Sin embargo, si no se incluye el sector sanitario, estos seis sectores coinciden con los seis principales sectores industriales por ingresos en Estados Unidos..[48] Para algunos de los agentes de amenazas más activos -por ejemplo, White Onibi- los ingresos de las víctimas son un factor importante a la hora de determinar si se va a proceder a la actividad de post-explotación después de haber conseguido el acceso inicial. Esto puede tener cierta influencia en la distribución de las víctimas por sectores.

60%

de todos los incidentes observados correspondieron a seis sectores (Manufactura, Comercio al detal y Consumo, Tecnología, Construcción, Servicios Financieros y Servicios Profesionales)



Caso de estudio de respuesta a incidentes:

HSE

El Health Service Executive (HSE) de la República de Irlanda encargó un informe a PwC sobre un ataque de Conti que interrumpió los sistemas informáticos del HSE en mayo de 2021. El HSE publicó este informe el 10 de diciembre de 2021, marcando uno de los primeros casos mundiales de "divulgación completa" tras un incidente de este tipo.[49]

El 14 de mayo de 2021, el ransomware Conti se activó en más de 3.500 estaciones de trabajo y 2.800 servidores del HSE, causando una interrupción generalizada y prolongada de los servicios sanitarios en Irlanda, con algunos centros sanitarios incapaces de acceder a los datos de los pacientes o programar citas a través de los sistemas electrónicos. Los orígenes del ataque se remontan a marzo de 2021, cuando un usuario abrió un archivo adjunto malicioso que había sido enviado por correo electrónico. Hubo un lapso de tiempo significativo entre el acceso inicial a la red y la actividad posterior a la explotación. Es probable que esto se deba a que el compromiso inicial fue llevado a cabo por una operación de acceso como servicio (AaaS), antes de que Conti asumiera el control del punto final comprometido para progresar en el ataque.

Conti es un sistema de ransomware "operado por humanos" y se despliega a través de la ejecución manual de comandos por lotes, en lugar de un malware que se propaga a través de una red automáticamente, cifrando indiscriminadamente cualquier infraestructura que encuentra. La operación de Conti siguió las TTPs conocidas asociadas con el agente de la amenaza, incluyendo el despliegue de Cobalt Strike para facilitar el movimiento lateral y la escalada de privilegios dentro de la red; el uso de otras herramientas incluyendo Mimikatz, para identificar y comprometer cuentas y sistemas de nivel de administrador, particularmente Active Directories; y, la exfiltración de datos antes del cifrado de archivos.

El impacto del ataque podría haber sido mucho mayor si Conti se hubiera activado en los sistemas médicos, así como en el núcleo del sistema informático de la víctima. Muchos de los factores que contribuyeron a la escala y el impacto del incidente no son exclusivos a HSE. El informe destaca las lecciones que todas las organizaciones deben tener en cuenta para prepararse para un ciberataque similar y para asegurarse que pueden mitigarlo y recuperarse de él.

Programas de afiliación

Los programas de afiliación siguieron siendo una fuerza impulsora de la escala y el ritmo de las operaciones de ransomware en 2021. Los programas de afiliación de ransomware generalmente ofrecen acceso a una cepa específica de ransomware sobre la base de un reparto de beneficios. En este esquema, un agente principal de la amenaza, como White Ursia, es responsable del desarrollo y la gestión del malware, y proporciona acceso a sus afiliados, cuya función es llevar a cabo los ataques. Los fondos obtenidos de las víctimas se dividen entre los operadores del ransomware y sus afiliados en acuerdos preestablecidos de reparto de beneficios. Esto permite a los agentes de las amenazas con habilidades de intrusión y explotación de la red adquirir acceso al ransomware y habilidades de monetización que no podrían desarrollar fácilmente por sí mismos, reduciendo las barreras de entrada.

Muchas de las operaciones de ransomware más prolíficas, como DarkSide, REvil y LockBit, dirigían abiertamente programas de afiliación de ransomware (Партнёрская программа); otras, como Conti, reclutaban a "pentesters" sin especificar sus objetivos finales. Los programas de afiliación se promocionaban principalmente en foros de delincuencia de habla rusa como Exploit y XSS. Como el número y la calidad de los afiliados (адвертов) eran un factor definitorio de los ingresos generados por muchas operaciones de ransomware, la competencia entre esquemas rivales se intensificó. Los agentes de la amenaza aumentaron su perfil mediante:

- depositando grandes sumas de criptomoneda en sus cuentas del foro, para demostrar el éxito financiero de su esquema;
- realizando entrevistas en los medios de comunicación para promocionar el éxito y los ingresos de sus operaciones, muchas de las cuales atrajeron una cobertura positiva en los foros delictivos en los que reclutaban afiliados;
- publicar enlaces a artículos de los medios de comunicación sobre sus operaciones;
- ofreciendo acuerdos competitivos de reparto de beneficios a sus reclutas; y,
- alegando superioridad técnica sobre sus competidores.

Figura 8: Anuncio de contratación de afiliados de DarkSide

Figura 9: REvil

Figura 10: Anuncio de LockBit 2.0 en el que se afirma un rendimiento técnico superior al de los esquemas rivales

Tabla comparativa de la velocidad de cifrado de algunos ransomware - 08.02.2021

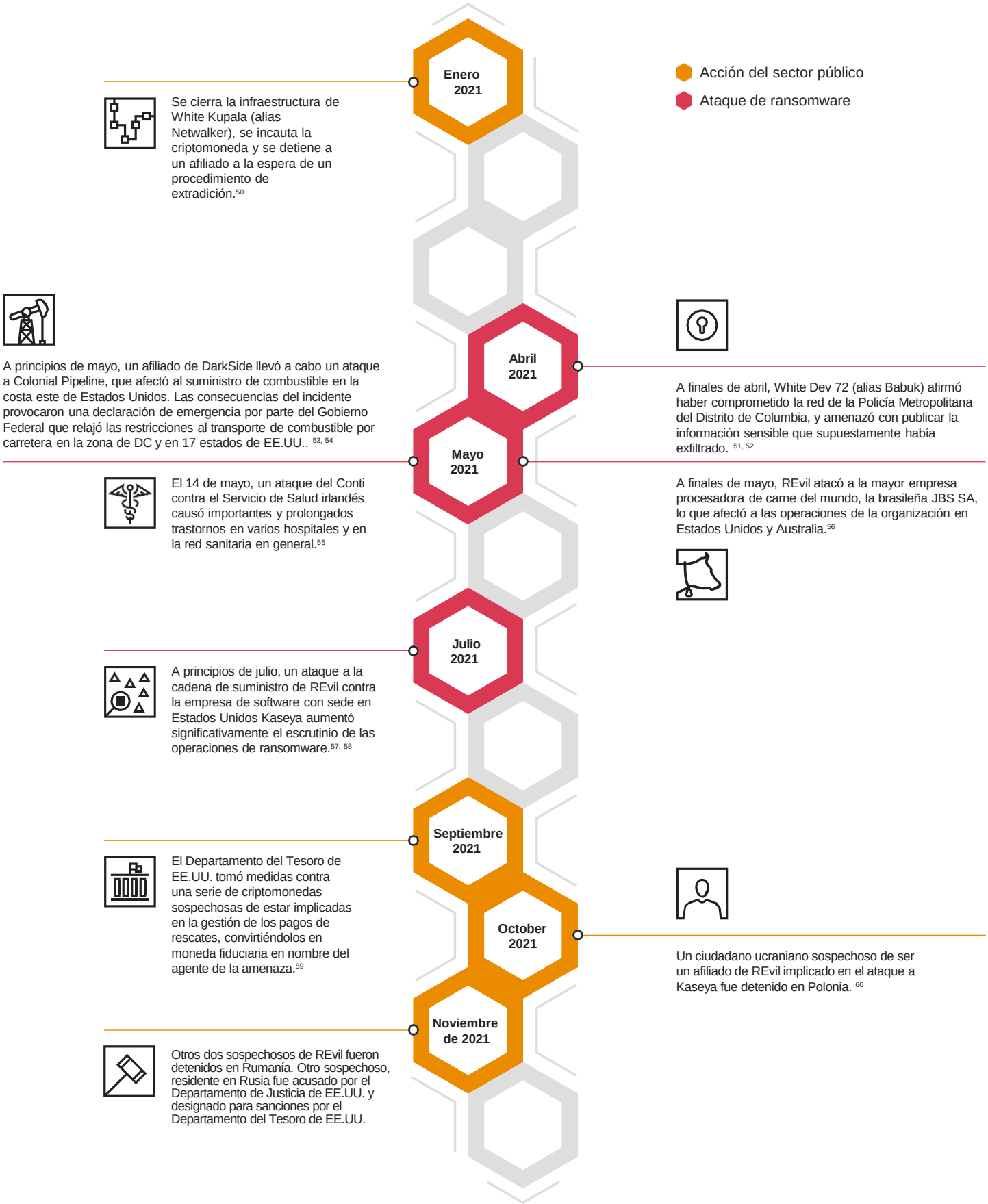
PC para la prueba: Windows Server 2016 x64 /8 core Xeon E5-2680@2.40Hz / 16 GB RAM / SSD

Name of the ransomware	Fecha de la muestra	Velocidad en MB por segundo	Tiempo empleado para el cifrado de 100 GB	Tiempo empleado en el cifrado de 1TB	Autodifusión	Tamaño de la muestra en KB	Número de archivos cifrados (Todos los archivos del sistema 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	extensión aleatoria
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	extensión aleatoria
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797

La política: la respuesta jurídica y reglamentaria

Una serie de incidentes que afectaron principalmente a organizaciones estadounidenses en la primera mitad de 2021 elevaron significativamente el perfil del ransomware:

Figura 11: Cronología de los ataques de ransomware más destacados y de las acciones del sector público



Expulsión masiva de los **esquemas** de afiliación

El aumento de la atención y la presión sobre los sistemas de ransomware, especialmente como consecuencia del incidente de Colonial

Pipeline, tuvo un impacto inmediato en los sistemas de afiliación. El 14 de mayo, los administradores del foro delictivo XSS eliminaron los mensajes relacionados con :

- Reclutamiento de afiliados;
- el alquiler de ransomware; y
- la venta de software de bloqueo (ransomware).

Aunque los administradores citaron varias razones para sus acciones, un punto clave fue que el ransomware se había vuelto "peligroso y tóxico... y estaba siendo vinculado con la geopolítica y los ataques patrocinados por el Estado". El otro foro principal en el que operaban los esquemas de afiliación, Exploit, también siguió su ejemplo, citando razones similares para su propia suspensión.[61]

La prohibición de los esquemas de afiliación no supuso la expulsión de de los agentes de amenazas de ransomware de los propios foros, aunque algunos se retiraron. Por ejemplo, White Ursia anunció que cerraría su esquema de afiliación REvil y "se volvería privado"; posteriormente canceló por completo sus membresías en el foro. White Apep anunció que cerraría la operación de ransomware DarkSide y publicó las claves de descifrado del malware.62 Sin embargo, otros, como White Janus (también conocido como LockBit), mantuvieron su membresía y simplemente transfirieron sus actividades de reclutamiento de afiliados a su sitio de fugas.

Figura 12: La administración de XSS prohíbe la actividad de ransomware en el sitio

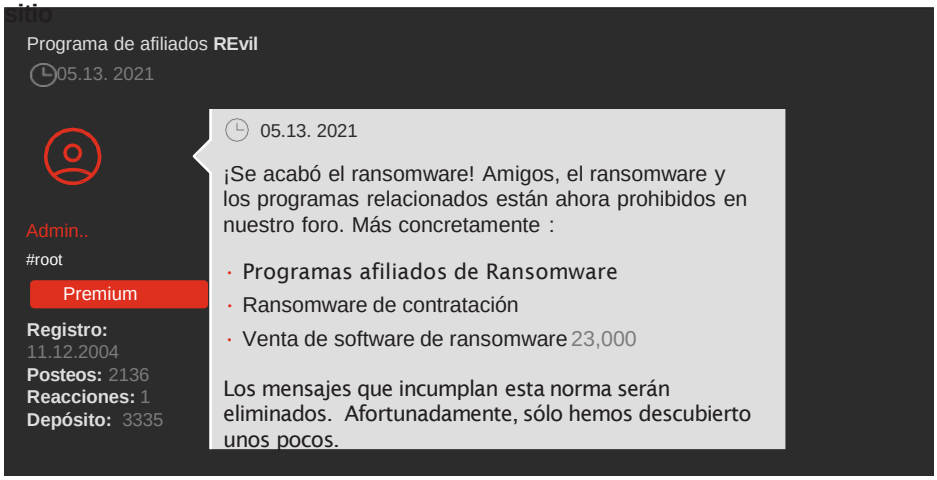


Figura 13: La Administración de Explotación hace lo mismo

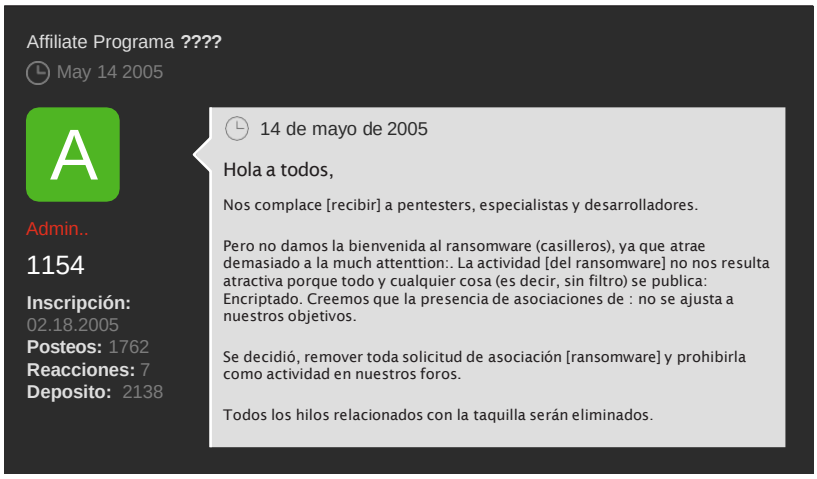
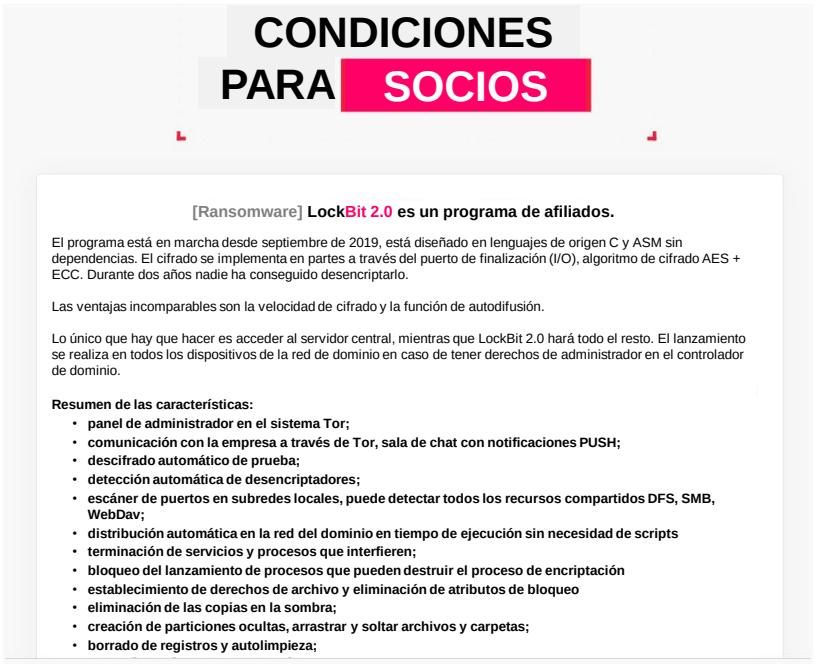
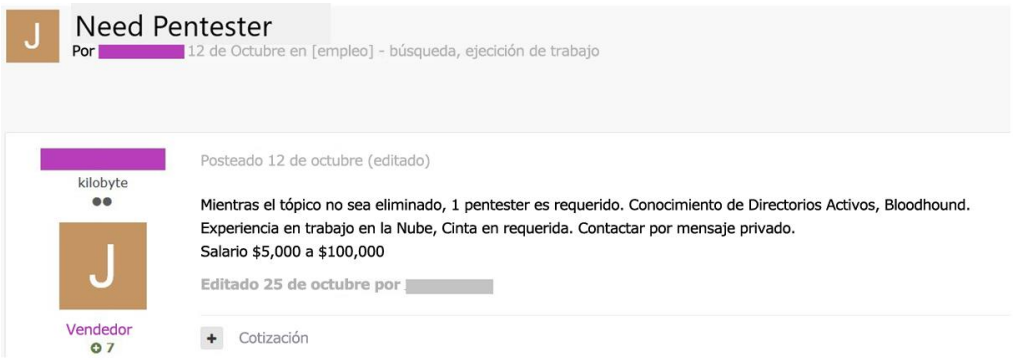


Figura 14: Anuncio de contratación de afiliados en el sitio de filtraciones de White Janus



Mientras que los esquemas de reclutamiento de afiliados abiertos fueron objeto de la prohibición, el reclutamiento de "pentesters" continuó sin mucha interrupción, con anuncios en las secciones de "búsqueda de trabajo" o "freelance" de Exploit y XSS en gran medida no afectados. Los anuncios no decían abiertamente que se estaba reclutando para operaciones de ransomware, pero las especificaciones del trabajo para muchos de los puestos vacantes tenían similitudes con campañas de reclutamiento de esquemas de afiliación anteriores.

Figura 15: Anuncio de reclutamiento de pentester por parte de un agente de amenazas no identificado



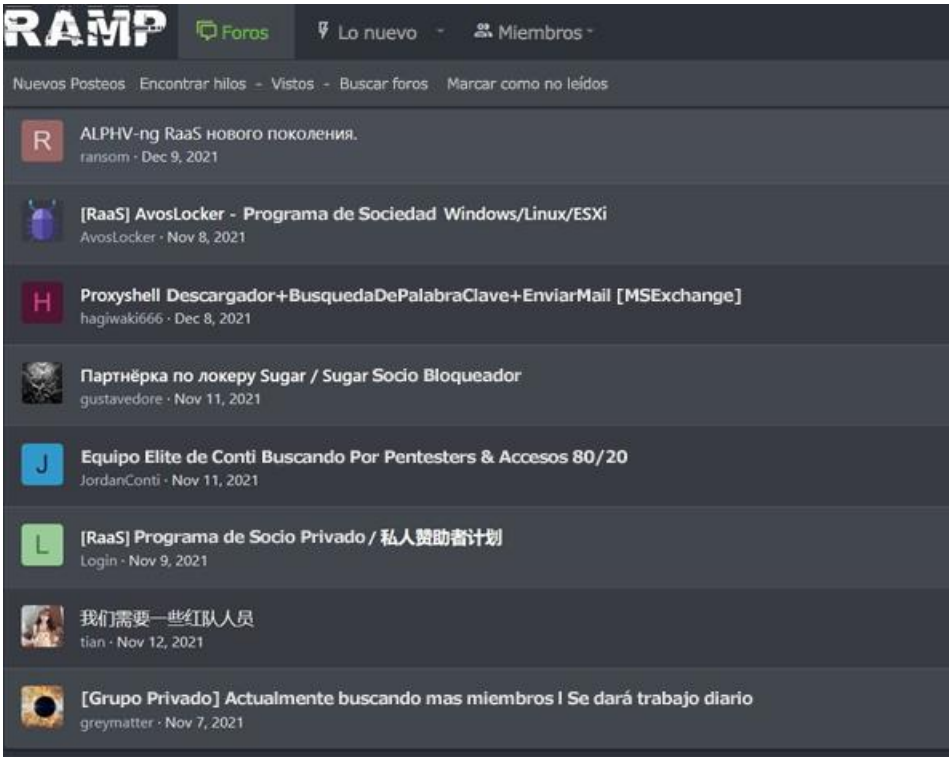
RAMPeando más

En respuesta a las prohibiciones de los foros sobre el reclutamiento de afiliados, a mediados de julio se creó un foro criminal que afirmaba atender específicamente las necesidades de las operaciones de ransomware y los programas de afiliados en particular. El sitio operaba inicialmente desde la dirección de la web oscura utilizada anteriormente por White Dev 72 (alias Babuk) para su sitio de filtraciones, y se llamaba a sí mismo RAMP, posiblemente como referencia a un sitio web oscuro anterior en ruso que se dedicaba a la venta de narcóticos.

El foro tiene una sección específicamente dedicada a los esquemas RaaS, así como anuncios que reclutan pentesters y acceso a redes corporativas.

Entre los esquemas de ransomware más destacados que están activos en RAMP se encuentran Conti, AvosLocker y BlackCat.

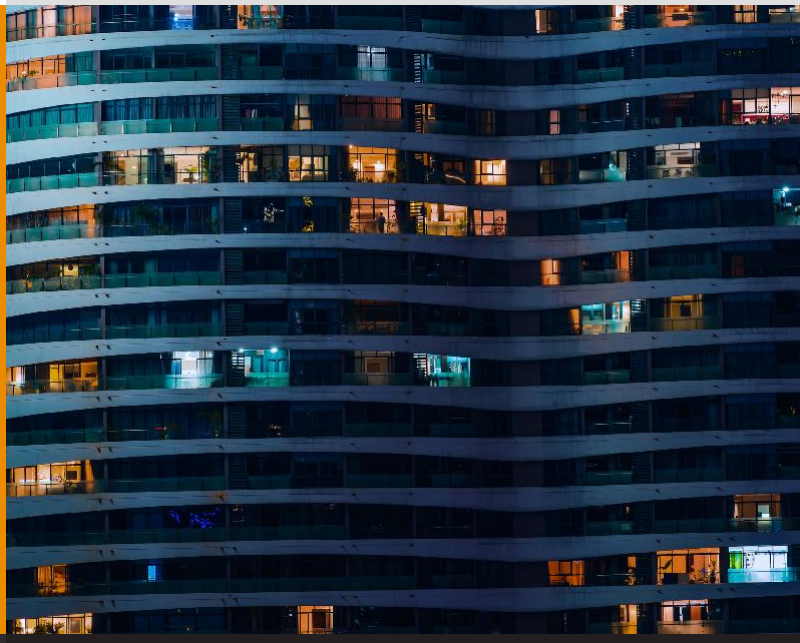
Figura 16: Anuncios de contratación de afiliados en el foro RAMP



Cambio de marca del ransomware

Como otra probable consecuencia de la creciente presión legal y política, en 2021 observamos uno de los mayores niveles de cambio de marca de ransomware de los últimos años. Los cambios de marca del ransomware tienen tres beneficios principales :

- permitiendo a los agente de la ciberdelincuencia establecidos "reiniciar" su programa después de sufrir un revés. (por ejemplo, después de que el descubrimiento de un fallo en su de cifrado de su ransomware, se publique un descifrador para el malware);
- proporcionar una oportunidad para pasar desapercibido y reducir el protagonismo de un grupo específico después de una cantidad significativa de actividad o campañas; y,
- Impedir o retrasar la atribución de los ataques, cuando el agente de la amenaza lo percibe como una ventaja operativa.



Estudio de caso de respuesta a incidentes:

Nuevo trabajo, ¿quién es? El operador de ransomware cambia los esquemas de afiliación

En febrero de 2021, el equipo de respuesta a incidentes de PwC respondió a un ataque Sodinokibi/REvil en una organización del sector agrícola con sede en Francia. La intrusión comenzó a mediados de enero, cuando un archivo adjunto malicioso, entregado a los empleados de la empresa a través de un correo electrónico de phishing, condujo a la instalación de QakBot en una estación de trabajo víctima.

Tras conseguir el acceso inicial, el agente de la amenaza desplegó Cobalt Strike para reforzar su presencia en el entorno de la víctima.
También comenzó a acceder a las credenciales de LSASS, confiando en el Protocolo de Escritorio Remoto de Windows (RDP) para moverse lateralmente por la red. El agente de la amenaza utilizó una mezcla de trabajos BITS, PowerShell y la interacción de la línea de comandos para instalar y ejecutar cargas útiles y tomar huellas digitales en la red. RClone, un software de código abierto utilizado para gestionar el contenido de los sistemas de
se utilizó para exfiltrar datos de los almacenamientos locales y en la nube de la víctima, antes de que el ransomware fuera detonado.

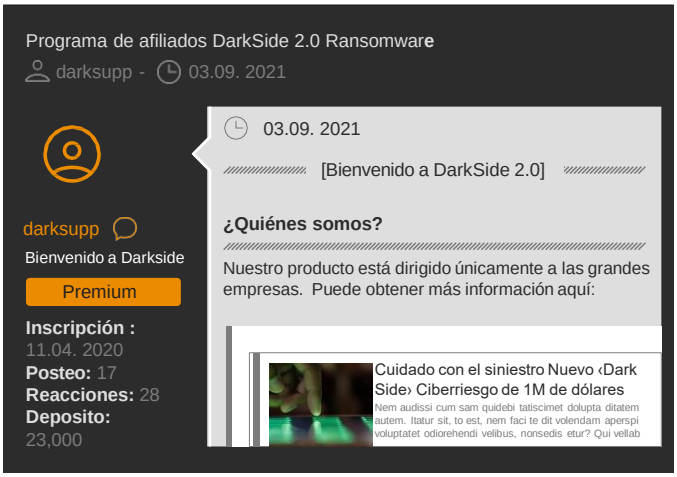
Aunque el agente de la amenaza desplegó en última instancia el ransomware Sodinokibi/ REvil, la forma en que operaba dentro del entorno de la víctima se alineaba más estrechamente con las técnicas que se sabe que adoptan los afiliados a otro programa de ransomware que PwC rastrea como White Samyaza (alias Egregor, Prolock). Por ejemplo, aunque también se ha observado que QakBot conduce a infecciones de REvil[63], está más fuertemente vinculado a las operaciones de White Samyaza[64]. La herramienta de línea de comandos RClone es utilizada con frecuencia, aunque no de forma exclusiva, por los operadores de Egregor/Prolock, sobre todo cuando la utilidad es renombrada como "svchost.exe" para mezclarse con el entorno de la víctima[65].
Además, los archivos del ransomware observados durante la respuesta al incidente estaban etiquetados con el nombre de la víctima.
Este esquema de nomenclatura es una característica exclusiva del ransomware Egregor y no suele observarse en el ransomware Sodinokibi/REvil (cuyos archivos se nombran a menudo utilizando un esquema de nomenclatura aleatorio).

Basándonos en las pruebas que hemos examinado, consideramos que es muy probable que una filial de Samyaza Blanca se trasladara a Ursia Blanca y desplegara a Sodinokibi/REvil utilizando las TTPs comúnmente observadas con las filiales de Samyaza Blanca.

Blue Lelantos

En diciembre de 2019, los miembros del grupo delictivo con sede en Rusia "Evil Corp" (rastreado por PwC como Blue Lelantos) fueron acusados por las autoridades estadounidenses y designados para las sanciones.[66] Las operaciones de Evil Corp continuaron a lo largo de 2020, pero los cambios en las operaciones de Evil Corp se hicieron evidentes a finales de ese año y cada vez más notables a principios de 2021. Las detecciones de WastedLocker,[67] uno de los principales sistemas de ransomware de Evil Corp, prácticamente desaparecieron a finales de 2020. Sin embargo, la operación de WastedLocker continuó a lo largo de 2021, a través de una sucesión de cambios de marca. A finales de 2020, las notas de rescate de WastedLocker empezaron a aparecer como ransomware Hades, Phoenix Cryptolocker en marzo, Payloadbin en junio y Macaw en octubre.[68] De forma similar, DoppelPaymer,[69] la operación de "doble extorsión" de Evil Corp, cesó efectivamente sus operaciones en mayo, con la última víctima añadida a su sitio de filtración ese mes. En junio, surgió un nuevo ransomware autodenominado "Grief" o "PayorGrief", que empezó a publicar datos de las víctimas en su sitio de filtraciones desde el principio. El análisis de las muestras de Grief reveló amplias similitudes de codificación entre él y DoppelPaymer, con un cambio importante en el uso de la criptomoneda Monero por parte de Grief para el pago de rescates. Consideramos que Grief es otro ejercicio de cambio de marca de Evil Corp, y es poco probable que sea el último.[70]

Figura 17: Posteo de anuncio "Bienvenido a Darkside 2.0".



Aunque no tenemos pruebas directas de las razones de los sucesivos ejercicios de cambio de marca emprendidos por Evil Corp en 2021, consideramos que es muy probable que sean consecuencia de la designación del grupo como entidad sancionada por las autoridades estadounidenses:

- Como en la mayoría de las operaciones de ransomware, la mayoría de sus víctimas se encuentran en Estados Unidos;
- Una organización que realice o facilite el pago de un rescate a una entidad sancionada podría incurrir en el incumplimiento de las sanciones de Estados Unidos y, por lo tanto, es menos probable que pague;
- El cambio de marca de WastedLocker y DoppelPaymer hizo más difícil, al menos a corto plazo, atribuir un incidente de ransomware a una entidad sancionada,
- El cambio de marca del código existente, en lugar de escribir nuevas variantes de ransomware desde cero, reduce los costes de oportunidad de Evil Corp y el tiempo necesario para mantener sus operaciones de ransomware.

White Apep

DarkSide (también conocida como BlackMatter), que PwC rastrea como White Apep, ha estado en funcionamiento desde al menos agosto de 2020, y ya había sufrido dos cambios de marca al cierre de 2021. El primero se produjo en enero de 2021, dos meses después del lanzamiento del programa de afiliados de DarkSide, cuando la empresa de seguridad Bitdefender desarrolló y lanzó públicamente una herramienta de descifrado[71] que permitía a las víctimas de DarkSide recuperar sus archivos. Las operaciones de White Apep entraron en pausa, probablemente para permitir que el agente de la amenaza se reequipara, y no se reanudaron hasta el 9 de marzo de 2021 bajo el nuevo nombre de "DarkSide 2.0". Su regreso vino acompañado de un relanzamiento de su programa de afiliados y presentó una versión actualizada del ransomware diseñada para evitar el descifrado con las herramientas existentes.[72]

Fue después de este primer cambio de marca cuando uno de los afiliados de DarkSide llevó a cabo uno de los incidentes más dañinos observados en 2021, el exitoso ataque a Colonial Pipeline, con sede en Estados Unidos, el 7 de mayo. El ataque provocó el cierre de las operaciones de su oleoducto de 5.500 millas, utilizado para suministrar casi la mitad del combustible de la Costa Este de Estados Unidos. El aumento de la atención prestada a DarkSide por el gobierno estadounidense, y el posterior desmantelamiento de la infraestructura, llevaron al agente de la amenaza a anunciar a mediados de mayo que cerraría sus operaciones.[73]

El segundo cambio de marca de White Apep llegó a finales de julio, en forma de un nuevo sistema RaaS titulado "BlackMatter". El nuevo ransomware compartía partes de su código, aunque no todas, con DarkSide 2.0; entre ellas se encontraban rutinas de código que implementaban la escalada de privilegios, la toma de huellas de las víctimas y las capacidades de red.[74]

La creciente presión de las fuerzas de seguridad llevó a White Apep a anunciar una vez más su salida de la escena del ransomware en noviembre de 2021. La decisión fue seguida poco después por el Departamento de Justicia de Estados Unidos, que anunció una recompensa de 10 millones de dólares por cualquier información potencial sobre el grupo.[75] A finales de 2021, las operaciones de White Apep permanecían inactivas.

Sin embargo, dado el número de transformaciones que han sufrido el ransomware y las operaciones en general de White Apep, consideramos que existe una probabilidad realista de que este cierre de operaciones sea una oportunidad para permanecer bajo el radar, sólo para resurgir con otro cambio de marca. Hay pruebas circunstanciales de que ALPHV-ng (alias BlackCat), que actualmente es rastreado por PwC como White Dev 101, es otra marca.

El esquema de afiliados del agente de la amenaza se lanzó en RAMP el 9 de diciembre de 2021, y el equipo de respuesta a incidentes de PwC ha respondido a múltiples incidentes de BlackCat realizados por un afiliado específico que anteriormente formaba parte del esquema de BlackMatter..

White Ursia

White Ursia fue uno de los agentes de amenazas de ransomware más activos en la primera mitad de 2021. La cara pública de su operación, utilizando las identidades en línea "UNKN" y "Unknown" en Exploit y XSS respectivamente, mantuvo un perfil alto, realizando entrevistas y promocionando el programa de afiliados de REvil. Es probable que la creciente presión a White Ursia, después de que se viera sometida a un mayor escrutinio tras los ataques de Kaseya y JBS, inició su primer movimiento offline en 2021. 'UNKN' ya había anunciado la decisión de "pasar a la oscuridad" tras la expulsión de los programas de afiliados de XSS y Exploit en mayo. El "Happy Blog" de White Ursia, el sitio de filtraciones utilizado para publicar datos de víctimas comprometidas, se desconectó a mediados de julio, al igual que su infraestructura de pago de rescates. Las operaciones de REvil cesaron y "UNKN" dejó de publicar comentarios sobre XSS o Exploit después del 4 de julio. El cierre de la infraestructura de pago de REvil, así como la desaparición de "UNKN", dañaron la reputación del agente de la amenaza.

En septiembre, nuevos personajes en línea - "REvil" en Exploit y "0_neday" en XSS- anunciaron que, tras la desaparición de "UNKN", habían podido restaurar las operaciones de REvil a partir de copias de seguridad. White Ursia reanudó sus operaciones y publicó los datos de seis víctimas entre el 10 de septiembre y el 14 de octubre, antes de que el sitio volviera a caer, esta vez probablemente de forma definitiva. '0_neday' afirmó haber perdido el control de la infraestructura de REvil tras un presunto ciberataque dirigido personalmente al actor de la amenaza y había decidido pasar desapercibido. El 14 de enero de 2022, el FSB anunció que había detenido a 14 sospechosos y registrado 25 locales relacionados con una investigación sobre la operación REvil.[76] Aunque al menos algunas de las detenciones se produjeron a principios de 2022, es muy probable que las autoridades rusas hayan desbaratado elementos de la operación REvil antes de las medidas adoptadas en enero de 2022. Varios agentes de amenazas criminales en XSS especularon que la desaparición de UNKN en julio y posterior "silencio de radio" era también el resultado de la acción del FSB. Sin embargo, es imposible verificar estas afirmaciones.

Compromiso en la cadena de suministro: la nueva normalidad

Los ataques a la cadena de suministro han sido durante mucho tiempo una fórmula probada y utilizada por múltiples agentes de amenazas. Aunque tradicionalmente se asocian con agentes de amenazas patrocinados por el Estado, los agentes de amenazas con motivación financiera también han tenido éxito en su explotación. A principios de 2021, White Austaras (también conocido como TA505), el agente de la amenaza que controla el ransomware CL0P, fue capaz de comprometer a múltiples organizaciones que utilizaban el software de transferencia de archivos heredado Accellion FTA. White Austaras exfiltró datos de menos de 25 víctimas y amenazó con exponerlos en el sitio de filtraciones CL0P si no se pagaba un rescate.[77, 78]

En julio de 2021, White Ursia comprometió a múltiples organizaciones que eran clientes de Kaseya, una empresa estadounidense especializada en software de gestión de redes y TI, abusando del software VSA de la empresa para entregar cargas útiles maliciosas. El ataque fue de una escala mucho mayor que el incidente de Accellion, con hasta 1.400 organizaciones afectadas por el ransomware REvil/Sodinokibi.[79]

Entrega y acceso

Sistemas de entrega

Los sistemas de entrega de malware han demostrado ser un compañero vital en los arsenales de los agentes de amenazas de ransomware. Se trata de piezas de software específicamente diseñadas para albergar cargas útiles maliciosas, que posteriormente son lanzadas por el agente de la amenaza para obtener una entrada inicial en un sistema o red de destino. En 2021, con agentes establecidos y nuevos participantes activos en el En 2021, con agentes establecidos y nuevos participantes en el mercado de la distribución de malware, los agentes de las amenazas cibernéticas tenían la opción de alternar entre varios y determinar la opción más fiable y segura para sus operaciones.

Emotet

Emotet, que PwC rastrea como White Taranis, es uno de los sistemas de entrega de malware más prominentes y de mayor duración. A principios de 2021 se produjo un desmantelamiento de la infraestructura de la red de bots de Emotet por parte de las fuerzas de seguridad internacionales, denominado Operación LadyBird. La operación, en la que se incautaron más de 700 dispositivos utilizados para los sistemas C2 de Emotet, junto con las detenciones realizadas en Ucrania,[80, 81] impidió que el agente de la amenaza llevara a cabo sus campañas maliciosas de spam y spear phishing (o ataque de correo electrónico dirigido) por correo electrónico durante una parte importante del año.

Sin embargo, a mediados de noviembre PwC observó que Trickbot, el troyano bancario operado por el grupo que PwC rastrea como White Magician, entregaba binarios maliciosos de Emotet a las máquinas infectadas de Trickbot y los ejecutaba en memoria. Es probable que se trate de un intento por parte del agente de la amenaza de ayudar a restaurar la infraestructura de mando y control de Emotet. Esta técnica está en línea con una actividad similar asociada a White Taranis, donde Emotet se utilizó como medio para ayudar a entregar binarios de Trickbot después de que se produjera un desmantelamiento similar de Trickbot en octubre de 2020.

Junto con la entrega de los binarios de Emotet y el regreso de su infraestructura de mando y control, también vimos la introducción de dos nuevos servidores de botnet de entrega de spam, Epoch 4 y Epoch 5. Esto se sumó a los otros tres servidores de la red de bots, Epoch 1, Epoch 2 y Epoch 3, que anteriormente fueron utilizados por White Taranis para infectar máquinas. También se observaron otras actualizaciones de las capacidades de cifrado de Emotet, utilizadas para cifrar el tráfico de red, y de sus protocolos de comunicación.82 Estas adiciones al arsenal de Emotet ponen de manifiesto las importantes capacidades a las que tiene acceso White Taranis y la continua amenaza que supone para las organizaciones.

La ausencia de Emotet durante la mayor parte de 2021 obligó a una parte importante de su base de clientes a buscar otras formas de distribución de malware. En 2021, sistemas de distribución de malware como Buerloader, Bazar, SquirrelWaffle e IcedID aumentaron significativamente su actividad, probablemente como resultado del vacío que dejó Emotet tras su retirada.

Más frío que IcedID

El agente de la amenaza que PwC rastrea como White Khione está detrás del sistema de entrega de malware IcedID (también conocido como Bokbot), que está asociado con sistemas de ransomware de alto perfil como Conti y Sodinokibi/REvil. Identificado por primera vez en 2017, IcedID fue desarrollado originalmente como un troyano bancario, capaz de robar información financiera. Sin embargo, al igual que otros troyanos bancarios, IcedID se reconvirtió posteriormente en una pieza de malware modular diseñada para proporcionar acceso remoto a las redes, que más tarde se vendería a otros usuarios como parte del modelo de "acceso como servicio".[83] En 2021, IcedID aumentó su capacidad en ausencia de Emotet, demostrando ser uno de los sistemas de entrega de malware más consistentes. Su capacidad principal reside en sus consistentes campañas de spam por correo electrónico, que se utilizan para iniciar la cadena de infección. Otras capacidades incluyen la ejecución remota de código y la inyección en el navegador web, lo que permite a IcedID realizar ataques de persona en el medio con el objetivo de extraer información financiera. Sin embargo, IcedID suele utilizarse para desplegar cargas útiles de mayor alcance, como Cobalt Strike.

Acceso como servicio (AaaS)

Los sistemas de entrega, como Emotet e IcedID, han sido siempre la opción de acceso inicial para muchos agentes de amenazas ciberriesgo. Sin embargo, su disponibilidad y accesibilidad pueden ser poco fiables, ya que algunos sistemas se ven obligados a desconectarse, mientras que otros requieren una relación de larga duración para poder acceder a los servicios de entrega de malware. Esto ha proporcionado un margen para que el mercado de acceso como servicio (AaaS) crezca en 2021. Estos mercados permiten la compra y venta de acceso a hosts comprometidos de una amplia gama de organizaciones y sectores, normalmente en forma de acceso RDP y VPN y VPN, así como webshells. Varios foros de delincuentes en lengua rusa, como Exploit y XSS, y mercados dedicados, como Odin y MagBo, se utilizan para anunciar listados de acceso.[84]

Uno de los principales motivos del aumento de la AaaS es la menor barrera de entrada que ofrece a los nuevos agentes de amenazas. La AaaS elimina la necesidad de que los agentes de amenazas lleven a cabo complejas campañas de intrusión o de phishing generalizado para recopilar credenciales. Con AaaS, la intrusión inicial ya se ha completado, lo que permite al comprador pasar directamente a la actividad posterior a la explotación y al despliegue de ransomware. En 2021, fuimos testigos de cómo varios agentes prolíficos de amenazas de ransomware o sus afiliados utilizaban AaaS como medio de acceso inicial, incluyendo White Janus (alias Lockbit 2.0) y White Apep (alias BlackMatter, DarkSide).

Figura 18: Apep blanco buscando acceso a redes corporativas en el foro Exploit

Programa de afiliación BlackMatter

07.10. 2021

BlackMatter

Byte

B

Vendedor

Inscripción: 19.07. 2021
Posteos: 3
Actividad: Otra
Deposito: 4.000000

10.07.2021

Se buscan redes corporativas en los siguientes países:

- USA
- CA
- AU
- GB

Todos los sectores excepto:

- Medico
- Instituciones estatales

Requerimientos:

- Ampliar los ingresos a partir $100 milliones
- 500 - 15,000 hosts
- No aceptamos redes que alguien ya haya intentado explotar

2 opciones de trabajo:

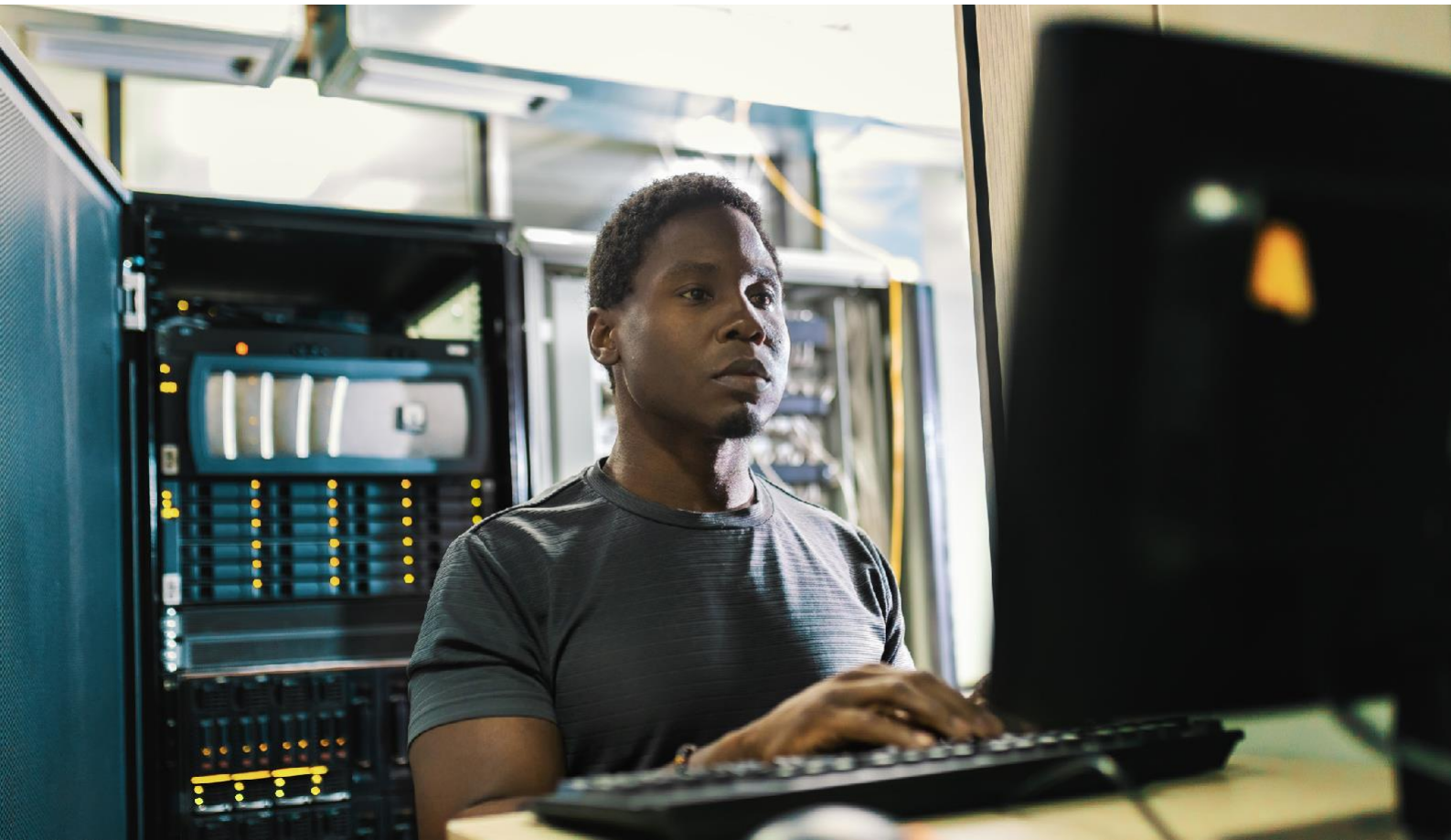
- Compra: de 3 a 100k
- Nos lo llevamos al trabajo (a discutir ndividualmente)

Esquema de trabajo:

- Elección de la opción de trabajo -> Acceso a la transferencia -> Verificación -> Lo tomamos o no (en caso de discrepancia)

Deposito:

- 120k



Actividad regional

En esta sección, describimos las campañas realizadas por los agentes de la amenaza que creemos que están basados en regiones geográficas específicas y que van desde operaciones de recopilación de información (en apoyo de objetivos estratégicos políticos y/o nacionales) hasta actividades con motivación financiera: tanto dirigidas como oportunistas. Al igual que en 2020, seguimos viendo que el panorama de las ciberamenazas se alinea con las circunstancias geopolíticas, y que los acontecimientos del mundo real influyen en las operaciones motivadas por el espionaje y el sabotaje por igual. Al igual que en 2020, seguimos viendo que el panorama de las ciberamenazas se alinea con la situación geopolítica, con acontecimientos del mundo real que influyen en las operaciones motivadas por el espionaje y el sabotaje por igual.

Asia-Pacífico

Disco duro para sobrevivir

En Corea del Norte, una pieza central de la doctrina política de Kim Jong-un es el continuo desarrollo de la fuerza nuclear del país, acompañado de un enfoque en las finanzas nacionales. En general, es muy probable que las operaciones de ciberriesgo hayan sido una de las principales vías del Estado norcoreano para frustrar el impacto de las sanciones internacionales y lograr sus objetivos estratégicos. La criptomoneda, en particular, es una fuente de ingresos crucial para el régimen de Corea del Norte, con múltiples agentes de amenazas basados en Corea del Norte que apuntan a organizaciones y personas relacionadas con la criptomoneda, en particular a los intercambios de criptomonedas, desde al menos 2017.[85]

El Bitcoin es plata, el compromiso es oro: el nuevo agente o agentes de la amenaza basada en Corea del Norte

A lo largo de 2021, observamos dos grupos principales de actividad que, según nuestra opinión, es muy probable que sean llevados a cabo por agentes de amenazas basados en Corea del Norte, y que tienen como blanco a entidades que operan con criptomonedas y el sector financiero a escala internacional. Inicialmente rastreamos estos dos grupos por separado, respectivamente como Black Alicanto (alias Dangerous Password, LeeryTurtle, CryptoMimic, CryptoCore, Operation SnatchCrypto)[86, 87] y Black Dev 2 (también conocida como Operación Gold Hunting, Operación SnatchCrypto). En última instancia, las coincidencias en las habilidades, la infraestructura y la victimología nos llevaron a evaluar que Black Alicanto y Black Dev 2 son probablemente el mismo agente de amenazas basado en Corea del Norte. Además, consideramos que es muy probable que este agente de la amenaza sea una evolución de Black Artemis' (aka Lazarus Group, HIDDEN COBRA) subgrupo financiero Bluenoroff.

A continuación, presentamos Black Alicanto y Black Dev 2 individualmente para dar una visión general de las diferentes TTPs que asociamos con los dos grupos de actividad.

Black Alicanto

Black Alicanto tiene una motivación financiera y ha estado activo al menos desde 2018, dirigiéndose a organizaciones de criptomonedas y entidades del sector de los servicios financieros. Si bien este agente de la amenaza suele utilizar documentos de señuelo relacionados con ascensos o bonificaciones de los empleados para inducir a los objetivos a abrir la carga útil, entre septiembre y diciembre de 2021 observamos que Black Alicanto utilizaba documentos de señuelo que presentaban descripciones de puestos de trabajo en empresas de los sectores de las finanzas y la criptomoneda, como Goldman Sachs, J.P. Morgan, Commerz AG, SALT Lending y Blockchain Intelligence Group.[88]

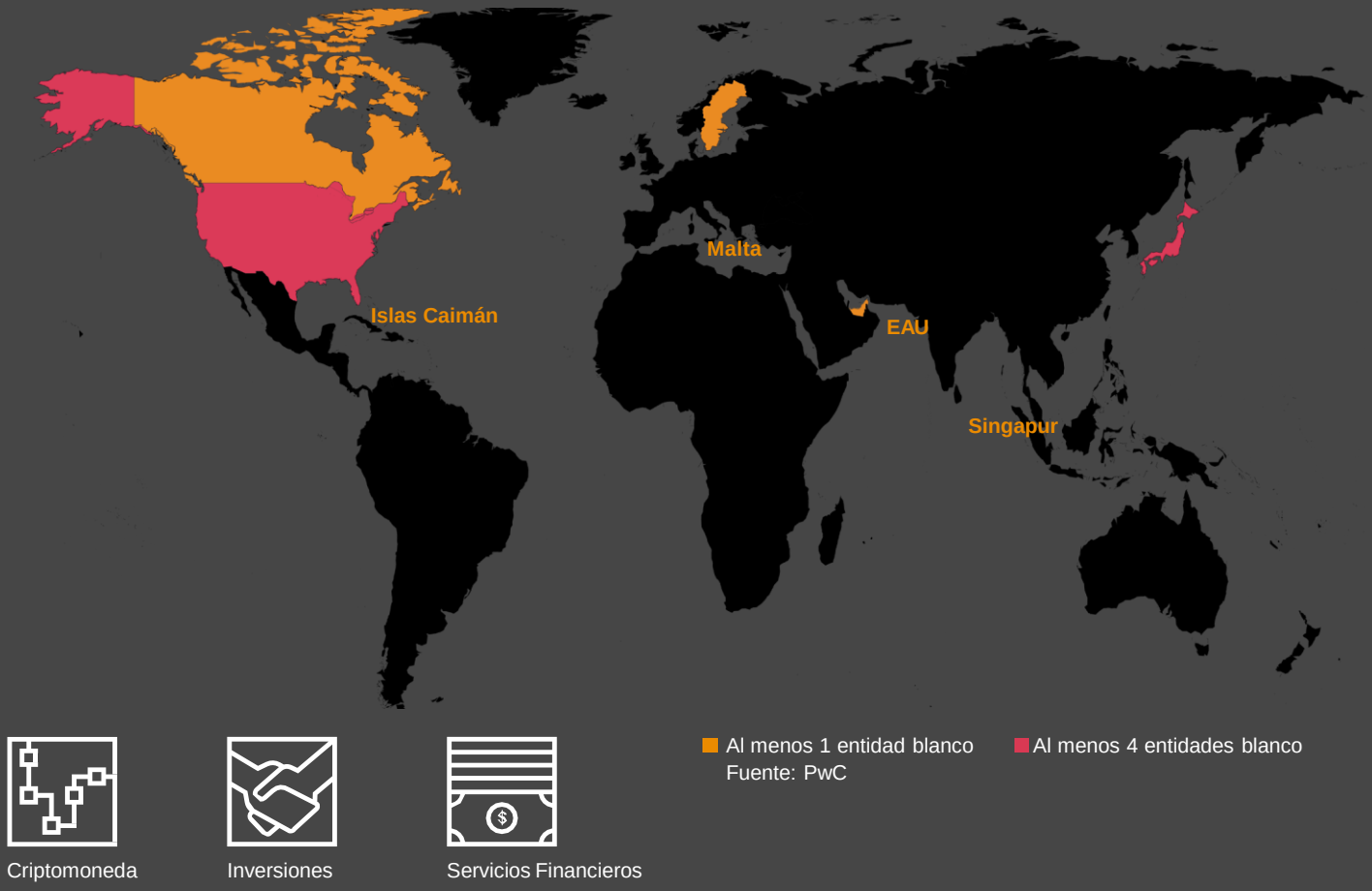
Black Alicanto envía inicialmente a los blancos correos electrónicos de spear phishing con archivos comprimidos adjuntos. Estos suelen contener documentos de doble extensión (archivos .LNK que se hacen pasar por documentos de Word o PDF) o documentos de señuelo protegidos por contraseña y archivos LNK maliciosos llamados Password.txt.lnk. como documentos de Word o PDF) o, documentos de enlace protegidos por contraseña y archivos LNK maliciosos llamados Password.txt.lnk. Los archivos de enlace abusan de los enlaces acortados por URL de Bit.ly para llevar al objetivo a descargar scripts maliciosos de dominios registrados por el agente de la amenaza. Black Alicanto se asegura de que sólo los objetivos reales, a diferencia de los investigadores de seguridad, reciban sus cargas útiles, y despliega manualmente las cargas útiles de la fase posterior sólo a aquellos.

Una de estas descargas es msoRAT[89, 90], un troyano de acceso remoto (RAT) que Black Alicanto despliega manualmente en los sistemas de las víctimas que le interesan. msoRAT es una evolución de un backdoor que ha sido utilizado durante años por BlueNoroff.[91, 92]

Black Dev 2

Desde al menos agosto de 2020, hemos seguido un grupo de actividad que inicialmente denominamos Black Dev 2 [93], dirigido principalmente a entidades del espacio de la criptomoneda y la tecnología financiera (FinTech), así como a empresas de Capital Riesgo (VC), en particular las que financian empresas relacionadas con la criptomoneda y la tecnología.

Figura 19: Distribución geográfica de las entidades blanco de Black Dev 2



Las intrusiones que asociamos con Black Dev 2 solían consistir en documentos de señuelo relacionados con una presentación de capital de riesgo o una presentación de la empresa, o con acuerdos de no divulgación. Los documentos señuelo traían una plantilla remota maliciosa desde un dominio registrado por el agente de la amenaza. Las macros de la plantilla remota descargaban una carga útil adicional -normalmente un backdoor malicioso y una Biblioteca De Enlace Dinámico (DLL) de perfil de la víctima- que se inyectaba en otro proceso en ejecución.

Al hacer un análisis cronológico de las horas de creación y última modificación de los documentos maliciosos creados por Black Dev 2, identificamos un patrón que coincide con el de un día de trabajo normal, que comienza alrededor de las 8 de la mañana y termina alrededor de las 6 de la tarde, con un intervalo de una o dos horas para almorzar en el medio, que coincide con la zona horaria GMT+9, que incluye a Corea del Norte.

También observamos que Black Dev 2 utilizaba una familia de malware que probablemente sea una variante de msoRAT, en una infraestructura que se solapa con otros servidores C2 de msoRAT utilizados por Black Alicanto.[94] Basándonos en la similitud de la configuración de la infraestructura y de las cadenas de intrusión adoptadas por Black Dev 2 y Black Alicanto, y en su victimología común, consideramos probable que Black Dev 2 y Black Alicanto sean el mismo agente de amenazas basado en Corea del Norte, y una evolución de Bluenoroff.

Misiones complementarias

Más allá del imperativo de seguir generando fondos para el régimen, los agentes de amenazas establecidos en Corea del Norte han seguido persiguiendo objetivos alineados con los objetivos estratégicos norcoreanos.

Black Banshee

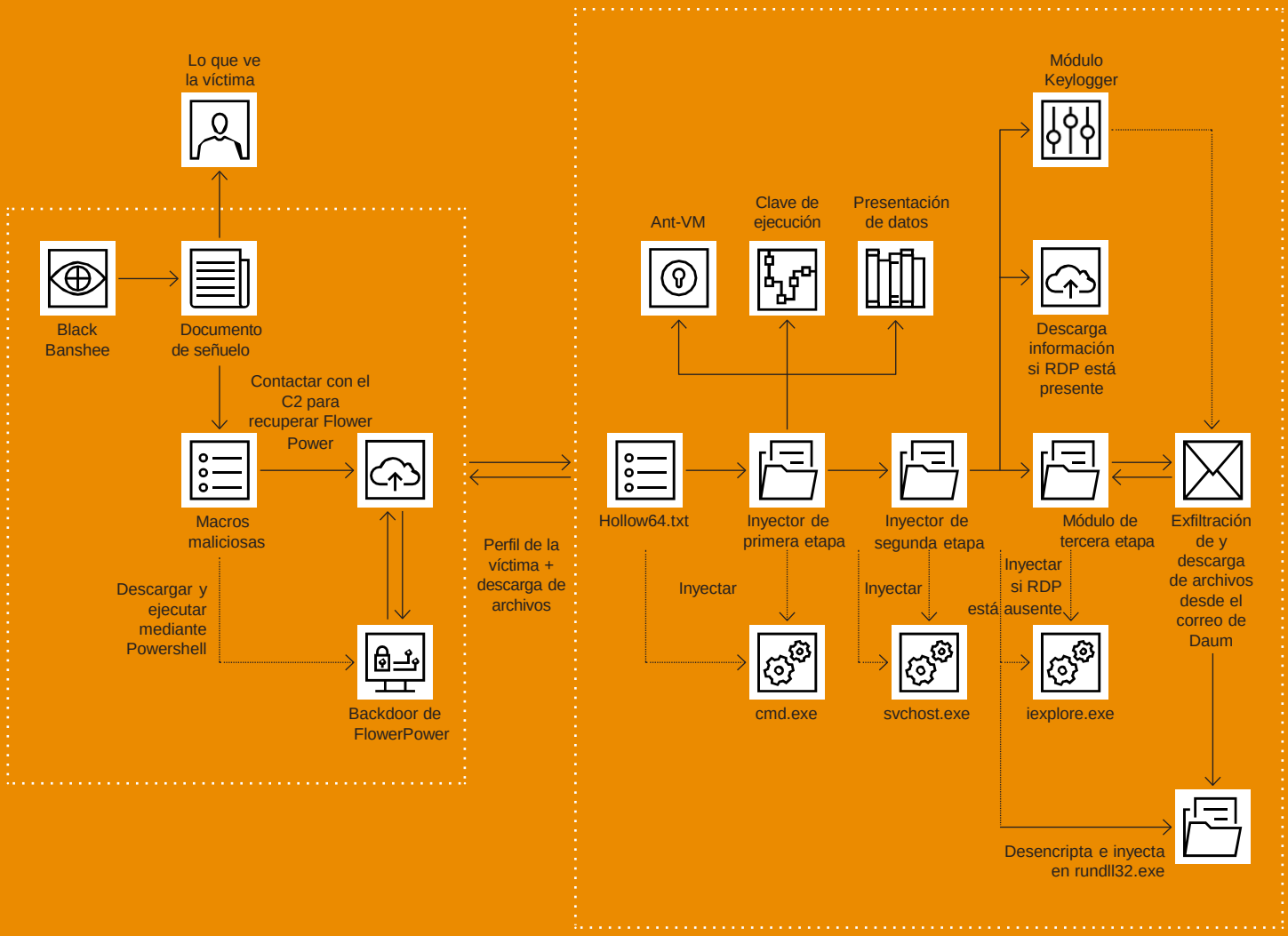
En 2021, los principales sectores de interés de Black Banshee (alias Kimsuky, Velvet Chollima) se mantuvieron en línea con los objetivos históricos del agente de la amenaza, e incluyeron:

- gobierno y sector público;
- diplomacia y política, incluidos los grupos de reflexión
- el mundo académico (con especial atención a la investigación nuclear y la política internacional)
- defensa y sector aeroespacial
- nuclear; y
- la sociedad civil y grupos específicos, como periodistas, ONG y grupos religiosos activos en relación con Corea del Norte.

La actualización de BravePrince

En 2021 observamos que Black Banshee mantuvo su enfoque en gran medida en estas prioridades, y renovó herramientas de su arsenal anterior en busca de sus objetivos regionales. Por ejemplo, Black Banshee desarrolló una versión actualizada de su backdoor BravePrince y la utilizó para atacar a víctimas surcoreanas.[95] El backdoor BravePrince actúa como perfilador de víctimas, keylogger y ladrón de información, exfiltrando los datos de las víctimas a través del servicio de correo electrónico surcoreano Daum. El backdoor también tiene la capacidad de exfiltrar archivos específicos de interés para Black Banshee, lo que sugiere no sólo la interacción directa del operador con el implante, sino también que el agente de la amenaza desplegó el backdoor específicamente a los objetivos de interés. La campaña se centró en entidades de Corea del Sur; probablemente pretendía obtener información diplomática, política y militar sobre la postura de Corea del Sur en relación con Corea del Norte, China y Rusia, así como con Estados Unidos. Una actualización sobre esta campaña publicada en noviembre de 2021[96] también la orientación detallada del material aeroespacial y de defensa, así como la investigación científica en campos específicos como el combustible de aviación.

Figura 19: Pasos de una cadena de intrusión de Black Banshee con el backdoor BravePrince



Política nuclear para BabySharks

Black Banshee también continuó realizando campañas de BabyShark durante la mayor parte del año[97], manteniendo su enfoque de larga data en temas nucleares, políticos y diplomáticos. Identificamos y notificamos al menos ocho víctimas que Black Banshee había comprometido desde agosto de 2021. Entre ellos se encontraban figuras diplomáticas, analistas actuales o antiguos de alto nivel en grupos de reflexión centrados en la región de Asia-Pacífico, académicos de alto nivel centrados en la historia, la política y la defensa de Asia-Pacífico, y empleados de ONG centradas en la península de Corea. Este objetivo también está en consonancia con las campañas anteriores llevadas a cabo por Black Banshee desde al menos finales de 2018, cuando observamos por primera vez que el actor de la amenaza comenzaba a dirigirse a figuras individuales que trabajaban en organizaciones supranacionales, incluidas las Naciones Unida.

Black Artemis

Black Artemis (también conocido como HIDDEN COBRA, Lazarus Group) continuó dirigiéndose en gran medida a los sectores aeroespacial y de defensa como parte de una campaña que rastreamos como ShowState.[98] La campaña persistió en 2021, basándose en documentos de ingeniería social y spear phishing con temática de oportunidades de trabajo para el sector aeroespacial y de defensa, ampliándose para incluir empresas de ingeniería y fabricación.[99]

Otra campaña de Black Artemis en 2021, dirigida a entidades de Corea del Sur, también incluía documentos maliciosos con macros para lograr el acceso inicial. Sin embargo, en este conjunto de intrusiones, las macros descargaban en el disco una imagen PNG que contenía datos maliciosos en formato comprimido, lo que dificultaba su detección estática por parte del software antivirus. A continuación, la macro convertía la imagen PNG en un archivo BMP y lo ejecutaba a través de mshta.exe. La carga útil ejecutable incrustada, una familia de malware que hemos denominado PaintJob[100], comparte similitudes con la rutina de cifrado utilizada por Dtrack, un conocido RAT que atribuimos al subgrupo de Black Artemis conocido como Andariel.

Black Artemis también fue un objetivo persistente de los investigadores de seguridad y vulnerabilidad a lo largo del año pasado. En enero de 2021, Google[101] y Microsoft[102] informaron de una campaña de ingeniería social de meses de duración que se basaba en perfiles de Twitter que se hacían pasar por investigadores de seguridad, así como en cuentas de LinkedIn, Telegram, Discord y Keybase. Black Artemis se ponía en contacto con los objetivos bajo el falso pretexto de colaborar en un proyecto de investigación de vulnerabilidades. A continuación, les enviaba un proyecto de Visual Studio con código malicioso que ejecutaba el dropper Comebacker, que finalmente conducía a la instalación del backdoor Klackring.

El agente de la amenaza también mantenía un blog de seguridad que actuaba como abrevadero, y dirigía a los investigadores de seguridad objetivo hacia él durante la conversación. Cuando los objetivos visitaban el sitio, un exploit de día cero de Chrome llevaba a la instalación de un servicio malicioso en su máquina, junto con una puerta trasera en memoria. Black Artemis podía entonces explotar el acceso que había obtenido a los sistemas de los investigadores de seguridad para identificar y robar investigaciones de seguridad ofensivas de interés.

Un esfuerzo paralelo de Black Artemis incluyó la selección de investigadores de seguridad ofensiva chinos con documentos maliciosos en idioma chino.[103] Los intentos de compromiso contra los investigadores de seguridad también incluyeron una versión troyanizada de IDA Pro[104], un software de desensamblaje ampliamente utilizado en la investigación de ciberseguridad y, en particular, en la investigación de la seguridad. en la investigación sobre ciberseguridad y, en particular, en el análisis de vulnerabilidades y el desarrollo de exploits.

Un año de actividad de agentes de amenazas con base en China

Planificar con tiempo

Hemos seguido observando una importante actividad de agente sde amenazas con base en China. Algunos de estos acto agente de amenazas, como Red Djinn, se centran en sectores industriales específicos como los semiconductores, la inteligencia artificial, la atención sanitaria (que incluye la investigación genética y la biotecnología), la computación cuántica y la exploración en los ámbitos espacial, marítimo y polar.[105] Otros, como Red Kelpie, persiguen (y en algunos casos permiten a otros llevar a cabo) objetivos significativamente más amplios.

Más allá de los objetivos estratégicos económicos, también seguimos observando actividades de espionaje centradas en el sector público; Red Vulture (alias Ke3chang, APT15, APT25, NICKEL) y Red Keres (alias APT31, ZIRCONIUM) son ejemplos destacados de este tipo de objetivos.

Red Djinn

El agente de la amenaza con sede en China que rastreamos como Red Djinn (alias BlackTech, Mobwork, Palmerworm) permaneció activo en 2021, utilizando herramientas conocidas (como PLEAD y TSCookie) y otras nuevas (como Consock, FlagPro y SpiderRAT).

A principios de 2021, observamos una serie de campañas de Red Djinn que utilizaban familias de malware conocidas como PLEAD y TSCookie, incluyendo variantes de Linux de ambas puertas traseras para ampliar la variedad de sistemas a los que podía dirigirse. El objetivo de estas campañas eran las organizaciones con sede en partes de Asia, e incluía una empresa de TI y telecomunicaciones. El agente de la amenaza registró dominios relacionados con tecnologías de nube y VPN, y las familias de malware contenían identificadores de campaña que probablemente indicaban el objetivo de los sectores de fabricación e ingeniería.

New Djinn

Aunque Red Djinn se ha centrado históricamente y de forma constante en atacar las economías más grandes de Asia, también hemos observado anteriormente objetivos más amplios por parte del agente de la amenaza. Por ejemplo, el agente de la amenaza se dirigió anteriormente a una filial en el extranjero de un proveedor de servicios gestionados (MSP) para realizar un ataque de "salto de isla" para moverse lateralmente a la red principal del MSP.

A través de nuestro rastreo de Consock[106, 107], una variante personalizada de Gh0stRAT asociada a Red Djinn (también conocida como Gh0stTimes) pudimos identificar al controlador del malware.

Figura 20: Times.exe, el controlador del malware Consock de Red Djinn

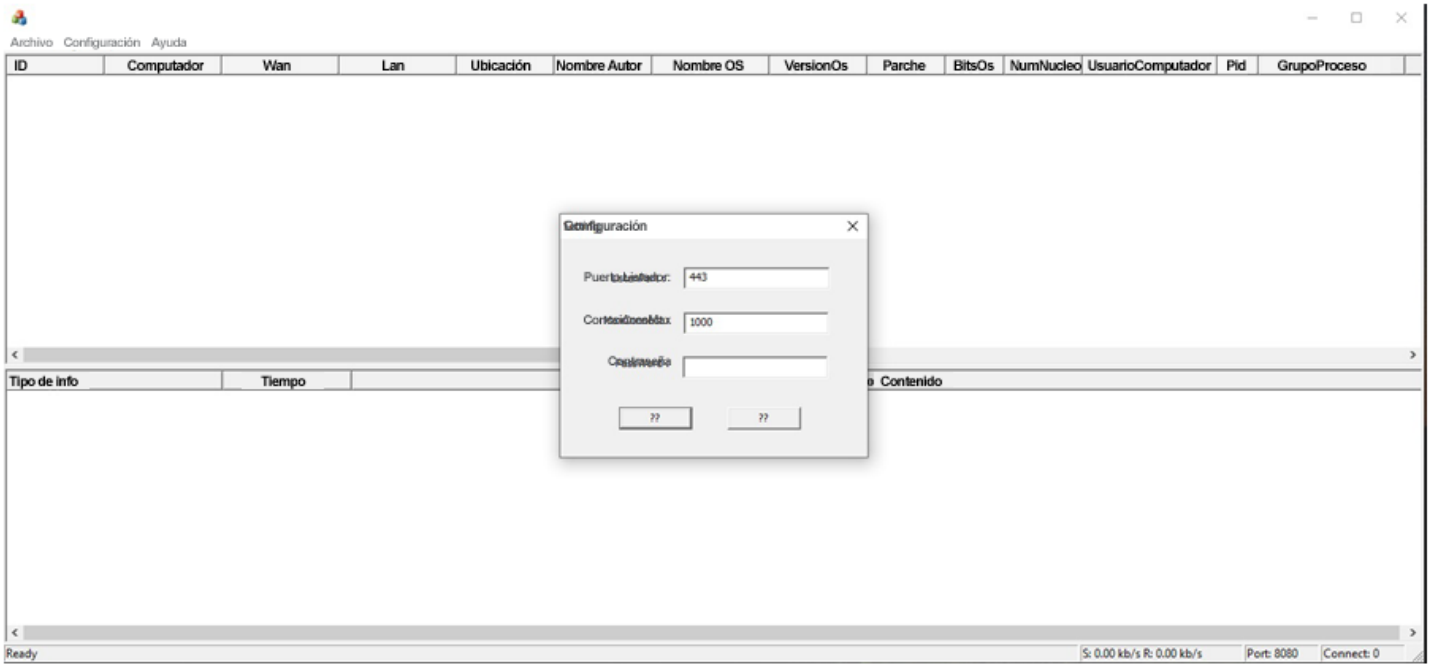
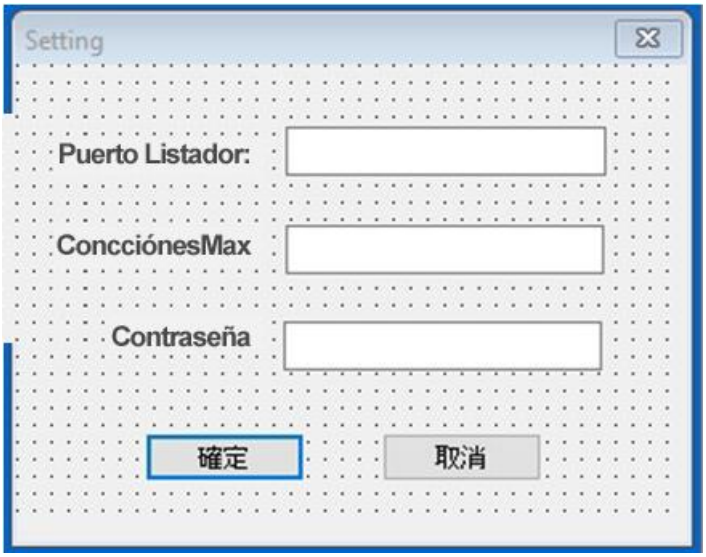


Figura 21: Times.exe se diseñó originalmente para sistemas en chino



También descubrimos señuelos de phishing selectivo utilizados por el actor de la amenaza para entregar tanto Consock como una nueva familia de malware que denominamos Flagpro.[108] Consideramos que es muy probable que Red Djinn utilizara Flagpro en su objetivo de la filial de un proveedor japonés de servicios de TI y desarrollador de software que opera en el este y el sur de Asia.
En nuestro análisis de esa campaña, identificamos una serie de scripts de explotación que, según nuestra opinión, es muy probable que sean utilizados por Red Djinn para sus operaciones. Los metadatos revelaron que algunos de ellos probablemente fueron tomados o adaptados de bases de datos de vulnerabilidad abiertas, como Seebug. Estos iban acompañados de carpetas que contenían datos que sugerían que Red Djinn había estado realizando reconocimientos de sistemas vulnerables a escala internacional. Además, identificamos código de explotación para dispositivos Citrix y Mikrotik que parecía estar todavía en desarrollo.[109] También identificamos actividad de Red Djinn que se remonta a marzo de 2021, explotando las vulnerabilidades de ProxyLogon, después de su divulgación inicial, para desplegar un nuevo backdoor que llamamos SpiderRAT.[110, 111]

Red Vulture
Red Vulture aumentó su ritmo operativo a lo largo de 2021. Observamos que Red Vulture llevó a cabo reconocimientos regulares en una variedad de organizaciones a lo largo del año, en los siguientes sectores:

- Gobierno;
- Aeroespacial y de Defensa;
- Educación; y
- ONGs.

Este reconocimiento consistía principalmente en que el actor de la amenaza navegaba por los sitios web y los servicios perimetrales (por ejemplo, VPN, correo electrónico) de las organizaciones objetivo. Se ha comprobado que el actor de la amenaza está escaneando masivamente en busca de vulnerabilidades.[112] El éxito de Red Vulture a la hora de atacar a las víctimas en 2021 se debió a menudo a su prolífico uso de exploits contra los sistemas de autenticación del perímetro (por ejemplo, las VPN).

El reconocimiento observado se centró en el objetivo de los Ministerios de Asuntos Exteriores (MFA), con un enfoque consistente en Europa y América del Sur.[113, 114, 115]

Red Keres
A principios de 2021, la Oficina Federal Alemana para la Protección de la Constitución (BfV) informó de que Red Keres tenía como objetivo instituciones como "ministerios y autoridades, organizaciones políticas y fundaciones" en toda Europa.[116]

Analizando la infraestructura de Red Keres revelada por el BfV, también identificamos pruebas que sugieren que el agente de la amenaza probablemente había comprometido, y estaba accediendo directamente, al servidor de correo electrónico del Ministerio de Asuntos Exteriores de un gobierno del sudeste asiático entre al menos diciembre de 2020 y febrero de 2021.[117] Por la misma época, observamos una actividad similar en el servidor de correo electrónico del Ministerio de Defensa de otro gobierno del sudeste asiático.

A finales de 2021, la Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) de Francia publicó un informe detallado sobre las TTP de Red Keres. El informe detallaba la configuración de la infraestructura de anonimización multicapa del actor de la amenaza, que incluía más de mil routers para pequeñas oficinas/oficinas domésticas (SOHO), una técnica en la que PwC ha observado que otros actores de la amenaza con base en China han invertido a lo largo de 2021. El informe también destacó las diferentes técnicas que Red Keres despliega cuando intenta obtener el acceso inicial a una víctima, que van desde el spear phishing, pasando por el forzamiento de contraseñas y el abuso de credenciales válidas, hasta la explotación de vulnerabilidades como ProxyLogon o en productos de redes privadas virtuales (VPN).

Red Kelpie

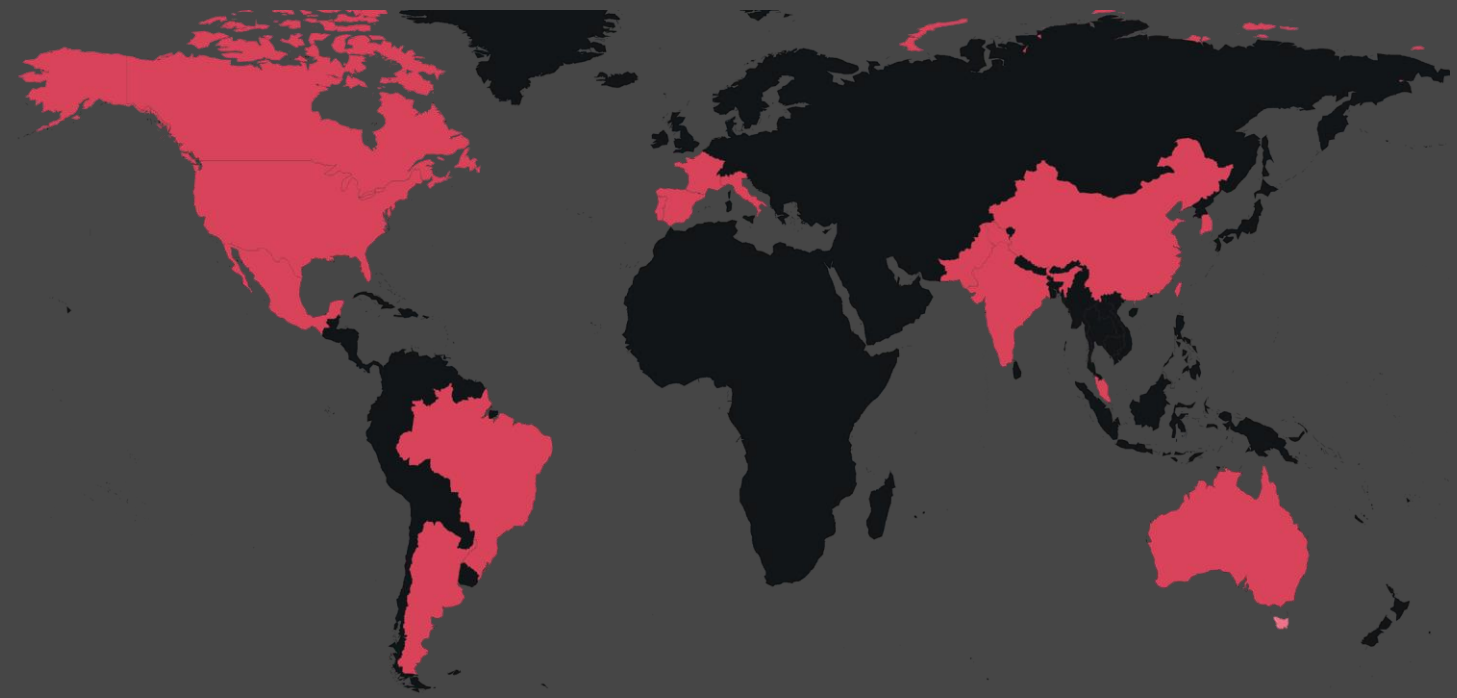
El actor de la amenaza que rastreamos como Red Kelpie (que se solapa con APT41 y BARIUM) se basa en una amplia variedad de familias de malware, incluyendo ShadowPad y CROSSWALK, así como en herramientas básicas como Cobalt Strike. Es prolífico en sus objetivos, que abarcan varios sectores estratégicamente importantes.

ChaChaLoader

En 2021, Red Kelpie llevó a cabo una serie de campañas utilizando el conocido cargador Motnug del agente de la amenaza, y una probable evolución llamada ChaChaLoader. Motnug y ChaChaLoader fueron utilizados para cargar Cobalt Strike, y en algunos casos raros una puerta trasera recientemente observada que ha sido llamada SIDEWALK en código abierto, y que es una probable evolución de la puerta trasera CROSSWALK.[118] Es plausible que los pocos casos en los que se desplegó SIDEWALK en lugar de CobaltStrike fueran para blancos de alto valor.

Estas campañas se dirigieron a diversos sectores, como los servicios financieros, el comercio minorista, las telecomunicaciones, la industria y la aviación.

Figura 22: Objetivo de la alcahofa roja en 2021



Servicios Financieros | Venta al detal | Telecomunicaciones | Manufactura | Aviación

Fuente: PwC

Vulnerabilidad de Confluence

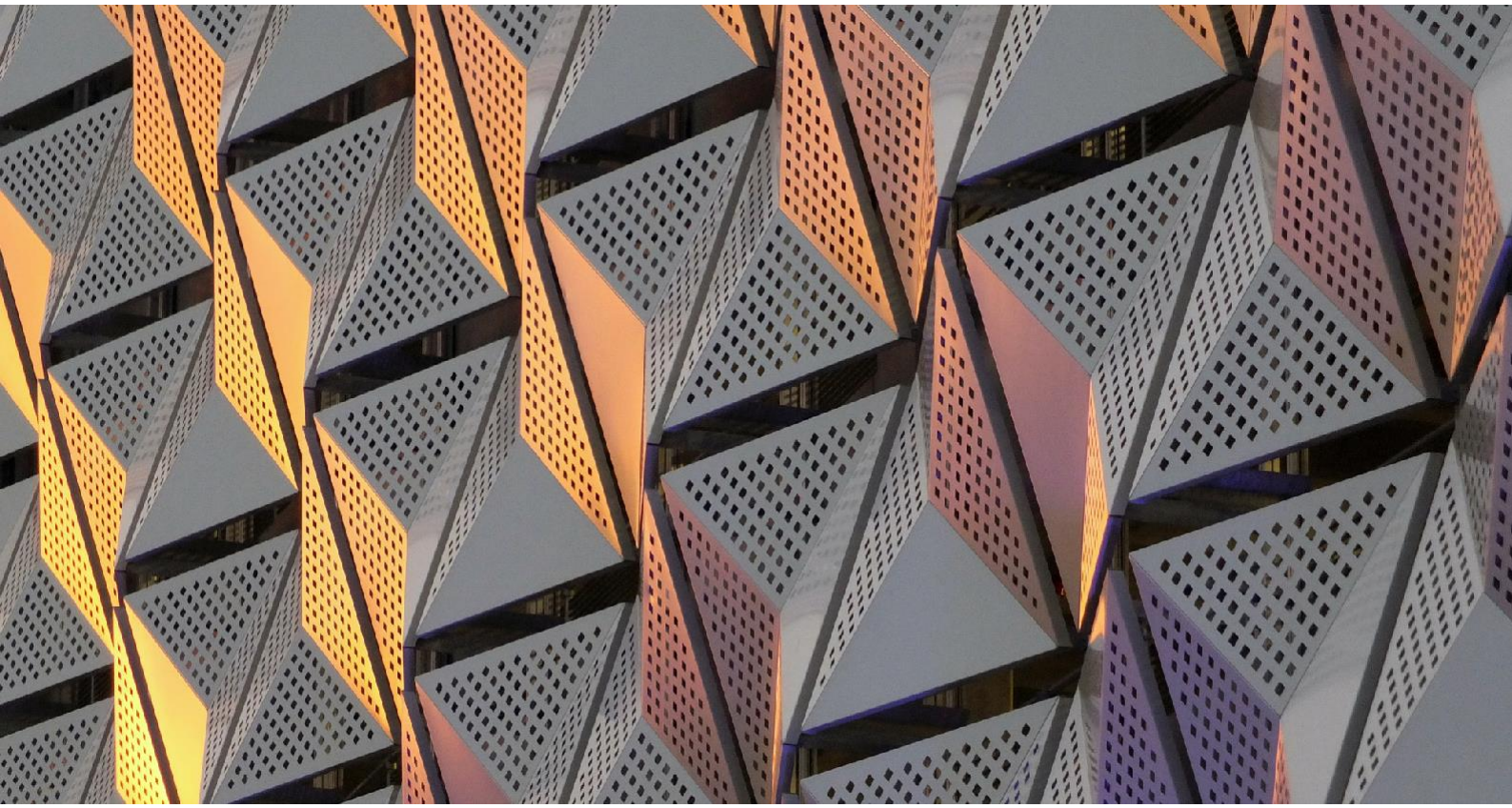
En años anteriores, Red Kelpie ha explotado en masa vulnerabilidades en la infraestructura de cara al público para obtener un acceso inicial, una táctica que también observamos en 2021. En particular, observamos que Red Kelpie explotaba la vulnerabilidad de ejecución de código de Atlassian Confluence CVE-2021-26084 para lanzar un script por lotes y una DLL utilizados para cargar y ejecutar Cobalt Strike.[119] Se ha observado anteriormente que Red Kelpie utiliza exploits de vulnerabilidades en el software de Citrix/Cisco para desplegar scripts por lotes muy similares, que también se sabe que cargan y ejecutan Cobalt Strike.[120]

Activo, a pesar de las acusaciones

En septiembre de 2020, el Departamento de Justicia de EE.UU. acusó a siete individuos con base en Asia alegando que estos individuos eran hackers informáticos, y que las intrusiones que llevaron a cabo fueron referidas en código abierto como APT41, BARIUM, Winnti, etc.[121]

A pesar de estas acusaciones, la actividad de Red Kelpie continuó a lo largo de 2021. Quizás el mayor coste para Red Kelpie debido a la acusación fue la incautación de cuentas, servidores y dominios utilizados por el agente de la amenaza, lo que le obligó a cambiar parte de su ritmo operativo.

a cambiar parte de su ritmo operativo. Hemos rastreado nuevos conjuntos de infraestructura utilizados por este agente de la amenaza a finales de 2020/2021, aunque hemos observado solapamientos con infraestructuras asociadas más antiguas atribuidas a la APT41/ BARIUM. Las acusaciones de varios de los operadores que están detrás de las campañas no parecen haber tenido un impacto general significativo en las operaciones del agente de la amenaza.



Estudio de caso de respuesta a incidentes:

El FUNRUN de Red Dev 14

PwC respondió a una intrusión en un think tank por parte de un actor de amenazas con sede en China, que identificamos como Red Dev 14.[122] Utilizando los exploits ProxyLogon, el actor de la amenaza dejó caer una webshell en un servidor Exchange local. Inicialmente, el actor de la amenaza intentó realizar un reconocimiento a través de la webshell (que consistía principalmente en la recopilación de información del sistema, como los nombres de usuario y los procesos en ejecución), y ejecutó comandos para volcar la memoria de LSASS con el fin de obtener credenciales a través de binarios vivos. El agente de la amenaza utilizó una variante de la puerta trasera llamada FUNRUN, que utilizó para soltar ProcDump para volcar la memoria de LSASS, así como para soltar Mimikatz en el disco.

Después de obtener con éxito las credenciales, el agente de la amenaza se movió lateralmente en la red a través de recursos compartidos remotos SMB, instalando el backdoor FUNRUN en otros hosts. El agente de la amenaza también ejecutó comandos para buscar otras webshells en el servidor Exchange. Esto probablemente se hizo para comprobar si el servidor Exchange ya había sido comprometido (probablemente por ProxyLogon), que informaría a Red Dev 14 si otro agente de la amenaza estuviera también presente en el sistema. Esto tiene el potencial de afectar a la forma en que lograría sus objetivos.

Desde el punto de vista de la atribución, ya habíamos observado el uso de la puerta trasera FUNRUN por parte del agente de la amenaza con sede en China que rastreamos como Red Pegasus (también conocido como APT9).[123] Sin embargo, ha pasado mucho tiempo entre la última vez que se observó a Red Pegasus utilizando esta puerta trasera (durante 2014 y 2015) y la actividad de FUNRUN de 2021 que observamos.
Basándonos en esta consideración, así como en el hecho de que el mecanismo de carga era diferente para este backdoor en comparación con el uso de Red Pegasus, y que no había solapamientos de infraestructura con Red Pegasus, decidimos rastrear esta actividad bajo el nuevo nombre de Red Dev 14.

Red Dev 14 víctimas comprometidas en múltiples geografías como parte de esta campaña, principalmente en el sector agrícola.

Llámame, tal vez: Actores de amenazas con base en China que apuntan a las telecomunicaciones

El sector de las telecomunicaciones sigue siendo un objetivo para múltiples actores de amenazas con base en China. Las organizaciones de este sector disponen de una gran variedad de información de gran valor, incluidos los datos de un proveedor de telecomunicaciones sobre sus clientes (que, dependiendo del proveedor, pueden ser metadatos sobre conexiones a sitios web o registros de llamadas). Este tipo de información puede ser explotada por los actores de la amenaza con fines de vigilancia, o para recopilar inteligencia tradicional sobre las actividades de objetivos específicos.

Por ejemplo, como se ha descrito anteriormente, seguimos viendo que Red Kelpie se dirige al sector de las telecomunicaciones,[124] así como que la herramienta compartida ShadowPad se utiliza para comprometer a los proveedores de telecomunicaciones.[125] Apoyamos una investigación de respuesta a incidentes a un proveedor de telecomunicaciones en el sudeste asiático, donde observamos una variante de la puerta trasera Evora utilizada por el agente de amenazas basado en China Red Salamander (alias LotusBlossom).[126]

Algunas cosas cambian y otras permanecen igual para los agentes de amenazas basados en la India

De nuestras investigaciones sobre las operaciones de los agentes de amenazas con base en la India, seguimos observando un estrecho enfoque en los países de relevancia estratégica para la India, en particular en sus vecinos cercanos, China y Pakistán. Hemos observado que casi todos los agentes de amenazas de espionaje con base en la India que rastreamos utilizan documentos de señuelo relacionados con la política o los asuntos políticos de los países objetivo, o con temas militares y de defensa.

Orange Kala (Donot)

Orange Kala (alias Donot) mantuvo en 2021 un ritmo operativo y un enfoque de objetivos similares a los del año anterior, con pocas variaciones en las TTP. En al menos un caso, el agentes de la amenaza utilizó un documento de señuelo relacionado con la tecnología de misiles.127 Este tema de señuelo no era nuevo para Orange Kala, ya que el contenido de varios otros documentos de señuelo desde al menos noviembre de 2020 estaba tomado tanto de artículos de prensa como de revistas centradas en gran medida en la tecnología de defensa de misiles. Sin embargo, mientras que la mayoría de los documentos anteriores sobre este tema se referían a Estados Unidos, esta campaña fue el primer caso en el que PwC observó que Orange Kala se centraba en la tecnología de misiles en la región de Asia-Pacífico. Tanto en esta campaña

Estudio de caso: Red Menshen, dirigida a los proveedores de telecomunicaciones

A lo largo de 2021 rastreamos y respondimos a múltiples intrusiones atribuidas a un agente de amenazas con base en China que hemos denominado Red Menshen.[128] Se ha observado que este agente de la amenaza se dirige a proveedores de telecomunicaciones en Oriente Medio y Asia, así como a entidades de los sectores gubernamental, educativo y logístico, utilizando una puerta trasera personalizada que denominamos BPFDoor. Este backdoor soporta múltiples protocolos para comunicarse con un C2, incluyendo TCP, UDP e ICMP, lo que permite al agente de la amenaza una variedad de mecanismos para interactuar con el implante.

Nuestra investigación ha demostrado que este agente de la amenaza utiliza una variedad de herramientas en su fase de post-explotación. Esto incluye variantes personalizadas de la herramienta compartida Mangzamel (incluyendo variantes de Golang), variantes personalizadas de Gh0st, y herramientas de código abierto como Mimikatz y Metasploit para ayudar en su movimiento lateral a través de los sistemas Windows[129, 130] También identificamos que el agente de la amenaza envía comandos a las víctimas de BPFDoor a través de Servidores Privados Virtuales (VPS) alojados en un proveedor conocido, y que estos VPS, a su vez, son administrados a través de routers comprometidos con base en Taiwán, que el agente de la amenaza utiliza como túneles VPN.

La mayor parte de la actividad de Red Menshen que observamos tuvo lugar de lunes a viernes (no se observó ninguna durante los fines de semana), y la mayor parte de la comunicación tuvo lugar entre la 01:00 y las 10:00 UTC.[131] Este patrón sugiere una ventana de actividad consistente de 8 a 9 horas para.

Este patrón sugiere una ventana de actividad consistente de 8 a 9 horas para el agente de la amenaza, con una probabilidad realista de que coincida con las horas de trabajo locales.

como a lo largo del año, Orange Kala se apoyó en gran medida en la herramienta de malware como servicio (MaaS) WarzoneRAT. En una campaña, el agente de la amenaza desplegó WarzoneRAT a través de una DLL maliciosa que, en última instancia, descodificaba y ejecutaba una larga serie de comandos de línea de comandos codificados.[132] Algunos de los documentos de señuelo de esa campaña, cargados en un escáner antivirus en línea de los Emiratos Árabes Unidos, giraban en torno a los nuevos buques de la Armada iraní, y otros en torno a los ejercicios navales multinacionales organizados por Pakistán, lo que sugiere el probable interés del agente de la amenaza por los temas militares.

Compartir es solidario

A lo largo del año, observamos varios cruces de TTP entre Orange Kala y otros agentes de amenazas con base en la India que todavía estamos investigando, pero que podrían ser indicativos de un mayor grado de interconexión entre los agentes de amenazas con base en la India de lo que se había considerado anteriormente. Durante febrero de 2021, rastreamos una campaña[133] que incluía una plantilla de archivo RTF malicioso con vínculos a las operaciones de Orange Kala y Orange Dev 1 (también conocido como CONFUCIUS) en 2020.[134] También se identificaron vínculos desde una campaña de 2017 dirigida a Pakistán y conocida como Operación Shaheen[135] La actividad de 2021 se centró en temas militares y de defensa, con documentos de señuelo que hacían referencia a propuestas de defensa y, en un caso, a la Marina Real de Tailandia. Se sabe que tanto Orange Kala como Orange Dev 1 han tenido como objetivo los sectores de la defensa y el gobierno en el pasado. La campaña de 2021 utilizó técnicas diferentes a las de la actividad similar reportada en 2020[136]añadiendo una capa adicional en la cadena de ataque, con los documentos RTF iniciales descargando un segundo RTF en la máquina de la víctima, y utilizando ese segundo RTF como descargador de una DLL maliciosa.

En junio de 2021, observamos una campaña de Orange Athos (también conocido como Patchwork) que incluía scripts VBA que ya habíamos observado que utilizaba Orange Kala en 2019.[137] Las macros VBA eran sorprendentemente similares en la actividad de 2019 y 2021, hasta los nombres de variables únicos; esto sugiere con una probabilidad realista que no eran el producto de un constructor de macros, sino macros a medida creadas por un agente de la amenaza y reutilizadas por otro. Mientras que el documento malicioso se basaba en la biografía de un individuo paquistaní tomada de Scribd.com, el agente de la amenaza alteró el texto original para afirmar que el padre del individuo solía trabajar para la Comisión de Investigación del Espacio y la Alta Atmósfera (SUPARCO), la agencia espacial nacional de Pakistán. El documento se utilizó para entregar a las víctimas el backdoor BADNEWS, un elemento básico del arsenal de Orange Athos desde hace tiempo. Otros informes de código abierto[138, 139] de principios de año hablaban de otros documentos de señuelo malicioso en torno a SUPARCO; estos entregaban WarzoneRAT a los objetivos y se atribuían al agente de amenazas en India Orange Dev 1.

Estas campañas muestran al menos un mínimo de herramientas compartidas, o de adaptación cruzada de herramientas simples, entre los agentes de amenazas con sede en la India. Sin embargo, observamos que esto sólo se da en el nivel de los vectores de acceso iniciales, ya que los agentes de la amenaza con base en la India todavía difieren en gran medida en su elección de las puertas traseras de la etapa posterior.

Orange Athos (Patchwork)

Orange Athos (también conocido como Patchwork) continuó haciendo un uso intensivo del backdoor BADNEWS (también conocido como BozokRAT) a lo largo de diferentes campañas en 2021, con sólo pequeños cambios en la base de código del malware desde que se informó por primera vez en código abierto en 2016.[140]

El agente de la amenaza mantuvo su enfoque anterior[141] en objetivos chinos y pakistaníes. En una campaña que observamos en abril de 2021, el agente de la amenaza utilizó un documento de señuelo relacionado con la cooperación militar entre China y Pakistán.[142] El documento era un archivo DOCX malicioso que explotaba CVE-2017-0261, una vulnerabilidad de Uso Después de Libre (UAF por sus siglas en ingles) que pertenece específicamente a las Imágenes Postscript Encapsuladas (EPS por sus siglas en ingles). Se trata de una técnica en la que hemos observado que el agente de la amenaza se ha basado sistemáticamente en varias campañas de 2020 con Herramientas, Técnicas y Procedimientos (TTP por sus siglas en ingles) casi idénticos, cada uno de ellos centrado en objetivos con sede en China.

Entre las intrusiones separadas, una[143] presentaba un señuelo que pretendía ser un formulario de la Junta Federal de Ingresos de Pakistán, en el que se pedía a los empleados de los departamentos del gobierno federal pakistaní que introdujeran sus datos personales para poder optar a para recibir un paquete especial de desgravación fiscal. Cuando las víctimas abrían el RTF, la misma vulnerabilidad mencionada anteriormente (CVE-2017-0261) conducía a la instalación del backdoor BADNEWS. Con la explotación continua de la vulnerabilidad específica, y el uso de herramientas que han sido bien documentadas en código abierto, parece que este es otro agente de amenaza que persistirá con TTPs probados y comprobados.

Orange Yali (BITTER)

A lo largo de 2021, identificamos varios sitios web que pretendían ser empresas paquistaníes legítimas y que creemos que probablemente fueron creados y mantenidos por el agente de amenazas basado en la India Orange Yali (alias BITTER) desde 2020. Los sitios web, que normalmente tienen poco o ningún contenido o texto de marcador de posición, se utilizaron para escenificar cargas útiles del backdoor "rkftl", a veces empaquetado como un instalador MSI, así como utilidades, como el cliente SSH y Telnet PuTTY. Orange Yali también siguió utilizando la familia de malware conocida como ArtraDownloader, e introdujo el uso de archivos CHM (HTML compilado) en una campaña dirigida específicamente a entidades chinas.[144, 145] Varios informes indicaron también que Orange Yali utilizó al menos dos exploits de día cero diferentes[146, 147] a lo largo de 2021, ambos adquiridos probablemente de un intermediario de exploits en lugar de ser desarrollados internamente por el agente de la amenaza.[148] Esto indica que al menos un agente de la amenaza basado en la India y motivado por el espionaje tiene los recursos para acceder al mercado privado de día cero, algo que no habíamos observado anteriormente de agentes de la amenaza activos en la región

El espionaje no es rentable: La actividad de los agentes de amenazas con base en Pakistán

A lo largo de 2021, Green Havildar (alias APT36, Transparent Tribe, Gorgon Group) siguió operando principalmente en línea con su probable objetivo principal de recopilar información de inteligencia (incluido el objetivo de los militares, el gobierno y el sector público en general, especialmente en la India). Este agente de la amenaza se basa en el spear phishing básico para el acceso inicial, con documentos de señuelo que varían desde los currículos de los individuos hasta los programas de conferencias, pasando por varias muestras relacionadas con el ejército y la defensa.[149]

Green Havildar es conocido por su uso de CrimsonRAT, que siguió operando a través de un modelo constructor: el RAT tiene un amplio conjunto de capacidades de vigilancia y exfiltración, un modelo de ofuscación de código consistente, y la capacidad del agente de la amenaza de cambiar con flexibilidad los puertos por los que se lleva a cabo la actividad C2. Entre abril y julio de 2021, el Team Cymru publicó informes en los que se exponía la configuración de la infraestructura C2 de Green Havildar, incluida la gestión del agente de la amenaza a través de RDP.[150, 151]

En 2021, observamos un aumento de la actividad de las operaciones de Green Havildar centradas en la ciberdelincuencia y motivadas por las finanzas (que aparecen en el código abierto bajo el nombre de Gorgon Group, alias Aggah, MasterMana). Al igual que en 2020, la mayoría de las campañas de spam de Gorgon Group incluían señuelos de documentos de PowerPoint y enlaces de OneDrive, que entregaban RATs básicos como AgentTesla, Remcos y Quasar. Además, observamos el uso de dos inyectores comunes separados por el agente de la amenaza RunPE y HCrypt.

Si bien se sabe que Gorgon Group también aloja scripts maliciosos de varias etapas en sitios de pasta públicos como Pastebin y Blogspot, también rastreamos una serie de campañas que utilizaban cuentas en The Internet Archive con fines similares. En agosto de 2021, se informó152 de que el Grupo Gorgon estaba utilizando sitios web comprometidos para montar descargas maliciosas de etapa siguiente y entregaba el RAT Warzone en lugar de los sitios de pasta, en un esfuerzo por evitar la detección y el desmantelamiento de sus habilidades escenificadas.[153]

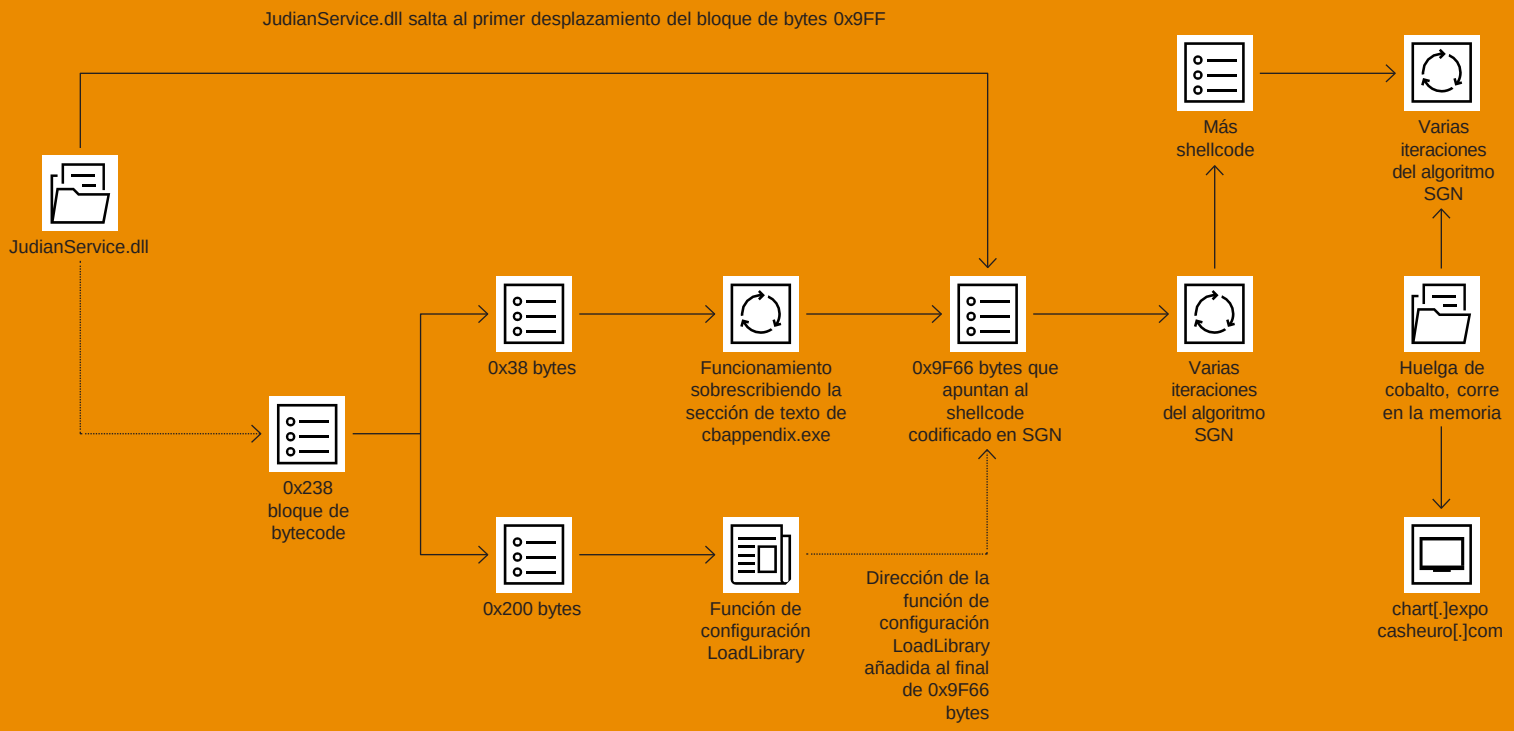
Mientras que las operaciones de recopilación de información de Green Havildar se centran principalmente en la India y ocasionalmente en países vecinos como Afganistán[154], la actividad de Gorgon Group tiene un alcance internacional que no se limita necesariamente a consideraciones políticas. Por ejemplo, a partir de abril de 2021 rastreamos una campaña del Gorgon Group dirigida a organizaciones de los Países Bajos y Corea del Sur[155], incluso en el sector manufacturero (un objetivo frecuente de este agente de la amenaza). En contraste con Green Havildar, Gorgon Group es relativamente indiscriminado en sus objetivos, y no hemos observado que despliegue ninguna capacidad personalizada.

(No) todo está tranquilo en el frente Scarlet: La actividad de los agentes de amenazas con base en Vietnam

Tras la atribución pública por parte de Facebook en diciembre de 2020 de Scarlet Ioke (alias Ocean Lotus, APT32) a CyberOne Group, una empresa de TI con sede en Vietnam, observamos una drástica reducción del ritmo operativo del agente de la amenaza, al menos en lo que respecta a las campañas conocidas y en curso. Por otra parte, las empresas chinas de ciberseguridad siguieron observando a Scarlet Ioke dirigiéndose a China durante el año pasado, lo que es coherente con el enfoque de los blancos de los agentes de la amenaza desde hace mucho tiempo. Por ejemplo, Sangfor [156] informó en marzo sobre la actividad de Scarlet Ioke utilizando un cargador comúnmente conocido como "DgBase.dll". El backdoor RotaJakiro de Linux[157], que también cuenta con funcionalidad de botnet, también se atribuyó en código abierto a Scarlet Ioke, basándose en las estrechas superposiciones de código entre RotaJakiro y el backdoor OceanLotus.

Entre finales de 2020 y septiembre de 2021, observamos una campaña[158] que incluía cargadores DLL para Cobalt Strike y MetaSploit que utilizaban varias capas de codificación Shikata Ga Nai para evitar la detección. En algunos casos, las cargas útiles de Cobalt Strike utilizaban el servicio web Glitch para llevar a cabo actividades de C2.

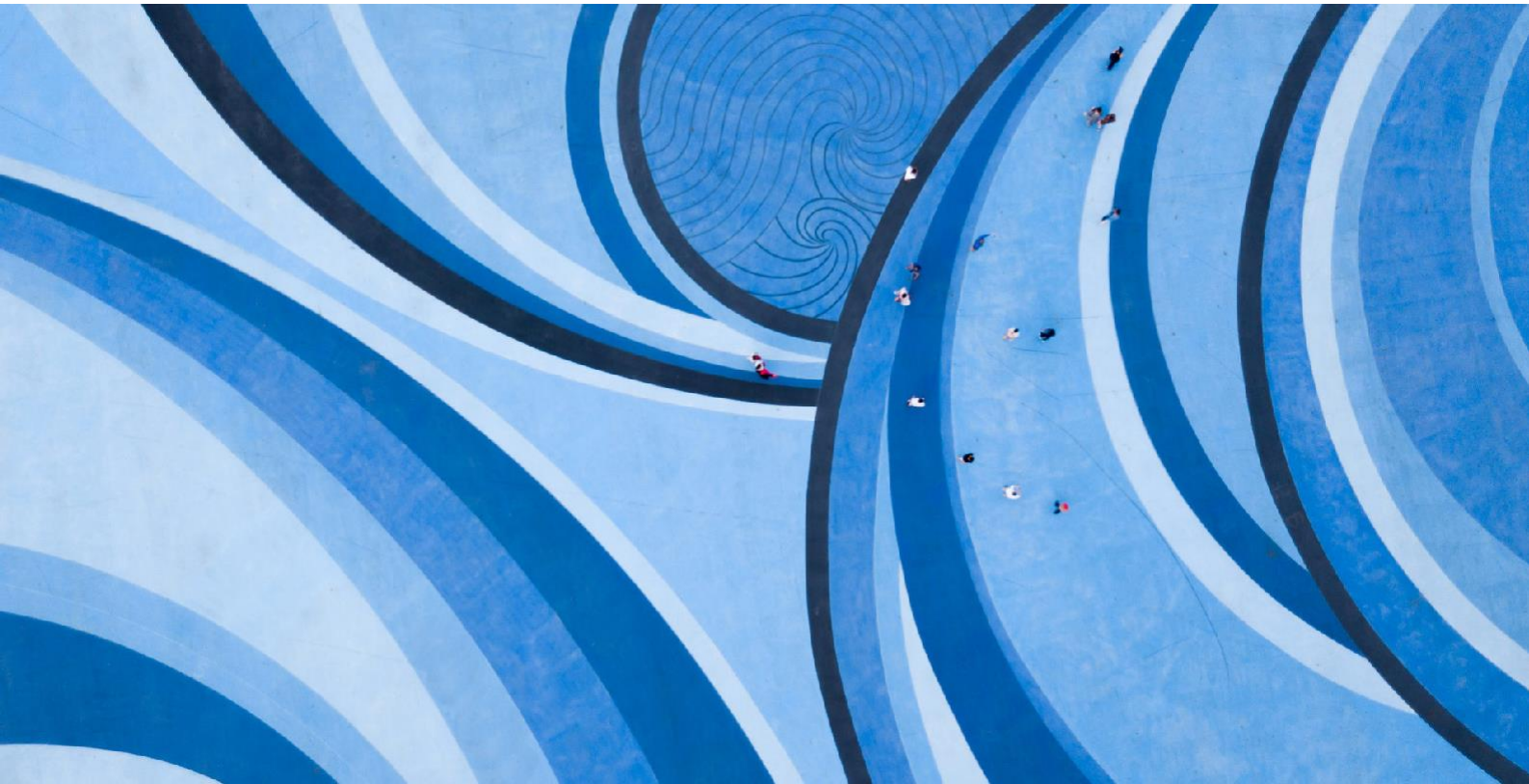
Figura 23: Una presunta cadena de ataque Scarlet Ioke cargando CobaltStrike Beacon en la memoria



En al menos un caso, la DLL fue cargada lateralmente por un binario legítimo de Kingsoft, un software utilizado predominantemente en los países de habla chino mandarín. Además, muchas de las muestras de Cobalt Strike que identificamos se hacían pasar por el servicio QQ de Tencent o por el motor de búsqueda chino Sogou, una táctica habitual de Scarlet Ioke. Estas pruebas sugieren con una probabilidad realista que los binarios estaban destinados a víctimas de habla china. Basándonos en las TTPs y en la selección de objetivos que observamos en esta campaña, consideramos que es una probabilidad realista que haya sido llevada a cabo por Scarlet Ioke. Los factores que contradicen esta evaluación incluyen la falta de vínculos directos con actividades anteriores de Scarlet Ioke, así como el uso de herramientas típicas de pruebas de penetración que también podrían formar parte de un ejercicio de equipo rojo nacional.

En última instancia, los agentes de las amenazas responden de forma diferente a la divulgación y la atribución. Algunos, como Red Kelpie y Yellow Garuda, podrían continuar sus operaciones sin alterar sus TTP, mientras que otros podrían cambiar sus herramientas y técnicas o incluso sufrir una reestructuración radical. Basándonos en las observaciones consideramos poco probable que Scarlet Ioke haya cesado sus operaciones. Por el contrario, consideramos que es probable que el agente de la amenaza se esté reequipando y reorganizando, con planes para aumentar la actividad en nuevas campañas.

“Los agentes de las amenazas responden de forma diferente a la revelación pública de su actividad. Algunos, como Red Kelpie y Yellow Garuda, continúan sus operaciones sin apenas cambios en sus TTPs, mientras que otros (posiblemente incluyendo a Scarlet Ioke) pueden cambiar sus herramientas y técnicas, o incluso sufrir una reestructuración radical."



Oriente Medio

Actividad de amenazas basadas en Irán

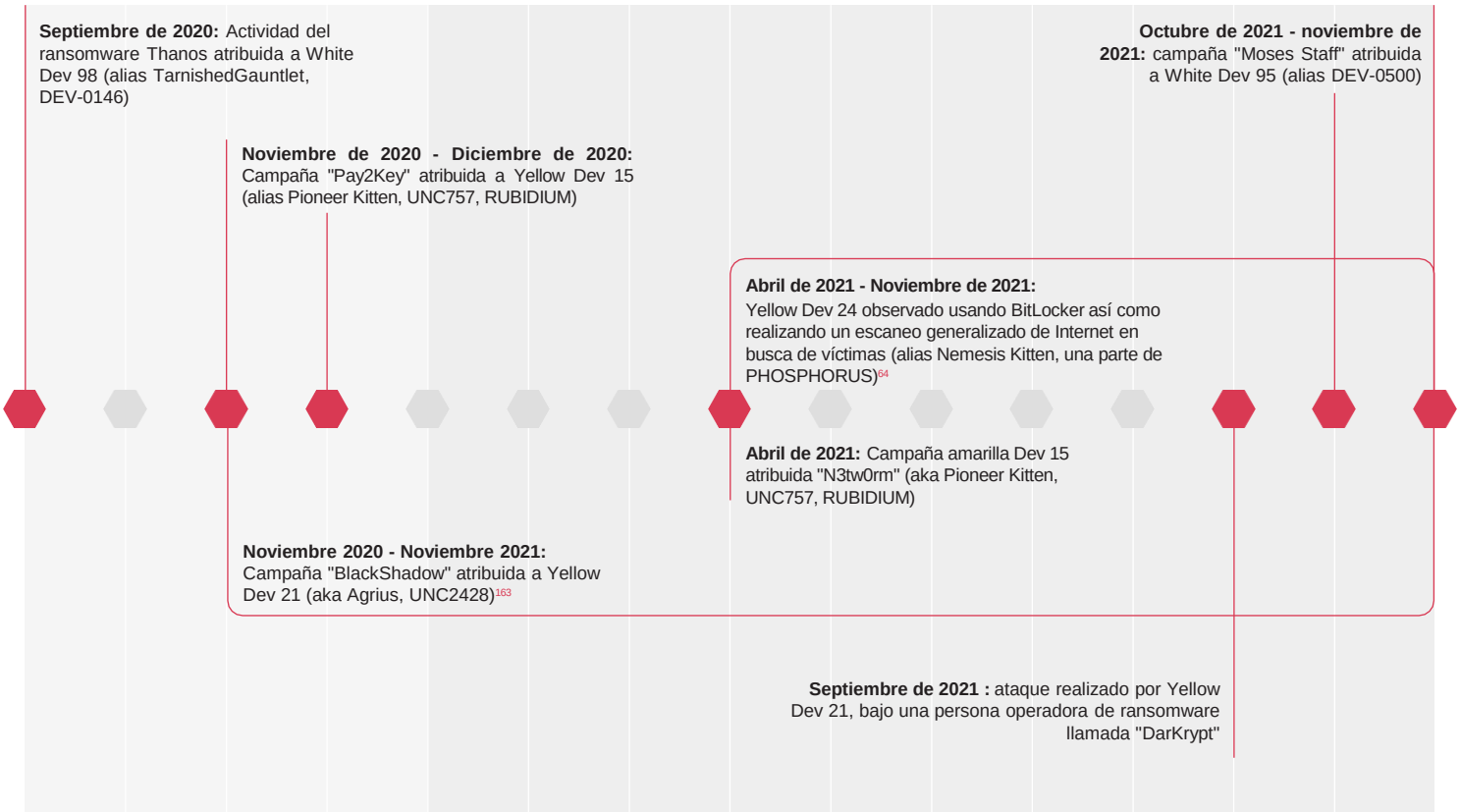
La cara cambiante de las operaciones de sabotaje

Los agentes de las amenazas con base en Irán tienen un largo historial de ataques de sabotaje destinados a destruir y perturbar a las organizaciones víctimas. Estos ataques ponen a los agentes de la amenaza en el punto de mira, lo que suele llevar a la atribución y al escrutinio de sus operaciones por parte de los sectores público y privado. En un intento de mitigar la atención no deseada, los agentes de la amenaza con base en Irán suelen culpar o hacerse pasar por colectivos de hacktivistas, una táctica que siguen adoptando los presuntos agentes de la amenaza con base en Irán, como White Dev 95 (alias Moses Staff).[159]

En un primer momento, a finales de 2020 y en 2021, observamos un tema de agentes de amenazas con base en Irán que amplían las tácticas de falsa motivación, incluyendo la actividad de Yellow Dev 15, Pay2Key y N3tw0rm, aprovechando el ransomware para el sabotaje en lugar de la ganancia financiera.[160] Cuando se utiliza junto con comportamientos hacktivistas, esto puede funcionar para sembrar la confusión sobre la verdadera naturaleza e intenciones de un agente de amenazas.

Agentes de amenazas con base en Irán, como Yellow Dev 15 y Yellow Dev 21, también se han hecho pasar por ciberdelincuentes en lugar de por hacktivistas en sus campañas de sabotaje, en las que también pretendían extorsionar a sus víctimas.[161] En una ocasión, Yellow Dev 21 amenazó con vender los datos de una víctima a terceros si no se realizaba un pago.[162]

PwC observó que los siguientes presuntos agentes de amenazas con base en Irán, con diferentes niveles de confianza, aprovechan el ransomware en sus campañas:



Caso de Estudio: N3tw0rm

A finales de abril de 2021, surgió una variante de ransomware llamada N3tw0rm dirigida a víctimas israelíes de los sectores del comercio minorista, la logística, las ONG y la construcción. El análisis técnico descubrió posteriormente similitudes entre N3tw0rm y otra variante de ransomware llamada Pay2Key, controlada por Yellow Dev 15, debido a su falta de seguimiento a la hora de proporcionar las claves de descifrado (en diciembre de 2021, el monedero de bitcoins que aparece en la nota de rescate de N3tw0rm seguía vacío, lo que significa que ninguna víctima pagó el rescate). Las motivaciones detrás de los ataques parecen alinearse con el sabotaje más que con lo financiero.[166] En diciembre de 2021, el monedero de bitcoin que aparece en la nota de rescate de N3tw0rm seguía vacío, lo que significa que ninguna víctima pagó el rescate.

Caso de Estudio: Moses Staff

A partir de septiembre de 2021, un agente de amenazas que se autodenomina "Moses Staff" inició una destructiva campaña de "bloqueo y filtración" contra organizaciones israelíes. Hemos rastreado al agente de la amenaza que está detrás de esta campaña como White Dev 95. La mayoría de las víctimas de la campaña observadas a finales de 2021 eran organizaciones israelíes cuyas huellas empresariales no se alinean con la declaración de la misión del agente de la amenaza, que expone varios delitos supuestamente cometidos por el Gobierno israelí. También abarcan una amplia gama de sectores: legal, logística, comercio minorista, servicios públicos, servicios profesionales, transporte, construcción, fabricación y servicios financieros. Esta victimología sugiere que los objetivos fueron probablemente elegidos de forma un tanto oportunista, centrándose únicamente en Israel como objetivo más que en exponer cualquier presunta acción indebida.

White Dev 95 también mostró múltiples similitudes con una serie de campañas centradas en Israel atribuidas a agentes de la amenaza con base en Irán que han tenido lugar a lo largo de 2021, y que buscaban específicamente la atención del público en un intento de dar impulso a sus actividades. A tal efecto, White Dev 95 opera múltiples plataformas plataformas digitales para filtrar datos de las víctimas, así como para relacionarse directamente con ellas a través de Twitter. Una de las principales diferencias entre la campaña "Moses Staff" y otras operaciones similares de agentes de amenazas con base en Irán, es que White Dev 95 se salta la fase de extorsión de sus ataques y prefiere filtrar los datos robados sin previo aviso. Esto probablemente contribuye a la confusión causada a las víctimas, maximizando el elemento destructivo de la campaña.

No se puede enseñar a un viejo agente de amenazas nuevas TTPs

La mayoría de los agentes de amenazas, con base en Irán, a los que seguimos la pista aparecieron con nuevos tipos de herramientas el año pasado, aunque también siguieron recurriendo a técnicas probadas. Los agentes de amenazas con base en Irán suelen ser conocidos por su uso de herramientas de código abierto, especialmente de seguridad ofensiva, así como por sus campañas de ingeniería social..

Herramientas Open source

Yellow Nix (también conocido como Static Kitten, MERCURY, MuddyWater) utilizó sistemáticamente herramientas comerciales de administración remota a lo largo de 2021, como ConnectWise Control (también conocido como ScreenConnect) y Remote Utilities, para obtener el acceso inicial a las víctimas.[167] También vimos que Yellow Nix utilizando intermitentemente documentos de Microsoft Office con macros, incluso utilizándolos como mecanismo de entrega para ConnectWise Control.[168]

tanto Yellow Dev 24[169] y Yellow Dev 15[170] han utilizado la herramienta de código abierto FRP, que permite que un sistema proporcione acceso a la red a los sistemas controlados por el agente de la amenaza situados fuera de la red de la víctima. Del mismo modo, Yellow Orc (alias APT 33, Refined Kitten, Stonedrill) es bien conocido por su uso de PoshC2, un marco C2 de código abierto utilizado para la explotación posterior y el movimiento lateral. En 2021, observamos nueva actividad de Yellow Orc, que incorporó un marco C2 similar disponible públicamente.[171]

Ingeniería social

Un denominador común entre muchos agentes de amenazas con base en Irán, es el uso de señuelos de phishing con temática de empleo o de contratación, al tiempo que recurren a las plataformas de las redes sociales para comunicarse directamente con los objetivos. para comunicarse directamente y generar confianza con los objetivos. En varios casos marginales, las técnicas de phishing e ingeniería social eludieron la autenticación multifactor (MFA); sin embargo, según nuestras observaciones, la MFA sigue siendo muy eficaz para frustrar la mayoría de los ataques.[172]

Yellow Maero (alias APT34, OilRig, COBALT GYPSY) tiene un largo historial de ingeniería social; en enero de 2021, observamos que utilizaba un folleto de contratación con la marca de un legítimo proveedor de servicios de TI con sede en Estados Unidos y que anunciaba una serie de diferentes puestos de TI, empresariales y de ingeniería disponibles en Oriente Medio.[173] Es probable que el documento de señuelo sea legítimo, aunque el agente de amenaza lo haya reutilizado maliciosamente.

En julio, el agente de amenazas que rastreamos como Yellow Orc (alias APT33, Elfin) llevó a cabo una campaña que incluía ofertas de empleo y un sitio web falso de búsqueda de empleo para puestos de trabajo principalmente en Oriente Medio, centrándose en los siguientes sectores: Petróleo y Gas, Química, Energía, Ciencias de la Vida, Manufactura, Minería, Infraestructura y Gobierno.[174] El contenido de los directorios abiertos también muestra que el agente de amenaza probablemente comenzó el año centrándose en los Estados Unidos a través de archivos HTA maliciosos, y al mismo tiempo llevó a cabo una operación aprovechando una pieza de malware que que se hizo pasar por un rastreador COVID-19 de la Organización Mundial de la Salud (OMS). [175] El directorio abierto evidenció que es probable que Yellow Orc también utilizara imágenes de un individuo femenino para hacer ingeniería social con sus objetivos.[176] Las imágenes se parecen a los informes de código abierto sobre el personaje "Marcella Flores" operado por el agente de amenazas que rastreamos como Yellow Liderc.177 Yellow Orc ha estado utilizando tácticas de ingeniería social con temática laboral desde al menos 2017.

Yellow Liderc (o Tortoiseshell, TA456)[178] y un agente de amenazas estrechamente relacionado que registramos como Yellow Dev 13 continuó a lo largo de 2021 utilizando LinkedIn y Facebook para la ingeniería social, manteniendo una red de empresas y personas de contratación falsas.[179, 180] Tanto Microsoft como Meta documentaron el proceso persistente y a la vez paciente de Yellow Liderc en el uso de las redes sociales, que a menudo abarca varios meses entre la conexión inicial con el objetivo y la entrega del contenido malicioso.[181, 182]

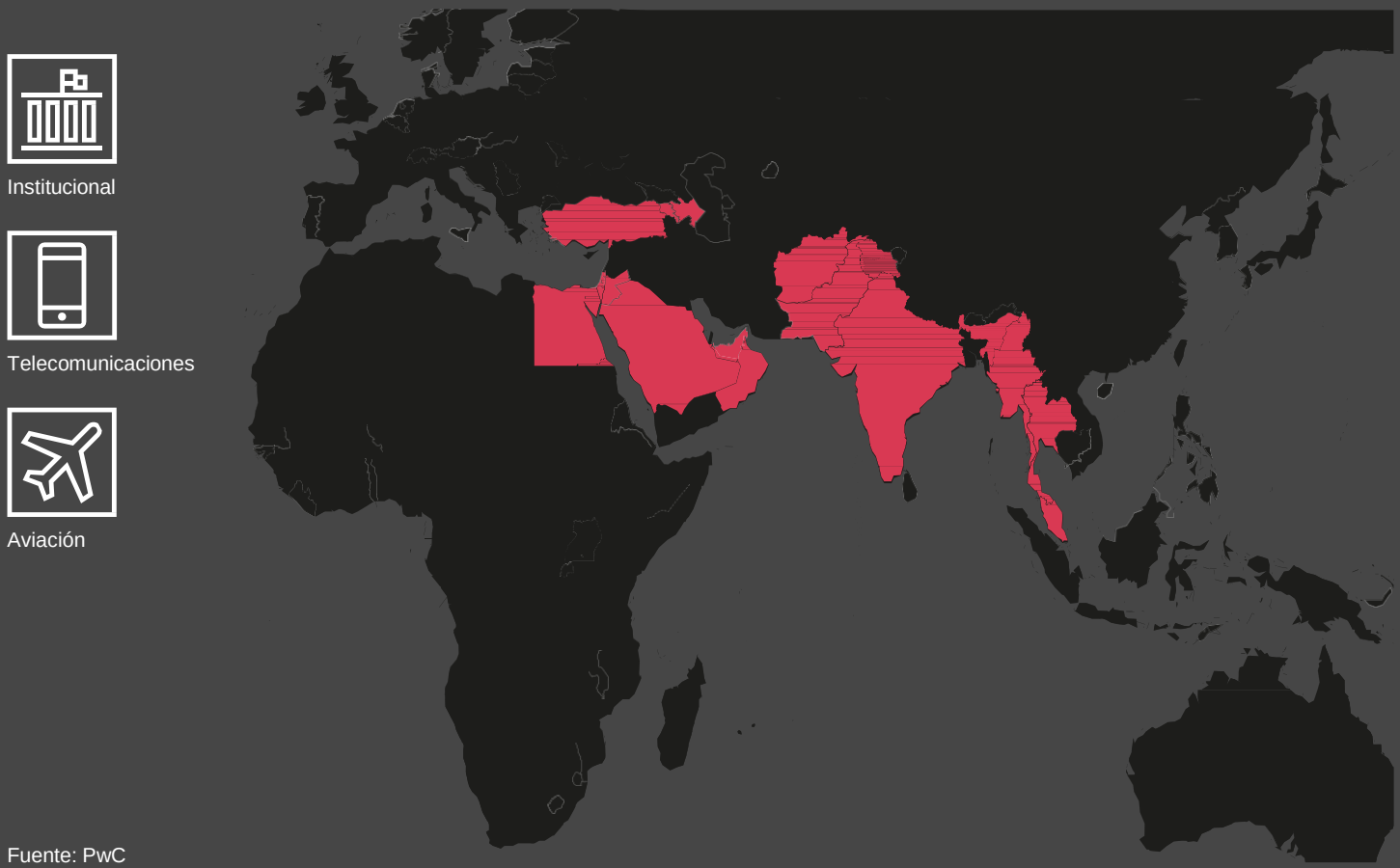
Ampliando horizontes

Yellow Nix

Yellow Nix siguió ampliando sus horizontes más allá de las regiones geográficas vecinas a Irán. Tras un año muy activo en 2020, en el que atacó a Europa en múltiples campañas, en septiembre de 2021 vimos cómo el agente de la amenaza se desplazaba hacia el sudeste asiático. Sus ataques a los sectores gubernamental, de la aviación y de las telecomunicaciones en Malasia, en particular, se produjeron tras las conversaciones de cooperación económica mantenidas entre funcionarios iraníes y malasios.[183] Este es el caso típico de Yellow Nix, cuya actividad suele reflejar estrechamente las inversiones políticas y comerciales de Irán. Yellow Nix también pareció dirigir un mayor nivel de interés hacia el sector de la aviación.

En septiembre de 2020, Estados Unidos sancionó a individuos asociados con Yellow Mimas, un agente de amenazas notorio por dirigirse a los sectores mundiales de la aviación y las telecomunicaciones con el fin de vigilar los movimientos de los viajeros. Desde entonces, los analistas de PwC no han observado la actividad de Yellow Mimas, y el agente de la amenaza también ha estado notablemente ausente en los informes de amenazas de fuente abierta. No está claro si Yellow Mimas ha entrado en un periodo de inactividad, pero el repunte de Yellow Nix en su objetivo de organizaciones de aviación demuestra que su
El aumento de Yellow Nix de atacar organizaciones de aviación demuestra que el requisito de su patrocinador de obtener inteligencia de este sector probablemente se está cumpliendo, aunque no está claro hasta qué punto Yellow Nix lo consigue. La reciente victimología de Yellow Nix también refleja la de Yellow Mimas, e indica que Yellow Nix puede estar llevando a cabo la vigilancia de individuos de interése engaged in conducting surveillance on individuals of interest.[184]

Figura 24: Geografías y sectores objetivo de Yellow Nix



Fuente: PwC

Yellow Dev 9

Informado por primera vez por fuentes abiertas en 2019, Yellow Dev 9 (alias Lyceum, Siamese Kitten), motivado por el espionaje, comparte similitudes en su victimología, infraestructura y herramientas con otro agente de amenazas basado en Irán que rastreamos como Yellow Maero.

Yellow Dev 9 continuó activo en 2021 apuntando a los sectores de telecomunicaciones y aviación africanos, haciendo ingeniería social en LinkedIn, y alojando su malware temático de reclutamiento en dominios que se hacen pasar por empresas de tecnología de la información.[185] A pesar de que varios investigadores de seguridad publicaron informes sobre Yellow Dev 9, el agente de la amenaza siguió desarrollando nuevas variantes de malware, denominadas puertas traseras "Milan" y "Shark", que utilizan la conectividad de red HTTP y DNS. La infraestructura de Yellow Dev 9 tiene un patrón específico, ya que el agente de la amenaza registró constantemente dominios de comando y control (C2) con nombres con temática de DNS, "actualización" y CDN durante 2021.[186] Se sabe que Yellow Dev 9 reutiliza su infraestructura histórica de sus campañas anteriores.[187]

Yellow Garuda

Uno de los agentes de amenazas más activos y de los que más se informó el año pasado fue Yellow Garuda (alias Charming Kitten, FÓSFORO, ITG18). Este agente de la amenaza es muy capaz y persistente, y aumentó su ritmo de operaciones en 2021 mientras mantenía una red de infraestructura de phishing en expansión.

Las campañas de Yellow Garuda van desde el simple phishing de credenciales[188] hasta el compromiso de sitios web legítimos[189] , pasando por el despliegue de malware para móviles[190] , el uso de bots de Telegram para tomar las huellas de los dispositivos de las víctimas[191] y la duplicación de los esfuerzos de ingeniería social.

Estas operaciones se traducen en una amplia selección de víctimas en todo el mundo y en múltiples sectores. La victimología a lo largo de 2021 incluyó conjuntos de objetivos internos dentro de Irán, así como países vecinos de Oriente Medio, y objetivos típicos tanto en Estados Unidos como en Europa.

Dispositivo amarillo 19

Un agente de la amenaza con base en Irán, al que PwC rastrea como Yellow Dev 19, fue observado atacando sitios web relacionados con las elecciones presidenciales de 2020 en Estados Unidos, en lo que el gobierno estadounidense evalúa como un intento de influir e interferir en las elecciones.[192] En mayo de 2021 evaluamos que Yellow Dev 19 probablemente estaba estrechamente asociado con el sector educativo iraní, específicamente en la forma de un estudiante o miembro de la facultad, lo que una acusación estadounidense de noviembre de 2021 apoya con el nombramiento de dos individuos de entre 23 y 26 años[193]. También identificamos que Yellow Dev 19 probablemente está interesado en dirigirse a entidades gubernamentales de Arabia Saudí.[194]

Según la acusación del gobierno estadounidense, la presunta empresa responsable de dirigir el intento de campaña es Emennet Pasargad, una empresa que actúa en apoyo del gobierno iraní[195]. Los analistas de PwC también han observado solapamientos entre esta empresa, junto con los miembros de su consejo de administración sancionados, y Yellow Liderc.[196] PwC evalúa que Emennet Pasargad y/o su personal están probablemente implicados en otras operaciones, como el ransomware con fines de sabotaje, y están estrechamente alineados con el Cuerpo de la Guardia Revolucionaria Islámica.

Yellow Dev 24

Desde al menos abril hasta noviembre de 2021, PwC observó que Yellow Dev 24 (también conocido como Nemesis Kitten, una parte de PHOSPHORUS) escaneó en masa los dispositivos orientados a Internet, incluidos los dispositivos de Fortinet y los servidores de Microsoft Exchange.[197] En algunos casos, Yellow Dev 24 desplegó posteriormente el ransomware a través de BitLocker, al tiempo que se basaba en herramientas de código abierto y en técnicas para vivir fuera del país. Yellow Dev 24 es uno de los varios agentes de amenazas con base en Irán que están adoptando el ransomware con fines de sabotaje, al tiempo que son capaces de llevar a cabo actividades de espionaje. Yellow Dev 24 también es oportunista en su selección de objetivos, lo que hace que este agente de amenazas sea relevante para una audiencia global.[198]

Las víctimas de esta campaña eran geográficamente diversas, e incluían organizaciones de Estados Unidos, Australia, los Emiratos Árabes Unidos y Sudáfrica,[199] ya que, según se informa, el agente de la amenaza comprometió casi 1.000 dispositivos en poco más de seis meses.[200] Se produjo una actividad ligeramente más selectiva (aunque todavía oportunista) a través de la pulverización de contraseñas en empresas de tecnología de defensa estadounidenses e israelíes, puertos de entrada del Golfo Pérsico y empresas de transporte marítimo mundial con presencia comercial en Oriente Medio.[201]

La actividad de las amenazas en Oriente Medio

Teal Dev 2
El agente de la amenaza Teal Dev 2 (alias StrongPity), con sede en Turquía, siguió desplegando su conocido backdoor StrongPity a lo largo de 2021, aunque, según nuestras observaciones, esta actividad se ralentizó en la segunda mitad del año. Salieron a la luz nuevas TTP de Teal Dev 2, con informes de código abierto que mostraban vínculos de infraestructura entre StrongPity y el malware para Android, que no se conocía previamente como parte del conjunto de herramientas del agente de la amenaza, pero que probablemente se ha utilizado desde al menos 2019.[202] Basándonos en estas observaciones, evaluamos que el aparente uso moderado de herramientas y técnicas específicas por parte de Teal Dev 2 probablemente les ha permitido pasar desapercibidos durante varios años, y es probablemente indicativo de campañas muy específicas.

Karkadann el Gris
Grey Karkadann (también conocido como Arid Viper, APT-C-23, y parte de la Gaza Cybergang) ha seguido utilizando técnicas probadas para atacar a entidades de la región de Oriente Medio, con un fuerte enfoque en la política palestina y las relaciones entre Palestina e Israel. A lo largo de 2021, esto incluyó el uso continuado de su malware para Windows Micropsia[203], que suele ir acompañado de documentos señuelo que coinciden con sus principales temas de ataque. También hemos observado que el desarrollo de su malware para móviles, que se distribuye a través de tiendas de aplicaciones de terceros o sitios controlados por el agente de la amenaza. Los informes de fuente abierta señalan que el arsenal de Grey Karkadann incluye ahora malware para iOS, además de sus conocidos implantes para Android.[204] El malware para móviles del agente de la amenaza contiene una amplia funcionalidad de vigilancia y ocultación, que a menudo se hace pasar por aplicaciones legítimas.[205]

White Dev 21
En mayo de 2021, observamos un grupo de actividad centrada en hablantes de árabe con interés en los asuntos de Oriente Medio.[206] La actividad se remontaba al menos a 2019, e implicaba el uso de documentos habilitados para macros con contenido que cubría una amplia gama de noticias y temas relacionados con Palestina, Líbano e Irak. Esto indica que el agente de la amenaza probablemente ha apuntado a múltiples víctimas separadas durante esta campaña. Los informes de fuente abierta han vinculado esta actividad a un agente de la amenaza conocido como WIRTE, y han destacado la focalización en una serie de organizaciones de alto perfil en sectores que incluyen entidades gubernamentales y diplomáticas, bufetes de abogados e instituciones financieras, lo que hace que el agente de la amenaza sea preocupante para una amplia variedad de sectores.[207] A partir de nuestras observaciones, WIRTE comparte solapamientos históricos de infraestructura con White Dev 21, un agente de la amenaza que observamos en 2019 utilizando señuelos de temática electoral y de relaciones diplomáticas relacionados con la política egipcia y palestina, y que evaluamos que probablemente sea una rama del Cybergang de Gaza.[208, 209]

Europe and former Soviet Union

Los actores de las amenazas con base en Rusia continuaron sus operaciones cibernéticas en 2021, buscando acceder a información confidencial o sensible. Esto ha incluido el ataque a ministerios gubernamentales en toda Europa, y al extranjero cercano de Rusia. Vimos que el agente de la amenaza Blue Athena (también conocido como Sofacy) se interesó especialmente por el sector de la minería y los recursos naturales en Asia Central.

También hemos seguido observando que el agente de amenazas Blue Otso, con sede en Rusia, ha atacado sistemáticamente a entidades de Ucrania.
Hemos seguido la actividad de Blue Otso dirigida a entidades del este de Ucrania, lo que ha llevado al Servicio de Seguridad de Ucrania (SBU) a desenmascarar a varios presuntos operadores de Blue Otso en noviembre de 2021.

Además, más allá de los agentes de amenazas basados en Rusia, nuestra investigación también incluyó el seguimiento de otras actividades maliciosas. White Tur es un ejemplo de agente de amenazas aún no atribuido cuyo interés se ha centrado en sectores y geografías muy específicos. Por otra parte, se ha observado a Rose Matsil, agente de amenazas con sede en Georgia, en relación con el ataque a organizaciones médicas en Rusia en 2021.

Blue Dev 5 - Un phisher 'noble'

La amenaza Blue Dev 5 demostró un cuidadoso manejo y técnicas novedosas, incluyendo el compromiso de los entornos de la nube de Microsoft y la explotación de las relaciones de confianza entre organizaciones.

Blue Dev 5 logró comprometer a varios revendedores de la nube y MSP, aprovechando las relaciones de confianza de estas organizaciones con sus clientes para comprometer los entornos de la nube de los clientes, y explotar el acceso proporcionado a los MSP con el fin de pivotar en las redes de sus clientes. Una vez que Blue Dev 5 obtiene el acceso a las organizaciones víctimas, pretende obtener un acceso persistente, sigiloso y a largo plazo a las instancias de Azure AD y Microsoft 365, incluyendo cuentas privilegiadas y datos sensibles. Blue Dev 5 ha demostrado altos niveles de seguridad operativa y ha tomado medidas para evadir las detecciones y dificultar que las organizaciones víctimas investigar las actividades sospechosas (por ejemplo, accediendo a las cuentas comprometidas de las organizaciones víctimas desde direcciones IP residenciales).
Actualmente no podemos vincular definitivamente a Blue Dev 5 con el agente de la amenaza que está detrás de los ataques a la cadena de suministro de SolarWinds que rastreamos como Blue Nova[211, 212]. Sin embargo, hemos observado un importante solapamiento de técnicas entre ambos, incluidas las utilizadas para realizar sofisticados ataques basados en la identidad contra entornos de nube de Microsoft. También observamos que tanto Blue Dev 5 como Blue Nova[213] aprovechan las relaciones de confianza de terceros para acceder a los entornos informáticos de las organizaciones.

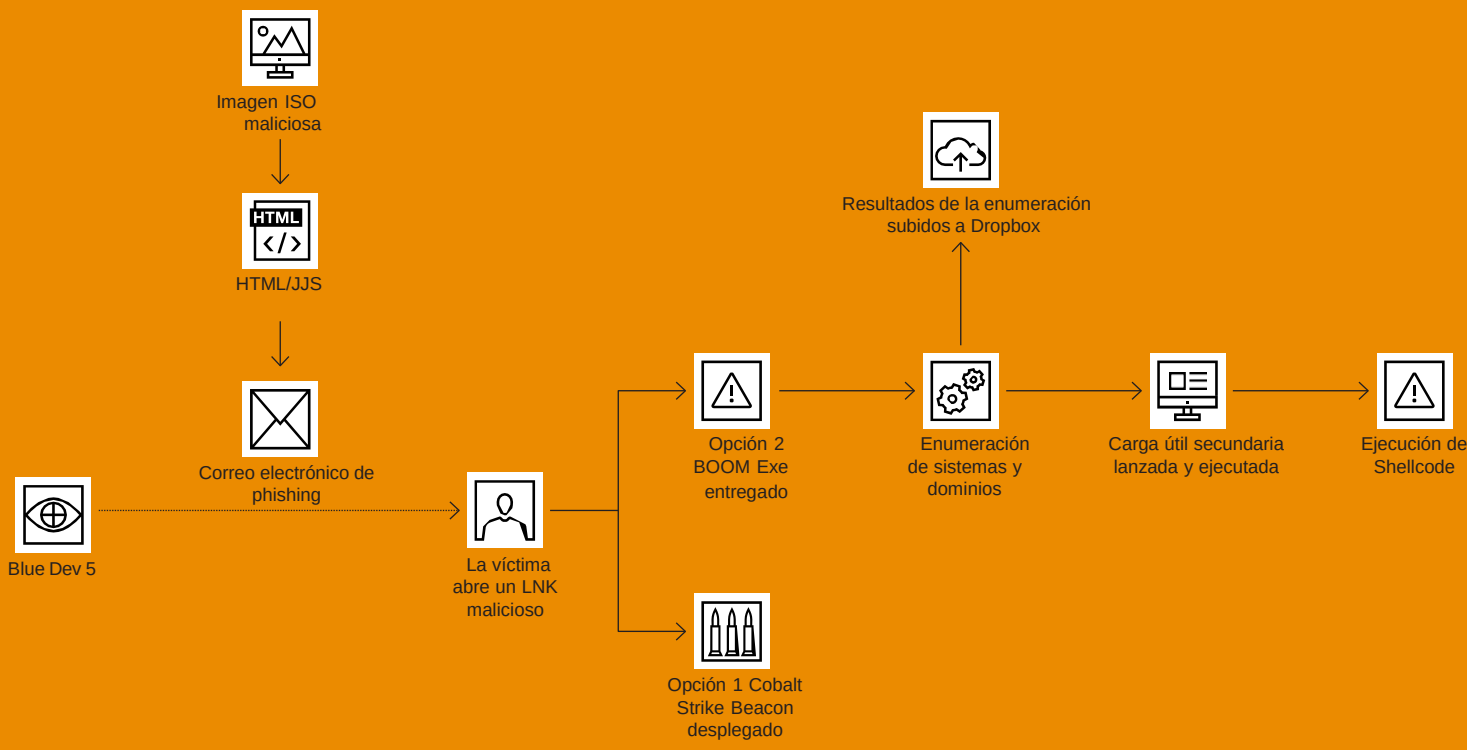
Las organizaciones preocupadas por la amenaza de Blue Dev 5 deberían tomar medidas para:

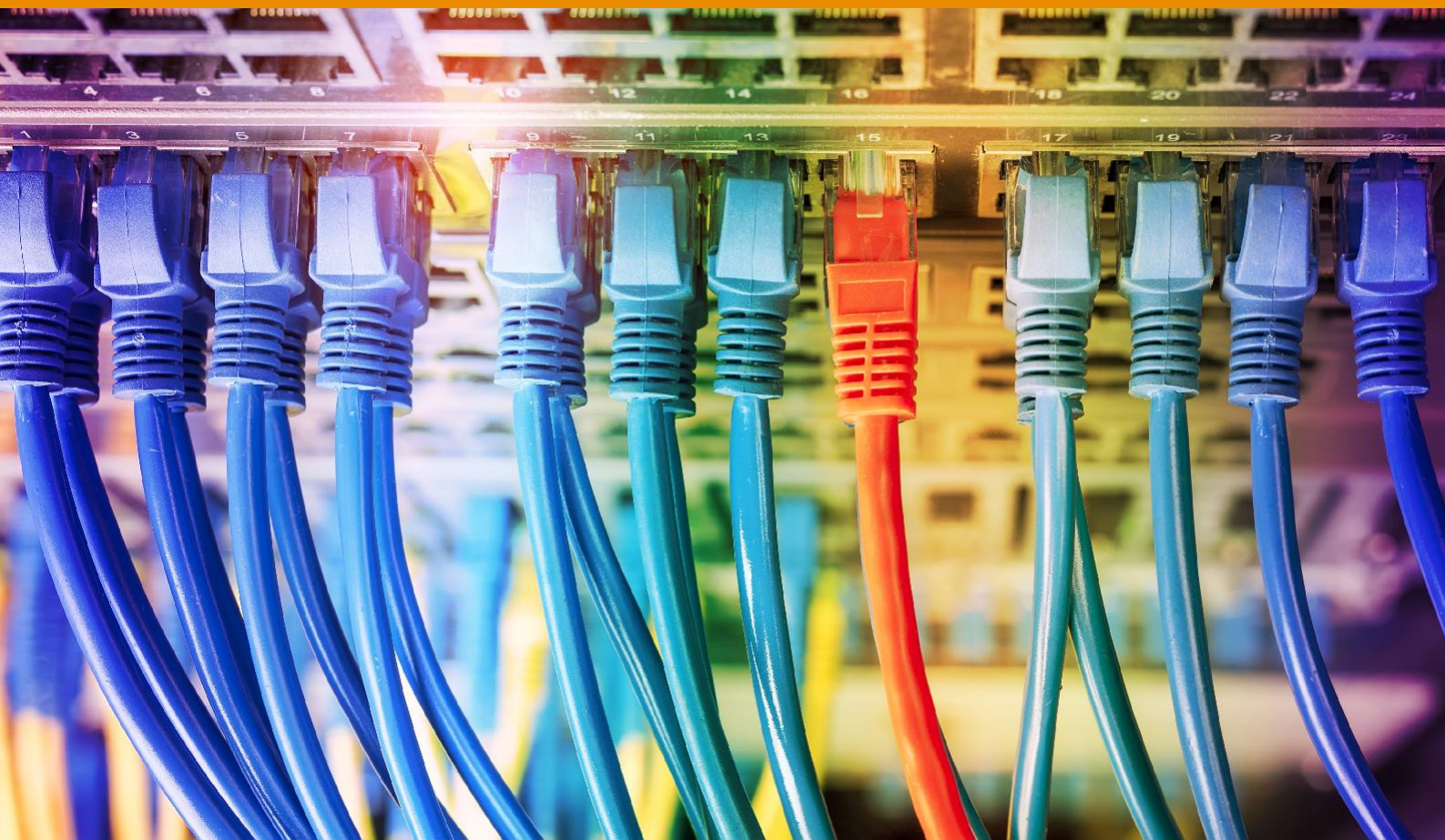
- Implementar una sólida estrategia de acceso privilegiado que incluya el uso de prácticas de administración seguras y restricciones estrictas en torno al uso del acceso privilegiado;
- Supervisar los registros de Azure AD y Microsoft 365 en busca de técnicas utilizadas para comprometer y abusar de las cuentas privilegiadas, técnicas de persistencia y eventos globales poco frecuentes; y,
- Auditar regularmente las configuraciones de la nube (Azure AD, Microsoft 365 y Azure) y las relaciones de confianza.

También se ha observado que Blue Dev 5 utiliza otras técnicas bien conocidas para acceder a los entornos de las organizaciones, como la pulverización de contraseñas y el uso de credenciales comprometidas.

Blue Dev 5 llamó la atención en mayo de 2021, cuando realizó una campaña de phishing haciéndose pasar por USAID (La Agencia de los Estados Unidos para el Desarrollo Internacional) para distribuir el malware Cobalt Strike Beacon empaquetado con un cargador personalizado. En este caso, obtuvimos la siguiente visión de esta actividad:

Figura 25: Una cadena de intrusión de Blue Dev 5 que implica la exfiltración de Dropbox



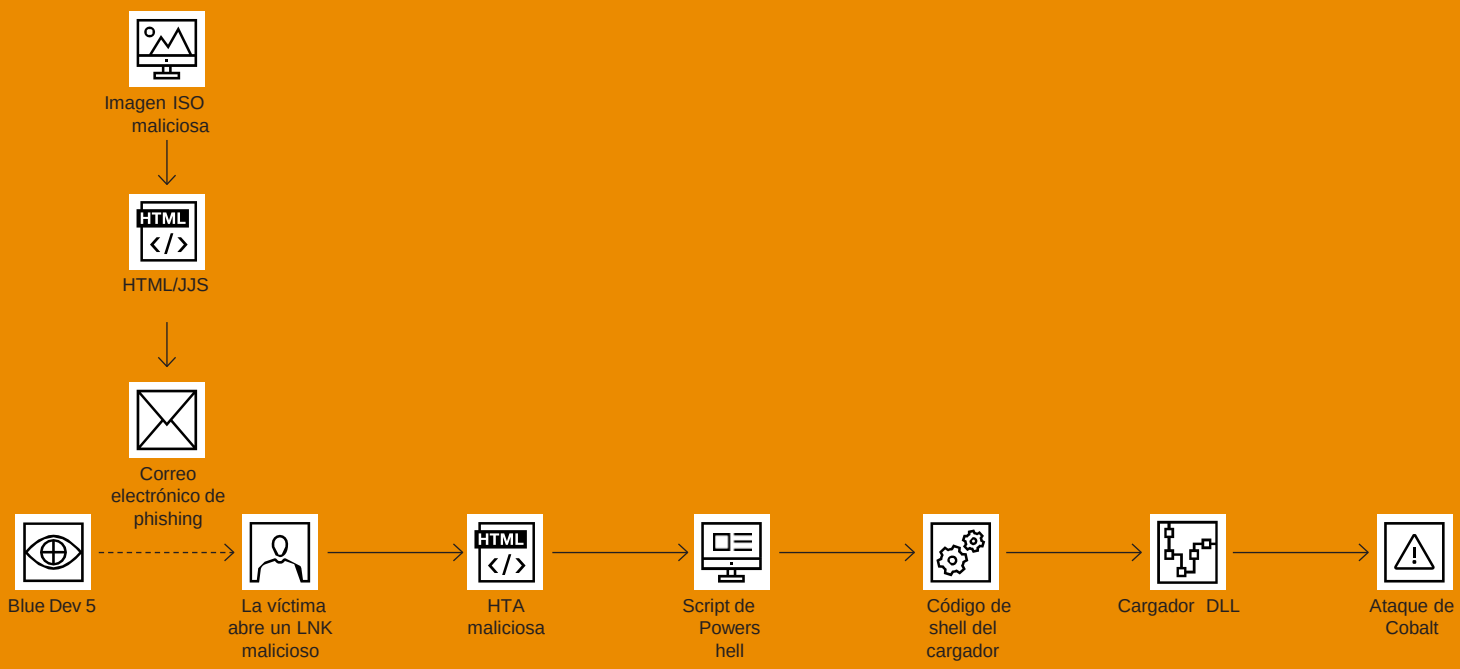


Hay pruebas de que los archivos adjuntos HTML de la primera fase fueron abiertos por personas que trabajaban en varias embajadas de Europa,[214] lo que permite comprender la amplitud de la selección de objetivos realizada por este agente de amenazas. Algunas cargas útiles utilizadas por Blue Dev 5 parecen haber sido más selectivas: una vista en marzo de 2021[215] buscaba variables de entorno relacionadas con el Ministerio de Asuntos Exteriores de un país de Europa del Este; otra suplantaba una actualización de un sistema de gestión de documentos del gobierno ucraniano.[216]

Al rastrear la infraestructura de Blue Dev 5 a lo largo del tiempo, también observamos que sus TTPs se vuelven más complejas. Por ejemplo, en un señuelo HTML que probablemente fue creado en noviembre de 2021, el agente de la amenaza había añadido varias etapas más entre el señuelo HTML inicial y la carga útil de Cobalt Strike Beacon entregada finalmente a los objetivos. En este caso, así como en otro que identificamos, el documento del señuelo pretendía notificar a la víctima que una embajada estaba cerrada debido a COVID-19.

Consideramos que es muy probable que Blue Dev 5 continúe activo durante el próximo año, y que sus TTPs continuarán evolucionando con el tiempo para evadir mejor la detección.

Figura 26: Una variante de una cadena de intrusión de acceso inicial de Blue Dev 5



El foco de atención en los Balcanes: White Tur

En enero de 2021, PwC observó un dominio de phishing dirigido al ejército serbio. [217] Poco después, identificamos una infraestructura adicional relacionada que mostraba un ataque a organizaciones gubernamentales y de defensa serbias y de la República Srpska en curso desde al menos 2017, que estamos rastreando en asociación con un agente de amenazas que llamamos White Tur. La República Srpska es una de las dos entidades federales de Bosnia-Herzegovina. Esta actividad ha tenido lugar en un contexto estratégico complejo, ya que la región de los Balcanes en su conjunto tiene una historia diversa, aunque díscola. Los objetivos de Serbia y de la República Srpska son de especial interés, ya que en los últimos meses algunas partes interesadas han hecho un llamamiento cada vez más fuerte para que la República Srpska adquiera más autonomía, o incluso para que se produzca una secesión.[218]

La infraestructura adicional reveló una actividad previa que el Ministerio del Interior de la República Srpska reveló en abril de 2020[219]: una campaña de spear phishing haciéndose pasar por el primer ministro de la República Srpska, que llevó a un archivo HTA malicioso que ejecutaba código PowerShell desde un dominio C2 que identificamos como conectado al dominio de phishing militar serbio.

El seguimiento continuado de la infraestructura relacionada durante el año identificó como objetivo a organizaciones serbias de investigación y desarrollo estrechamente relacionadas con el ejército y la defensa.220 En septiembre de 2021, White Tur llevó a cabo un compromiso estratégico de la web.

En septiembre de 2021, White Tur llevó a cabo un compromiso estratégico de la web en un sitio web para alojar documentos y archivos armados con temas relacionados con la República Srpska y la defensa221 ; antes de esto, los archivos armados de White Tur se habían alojado en una infraestructura registrada por un agente de amenazas.

En términos de capacidades, observamos que White Tur utilizaba documentos armados con macros que conducían a una puerta trasera JScript.

Por otra parte, White Tur desplegó una puerta trasera de Windows, empaquetada en un archivo armado que contenía el proyecto de código abierto OpenHardwareMonitor, que utilizaba objetos de transferencia de bits COM para enviar información al C2.

En general, consideramos que White Tur es probablemente un agente de amenaza motivado por el espionaje, y que es probable que esté alineado con un estado nacional. Teniendo en cuenta las tensiones regionales, hay varios candidatos potenciales a participar en esta actividad, tanto en los Balcanes como en otros lugares. En la actualidad, no disponemos de suficientes pruebas técnicas para realizar una evaluación de alta confianza en cuanto a los posibles patrocinadores de White Tur. Sin embargo, consideramos que es probable que los Balcanes sigan siendo una región de interés para agentes de amenazas de diversos orígenes y motivaciones, entre ellos White Tur. **En nuestro blog** analizamos más a fondo a White Tur.

Cabeza en las nubes: Blue Odin

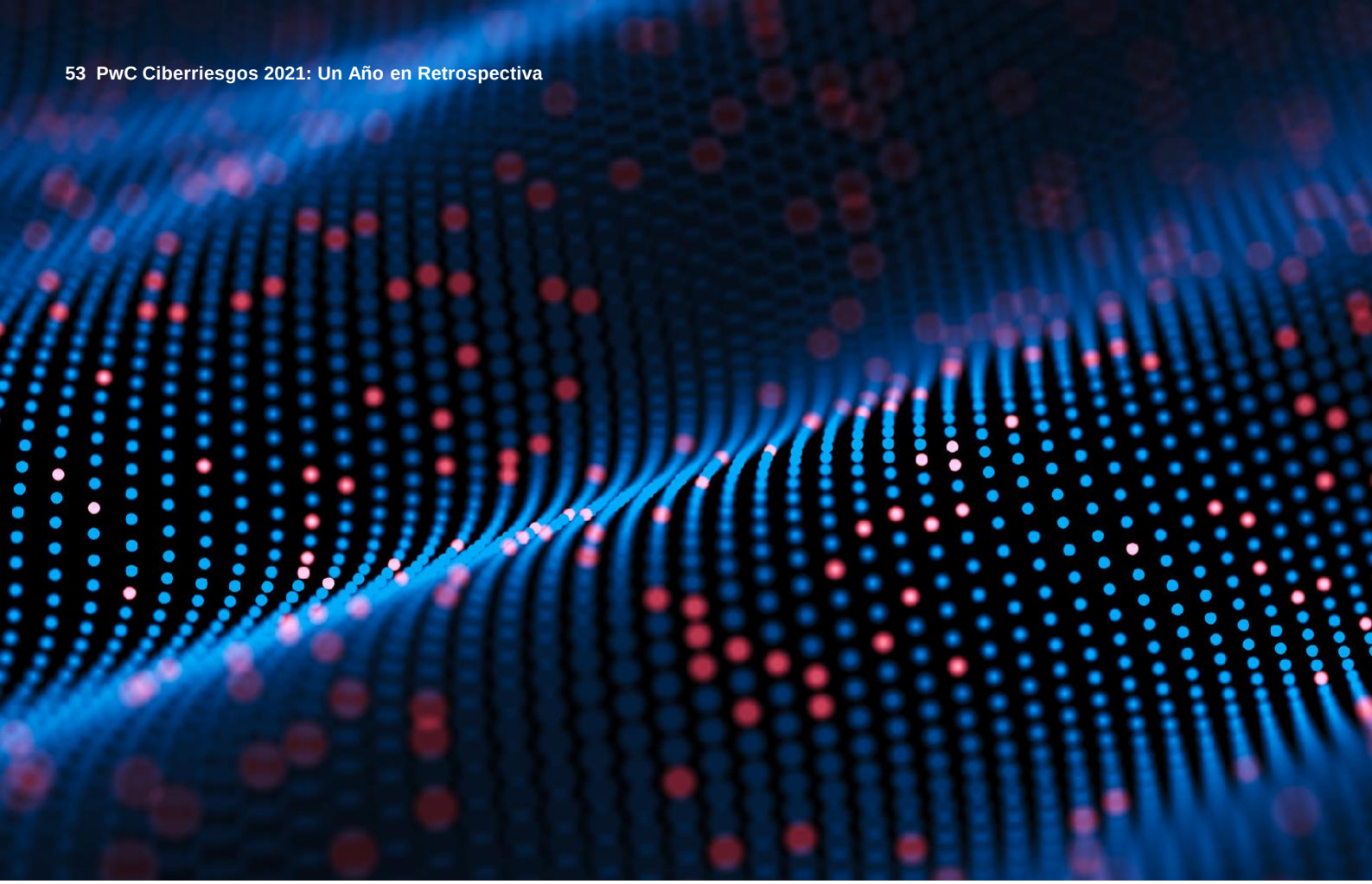
Blue Odin (también conocido como CloudAtlas) es un agente de amenazas conocido por dirigirse a diversas organizaciones de Rusia y de las regiones ucranianas anexas a Rusia utilizando documentos maliciosos, y por controlar estrechamente las cargas útiles que entregan estos documentos con el fin de aumentar la dificultad de los investigadores para rastrearlo.

En 2021, observamos varias facetas nuevas en la actividad de Blue Odin, desde errores de seguridad operativa (OPSEC) hasta nuevas TTP. En un caso, un documento malicioso utilizado para dirigirse al Ministerio de Defensa de un país de Europa Central contenía enlaces incrustados a un servicio de traducción en línea, que parecen haber sido utilizados para traducir la fuente del contenido del señuelo de su inglés original al ucraniano. Esto, a su vez, sugiere que el operador que preparó el documento podría hablar ucraniano como primera lengua.

Otra observación fue el uso de Responder por parte de Blue Odin a principios de 2021. Responder es una herramienta de código abierto utilizada para realizar ataques de autenticación forzada SMB. En este tipo de ataque, el sistema de la víctima intenta autenticarse en un servidor controlado por el agente de la amenaza utilizando NTLM, lo que permite al agente de la amenaza capturar hashes de desafío. Estos pueden ser forzados posteriormente fuera de línea para recuperar la contraseña de la víctima. El documento malicioso en cuestión se dirigía probablemente a personas relacionadas con asuntos exteriores y entidades diplomáticas, y contenía rutas UNC a imágenes en servidores controlados por el agente de la amenaza.

servidores que dieron lugar al ataque de autenticación forzada descrito anteriormente. Curiosamente, una de las direcciones IP incrustadas en el documento era probablemente un error tipográfico; la IP especificada no parecía albergar un servidor Responder, sino una dirección IP con un solo carácter de diferencia. Esto representa una desviación de las técnicas anteriores utilizadas en los documentos maliciosos del agente de la amenaza, que generalmente utilizaban enlaces de plantillas remotas. En otros aspectos, la actividad de Blue Odin sigue siendo muy similar a la observada anteriormente: por ejemplo, un documento malicioso observado en diciembre de 2021[222] que traía una plantilla remota que contenía un exploit Equation Editor, que descargaba y ejecutaba un HTA, y a su vez desplegaba una variante de VBShower. Esta cadena es muy similar a la de exploits documentada por primera vez por Kaspersky en 2019.[223]

A partir de la actividad que observamos, evaluamos que existe una probabilidad realista de que el objetivo de Blue Odin se alinee con las prioridades estratégicas ucranianas, en lugar de las rusas. Por ejemplo, la actividad de Blue Odin dentro de las fronteras de Ucrania parece centrarse principalmente en las regiones separatistas autoproclamadas en el este de Ucrania, y en Crimea. También hemos observado que Blue Odin se dirige a organizaciones rusas, incluidos los sectores energético y gubernamental[224]



La montaña rusa de Blue Otso

Blue Otso (también conocido como Gamaredon, Armageddon) ha experimentado tanto éxitos sustanciales como grandes contratiempos en 2021, desde compromisos de gran alcance de sistemas sensibles, hasta la exposición del Servicio de Seguridad de Ucrania.

En febrero, el Centro de Coordinación Nacional de Ciberseguridad de Ucrania informó de que Blue Otso había comprometido los sistemas de gestión de documentos del gobierno ucraniano conocidos como SEI EB[225] y ASKOD[226]. Aunque los indicadores iniciales de compromiso eran escasos, identificamos un conjunto de archivos que probablemente fueron subidos a un escáner antivirus en línea por una o varias personas implicadas en la respuesta a incidentes relacionados con un único servidor ASKOD.[227] Estos archivos incluían diversas herramientas de malware de Blue Otso, como scripts de descarga, herramientas de exfiltración, un cliente VNC y un script utilizado para añadir referencias de plantillas remotas a documentos de Microsoft Word, lo que coincide con las evaluaciones realizadas por el NCCC. Estos archivos también incluían marcas de tiempo de modificación de archivos, que evaluamos que probablemente sean precisas a las horas de despliegue o modificación en la máquina víctima. Estas marcas de tiempo sugieren que el agente de la amenaza probablemente tuvo acceso a la víctima desde al menos el 5 de febrero de 2021, varias semanas antes de que se revelara el incidente.

Las operaciones de Blue Otso también sufrieron notables interrupciones en 2021. El primer ejemplo de interés lo hizo público el Servicio de Seguridad de Ucrania en abril, cuando reveló la detención de alguien en relación con un individuo que enviaba mensajes a los números personales de los empleados del SBU.[228] Estos mensajes contenían un enlace a un sitio web que posteriormente identificamos como murders-dkr[.]ru, que contenía un enlace a un fichero de archivo que supuestamente contenía listas de oficiales del SBU que tenían recompensas impuestas por una de las entidades separatistas. Este fue un primer indicador disponible en código abierto de que Blue Otso, que anteriormente se consideraba un agente de amenazas con base en Rusia, podría estar apoyado por actividades desde regiones no ocupadas dentro de las fronteras de Ucrania.

Esto se amplió posteriormente en noviembre de 2021, cuando el SBU reveló las identidades de varios operadores de Blue Otso, y alegó que la actividad del agente de la amenaza está vinculada a una unidad del FSB con sede en Crimea.[229], [230] Esta unidad está supuestamente subordinada al 18º Centro del FSB, también conocido como Centro de Seguridad de la Información, una unidad que ya ha sido vinculada a violaciones de datos por el Departamento de Justicia de Estados Unidos. Al parecer[231] el SBU sugirió por primera vez la implicación del Centro 18 en 2015, momento en el que también sugirió la implicación del Centro 16 del FSB, más conocido por su asociación con Blue Python (alias Turla, Snake). Nuestro análisis[232] señaló que este anuncio se produjo en medio de informes sobre un aumento de la presencia militar rusa cerca de la frontera compartida entre Ucrania y Rusia a raíz de ejercicios militares a gran escala, antes de que estallara la guerra en Ucrania.

Un análisis más reciente sugiere que Blue Otso no se ha dejado intimidar por esta revelación; consideramos que es muy probable que este agente de la amenaza siga activo en 2022 y en adelante.

Nueva amenaza

Agentes destacados

En esta sección, destacamos agentes de ciber amenazas específicos que descubrimos en 2021. Esto no significa que los agentes de la amenaza no estuvieran activos anteriormente. Sin embargo, dado que ampliamos continuamente nuestro rastreo e identificamos nuevos agentes de amenazas sobre la base de nuestra visibilidad y recopilación, creemos que es valioso dar cobertura en este informe a los agentes de amenazas menos conocidos, y a los que todavía estamos en proceso de comprender plenamente. Los agentes de la amenaza que describimos a continuación han sido incluidos porque mostraban una actividad interesante, ya sea por sus capacidades, sus objetivos, sus vínculos con otros agentes de la amenaza o por el tipo de operaciones que realizan.

Red Dev 17

En 2021, comenzamos a rastrear una serie de intrusiones bajo el nombre de Red Dev 17 que, según nuestra opinión, es muy probable que haya sido realizada por un agente de amenazas con sede en China. Nuestro análisis sugiere que Red Dev 17 ha estado activo al menos desde 2017.

Los objetivos observados de Red Dev 17 se encuentran principalmente en la India, e incluyen el ejército indio, una empresa multinacional de tecnología con sede en la India y una empresa estatal de energía. Evaluamos que es muy probable que el agente de la amenaza detrás de las intrusiones asociadas a Red Dev 17 sea también responsable de la campaña conocida en código abierto como Operación NightScout.

Red Dev 17 es un usuario del marco de armamento de documentos 8.t (también conocido como RoyalRoad), y abusa de utilidades benignas como los binarios de Logitech o Windows Defender para cargar lateralmente y ejecutar variantes de Chinoxy o PoisonIvy en los sistemas de las víctimas.

Hemos identificado vínculos de capacidad e infraestructura entre Red Dev 17 y el agente de la amenaza que llamamos Red Hariasa (alias FunnyDream APT), así como solapamientos de infraestructura con Red Wendigo (alias Icefog, RedFoxtrot), y con los servidores C2 de ShadowPad. En este momento, no tenemos pruebas suficientes para vincular directamente a Red Dev 17 con ninguno de estos agentes de la amenaza.

Sin embargo, evaluamos con una probabilidad realista que Red Dev 17 opera dentro de un grupo de agentes de amenazas que comparten herramientas e infraestructura, así como un fuerte enfoque en el sudeste de Asia y Asia Central.

Blue Dev 6

En octubre de 2021, observamos varios documentos armados que utilizaban trabajadores de Cloudflare como canal C2. Consideramos que esta actividad fue probablemente llevada a cabo por Blue Dev 6 (también conocido como ReconHellCat), un agente de amenazas del que QuoIntelligence informó por primera vez en agosto de 2020.[233] Los documentos armados utilizaban plantillas y macros remotas para ejecutar una carga útil descargada de un trabajador C2 de Cloudflare. El paquete, que estaba muy encubierto, tenía varias similitudes con el malware BlackSoul (también conocido como BlackWater), incluido el código utilizado para modificarse a través de las carpetas del navegador y autenticar durante la comunicación C2. Las campañas que analizamos se dirigían a una serie de sectores, como la energía, la defensa y el gobierno, así como a una organización humanitaria internacional.

Yellow Dev 23

Rastreamos un nuevo grupo de actividad centrado en los sectores de las telecomunicaciones y la TI como Yellow Dev 23 (alias MalKamak, DEV-0270). Las fuentes abiertas informaron sobre este agente de la amenaza a finales de 2021 y describieron una campaña que se centraba en gran medida en Israel, concretamente en sus sectores de TI y telecomunicaciones.[234, 235] Además de los informes de fuentes abiertas, observamos que el agente de la amenaza utilizaba dominios escritos deliberadamente para confundir entre febrero y julio que falsificaban los inicios de sesión de Facebook y Office365. Varias de las muestras de malware atribuidas en código abierto a este agente de la amenaza se solapan con otro agente de la amenaza basado en Irán que rastreamos como Yellow Liderc, que es conocido por dirigirse al sector de las TI en Oriente Medio.[236]

Estudio de caso de respuesta a incidente:

White Dev 89 llamando

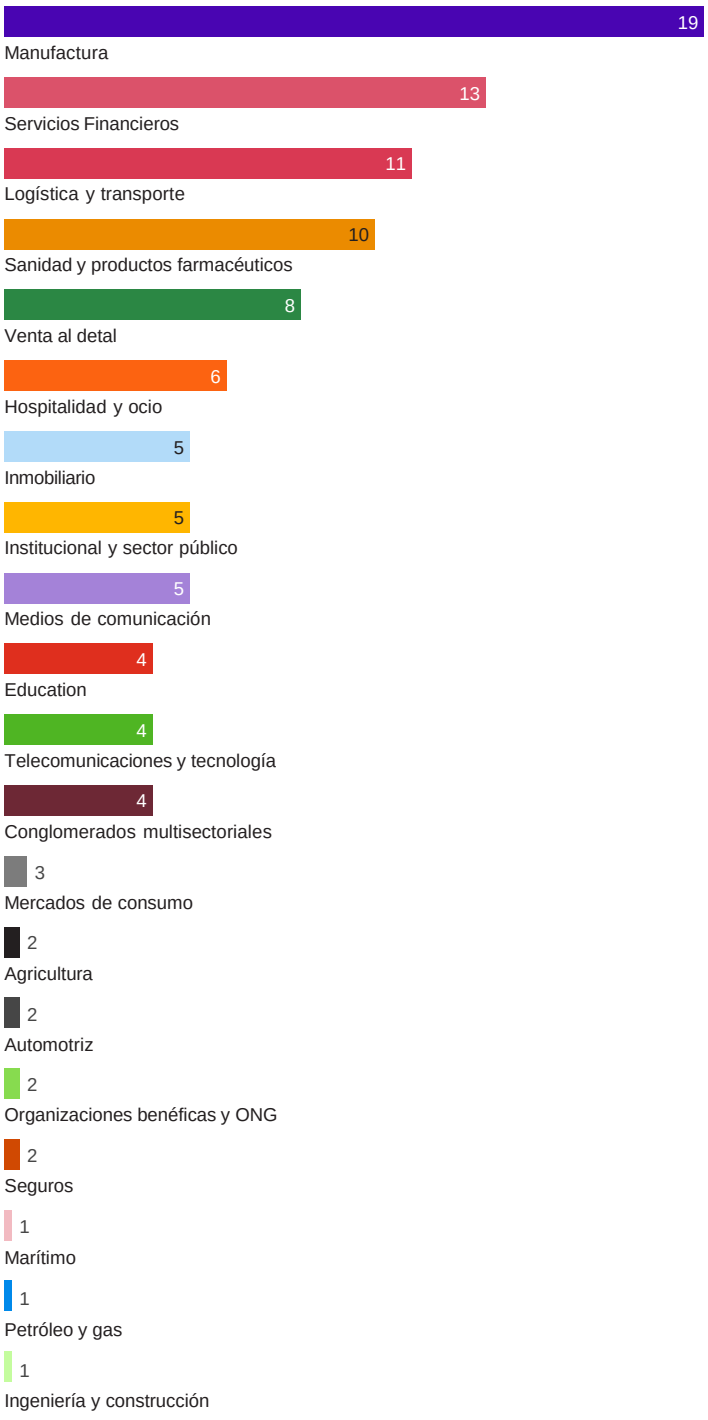
En 2021, apoyamos una investigación de respuesta a incidentes en una organización de salud que involucraba a un agente de amenazas que denominamos White Dev 89. Se observó que este agente de amenazas realizaba un ataque oportunista, probablemente a través de campañas de publicidad maliciosa, para ofrecer a sus víctimas aplicaciones troyanizadas como Zoom, AnyDesk y Windscribe. Éstas instalaban las respectivas aplicaciones legítimas, pero al mismo tiempo soltaban y ejecutaban un script malicioso de PowerShell (probablemente una versión modificada de un agente de PowerShellEmpire). Este acceso permitía al agente de la amenaza realizar un reconocimiento básico del sistema infectado. [237]

Una vez que White Dev 89 perfiló una máquina comprometida, observamos que lanzaba un script PowerShell adicional para desplegar Cobalt Strike Beacon. Esto desencadenó más actividad - incluyendo el movimiento lateral a través de SMB (Bloque de Mensajes del Servidor) a otros sistemas en la red. Otras técnicas de movimiento lateral que White Dev 89 utilizó incluyeron el compromiso de cuentas de alto privilegio, la ejecución de herramientas como ADFind y BloodHound para mapear la red objetivo, y el uso de 7-ZIP y SubInAcl durante la post-explotación.

Aunque los objetivos finales de este agente de la amenaza no están claros, encontramos conexiones con otras campañas conocidas. En particular, encontramos coincidencias con la infraestructura utilizada previamente en las campañas de QakBot, lo que nos lleva a la hipótesis de que, o bien White Dev 89 es el mismo agente de amenazas detrás de QakBot, o que ha utilizado previamente QakBot para el acceso inicial.

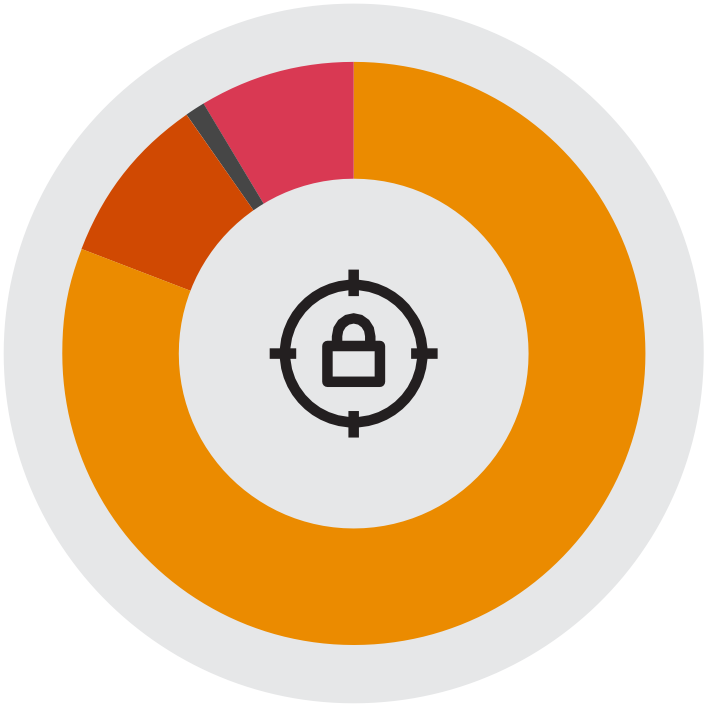
Estadísticas de respuesta a incidentes de PwC

Figura 27: Casos de ransomware en IR por sector 2021



Fuente: PwC

Figura 28: Incidentes por tipo 2021



Amenazas Persistentes Avanzadas, 6, **5.2%**

Crimen, 92, **77.3%**

De adentro, 11, **9.2%**

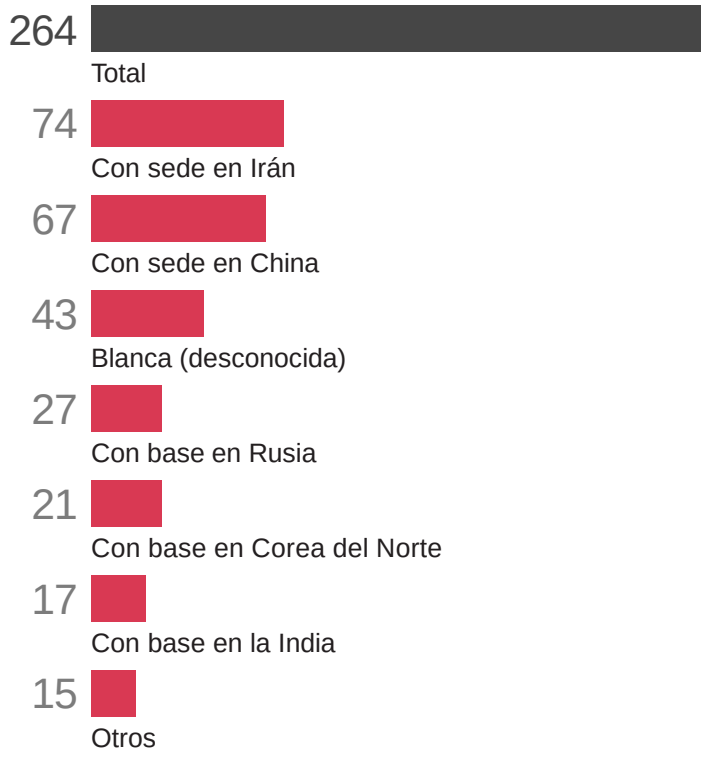
Hacktivista, 1, **0.8%**

Desconocido, 9, **7.5%**

Fuente: PwC

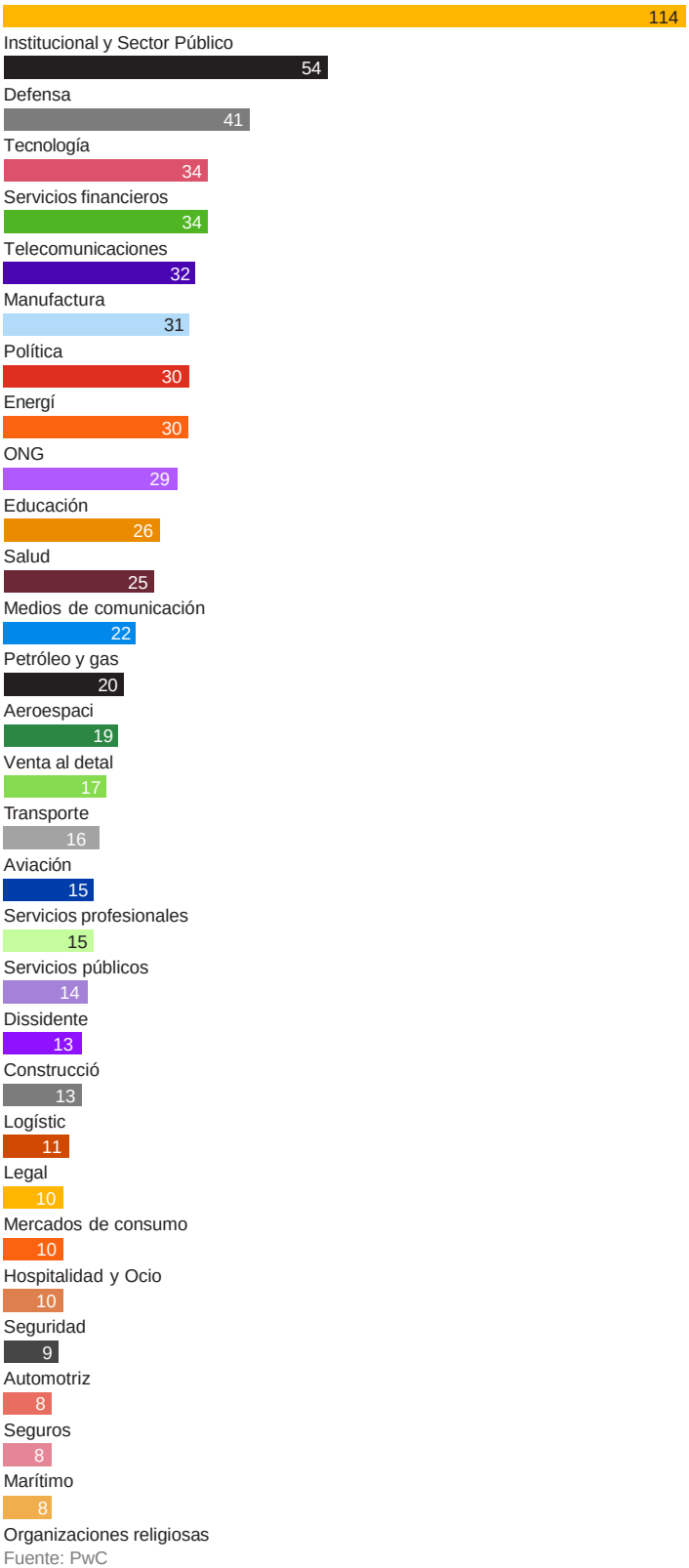
Estadísticas de los informes de PwC sobre Inteligencia de Amenazas

Figura 29: Informes por ubicación del agente de la amenaza 2021



Fuente: PwC

Figura 30: Informes por sector 2021



Fuente: PwC

Sectores foco

En esta sección, destacamos las principales ciberamenazas que observamos en 2021 en una selección de sectores.

Telecomunicaciones

En 2021 se observó un interés continuado en el sector de las telecomunicaciones por parte de agentes de amenazas motivados por el espionaje, probablemente con el fin de recopilar información sensible, como hemos observado en años anteriores[238].

Como se ha mencionado anteriormente en este informe, Red Menshen (antes Red Dev 18) desplegó su malware BPFDoor a medida en múltiples organizaciones de la región de Asia-Pacífico, incluidos proveedores de telecomunicaciones con sede en varios países[239].

PwC ha observado que otros agentes de amenazas con sede en China se dirigen al sector de las telecomunicaciones, como Red Kelpie (también conocido como APT41), que utilizó su malware Motnug loader en un proveedor con sede en Pakistán. [240] Esta misma víctima también parece haber sido objetivo del agente de amenazas con sede en Irán Yellow Mora[241]: a principios de 2021, PwC analizó una campaña de Yellow Mora (también conocido como Greenbug) dirigida al sector de las telecomunicaciones en el sur de Asia. [242] Nuestro análisis demostró que Yellow Mora probablemente pasó un período de tiempo prolongado en el entorno de la víctima, lo que concuerda con los informes públicos sobre la forma de operar de este agente de amenazas. [243] Una actividad similar de Yellow Nix (alias Static Kitten, MERCURY, MuddyWater), que comenzó en enero y continuó durante todo el año, tuvo como objetivo un gran número de organizaciones de telecomunicaciones en Oriente Medio, Asia Meridional, el Sudeste Asiático y Asia Central.[244] PwC considera que es probable que este objetivo tenga, al menos en parte, la intención de vigilar y rastrear a los individuos, lo que coincide con el objetivo histórico de este sector por parte de grupos estrechamente alineados como Yellow Mimas. [245]

Este sector tampoco ha escapado a las operaciones de ransomware. El nuevo ransomware Macaw de Blue Lelantos, por ejemplo, se desplegó contra una empresa de

de telecomunicaciones con sede en Estados Unidos, mientras que White Janus y White Apep -dos de los operadores de ransomware más activos de 2021- también apuntaron a múltiples entidades de este sector con los ransomware Lockbit 2.0 y Darkside/BlackMatter, respectivamente. En general, varias empresas estatales de telecomunicaciones, así como

de telecomunicaciones estatales, así como proveedores de telecomunicaciones privados de alto perfil, han sido víctimas del ransomware en el último año, incluyendo la Corporación Nacional de Telecomunicaciones de Ecuador, Schepisi Communications y la española MasMovil.

Tecnología

La tecnología innovadora es valiosa para quienes buscan replicar productos y servicios, y la propiedad intelectual sigue siendo de la propiedad intelectual sigue siendo buscada por los agentes de las amenazas. Las propias empresas tecnológicas pueden ser objetivo de ataques a la cadena de suministro y al salto de isla, especialmente cuando prestan servicios (incluidos los de TI y ciberseguridad) a los clientes. En 2021, varias compañías aéreas (entre ellas miembros de la alianza One Star y otras aerolíneas individuales de la región de Asia-Pacífico) se vieron comprometidas a través de una violación inicial de sus proveedores de tecnología de comunicación compartida: SITA.[246] El análisis de fuente abierta247 de este conjunto de intrusiones señaló a Red Kelpie como el probable autor. También se observó que Red Djinn intentaba un tipo de intrusión similar, en la que el agente de la amenaza se dirigía a filiales extranjeras de empresas japonesas que probablemente se desplazaban lateralmente y entraban en la red principal del blanco.

Se observó que los agentes de la amenaza utilizaban nombres de empresas tecnológicas en los certificados SSL asociados a su infraestructura maliciosa, como se identificó con los agentes de la amenaza basados en China, donde se identificó la infraestructura C2 de ShadowPad haciéndose pasar por NVIDIA Corporation[248]. También observamos muestras de malware HyperBro firmadas con un certificado perteneciente a una empresa de aplicaciones móviles. Aunque hay pruebas que sugieren que el malware HyperBro podría ser compartido por varios agentes de amenazas con base en China, su usuario original es Red Phoenix (también conocido como APT27, Emissary Panda, Lucky Mouse). Hemos observado que Red Phoenix sigue apuntando específicamente al sector tecnológico, y hemos identificado su compromiso con al menos una empresa tecnológica con sede en EE UU.

Los ciberdelincuentes también han atacado el sector tecnológico, y Acer se ha visto comprometida por el ransomware Revil en dos ocasiones distintas: en la segunda, la empresa recibió una petición de rescate de 50 millones de dólares, una de las más altas conocidas públicamente hasta la fecha[249].

Por último, las empresas tecnológicas israelíes también recibieron atención no deseada (supuestamente una campaña de "hacktivismo") por parte de White Dev 95, que, según nuestra opinión, es muy probablemente un agente de amenazas motivado por el sabotaje que lleva a cabo una operación de información (OI) contra Israel. En lugar de utilizarla para extorsionar, el agente de la amenaza cifra las redes de sus víctimas y procede inmediatamente a filtrar los datos robados, actividad que lleva el sello de las operaciones de "bloqueo y filtración".

Servicios financieros

Las organizaciones del sector de los servicios financieros siguieron siendo un objetivo de gran valor para los ciberdelincuentes. A lo largo de más de tres meses de listados en los mercados delictivos RaidForums, XSS y Exploit, las entidades de servicios financieros se situaron sistemáticamente entre los tres sectores más afectados.

Tenían un precio más alto en relación con otros sectores afectados, sin duda debido a que los listados de servicios financieros son de mayor interés para los compradores en términos de potenciales ganancias financieras.

Los grupos de delincuencia organizada establecidos pueden dirigirse específicamente a las entidades de servicios financieros debido a la expectativa de grandes pagos de rescate. Por ejemplo, a principios de 2021 la compañía de seguros estadounidense CNA se vio inicialmente comprometida cuando sus empleados ejecutaron una falsa actualización del navegador. Al parecer, la organización acabó pagando un rescate de 40 millones de dólares. En mayo de 2021, los operadores del ransomware Avaddon filtraron datos pertenecientes a las divisiones del Grupo AXA con sede en Asia (incluida la información personal de los clientes), y que contenían datos médicos sensibles; también amenazaron con atacar los sitios web de AXA con un ataque de denegación de servicio distribuido (DDoS) si no se pagaba un rescate. Más recientemente, a finales de noviembre de 2021, observamos una campaña de MirrorBlast realizada probablemente por White Austaras, que incluía correos electrónicos no deseados que sugerían que se dirigían a compañías de seguros con sede en Canadá y Francia, así como a una serie de empresas de gestión de activos y patrimonios con sede en Estados Unidos y Hong Kong.[250]

Los agentes de la amenaza basados en Corea del Norte siguieron planteando una grave amenaza para las organizaciones de servicios financieros en todos los ámbitos, desde las empresas de inversión y de capital riesgo hasta los intercambios de criptomonedas (o cualquier otra organización que maneje criptodivisas). Una acusación del Departamento de Justicia de EE.UU. de febrero de 2021 contra ciudadanos norcoreanos (que se cree que forman parte de Black Artemis) afirma que el agente de la amenaza robó 11,8 millones de dólares de una institución financiera de Nueva York utilizando aplicaciones de comercio de criptodivisas troyanizadas.[251] Black Alicanto y Black Dev 2 han atacado constantemente a las entidades de servicios financieros, a menudo enviando correos electrónicos de phishing selectivo a los objetivos, así como utilizando documentos de señuelo relacionados con la criptomoneda, o simulando ser lanzamientos legítimos de empresas conjuntas.

Ventas al detal

En 2021, los operadores de ransomware siguieron apuntando al sector minorista, explotando la necesidad de los minoristas de mantener un tiempo de funcionamiento ininterrumpido, presionando así a sus víctimas para que paguen el rescate rápidamente. La rápida digitalización del sector minorista ha llevado a los agentes del ransomware a paralizar los sistemas de pago de los puntos finales, lo que ha provocado una pérdida de ingresos, presionando aún más a la organización para satisfacer la demanda de rescate.

De las variantes de ransomware que se han observado dirigidas al sector minorista, Conti, operado por el agente de la amenaza White Onibi, fue la más activa. Este ransomware se utilizó para atacar a minoristas, desde tiendas de ropa hasta joyerías, para pagar grandes rescates o robar información confidencial única[252, 253, 254] que White Onibi subastó en 2021[255].

Otros operadores de ransomware también apuntaron al sector minorista. Como parte del ataque a la cadena de suministro contra Kaseya, el ransomware Sodinokibi infectó la red de Visma Esscom, un proveedor de TI. Como resultado de la infección de Visma Esscom, más de 500 tiendas individuales de Coop en toda Suecia tuvieron que cerrar después de que sus sistemas de pago quedaran fuera de servicio.[256] En otro ejemplo, en diciembre de 2021 un incidente de ransomware que afectó al minorista SPAR obligó a desconectar, en algunos casos durante varios días, a 330 tiendas del Reino Unido. Estos incidentes son sólo algunos de los numerosos que afectaron al sector minorista en 2021 y que amenazaron el funcionamiento normal de las empresas.[257, 258, 259, 260]

Nuestro análisis de los listados en los mercados delictivos mostró que, si bien la mayoría de los listados de empresas de venta al por menor contenían datos de clientes, varios (en particular en el foro Exploit) prometían a los compradores la posibilidad de redirigir los pagos con tarjeta en los sitios web de comercio electrónico. Para las marcas que operan en el espacio del comercio electrónico también vale la pena recordar que las operaciones de robo de tarjetas de crédito conocidas como "Magecart" están en curso[261] , y el NCSC del Reino Unido notificó a más de 4.000 pequeños y medianos minoristas justo antes del período de ventas del Viernes Negro que estaban utilizando portales de pago comprometidos en sus plataformas de comercio electrónico Magento.

Caso de Estudio de respuesta a incidente:

DarkSide: del acceso inicial a la petición de recompensa en cuatro horas

En abril de 2021, los equipos de Respuesta a Incidentes de PwC de varios países apoyaron a un cliente minorista global que había sido víctima de un ataque de ransomware perpetrado por DarkSide (rastreado por PwC como White Apep).

El análisis del incidente determinó que el agente de la amenaza aprovechó inicialmente una herramienta de acceso remoto conocida como LogMeIn para obtener acceso al entorno informático del cliente. Esta herramienta era utilizada con fines legítimos por uno de los proveedores de servicios de TI de la organización para permitir el acceso remoto para el mantenimiento de las estaciones de trabajo de la tienda y los sistemas de apoyo. La intrusión inicial utilizó una funcionalidad del software LogMeIn por la que los usuarios con credenciales válidas pueden acceder remotamente a un sistema sin que ningún empleado del cliente tenga que interactuar con él.

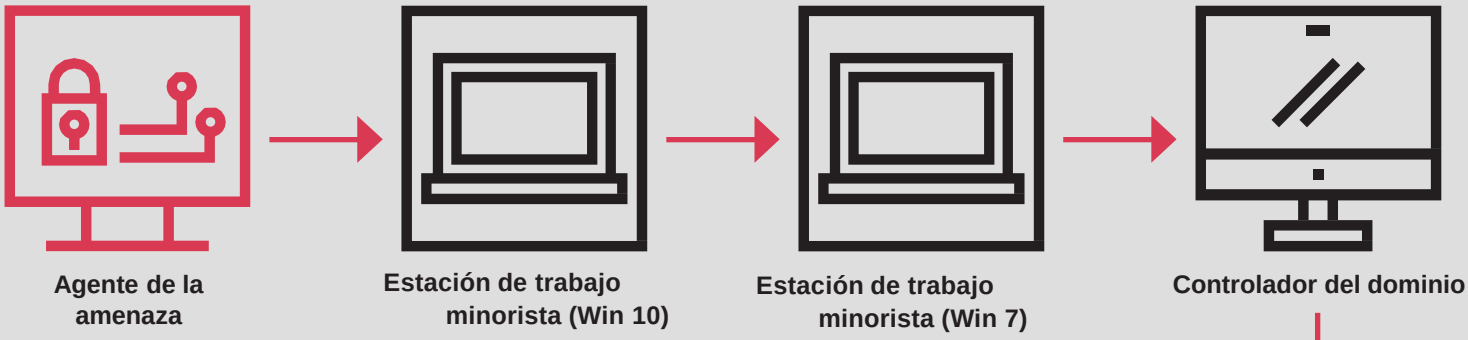
Después de comprometer al cliente de la tienda minorista en el país A, el agente de la amenaza descargó herramientas de administración, utilizándolas para realizar un reconocimiento interno en la red del cliente. Simultáneamente, elevó sus privilegios a una cuenta administrativa por defecto utilizada en todo el dominio a través del volcado de memoria de LSASS. Utilizando los privilegios elevados, el agente de la amenaza se dirigió a los sistemas del País B que estaban al final de su vida útil y no recibían actualizaciones.

A continuación, el agente de la amenaza utilizó las credenciales recopiladas de estos sistemas para crear un usuario administrador de dominio, generando y almacenando la contraseña de la cuenta en una cuenta de LastPass perteneciente al agente de la amenaza.

Una vez que el agente de la amenaza había vulnerado el controlador de dominio, creó una tarea programada y la desplegó en todos los ordenadores de la infraestructura de TI del cliente, ordenándoles que descargaran y ejecutaran el ransomware. El tiempo transcurrido desde el ataque inicial hasta el despliegue del ransomware fue de unas cuatro horas. Mientras el operador del ransomware exigía un rescate de 12 millones de dólares, el cliente consiguió establecer procesos de negocio manuales para mantener la organización operativa a lo largo de los esfuerzos de respuesta al incidente y de recuperación, que duraron tres semanas.

DarkSide

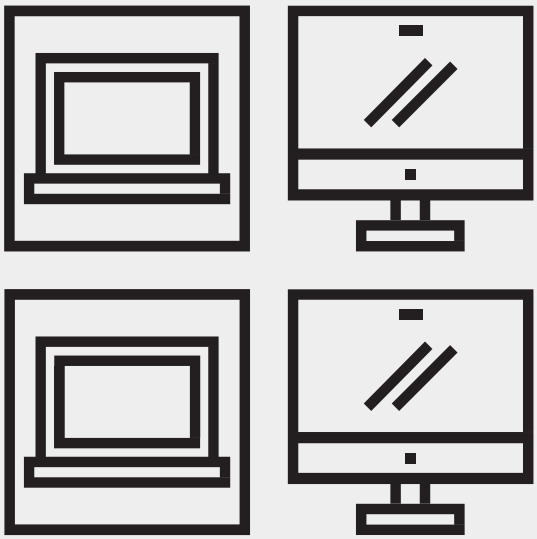
Del acceso inicial a la petición de rescate en cuatro horas



El agente de la amenaza vulnera una estación de trabajo de una tienda minorista en el país A, utilizando las credenciales RDP legítimas del proveedor de servicios del cliente

Después de realizar una conexión remota con éxito, el agente de la amenaza utiliza LOLbins para desplazarse lateralmente a una estación de trabajo de una tienda minorista en el país B

El agente de la amenaza roba contraseñas, obteniendo privilegios de administrador de dominio, y compromete con éxito el controlador de dominio en el país C



Utilizando los privilegios y el acceso al controlador de dominio, el agente de la amenaza despliega el ransomware en una ubicación de red compartida para eludir la detección del antivirus y, a continuación, despliega el ransomware en el entorno informático, inutilizando los sistemas.

Caso de Estudio de respuesta a incidente:

ShinyHunters a la caza del tesoro

En diciembre de 2021, PwC respondió a un incidente en un cliente minorista con sede en la India que había observado inicialmente un pico en la utilización de los recursos del sistema a través de su infraestructura en la nube, y posteriormente recibió un correo electrónico de rescate del agente de la amenaza ciberdelictiva que rastreamos como White Dev 100 (también conocido como ShinyHunters).

El análisis reveló que el agente de la amenaza accedió inicialmente a la red utilizando una clave de acceso a la nube comprometida que pertenecía a un antiguo miembro de la dirección de la organización. El agente de la amenaza utilizó las credenciales comprometidas para obtener acceso a la consola web de la infraestructura del cliente. No pudo acceder a ninguna de las instancias y procedió a ejecutar comandos de reconocimiento para mapear la red.

El agente de la amenaza fue capaz de crear nuevas instancias y claves SSH, inyectándolas finalmente en el almacén de claves autorizadas por SSH. Estas acciones, combinadas con las modificaciones en el grupo de seguridad, permitieron al agente de la amenaza entrar libremente en el entorno del cliente mediante SSH. Además, accedió a una serie de directorios de directorios .ssh y copió las claves SSH privadas disponibles para apoyar su movimiento lateral. A medida que el agente de la amenaza se desplazaba por la red, identificaba sistemas de interés, incluyendo instancias de prueba y automatización que explotaba para obtener más acceso. Durante este tiempo, el agente de la amenaza mantuvo el acceso a múltiples ventanas de terminal en el entorno comprometido. A partir del análisis de la actividad no ha sido posible determinar si había varios operadores o un solo individuo.

Manufactura

Para las organizaciones del sector manufacturero, cualquier ataque que pueda afectar a la disponibilidad o integridad de los sistemas infectados supone un riesgo crítico para la organización. Estos ataques provocan paradas operativas, ralentizaciones en la producción y en las entregas, lo que supone una pérdida de ingresos, así como elevados costos de reparación que se suman a las dificultades para volver al servicio. También hay problemas en cadena, como retrasos en los plazos de producción, incumplimiento de los contratos con los proveedores y daños a la reputación. El sector sufre cada vez más ataques importantes y selectivos, que van desde empleados descontentos que venden datos sensibles a la competencia hasta ataques de ransomware realizados por sofisticados grupos de delincuencia organizada.

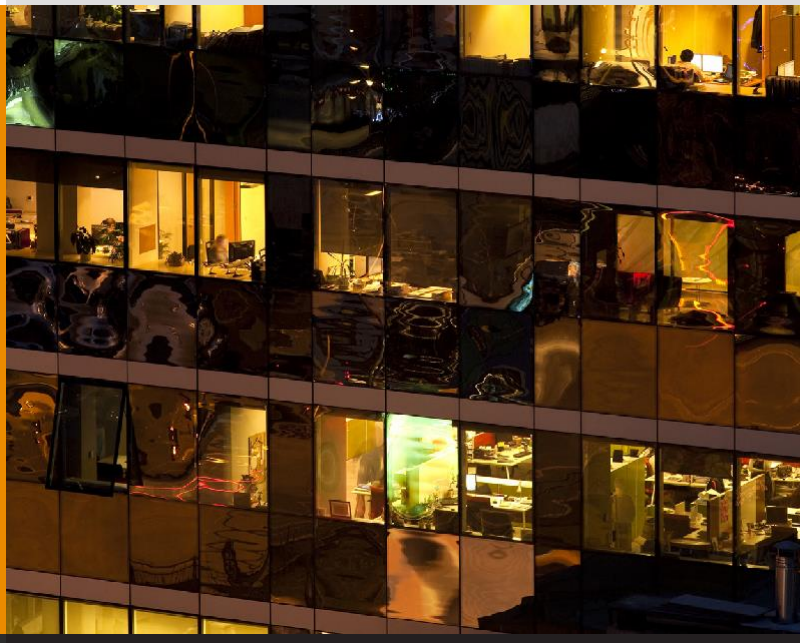
Entre enero y mayo de 2021, los operadores de las campañas de ransomware de BlackMatter se dirigieron a las organizaciones del sector manufacturero más que a ningún otro, en una serie de sofisticados ataques que supusieron más de 17,5 millones de libras esterlinas en pagos de bitcoins [262]. Lockbit 2.0 también mostró un fuerte enfoque en las organizaciones de manufactura, con el 21% de los datos del sitio de fuga entre enero y septiembre de 2021 pertenecientes a las víctimas en el sector.

Los ataques BEC siguen siendo una amenaza importante para todos los sectores, incluido el manufacturero. En 2021, PwC observó una campaña probablemente asociada a Bronze Dev 2 (también conocida como SilverTerrier), con sede en Nigeria, que se dirigía a organizaciones del sector manufacturero mediante el envío de correos electrónicos de spear phishing con un archivo adjunto malicioso que se hacía pasar por un documento presupuestario urgente, que entregaba la RAT AgentTesla.

El espionaje sigue siendo frecuente en el sector manufacturero, que históricamente ha atraído un gran interés por parte de los agentes de las amenazas de recopilación de información debido a su asociación con los clientes de los sectores de defensa y aeroespacial. En general, es probable que la inversión en tecnología que se está produciendo en el sector dé lugar a un nuevo aumento del interés. En abril de 2021, Black Artemis envió documentos de señuelo armados, que se hacían pasar por solicitudes de empleo, a empresas manufactureras que desplegaron descargas maliciosas en la red de la víctima [263]. El impacto de un ataque de espionaje exitoso puede resultar en la pérdida de competitividad en mercados internacionales ya muy ajustados, así como en sanciones regulatorias si se accede a datos personales en una intrusión.

Caso de Estudio de respuesta a incidente:

Empresa multinacional manufacturera enfrentando a LockBit



En marzo de 2021, PwC respondió a un incidente de ransomware que afectaba a una corporación multinacional que operaba en el sector de la fabricación industrial, donde un operador de LockBit ejecutó el ransomware en servidores y estaciones de trabajo de diez países diferentes.

El análisis y la investigación del incidente pusieron de manifiesto que, a partir del cuarto trimestre de 2020, el agente de la amenaza comenzó a recopilar información sobre el cliente y a preparar el ataque.

Después de obtener el acceso inicial, el agente de la amenaza utilizó el servicio de alojamiento de archivos MEGA para descargar el malware y realizó búsquedas en la web para conocer la ubicación y la naturaleza de los sistemas infectados. Posteriormente, el agente de la amenaza descargó y ejecutó herramientas de escáner de red (Softperfect Network Scanner) y realizó movimientos laterales utilizando cuentas comprometidas y con el apoyo de herramientas populares (incluyendo Mimikatz).

A lo largo de los meses siguientes, el agente de la amenaza comprometió un controlador de dominio en los Estados Unidos, luego se trasladó a otro servidor en EE.UU, y en marzo de 2021 empleó un controlador de dominio en Japón para distribuir el ransomware.

En los momentos finales del ataque, el agente de la amenaza interactuó con la solución antimalware del cliente para asegurarse de que el ransomware no se detuviera, y finalmente distribuyó y ejecutó el ransomware. Aunque el ataque causó importantes trastornos a la organización víctima, no hubo pruebas claras de exfiltración de datos.

Conclusión

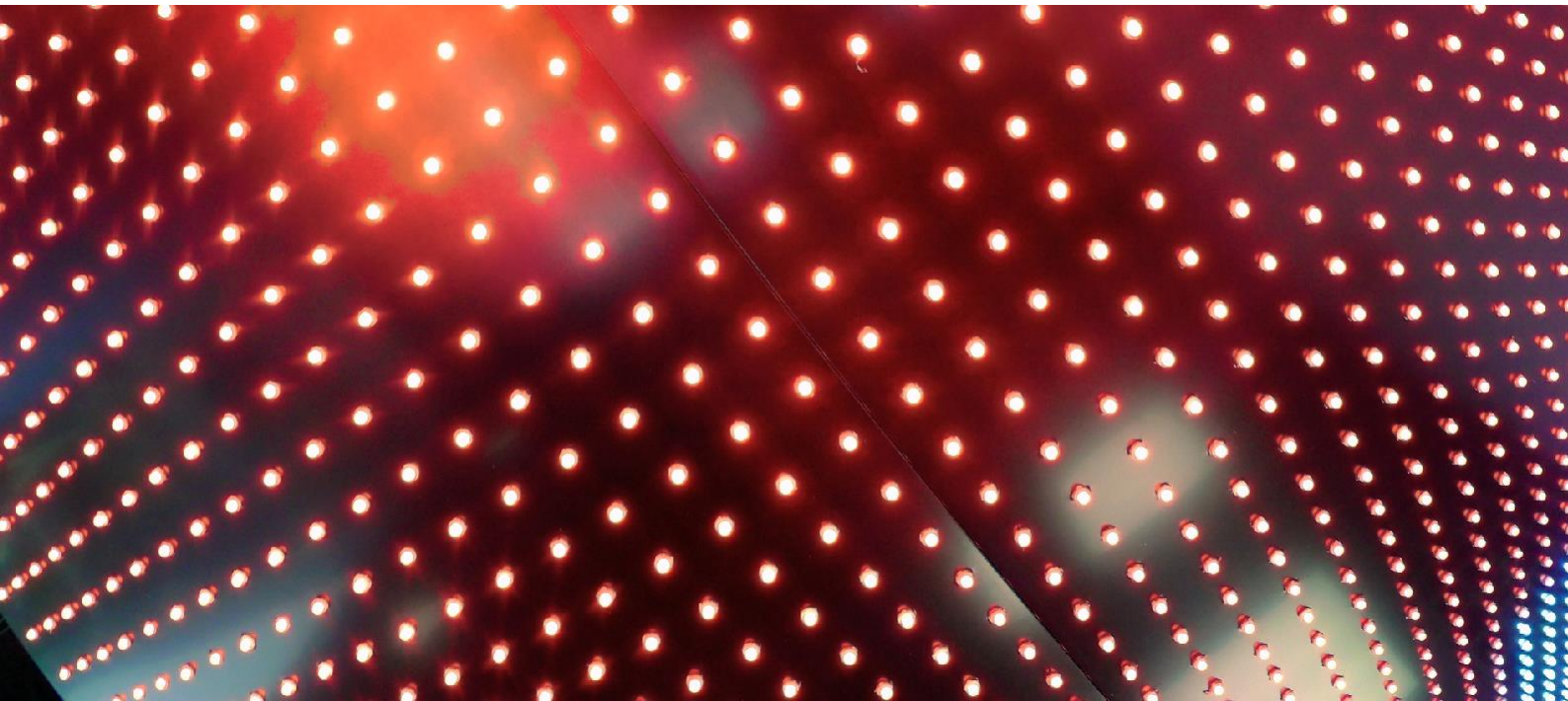
En 2021, el panorama de las ciberamenazas siguió a ver un aumento de los agentes de amenazas de todos los niveles de motivación y habilidad.

Al igual que en los últimos años, el ransomware sigue siendo la amenaza más generalizada y de impacto inmediato para las organizaciones de todos los tamaños y sectores en todo el mundo, y los desarrolladores de ransomware siguen aumentando sus esquemas de afiliación en tamaño, ingresos y capacidades. Los ataques a la cadena de suministro se han convertido en la "nueva normalidad" del panorama de las ciberamenazas, y los ciberdelincuentes los han incorporado a su agenda para conseguir el máximo impacto.

Al mismo tiempo, un tipo diferente de amenaza para una sociedad digital segura se ha puesto de manifiesto con la de los intendentes digitales: tanto los tradicionalmente alineados con las operaciones patrocinadas por el Estado, como los intermediarios comerciales del sector privado que proporcionan a una amplia gama de clientes herramientas y capacidades ofensivas de alto nivel.

Todas estas amenazas han culminado en un renovado enfoque en Las vulnerabilidades de día cero, con varios ejemplos que permiten tanto operaciones dirigidas como ataques a gran escala, y los crecientes incentivos financieros y estratégicos que empujan a explotar la actividad de investigación y desarrollo.

Evaluamos que los temas que han surgido o han continuado en 2021 -incluyendo el ransomware y el ecosistema criminal que lo rodea, la importancia de los intermediarios de vulnerabilidades y herramientas, y las consecuencias de las vulnerabilidades recién descubiertas que afectan a las víctimas no preparadas - continuarán en 2022. Ante las vulnerabilidades e incidentes que acaparan los titulares, la ciberseguridad está cada vez más presente en la opinión pública, y es aún más importante que nunca que los defensores continúen colaborando, compartiendo y apoyando a las organizaciones y a la sociedad; centrándose en las medidas de prevención y detección, así como en los planes de mitigación de incidentes y de respuesta que puedan obstaculizar a los agentes de amenazas de amenazas de forma eficaz.



Ciberseguridad de PwC

Si desea más información sobre cualquiera de las amenazas detalladas en este informe, no dude en ponerse en contacto con nosotros en threatintelligence@pwc.com.

PwC es reconocida mundialmente por los analistas del sector como líder en ciberseguridad; como una empresa con una sólida capacidad de prestación de servicios a nivel mundial y con la capacidad de abordar los retos de seguridad y riesgo a los que se enfrentan nuestros clientes.

Apoyamos nuestra estrategia de seguridad a nivel directivo y nuestros servicios de consultoría con la experiencia adquirida en la primera línea de la ciberdefensa a través de nuestros conocimientos técnicos especializados en servicios como la ciberdefensa gestionada, el red teaming, la respuesta a incidentes y la inteligencia sobre amenazas.

Apoyamos nuestra estrategia de seguridad a nivel directivo y nuestros servicios de consultoría con la experiencia obtenida en la primera línea de la ciberdefensa a través de nuestra experiencia técnica en servicios como la ciberdefensa gestionada, el red teaming, la respuesta a incidentes y la inteligencia sobre amenazas.

Reunimos a un equipo de especialistas con experiencia en gestión de la seguridad, detección y monitoreo de amenazas, inteligencia sobre amenazas, arquitectura y consultoría de seguridad, cambio de comportamiento y asesoramiento normativo y jurídico en nuestros esfuerzos por ayudar a nuestros clientes a proteger lo que más les importa.

Estamos especializados en la prestación de los servicios necesarios para ayudar a los clientes a resistir, detectar y responder a los ciberataques avanzados. Esto incluye eventos de crisis como violaciones de datos, ataques de ransomware, espionaje económico e intrusiones en objetivos, incluyendo los comúnmente conocidos como APTs. Nuestra investigación de inteligencia sobre amenazas es la base de todos nuestros servicios de seguridad, y es utilizada por organizaciones del sector público y privado de todo el mundo para proteger las redes, proporcionar conocimiento de la situación e informar sobre la estrategia.

Notas finales

1. '2021 ha batido el récord de ataques de hacking de día cero', MIT Technology Review: Patrick Howell O'Neill, https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/ (23 de septiembre de 2021)
2. La nueva coalición de gobierno alemana promete no comprar exploits', Recorded Future, https://therecord.media/new-german-government-coalition-promises-not-to-buy-exploits/ (8 de diciembre de 2021)
3. Divulgación completa (de vulnerabilidades)', Inteligencia de Amenazas de PwC, CTO-SIB-20210810-01A
4. Juega a juegos malvados, gana premios malvados", Inteligencia de Amenazas de PwC, CTO-SIB-20210625-01A
5. Google, 'Projecto Cero', https://googleprojectzero.blogspot.com/
6. 'Brillando una luz sobre el uso de ShadowPad a lo largo de 2019', Inteligencia de Amenazas de PwC, CTO-TIB-20200213-01A
7. 'Persiguiendo sombras', Inteligencia de Amenazas de PwC, CTO-TIB-20211021-01A
8. 'My, My, MySSL seguimiento de la infraestructura C2 mediante la reutilización de certificados Inteligencia de Amenazas de PwC, CTO-TIB-20210226-01B
9. “HAFNIUM explota las vulnerabilidades de Exchange", Inteligencia de Amenazas de PwC, CTO-QRT-20210303-01A
10. “HAFNIUM se dirige a los servidores Exchange con exploits de día cero", Microsoft, https://www.microosoft.com/security/blog/2021/03/02/ hafnium-targeting-exchange-servers/ (2 de marzo de 2021)
11. 'Operación Exchange Marauder: Explotación activa de múltiples vulnerabilidades de día 0 de Microsoft Exchange ', Volexity: Josh Grunzweig, Matthew Meltzer, Sean Koessel, Steven Adair, Thomas Lancaster, https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-0-day-vulnerabilities/ (2 de marzo de 2021)
12. Eat, Sleep, Liderc, Repeat', Inteligencia de Amenazas de PwC, CTO-TIB-20210730-01A
13. 'Atrapado en una.NET', Inteligencia de Amenazas de PwC, CTO-TIB-20210211-02A
14. Ciberriesgos 2020: Un año en Retrospectiva', Inteligencia de Amenazas de PwC
15. ‘Una mirada más cercana a los intendentes comerciales’, Inteligencia de Amenazas de PwC, CTO-SIB-20210906-01A
16. "Enganchando a Candiru sale a relucir otro vendedor de spyware mercenario", Citizen Lab, https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware- vendor-comes-into-focus/ (15 de julio de 2021)
17. "Proteger a los clientes de un agente ofensivo del sector privado que utiliza exploits de día 0 y malware DevilsTongue", Microsoft, https://www.microsoft.com/security/ blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilsstongue-malware/ (15 de julio de 2021)
18. 'Cómo protegemos a los usuarios de los ataques 0-day', Google, https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/ (14 de julio de 2021)
19. “Otro intendente comercial", Inteligencia de Amenazas de PwC, CTO-TIB-20210806-02A
20. “Otro intendente comercial", Inteligencia de Amenazas de PwC, CTO-TIB-20210806-02A
21. ‘Una mirada más cercana a los intendentes comerciales', Inteligencia de Amenazas de PwC, CTO-SIB-20210906-01A
22. ‘FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild', CitizenLab: Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, Ron Deibert, https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/ (13 de septiembre de 2021)
23. 'Una inmersión profunda en un exploit de iMessage de NSO zero-click: Remote Code Execution’, Google Project Zerolan Beer & Samuel Groß, https://googleprojectzero.blogspot. com/2021/12/a-deep-dive-into-nso-zero-click.html (15 de diciembre de 2021)
24. Comercio añade a NSO Group y otras empresas extranjeras a la lista de entidades por actividades cibernéticas maliciosas", Departamento de Comercio de los Estados Unidos, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-andother-foreign-companies-entity-list (3 de noviembre de 2021)
25. Sólo se hace clic dos veces: la proliferación global de FinFisher", CitizenLab: Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri y John Scott-Railton, https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ (13 de marzo de 2013)
26. FinSpy: hallazgos no vistos", Kaspersky, https://securelist.com/finspy-unseen-findings/104322/ (28 de septiembre de 2021)
27. 'Exclusiva: Una empresa estadounidense teme que sus hackeos de Windows hayan ayudado a la India a espiar a China y Pakistán", Forbes: Thomas Bewster, https://www.forbes.com/sites/thomasbrewster/2021/09/17/exodus-american-tech-helped-india-spy-on-china/?sh=13286ba07009 (17 de septiembre de 2021)
28. “Espionaje con presupuesto: Dentro de una operación de phishing con objetivos en la comunidad tibetana", CitizenLab: Masashi Crete-Nishihata, Jakub Dalek, Etienne Maynier, John Scott-Railton, https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/ (30 de enero de 2018)
29. 'Red Dev Redemption', Inteligencia de Amenazas de PwC, CTO-TIB-20210202-01A
30. 'Red Dev Redemption 2', Inteligencia de Amenazas de PwC, CTO-TIB-20210223-01A
31. Red Dev Redemption 3', Inteligencia de Amenazas de PwC, CTO-TIB-20210401-01A
32. '"LuoYu": El espía que se cuela en múltiples plataformas', Team T5: Leon & Shui, https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf (28 de enero de 2021)
33. 'Red Dev 7 recibe un nombre Nue', Inteligencia de Amenazas de PwC, CTO-TIB-20201016-01A
34. ‘APT reporte de tendencias Q2 2017’, Kaspersky, https://securelist.com/apt-trends-report-q2-2017/79332/ (8th August 2017)
35. 'LootRAT se ocupa de cuatro de un tipo', Inteligencia de Amenazas de PwC, CTO-TIB-20200130-02A
36. Amenazas en el punto de mira: February 2021', Inteligencia de Amenazas de PwC, CTO-TUS-20210317-01A
37. 'Malware WinDealer utilizado pory LuoYu Grupo de Ataque', JPCERT: Yuma Masubuchi, https://blogs.jpcert.or.jp/en/2021/10/windealer.html#1 (26 de octubre de 2021)
38. Amenazas en el punto de mira: April 2021', Inteligencia de Amenazas de PwC, CTO-TUS-20210511-01A
39. White Dev 75, como disparar a un pez en un barril", Inteligencia de Amenazas de PwC, CTO-TIB-20210303-01A
40. Nueva infraestructura de White Dev 75", Inteligencia de Amenazas de PwC, CTO-TIB-20211015-01A
41. "Cuando las mejores prácticas no son suficientes: Las grandes campañas de ataques de phishing en Oriente Medio y el Norte de África tienen como objetivo a los usuarios conscientes de su privacidad', Amnistía, https:// www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/ (19 de diciembre de 2018)
42. La evolución de los ataques de phishing dirigidos a periodistas y defensores de los derechos humanos de Oriente Medio y el Norte de África', Amnistía Internacional, https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/ (16 de agosto de 2019)
43. 'La herramienta VIP de Telegram de Yellow Garuda', PwC Threat Intelligence, CTO-TIB-20220110-01A

44. UNC788: DÉCADA DE OPERACIONES DE RECOLECCIÓN DE CREDENCIALES Y VIGILANCIA DE IRÁN, VB2021 localhost, https://vblocalhost.com/uploads/VB2021- Haeghebaert.pdf (October 2021)
45. "Un ramo fresco de malware", Inteligencia de Amenazas de PwC, CTO-TIB-20210511-02A
46. 'Lockbit 2.0', Inteligencia de Amenazas de PwC, CTO-TIB-20211027-02A
47. CTO-TIB-20211209-01A – Nothing elseBlackMatters, CTO-TIB-20210827-01A - Cómo ser un operador de ransomware
48. Economía de Estados Unidos por sectores", Wikipedia, https://en.wikipedia.org/wiki/Economy_of_the_United_States_by_sector
49. https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html
50. 'El Departamento de Justicia lanza una acción global contra el ransomware NetWalker', Departamento de Justicia de los Estados Unidos https://www.justice.gov/opa/pr/department-justice- launches-global-action-against-netwalker-ransomware, 27 de enero de 2021
51. "Babuk - Un nuevo chico en el barrio", Inteligencia de Amenazas de PwC, CTO-TIB-20210201-02A
52. 'Una banda de ransomware filtra datos del Departamento de Policía Metropolitana', BleepingComputer: Sergiu Glatan, https://www.bleepingcomputer.com/news/security/ ransomware-gang-leaks-data-from-metropolitan-police-department/ (11 de mayo de 2021)
53. 'DarkSide', Inteligencia de Amenazas de PwC, CTO-QRT-20210512-01A
54. 'Los hackers han entrado en Colonial Pipeline utilizando una contraseña comprometida', Bloomberg: William Turton, Kartikay Mehrotra, https://www.bloomberg.com/news/ articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password (4 de Junio de 2021)
55. 'Ataque de ransomware al sector sanitario - ACTUALIZACIÓN 2021-05-16', Ireland National Cybersecurity Centre, https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf (16 de Mayo de 2021)
56. 'JBS: Un ciberataque afecta al mayor proveedor de carne del mundo', BBC, https://www.bbc.co.uk/news/world-us-canada-57318965 (2 de Junio de 2021)
57. 'La cadena de suministro de Kaseya se ve comprometida', Inteligencia de Amenazas de PwC, CTO-QRT-20210703-01A
58. 'Aviso importante 4 de agosto de 2021', Kaseya, https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-August-4th-2021 (4 de Agosto de 2021)
59. 'El Departamento del Tesoro adopta medidas contundentes contra el ransomware', Departamento del Tesoro de los Estados Unidos, https://home.treasury.gov/news/press-releases/jy0364, 21 de Septiembre de 2021
60. 'Detenido e imputado un ucraniano por el ataque de ransomware a Kaseya', Departamento de Justicia de EE.UU., https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged- ransomware-attack-kaseya, 8 de Noviembre de 2021
61. 'Ransomware obtiene más prohibición por su dinero', Inteligencia de Amenazas de PwC, CTO-SIB-20210525-01A
62. 'DarkSide', PwC Threat Intelligence, CTO-QRT-20210512-01A
63. 'Entendiendo REvil: La banda de ransomware detrás del ataque Kaseya VSA', Palo Alto Unit 42: John Martineau, https://unit42.paloaltonetworks.com/revil-threat- actors/ (6 de Julio de 2021)
64. 'QakBot – un baño en la charca', Inteligencia de Amenazas de PwC, CTO-TIB-20200515-02A
65. 'Egregor Conoce al nuevo jefe', Inteligencia de Amenazas de PwC, CTO-TIB-20201203-01A
66. 'Rezident evil: Acusación de Dridex', Inteligencia de Amenazas de PwC, CTO-SIB-20200102-01A
67. 'WastedLocker - EvilCorp's nueva evidencia reveladora', Inteligencia de Amenazas de PwC, CTO-TIB-20200730-01A
68. 'Nuevo Mundo, Nuevo Macaw', Inteligencia de Amenazas de PwC, CTO-QRT-20211117-01A
69. 'Un nuevo DoppelPaymer', Inteligencia de Amenazas de PwC, CTO-TIB-20200710-01A
70. 'Causar más pena', Inteligencia de Amenazas de PwC, CTO-TIB-20211028-01A
71. 'Darkside Herramienta de descifrado de ransomware', Bitdefender, https://www.bitdefender.com/blog/labs/darkside-ransomware-decryption-tool/ (11 de enero de 2021)
72. 'Darkside', Inteligencia de Amenazas de PwC, CTO-QRT-20210512-01A
73. 'DarkSide, Culpado por el ataque al gasoducto, dice que está cerrando' New York Times, https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html (14 de mayo de 2021)
74. 'Nothing else BlackMatters', Inteligencia de Amenazas de PwC, CTO-TIB-20211209-01A
75. 'Ofertas de recompensa por información para llevar a los co-conspiradores de la variante de ransomware DarkSide ante la justicia', Departamento de Estado de los Estados Unidos, https://www.state.gov/reward-offers-for- information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/ (4 de Noviembre de 2021)
76. 'Tribunal de Moscú arresta a todos los hackers de ransomware REvil detenidos después de una solicitud del FBI a Rusia', TASS, https://tass.com/russia/1388649 (15 de Enero de 2022)
77. 'Explotación de Accellion File Transfer Appliance', Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA), https://www.cisa.gov/uscert/ncas/alerts/aa21-055a, 24 de Febrero de 2021
78. 'Accellion proporciona información actualizada sobre el incidente de seguridad de FTA tras los hallazgos preliminares de Mandiant', Accellion, https://www.globenewswire.com/news- release/2021/02/22/2179666/0/en/Accellion-Provides-Update-to-FTA-Security-Incident-Following-Mandiant-s-Preliminary-Findings.html (22 de Febrero de 2021)
79. 'Comprometimiento de la cadena de suministro de Kaseya', Inteligencia de Amenazas de PwC, CTO-QRT-20210703-01A
80. 'Emotet regresa', Inteligencia de Amenazas de PwC, CTO-QRT-20211116-01A
81. 'El malware más peligroso del mundo, Emotet, interrumpido a través de una acción global', Europol, https://www.europol.europa.eu/media-press/newsroom/news/ world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action (18 de Noviembre de 2021)
82. 'En qué se diferencia el nuevo Emotet de las versiones anteriores', Intel 471, "https://intel471.com/blog/emotet-returns-december-2021", 9 de diciembre de 2021
83. 'Colder than IcedID', Inteligencia de Amenazas de PwC telligence, CTO-TIB-20210511-01A
84. 'AaaS you like it', Inteligencia de Amenazas de PwC, CTO-SIB-202108802-01A
85. 'Informe del Grupo de Expertos establecido en virtud de la resolución 1874 (2009)', Consejo de Seguridad de las Naciones Unidas, https://www.securitycouncilreport.org/atf/ cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf (30 de agosto de 2019)
86. 'Todos los LNKs llevar de vuelta a Black Dev 1 Part 1', Inteligencia de Amenazas de PwC, CTO-TIB-20210408-01A
87. 'Todos los LNKs llevan de vuelta a Black Dev 1 Part 2', Inteligencia de Amenazas de PwC, CTO-TIB-20210525-01A
88. '¿A quién contrata Alicanto Negro?', Inteligencia de Amenazas de PwC, CTO-TIB-20210913-01A
89. 'Todos los LNKs llevar de vuelta a Black Dev 1 Part 1', Inteligencia de Amenazas de PwC, CTO-TIB-20210408-01A
90. 'Desvelando el Cryptomimic', NTT Security: Hajime Takai, Shogo Hayashi, Rintaro Koike https://vb2020.vblocalhost.com/uploads/VB2020-Takai-etal.pdf (2020)
91. 'La campaña de Lazarus Group apunta a la vertical de criptomonedas', F-Secure, https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2. pdf (18 de agosto de 2020)
92. 'Atribuyen a LAZARUS los ataques contra las bolsas de criptomonedas - Corea del Norte', ClearSky, https://www.clearskysec.com/wp-content/uploads/2021/05/CryptoCore- Lazarus-Clearsky.pdf (Mayo 2021)
93. 'Inyección de capital', Inteligencia de Amenazas de PwC, CTO-TIB-20210630-03A
94. 'El bitcoin es plata, el compromiso es oro: Los nuevos agentes de amenazas basados en Corea del Norte a la caza de criptomonedas', PwC: Sveva Vittoria Scenarelli, https://www.youtube.com/watch?v=BOZecjABjSk

95. El Banshee, la Flor, el Dragón y el Príncipe", Inteligencia de Amenazas de PwC, CTO-TIB-20210508-01A
96. Los atacantes norcoreanos utilizan blogs maliciosos para enviar malware a objetivos surcoreanos de alto nivel", Cisco Talos: Jung soo An, Asheer Malhotra, Kendall McKay, https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html (10 de noviembre de 2021)
97. 'Política nuclear para BabySharks', Inteligencia de amenazas de PwC, CTO-TIB-20211014-01A
98. 'Ciberamenazas 2020: Un año en retrospectiva', Inteligencia de Amenazas de PwC (2020)
99. El trabajo de tus sueños te espera - sólo tienes que activar la edición", Inteligencia de Amenazas de PwC, CTO-TIB-20210916-01A
100. Pinta uno de tus archivos BMP", Inteligencia de Amenazas de PwC, CTO-TIB-20210428-01A
101. Nueva campaña dirigida a los investigadores de seguridad", Google, https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/ (25 de enero de 2021)
102. ZINC ataca a los investigadores de seguridad", Microsoft, https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/ (28 de enero de 2021)
103. Los hackers norcoreanos fueron sorprendidos espiando a la brigada cibernética de China", The Daily Beast: Shannon Vavra, https://www.thedailybeast.com/north-korean-hackers-caught- snooping-on-chinas-cyber-squad (22 de noviembre de 2021)
104. @ESETresearch, Twitter, https://twitter.com/ESETresearch/status/1458438155149922312?s=20 (10 de noviembre de 2021)
105. El plan quinquenal de China tiene 7 objetivos tecnológicos", S&P Global, https://www.spglobal.com/marketintelligence/en/newsinsights/latest-news- headlines/china-s-5-year-plan-has-7-technology-targets-watch-for-responses-63161384 (15 de marzo de 2021)
106. 'BlackTechs ELF-esteem', Inteligencia de Amenazas de PwC, CTO-TIB-20210329-01A
107. 'BlackTech's Gh0st', Inteligencia de Amenazas de PwC, CTO-TIB-20201113-01A
108. 'Palmerworm: Banda de espionaje apunta a los medios de comunicación, las finanzas y otros sectores', Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ palmerworm-blacktech-espionage-apt (29 de septiembre de 2020)
109. 'Red Djinn's alertass', Inteligencia de Amenazas de PwC, CTO-TIB-20210903-02B
110. 'Back to Black(Tech): un análisis de las recientes BlackTech y un directorio abierto lleno de exploits', PwC: Sveva Vittoria Scenarelli, Adam Prescott, https://vblocalhost.com/ conference/presentations/back-to-blacktech-an-analysis-of-recent-blacktech-operations-and-an-open-directory-full-of-exploits/ (7 de octubre de 2021)
111. 'Red Djinns spider web', Inteligencia de Amenazas de PwC, CTO-TIB-20211202-01A
112. 'NICKEL apuntando a organizaciones gubernamentales a través de América Latina y Europa', Microsoft, https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting- government-organizations-across-latin-america-and-europe/ (6
113. El Ministerio de Seguridad del Estado de China y la actividad de los agentes de amenazas cibernéticas', US CISA, https://us-cert.cisa.gov/ncas/alerts/aa20-258a (24 de octubre de 2020)
114. 'Un comité de buitres', Inteligencia de Amenazas de PwC, CTO-SIB-20210722-01A
115. 'Okrum y Ketrican: Un vistazo a la reciente actividad del grupo Ke3chang', ESET, julio de 2019, https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf
116. 'BfV Cyber-Brief Nr. 01/2021 - Bedrohung deutscher Stellen durch Cyberangriffe der Gruppierung APT31', Bundesamt für Verfassungsschutz, https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-cyberabwehr/broschuere-2021-01-bfv-cyber-brief-2021-01 (18 de enero de 2021)
117. 'Red Keres fluye hacia el Sudeste Asiático', Inteligencia de Amenazas de PwC, CTO-TIB-20210211-01A
118. Aprendiendo a ChaCha con Red Kelpie', Inteligencia de Amenazas de PwC, CTO-TIB-20210624-02A
119. Explotación activa de CVE-2021-26084', Inteligencia de Amenazas de PwC, CTO-QRT-20210906-01A
120. 'Esto no es una prueba: APT41 inicia una campaña de intrusión global utilizando múltiples exploits', Mandiant, https://www.mandiant.com/resources/apt41-initiates-globalintrusion- campaign-using-multiple-exploits (25 de marzo de 2020)
121. 'Siete ciberacusados internacionales, incluyendo agentes "Apt41", Acusado en relación con campañas de intrusión informática contra más de 100 víctimas en todo el mundo", Departamento de Justicia de los Estados Unidos, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer (16 de septiembre de 2020)
122. 'Introduciendo Red Dev 14', Inteligencia de Amenazas de PwC, CTO-TIB-20210412-01A
123. Mandiant, 'Grupos de amenazas persistentes avanzadas', https://www.mandiant.com/resources/apt-groups
124. 'Aprendiendo a ChaCha con Red Kelpie', Inteligencia de Amenazas de PwC, CTO-TIB-20210624-02A
125. 'ShadowPad no un cert muerto', Inteligencia de Amenazas de PwC Inteligencia de Amenazas de PwC, CTO-TIB-20211116-02A
126. 'Dentro de una caja de herramientas roja', Inteligencia de Amenazas de PwC, CTO-TIB-20210518-01A
127. 'Orange Kala entra en la Zona de Guerra', Inteligencia de Amenazas de PwC, CTO-TIB-20210112-01A
128. 'Comprometer las telecomunicaciones euroasiáticas sólo por diversión', Inteligencia de Amenazas de PwC, CTO-TIB-20210709-01A
129. 'Una mirada a Red Dev 18', Inteligencia de Amenazas de PwC, CTO-TIB-20210831-02A
130. 'De Gh0sts and Golang', Inteligencia de Amenazas de PwC, CTO-TIB-20211011-01A
131. 'Red Dev 18 Otros desarrollos', Inteligencia de Amenazas de PwC, CTO-QRT-20210727-01A
132. Los scripts por lotes están bien", Inteligencia de Amenazas de PwC, CTO-TIB-20210223-02A
133. 'Orange Kala o Orange Dev 1 - tú decides', Inteligencia de Amenazas de PwC, CTO-TIB-20210520-01A
134. 'BAHAMUT: Masters de Hack-for-Hire de Phishing, Fake News, y Fake Apps', Blackberry Cylance, https://www.blackberry.com/us/en/forms/enterprise/bahamut-report (octubre de 2020)
135. 135. The White Company: Dentro de la campaña de espionaje de la Operación Shaheen", Cylance, https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/ resources/ knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf (18 de marzo de 2021)
136. 'BAHAMUT: Masters de Hack-for-Hire de Phishing, Fake News, y Fake Apps', Blackberry Cylance, https://www.blackberry.com/us/en/forms/enterprise/bahamut-report (octubre de 2020)
137. 'Compartir es cuidar", Inteligencia de amenazas de PwC, CTO-TIB-20210818-01A
138. 'Confucius APT despliega Warzone RAT', Uptycs: Abhijit Mohanta, Ashwin Vamshi, https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat (12 de enero de 2021)
139. 'Warzone RAT - Cuidado con el malware troyano que roba datos disparando desde varios documentos de Office', Quickheal: Ayush Puri, https://blogs.quickheal.com/ warzonerat-beware-of-the-trojan-malware-stealing-data-triggering-from-various-office-documents/ (1 de julio de 2021)
140. 'Monsoon - Análisis de una campaña APT', Forcepoint https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysisreport. pdf
141. Ciberamenazas 2020: Un año en retrospectiva', Inteligencia de amenazas de PwC
142. 'Orange Athos tiene malas noticias para sus adversarios", Inteligencia de Amenazas de PwC, CTO-TIB-20210204-02A
143. "Amenazas en el punto de mira en octubre de 2021", Inteligencia de Amenazas de PwC, CTO-TUS-20211118-01A

144. Orange Yali sigue instalándose en Pakistán", Inteligencia de Amenazas de PwC, CTO-TIB-20210527-02A
145. 'Operación "Magichm": Publicación de archivos CHM y posterior operación de la organización BITTER', QiAnXin, https://ti.qianxin.com/blog/articles/%22operationmagichm%22: CHM-file-release-and-subsequent-operation-of-BITTER-organization/ (15 de marzo de 2021)
146. El exploit de día 0 del núcleo de Windows (CVE-2021-1732) es utilizado por BITTER APT en un ataque dirigido", DBAPPSecurity, https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/ windows-kernel-0-day-exploit-is-used-by-bitter-apt-in-targeted-attack/ (10 de febrero de 2021)
147. Vulnerabilidad de día 0 en el gestor de Windows de escritorio (CVE-2021-28310) utilizado en la naturaleza", Kaspersky: Boris Larin, Costin Raiu, Brian Bartholomew, https://securelist. com/0-day-vulnerability-in-desktop-window-manager-cve-2021-28310-used-in-the-wild/101898/ (13 de abril de 2021)
148. Reportes de tendencias APT del segundo trimestre de 2021, Kaspersky, https://securelist.com/apt-trends-report-q2-2021/103517/ (29 de julio de 2021)
149. CrimsonRAT - Exportación premium de Green Havildars', Inteligencia de Amenazas de PwC, CTO-TIB-20210310-02A
150. 'Mapeo de la Infraestructura APT de la Tribu Transparente Parte 1: A High-Level Study of CrimsonRAT Infrastructure October 2020 - March 2021', Team Cymru: Joshua Picolet, https://team-cymru.com/blog/2021/04/16/transparent-tribe-apt-infrastructure-mapping/ (16 de abril de 2021)
151. Mapeo de la Infraestructura APT de Transparent Tribe Parte 2: Una inmersión más profunda en la identificación de la infraestructura de CrimsonRAT Octubre 2020 - Junio 2021', Team Cymru: Joshua Picolet, https://team-cymru.com/blog/2021/07/02/transparent-tribe-apt-infrastructure-mapping-2/ (2 de julio de 2021)
152. Aggah está utilizando sitios web comprometidos para atacar a empresas de toda Asia, incluida la industria manufacturera de Taiwán", Anomali, https://www.anomali.com/blog/ aggahusing-compromised-websites-to-target-businesses-across-asia-including-taiwan-manufacturing-industry (12 de agosto de 2021)
153. Ciberamenazas 2020: Un Año en Retrospectiva', Inteligencia de Amenazas de PwC
154. Amenazas en la mira - diciembre de 2020', Inteligencia sobre Ciberamenazas de PwC, CTO-TUS-20210111-01A
155. 'No hay suficiente maná para llevar a cabo esa operación', Inteligencia de Amenazas de PwC, CTO-TIB-20210630-02A
156. '针对性伪装攻击, 终端信息安全的间谍--海莲花 APT', Sangfor, https://mp.weixin.qq.com/s/WnKc0JbjA5_IsjPFSzFoYA (31 de marzo de 2021)
157. 'RotaJakiro: Una puerta trasera secreta de larga vida con 0 detección VT', 360 Netlab, https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/ (28 de abril de 2021)
158. No eres Shikata Ga Nai, créelo", Inteligencia de Amenazas de PwC, CTO-TIB-20211102-02A
159. "¿De quién es la campaña?", Inteligencia de Amenazas de PwC, CTO-TIB-20211121-01A
160. Ransomware o sabotaje, esa es la cuestión", Inteligencia de Amenazas de PwC, CTO-SIB-20210927-01A
161. Ransomware o sabotaje, esa es la cuestión", Inteligencia de Amenazas de PwC, CTO-SIB-20210927-01A
162. De quién es la campaña", Inteligencia de Amenazas de PwC, CTO-TIB-20211121-01A
163. Nueva versión del ransomware Apostle reaparece en un ataque dirigido a la educación superior", SentinelOne, https://www.sentinelone. com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/#:~: text=New%20Version%20Of%20Apostle%20Ransomware%20Reemerges%20In%20Targeted%20Attack%20On%20Higher%20Education,-Amitai%20Ben%20Shushan&text=SentinelLabs%20has%20been%20tracking%20the,destructive%20attacks%20starting%20December%202020. (30 de septiembre de 2021)
164. Tendencias cambiantes en la actividad de los agentes de amenazas iraníes - presentación de MSTIC en la CyberWarCon 2021', Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolving- trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/ (16 de noviembre de 2021)
165. Agente de amenazas vestido elegantemente", Inteligencia de amenazas de PwC, CTO-TIB-20211222-02A
166. Pay2Key to N3tw0rm', Inteligencia sobre amenazas de PwC, CTO-TIB-20210513-01A
167. Conexiones perdidas", Inteligencia de Amenazas de PwC, CTO-TIB-20210216-01A
168. Un recuerdo del pasado", Inteligencia de Amenazas de PwC, CTO-TIB-20210622-01A
169. Escaneando Internet en busca de vulnerabilidades", Inteligencia de Amenazas de PwC, CTO-TIB-20211118-01A
170. Los misterios de Pay2Key", Inteligencia de Amenazas de PwC, CTO-SIB-20210113-01A
171. El [redactado] arroja luz sobre una campaña", Inteligencia de Amenazas de PwC, CTO-TIB-20210712-01A
172. White Dev 75, como disparar a un pez en un barril", Inteligencia de Amenazas de PwC, CTO-TIB-20210303-01A
173. 'Yellow Maeros Art Attack', Inteligencia de Amenazas de PwC, CTO-TIB-20210226-02A
174. Trabajo nuevo, mismo malware", Inteligencia de Amenazas de PwC, CTO-TIB-20210806-01A
175. El [redactado] arroja luz sobre una campaña, Inteligencia sobre amenazas de PwC, CTO-TIB-20210712-01A
176. El [redactado] arroja luz sobre una campaña, Inteligencia sobre Amenazas de PwC, CTO-TIB-20210712-01A
177. Sabía que eras un problema: TA456 Targets Defense Contractor with Alluring Social Media Persona', Proofpoint, https://www.proofpoint.com/us/blog/threat-insight/ iknew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media (28 de julio de 2021)
178. Por supuesto que soy real....', Inteligencia de Amenazas de PwC, CTO-SIB-20210818-01A
179. Comer, Dormir, Liderc, Repetir', Inteligencia de Amenazas de PwC, CTO-TIB-20210730-01A
180. Respuestas de los agentes de amenazas basados en Irán a las crecientes tensiones geopolíticas", Inteligencia de Amenazas de PwC, CTO-SIB-20200108-01A
181. Tomar medidas contra los piratas informáticos en Irán", Meta, https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/ (15 de julio de 2021)
182. Evolving trends in Iranian threat actor activity - MSTIC presentation at CyberWarCon 2021', Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021 (16 de noviembre de 2021)
183. 'Yellow Nix se desplaza al sureste', Inteligencia de Amenazas de PwC, CTO-TIB-20211015-03A
184. 'Yellow Nix tiene una queja' , Inteligencia de Amenazas de PwC, CTO-TIB-20211216-02A
185. Nueva campaña de espionaje iraní por "Siamesekitten" - Lyceum", ClearSky, https://www.clearskysec.com/siamesekitten (17 de agosto de 2021)
186. Encontrar a Yellow Dev 9, Inteligencia de Amenazas de PwC, CTO-TIB-20211028-02A
187. Lyceum llamando', Inteligencia de Amenazas de PwC, CTO-TIB-20200605-01A
188. " Consigue tu brillo en Yellow Garuda", Inteligencia de Amenazas de PwC, CTO-TIB-20210514-01A
189. Sólo si te invitan", Inteligencia de Amenazas de PwC, CTO-QRT-20210907-01A
190. Un nuevo ramo de malware", Inteligencia de Amenazas de PwC, CTO-TIB-20210511-02A
191. Bot de Telegram Gatitos Encantadores', Inteligencia de Amenazas de PwC, CTO-TIB-20210909-01A
192. Alerta (AA20-304A) Actor iraní de amenazas persistentes avanzadas identificado obteniendo datos de registro de votantes', US CISA, https://us-cert.cisa.gov/ncas/alerts/aa20-304a
193. Aprendiendo en el trabajo con Yellow Dev 19", Inteligencia de Amenazas de PwC, CTO-TIB-20201118-02A
194. Aprendiendo en el trabajo con Yellow Dev 19', Inteligencia de Amenazas de PwC, CTO-TIB-20201118-02A
195. El Tesoro sanciona a los ciberagentes iraníes por intentar influir en las elecciones presidenciales de 2020", Departamento del Tesoro de los Estados Unidos, https://home.treasury.gov/news/press-releases/jy0494 (18 de noviembre de 2021)
196. Nuevas filtraciones y posibles vínculos con el IRGC", PwC Threat Intelligence, CTO-SIB-20210809-01A

197. Escaneo de vulnerabilidades en Internet", Inteligencia de Amenazas de PwC, CTO-TIB-20211118-01A
198. Escaneo de vulnerabilidades en Internet", Inteligencia de Amenazas de PwC, CTO-TIB-20211118-01A
199. Escaneo de vulnerabilidades en Internet", Inteligencia de Amenazas de PwC, CTO-TIB-20211118-01A
200. Tendencias cambiantes en la actividad de los agentes de amenazas iraníes - presentación de MSTIC en la CyberWarCon 2021", Microsoft, https://www.microsoft.com/security/blog/2021/11/16/ evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021 (16 de noviembre de 2021)
201. Tendencias cambiantes en la actividad de los agentes de amenazas iraníes - Presentación de MSTIC en la CyberWarCon 2021", Microsoft, https://www.microsoft.com/security/blog/2021/11/16/ evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021 (16 de noviembre de 2021)
202. El grupo StrongPity APT despliega por primera vez malware para Android", Trend Micro, https://www.trendmicro.com/en_us/research/21/g/strongpity-apt-group-deploysandroid-malware-for-the-first-time.html (21 de julio de 2021)
203. Amenazas en el punto de mira noviembre de 2021", Inteligencia de amenazas de PwC, CTO-TUS-20211203-01A
204. Tomando medidas contra Arid Viper', Facebook, https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf (abril de 2021)
205. Escondiéndose a plena vista', PwC Inteligencia de Amenazas, CTO-TIB-20211126-01A
206. Phishing en Oriente Medio", inteligencia de amenazas de PwC, CTO-TIB-20210629-02A
207. La campaña de WIRTE en Oriente Medio "vive de la tierra" desde al menos 2019", Kaspersky, https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-theland-since-at-least-2019/105044/ (29 de noviembre de 2021)
208. 'Elecciones en Palestina - en el camino de la campaña' , Inteligencia de amenazas de PwC, CTO-TIB-20191216-02A
209. Hay un ("Houdini") RAT en la embajada", Inteligencia de Amenazas de PwC, CTO-TIB-20191112-01A
210. Nota: actualmente no agrupamos la actividad de Blue Dev 5 con el mismo agente de amenazas que realizó la actividad de SolarWinds, que rastreamos como Blue Nova, debido a las diferencias en las TTP observadas.
211. El NCSC del Reino Unido considera que es muy probable que este agente sea el Servicio de Inteligencia Exterior de Rusia (SVR).
212. Reino Unido y Estados Unidos denuncian a Rusia por el ataque a SolarWinds", NCSC, https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise (15 de abril de 2021)
213. Blue Nova apuntó a Mimecast para obtener acceso a las claves utilizadas para autenticar las cuentas de servicio en los servidores de correo de las víctimas, además de apuntar al software desarrollado por SolarWinds.
214. Blue Dev 5 - Las raíces del ataque", Inteligencia de Amenazas de PwC, CTO-TIB-20210608-01A
215. ' Blue Dev 5 - Misterios del exterior', Inteligencia de Amenazas de PwC, CTO-TIB-20210527-01A
216. "NobleBaron | Los nuevos instaladores envenenados podrían utilizarse en ataques a la cadena de suministro", Volexity, https://www.sentinelone.com/labs/noblebaron-new-poisoned- installerscould-beused-in-supply-chain-attacks/ (1 de junio de 2021)
217. '(Darth) Vladars bajo ataque Parte 1', Inteligencia de Amenazas de PwC, CTO-TIB-20210310-01A
218. 'Bosnia está en peligro de romperse, advierte un alto funcionario internacional', The Guardian, https://www.theguardian.com/world/2021/nov/02/bosnia-is-in-danger-of- breakingup-warns-eus-top-office-in-the-state (2 de noviembre de 2021)
219. 'MINISTARSTVO UNUTRAŠNJIH POSLOVA REPUBLIKE SRPSKE', Ministerio del Interior de la República Srpska, https://mup.vladars.net/lat/index.php?vijest=vtk&id=23325&vrsta=aktuelnosti (24 de abril de 2020)
220. (Darth) Vladars bajo ataque Parte 2', Inteligencia de Amenazas de PwC, CTO-TIB-20210423-01A
221. (Darth) Vladars bajo ataque Parte 3', Inteligencia de Amenazas de PwC, CTO-TIB-20210903-01A
222. Cazando servidores Blue Odin', Inteligencia de Amenazas de PwC, CTO-TIB-20211215-01A
223. 'Actividad reciente de Cloud Atlas' Kaspersky, https://securelist.com/recent-cloud-atlas-activity/92016/ (12 de agosto de 2019)
224. 'Explorando Blue Odin', Inteligencia de amenazas de PwC, CTO-TIB-20210308-01A
225. 'El NCCC del NSDC de Ucrania advierte de un ciberataque al sistema de gestión de documentos de los organismos estatales', NCCC, https://www.rnbo.gov.ua/en/Diialnist/4823. html (24 de febrero de 2021)
226. El NCCC del NSDC de Ucrania ha actualizado la información sobre los ciberataques al sistema de gestión de documentos de los organismos estatales", NCCC, https://www.rnbo.gov. ua/en/Diialnist/4824.html (25 de febrero de 2021)
227. Dentro del compromiso de ASKOD', Inteligencia de amenazas de PwC, CTO-TIB-20210319-01A
228. El SBU descubre a un hacker a la caza de información personal de sus empleados", Servicio de Seguridad de Ucrania, https://ssu.gov.ua/en/novyny/sbu-vyiavyla-khakera-yakyi-poliuvav- napersonalni-dani-spivrobitnykiv-sluzhby (23 de abril de 2021)
229. SSU identifica a los hackers del FSB responsables de más de 5.000 ciberataques contra Ucrania', Servicio de Seguridad de Ucrania, https://ssu.gov.ua/en/novyny/sbu-vstanovylakhakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy (4 de noviembre de 2021)
230. Ucrania revela la identidad de los miembros de Gamaredon y los relaciona con el FSB ruso", The Record: Catalin Cimpanu, https://therecord.media/ukraine-discloses-identity- ofgamaredon-members-links-it-to-russias-fsb/ (4 de noviembre de 2021)
231. Operación Armagedón: El ciberespionaje como componente estratégico de la guerra moderna rusa', Looking Glass Cyber, https://web.archive.org/web/20190921173500/https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf (28 de abril de 2015)
232. 'Blue Otsos Armageddon', Inteligencia sobre amenazas de PwC, CTO-SIB-20211210-01A
233. El ReconHellcat utiliza el tema del NIST como señuelo para distribuir el nuevo malware BlackSoul', QuoIntelligence, https://quointelligence.eu/2021/01/reconhellcat-uses-nist-theme- aslure-to-deliver-new-blacksoul-malware/ (6 de enero de 2021)
234. Operación GhostShell: Novel RAT Arremete contra las empresas globales aeroespaciales y de telecomunicaciones', Cybereason, https://www.cybereason.com/blog/operation-ghostshell-novel- rattargets-global-aerospace-and-telecoms-firms (6 de octubre de 2021)
235. DEV-0343, vinculado a Irán, apunta a los sectores de defensa, GIS y marítimo", Microsoft, https://www.microsoft.com/security/blog/2021/10/11/iran-linked-dev-0343-targetingdefense-gis-and-maritime-sectors/ (11 de octubre de 2021)
236. El grupo Tortoiseshell apunta a proveedores de TI en Arabia Saudí en probables ataques a la cadena de suministro', Symantec, https://symantec-enterprise-blogs.security.com/blogs/ threatintelligence/tortoiseshell-apt-supply-chain (18 de septiembre de 2019)
237. 'Una llamada de Zoom con White Dev 89', Inteligencia de amenazas de PwC
238. 'Ciberamenazas 2020: Un año en retrospectiva', Inteligencia sobre amenazas de PwC
239. Las telecomunicaciones de Eurasia se ven comprometidas por diversión, Inteligencia de Amenazas de PwC, CTO-TIB-20210709-01A
240. Aprendiendo a ChaCha con Red Kelpie', Inteligencia de Amenazas de PwC, CTO-TIB-20210624-02A
241. Yellow Mora está escuchando", inteligencia sobre amenazas de PwC, CTO-TIB-20210426-01A
242. Yellow Mora está escuchando", Inteligencia de Amenazas de PwC, CTO-TIB-20210426-01A
243. El grupo de espionaje sofisticado se centra en los proveedores de telecomunicaciones del sur de Asia", Symantec, https://symantec-enterprise-blogs.security.com/blogs/threatintelligence/greenbug-espionage-telco-south-asia (19 de mayo de 2020)

244. Yellow Nix trabajando horas extras a distancia", Inteligencia de Amenazas de PwC, CTO-TIB-20210309-01A
245. El Tesoro sanciona a los agentes cibernéticos respaldados por el Ministerio de Inteligencia iraní", Departamento del Tesoro de EE.UU., https://home.treasury.gov/news/press-releases/sm1127 (17 de septiembre de 2020)
246. Boletín Cibernético Global - Junio 2021', Inteligencia de Amenazas de PwC, CTO-GCB-20210706-01A
247. Gran robo a una aerolínea: APT41 probablemente detrás de un ataque de terceros a Air India', Group-IB: Nikita Rostov ev, https://blog.group-ib.com/colunmtk_apt41 (10 de junio de 2021)
248. ShadowPad no es una certeza", Inteligencia de Amenazas de PwC, CTO-TIB-20211116-02A
249. Acer confirma un segundo ciberataque en 2021", ZDNet: Jonathan Greig, https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/ (14 de octubre de 2021)
250. Ha sido un MirrorBlast', Inteligencia de Amenazas de PwC, CTO-TIB-20211025-01A
251. El bebé del billón de dólares", Inteligencia de Amenazas de PwC, CTO-SIB-20210322-01A
252. Ransomware Conti: más de 25 millones de dólares en sólo cuatro meses", Acronis, https://www.acronis.com/en-us/cyber-protection-center/posts/conti-ransomware-rakes- inover-25-million-in-just-four-months/ (23 de noviembre de 2021)
253. El minorista Fat Face paga un rescate de 2 millones de dólares a la banda Conti, Bank Info Security, https://www.bankinfosecurity.com/retailer-fat-face-pays-2-million-ransom-to- contigang-a-16277 (26 de marzo de 2021)
254. 'La multinacional joyera Graff afectada por la banda Conti. Data of its rich clients are at risk, including Trump and Beckham', Security Affairs, https://securityaffairs.co/wordpress/123980/cyber-crime/conti-ransomware-graff-jeweller.html (31 de octubre de 2021)
255. La banda del ransomware Conti comienza a vender el acceso a las víctimas", Krebs on Security, https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/ (25 de octubre de 2021)
256. El supermercado Coop cierra 500 tiendas tras el ataque del ransomware Kaseya", Bleeping Computer, https://www.bleepingcomputer.com/news/security/coop-supermarketcloses-500-stores-after-kaseya-ransomware-attack/ (3 de julio de 2021)
257. Cientos de tiendas SPAR se ven obligadas a cerrar tras un importante incidente cibernético", Teiss, https://www.teiss.co.uk/spar-supermarket-cyber-incident/ (13 de diciembre de 2021)
258. NCSC statement on cyber incident affecting Spar stores', NCSC, https://www.ncsc.gov.uk/news/spar-stores-incident (10 de diciembre de 2021)
259. El minorista canadiense Home Hardware se ve afectado por un ransomware", ITWorld Canada, https://www.itworldcanada.com/article/canadian-retailer-home-hardware-hit- byransomware/445416 (2 de abril de 2021)
260. La empresa matriz de Office Depot prevé pérdidas de más de 20 millones de dólares por un ataque de malware", Retail Dive, https://www.retaildive.com/news/office-depot-parent-expects-over-20m-loss- dueto-malware-attack/597544/ (30 de marzo de 2021)
261. 'Los muchos tentáculos del Grupo Magecart 8', Malwarebytes: Jérôme Segura, https://blog.malwarebytes.com/threat-intelligence/2021/09/the-many-tentacles-ofmagecart-group-8/ (13 de septiembre de 2021)
262. 'Nothing else BlackMatters', Inteligencia de Amenazas de PwC, CTO-TIB-20211209-01A
263. El trabajo de tus sueños te espera, sólo tienes que activar la edición", Inteligencia de Amenazas de PwC, CTO-TIB-20210916-01A

pwc.com/cyber-security