Conti Ransomware: una amenaza vigente y de alto perfil

Abril, 2022

pwc

¿Quiénes son?

Conti es considerado un grupo que genera variantes de ransomware-as-a-service (RaaS) proveniente de Rusia. Este modelo de negocio se caracteriza por incluir un panel de administración desde donde los afiliados al servicio pueden crear y gestionar los perfiles de sus víctimas para recolectar información. Los desarrolladores del ransomware venden esta tecnología a sus miembros para que estos ejecuten los ataques.

De acuerdo con la información que se tiene, se especula que existe una variación en su estructura que lo diferencia del típico modelo de afiliación. Es posible que los desarrolladores de Conti paguen un salario a los que despliegan el ransomware en lugar de un porcentaje de las ganancias por un ataque exitoso.

Se cree que Conti es controlado por un grupo cibercriminal ruso llamado Wizard Spider, conocidos por crear y operar el malware TrickBot. Se ha identificado que Conti comparte parte de su código con Ryuk ransomware, también controlado por Wizard Spider.

“Conti suele utilizar la modalidad de doble extorsión, también conocida como doxing, que consiste en divulgar públicamente información confidencial de sus víctimas sin el consentimiento de éstas, para posteriormente amenazarlas con publicar más información si no realizan el pago del dinero exigido para el rescate de los datos”, indicó Isaac Rodríguez, Gerente de los servicios de Ciberseguridad y Privacidad de PwC Costa Rica.

Los objetivos comunes de Conti son organizaciones de infraestructura crítica con alto perfil como hospitales, entidades de gobiernos y financieras, que cuentan con los recursos suficientes para pagar importantes sumas de dinero o que necesitan de su información para poder operar con normalidad.

¿Qué los motiva?

“La principal motivación es financiera, sin embargo, debe tomarse en consideración la crisis geopolítica dada la invasión de Rusia a Ucrania, Conti abiertamente ha dado su apoyo a Rusia y se ha puesto a disposición de dicho país”, explicó Rodríguez.

Dado el apoyo de Conti a Rusia, algunos integrantes del grupo, en señal de protesta y apoyo a Ucrania, filtraron chats y documentos internos dando a conocer la estructura organizacional de Conti. Este movimiento es conocido como los Conti Leaks. *Check Point Research* luego de analizar los documentos determinó que Conti tiene departamentos encargados de su administración, finanzas y recursos humanos, junto con una jerarquía organizativa clásica con líderes de equipo que dependen de la alta Dirección.

pwc

Adicionalmente, *Check Point Research* determinó que a los empleados se les paga con Bitcoins, tienen bonificaciones de desempeño y oportunidades de entrenamiento. Los negociadores reciben comisiones que van desde 0.1% hasta 1% de lo pagado por las víctimas de cada ataque de ransomware exitoso. Existe un programa de referencia que reconoce a los empleados que recluten a otros y trabajen para Conti al menos por un mes. También, existe la figura de empleado del mes, donde la persona gana una bonificación de la mitad de su salario. Cabe mencionar que, el proceso de reclutamiento se realiza tanto por vías legítimas, mediante servicios de búsqueda de talentos (headhunting) rusos, como de forma ilegítima con cibercriminales.

Finalmente, se llegó a la conclusión de que no todos los empleados de Conti saben que son parte de un grupo criminal, ya que se evidenció que muchos creían que trabajaban para una organización normal.

¿Cómo ejecutan sus ataques?

Según los análisis e investigaciones se sabe que Conti opera de la siguiente manera:

1. **Reconocimiento**

Conti cuenta con equipos encargados de recolectar información sobre los gerentes, empleados, infraestructura tecnológica y operación de sus víctimas desde fuentes de acceso público como internet, para definir posteriormente la estrategia del ataque. Este equipo también puede relacionarse con personas objetivo, haciéndose pasar por personal de marketing o de ventas, para recopilar mayor detalle e información sobre los directivos, ejecutivos y el funcionamiento de la empresa.

2. **Pruebas de malware**

Conti dedica tiempo para desarrollar y poner a prueba sus scripts y payloads contra los sistemas comunes de detección como antivirus y detección y respuesta de usuario final (EDR), para validar que sus acciones sean indetectables y no generen alertas que puedan levantar sospechas sobre sus movimientos dentro de la red de la víctima. Según los Conti Leaks, estas pruebas se ejecutan con software de antivirus ampliamente utilizados como Windows Defender, ESET Nod 32, Avast Home, Kaspersky y Bitdefender.

3. **Mando y control**

Conti requiere de una infraestructura robusta para poder ejecutar sus ataques, lo que incluye mantener servidores proxy, servidores para los payloads, dominios C2, servidores virtuales privados (VPS) y amplio almacenamiento para guardar la información filtrada de las víctimas. Según Conti Leaks, se sabe que Conti ha utilizado servicios de ZEHost como proveedor para el hosting de esta infraestructura.

4. Campañas de phishing

Conti ataca a sus víctimas mediante campañas de phishing, utilizando correos dirigidos a personal clave que contienen enlaces o archivos adjuntos maliciosos, los cuales son utilizados para descargar malware como TrickBot, Bazar backdoor y aplicaciones legítimas como Cobalt Strike o AnyDesk. Las últimas son utilizadas posteriormente de forma maliciosa para realizar movimientos laterales dentro de la red y descargar el ransomware.

5. Ejecución de ataques y permanencia en la red

Entre otras técnicas utilizadas por Conti para filtrarse y mantenerse en la red de las organizaciones víctimas se encuentran:

- Uso de credenciales robadas o débiles en el Protocolo de Escritorio Remoto (RDP) expuesto en internet.
- Reclutamiento de *insiders*, es decir, personas que trabajan para la empresa y que están dispuestas a entregar credenciales o información confidencial para que el grupo pueda filtrarse en la red.
- Explotación de vulnerabilidades en equipos que no han sido parcheados, por lo que a través de estas pueden escalar privilegios y moverse lateralmente en la red de la víctima.
- Ejecución de un *getuid* payload antes de utilizar payloads más agresivos para reducir el riesgo de activar alguna alerta en los equipos de seguridad o antivirus.
- Uso de herramientas de penetración para escanear y lanzar ataques de fuerza bruta a routers, cámaras, dispositivos de almacenamiento en la red con interfaces web.
- Uso de ataques de fuerza bruta al protocolo de autenticación Kerberos.
- Filtración de archivos utilizando el software Rclone.

Una vez en la red, Conti instala puertas traseras para el mando de control y así filtrar toda la información de la víctima que sea posible previo a cifrarla. Conti se caracteriza por utilizar herramientas que se encuentran usualmente en las redes de sus víctimas como ayuda en sus ataques, incorporando, según sea necesario, herramientas como Mimikatz y Sysinternals para escalar privilegios y moverse lateralmente dentro de la red. La ventaja de emplear software familiar para los empleados como AnyDesk, es que a simple vista no se detecta actividad anómala dado que son herramientas que se ejecutan frecuentemente.

Mediante las campañas de spear phishing logran que con documentos de Word maliciosos (con scripts de PowerShell), puedan tener a disposición herramientas como Cobalt Strike e infectar la red con el malware Emotet. Esto le permite a Conti desplegar su ransomware, sin embargo, a diferencia de otras bandas de RaaS, Conti ha sido visto dentro de la red de sus víctimas durante varios días o semanas antes de desplegar el ransomware, utilizando bibliotecas de enlaces dinámicos (DLL) para la entrega de éste.

6. Remoción de copias de seguridad

El éxito del grupo se basa en su metodología y estrategia para eliminar las copias de seguridad, forzando a sus víctimas a pagar por los respaldos. Conti recluta a un equipo de personas con experiencia en la identificación, localización y desactivación de copias de seguridad. El equipo de eliminación utiliza Veeam (una plataforma de soluciones de copia de seguridad, recuperación y gestión de datos para entornos físicos, virtuales y en la nube), busca usuarios privilegiados de Veeam para filtrar, eliminar o cifrar las copias de seguridad y así asegurarse de que no exista posibilidad de que la víctima recupere sus archivos. Por lo tanto, hasta las copias oscuras (shadow copies) de los equipos infectados se ven comprometidas.

7. Amenazas

Si las víctimas deciden no adherirse a las demandas de rescate en un plazo de dos a ocho días, Conti llama a la víctima utilizando números de teléfono de protocolo de voz sobre Internet (VoIP). También se ha identificado que los atacantes utilizan ProtonMail, un servicio de correo web que ofrece cifrado de extremo a extremo para la comunicación.

¿Dónde publican los ataques?

El grupo tiene un blog llamado Conti News en el que publican los nombres de sus víctimas y posteriormente suben muestras de los datos robados, informan a los visitantes de cuándo publicarán todos los datos, cuántos datos tienen, la tarifa en Bitcoin que piden y mensajes de amenazas para presionar a sus víctimas.

El blog también advierte a las organizaciones con el mensaje: "*Si eres un cliente que rechazó el trato y no encontraste tus datos en el sitio web, significa que los datos fueron vendidos*".

¿Qué medidas se pueden tomar para protegerse del ransomware?

Autenticación de multiple factor

- Implementar la autenticación de múltiples factores para el acceso remoto, además de implementarlo de manera obligatoria en todos los sistemas para los usuarios con privilegios administrativos.

Redes

- Mantener la red segmentada para reducir la propagación y el impacto del ransomware.
- Filtrar el tráfico de red para prohibir las comunicaciones de entrada y salida con direcciones IP maliciosas conocidas.

Cultura de ciberseguridad

- Desarrollar e implementar un programa de capacitación y concientización de usuarios para sensibilizarlos sobre las amenazas cibernéticas. Además de visualizar la operación de grupos criminales los cuales buscan ponerse en contacto con empleados para que les faciliten sus credenciales u otra información confidencial a cambio de una suma de dinero.
- Realizar ejercicios de phishing para determinar y aumentar el nivel de conciencia sobre seguridad que tiene el personal.

Filtrado de tráfico

- Activar filtros de spam para evitar que correos electrónicos de campañas de phishing y spam lleguen a los usuarios finales.
- Filtrar los correos electrónicos que contengan archivos ejecutables.
- Implementar una lista de bloqueo de URLs para evitar que los usuarios accedan a sitios web maliciosos.

Gestión de vulnerabilidades

- Configurar los antivirus/antimalware para que realicen escaneos regulares de los activos de la red.
- Mantener las firmas del antivirus/antimalware actualizados.
- Actualizar oportunamente el software, los sistemas operativos, las aplicaciones y el firmware de todos los componentes de la infraestructura tecnológica.

Herramientas de detección y respuesta

- Implementar herramientas de respuesta y detección de puntos finales para mantener un alto grado de visibilidad del estado de seguridad de los equipos.

Protocolo de Escritorio Remoto

- Realizar una evaluación de riesgo sobre el uso de RDP, si se considera que el RDP es necesario desde el punto de vista operativo, se debe restringir las fuentes de origen y exigir la autenticación multifactor.

Uso permitido de aplicaciones

- Definir una lista de aplicaciones permitidas, donde sólo se autorice el uso de programas incluidos en dicho listado.
- Eliminar cualquier aplicación que no se encuentre en el listado de aplicaciones permitidas y que no se considere necesaria para la operación del negocio.
- Investigar cualquier alerta sobre el uso de software no autorizado, especialmente si el mismo está asociado al escritorio remoto, monitorización y gestión remota.

Respaldos

- Realizar copias de seguridad de manera regular y almacenarlas en una ubicación diferente con sus respectivos controles de seguridad. Se debe verificar que los respaldos se encuentren libres de indicadores de compromiso y encriptados.
- Realizar pruebas de las copias de seguridad con regularidad para garantizar la integridad de los datos.

Resiliencia cibernética

- Revisar el plan de continuidad de la organización para asegurarse de que los protocolos de contingencia y recuperación ante desastres se mantengan vigentes. Asimismo debe revisarse el plan de respuesta a incidentes.
- Realizar pruebas sobre los planes de continuidad y el plan de respuesta a incidentes.

Sobre PwC

PwC es reconocida mundialmente como líder en ciberseguridad; como una firma con sólidas capacidades globales de entrega y la capacidad de abordar los desafíos de seguridad y riesgo que enfrentan nuestros clientes.

Respaldamos nuestra estrategia de seguridad a nivel gerencial y los servicios de consultoría de asesoramiento poseen la experiencia obtenida de las primeras líneas de ciberdefensa a través de nuestra experiencia técnica de nicho en servicios como Managed Cyber Defense, Red Teaming, respuesta a incidentes e inteligencia de amenazas.

Nuestro equipo de inteligencia de amenazas se especializa en brindar los servicios que ayudan a los clientes a resistir, detectar y responder a ataques cibernéticos avanzados. Esto incluye eventos de crisis como filtraciones de datos, espionaje económico e intrusiones dirigidas, incluidas las comúnmente conocidas como APT.

Nos diferenciamos por nuestra capacidad de combinar sólidas capacidades técnicas con pensamiento estratégico, con nuestra investigación realizada por nuestros expertos internos reclutados principalmente en los gobiernos, las fuerzas armadas y los servicios de seguridad, lo que nos brinda una perspectiva única y una amplia gama de contactos. Nuestra investigación única e inteligencia de seguridad, experiencia técnica y comprensión del riesgo cibernético ayudan a los clientes a obtener la claridad que necesitan para adaptarse con confianza a nuevos desafíos y oportunidades. Nuestra investigación de inteligencia de amenazas sustenta todos nuestros servicios de seguridad y es utilizada por organizaciones del sector público y privado de todo el mundo para proteger las redes, brindar conocimiento de la situación e informar la estrategia.

pwc