pwc

サイバー脅威——2022年を振り返る

www.pwc.com/jp

エグゼグティブサマリー

2022 年におけるサイバー脅威を巡る状況は、現実世界の事象や地政学的緊張を反映したものとなった。特に、この年の大半において、ロシアによるウクライナ侵攻の影響が見られた。2022 年の混沌とした幕開けを告げたのは Log4Shell であった。そこで浮き彫りとなったのは、業界の協力関係がいかにポジティブな影響をもたらすか、環境内で広く使われているソフトウェアのフットプリントの理解やパッチの適用がいかに重要であるか、という点であった。

Log4Shell は、2022 年に明らかとなった脆弱性の中でも稀な事例であった。というのも、脅威アクターは攻撃を行う際に、既知の脆弱性やエクスプロイト、ツール（Cobalt Strike など）を使用し続けたのである。しかし、2022 年を通じて、動機や知識面でさまざまに異なる脅威アクターが強化されたツールやフレームワークを用いる例や、防御者のセキュリティ対策の裏をかくために、従来の行動パターンを変える例も見られた。さらにこの年は、脅威アクターがクラウド環境や ID・特権アクセス機能を標的とする事例も増加した。

ロシアによる侵攻が全面戦争へとエスカレートする中、ウクライナは世界中の政府やサイバーセキュリティ組織とともに、複数のワイパー型マルウェア亜種を展開するロシア拠点の脅威アクターによる、一連の妨害工作を追跡調査し対応を図った [1,2,3]。こうした妨害攻撃は紛争地域（ウクライナおよびロシアが併合した領域内）にとどまり、その影響は 2015～2016 年にロシア拠点の脅威アクターがウクライナ電力網を標的とした際にもたらした影響ほどではなかった。フィッシング・ターゲット型攻撃の顕著な変化に見られるように、スパイ活動を目的とする複数の脅威アクターがこの世界を揺るがす事象に反応し、連携する一方で、この侵攻によって、一部のサイバー犯罪脅威アクターや脅威者、ハクティビスト（Blue Kurama、別名 Killnet など）が、自ら親ウクライナ派または親ロシア派を宣言した上で、戦争下において自身が「敵」とみなした政府・民間セクターの組織を標的とする、といったように、工作活動や公的声明において反応・対応する行為が活発化した。

---

[1] 'ESET Research jointly presents Industroyer2 at Black Hat USA with Ukrainian government representative', ESET, https://www.eset.com/int/about/newsroom/press-releases/events/eset-research-jointly-presents-industroyer2-at-black-hat-usa-with-ukrainian-government-representativ/ (25th August 2022)

[2] 'NCSC advises organisations to act following Russia's attack on Ukraine', UK National Cyber Security Centre (NCSC), https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences (18th March 2022)

[3] 'Alert AA22-110A - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', US Cybersecurity & Infrastructure Agency (CISA), https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (20th April 2022)

ウクライナにおけるロシアの侵攻に加え、2022 年のサイバー脅威環境において、引き続き中国拠点の脅威アクターによる活動の最適化・高度化が見られた。ただし、それらの活動の標的については例年と大きく変化することはなかった。これらの脅威アクターが、プロキシネットワーク（RedRelay など）や共有マルウェア、エクスプロイト、ツールセット（ShadowPad や ScanBox など）といった、obfuscation-as-a-service（難読化サービス）を用いる事例が増加している。こうした手法を用いた最も有名かつ大規模な脅威アクターは、Red Scylla（別名 CHROMIUM、ControlX、Earth Lusca、Aquatic Panda）であり、少なくとも全世界 70 組織を標的とした。他の脅威アクターも非常に多くの地域に影響をもたらす高度な活動を展開し、一部は通信セクターへの集中攻撃を続けた。

イラン拠点の脅威アクターは、アルバニア政府への妨害攻撃、抗議者や反体制派を標的とする攻撃、主に中東や欧米のさまざまな業界の組織を標的とする攻撃など、2022 年も注目を集めた。こうした活動は、イラン政府の優先事項と合致している事例が多かった。北朝鮮を拠点とする脅威アクターは、引き続き金融サービス、暗号資産および分散型金融（DeFi）組織を標的として、金銭的窃取額を倍増させた。

全体として、PwC が 2022 年に解析した高度な持続的脅威（APT）は、国際社会のごく一部で、対象国の経済的孤立を狙った活動は続いていたものの、標的とするパターンはこれまで見られていたものと概ね合致していると思われる。ただし、一部の脅威アクターはその活動を大幅に伸展させた。2022 年、西側諸国を拠点とする活動もあったと PwC は推察しているが、十分な証拠が得られていないこともあり、本レポートでは大きく取り上げない。

また、サイバー犯罪エコシステムにおいては、年間を通じて、一部の事例における活動の高度化や世界中の組織が頭を悩ませる新たな進展も見られた。多くの組織にとって、サイバー関連の最大の懸念事項は引き続きランサムウェアであったが、より多産の傑出したランサムウェア脅威アクターの再編成や再調整が行われたと思しき形跡も認められた。そして、リークサイトの被害者数は昨年とほぼ同等であった。

2022 年で際立った数の被害者を生んだ脅威アクターのうち、最も懸念されたのは White Dev 111（別名 LAPSUS$ Group）であった。標的に対して、「スマッシュ＆グラブ」や「ハック＆リーク」活動を次々と仕掛けたのである。こうした攻撃の多くは、ソーシャルエンジニアリングその他の戦術を用いて、被害組織のセキュリティ対策やユーザーを消耗させるというものであった。この 1 年、サイバーによる詐欺も多発し、脅威アクターにとってアクセスやエクスプロイト、ツールがより一般的なものとなり、さまざまなサイバー犯罪に参入するハードルが下がっている傾向が一層浮き彫りとなった。

PwC について

PwC は、世界 152 カ国で 20 万社を超えるクライアントにサービスを提供しており、世界有数の規模を誇るグローバルなプロフェッショナル・サービス・ネットワークという優位性を活かして、各クライアントに合わせたグローバルな脅威インテリジェンス情報を各地域のクライアントに提供している。PwC が実施する調査は、PwC のセキュリティサービスを支えるものであり、世界各地の公共・民間セクターの組織において、ネットワークの保護、状況認識、戦略情報の提供に利用されている。

PwC の脅威インテリジェンスは、PwC の検出能力と、脅威に焦点を当てた調査や新たな問題を認識する積極的活動を組み合わせ、悪意ある活動の検出における課題を特定・対策し、脅威に関する知識を深め、実用的なインテリジェンスをレポートとしてまとめている。PwC の脅威インテリジェンスチームは、オーストラリア、ドイツ、イタリア、オランダ、ノルウェー、スウェーデン、英国、米国などグローバルなメンバーで構成されている。本レポートでは、PwC の脅威インテリジェンスが取り組み、レジリエントなサイバー戦略に関する情報をもたらしたさまざまな検出例 [4]を紹介する。

[4] Please see *Appendix D - Defender index* for a quick guide to all detection content in this report.

目　次


検出内容


インシデント対応に関する知見


利用可能な詳細情報


特定の PwC メンバーファームが得た知見


重要な教訓


脅威に関する知見

2022 年における主な事象

本レポートに詳述した 2022 年の事象

1 月
2021 年 12 月の公表以降も Log4Shell の影響続く（p.6）

2 月
ロシアのウクライナ侵攻開始（p.8）

3 月
Blue Cronus（別名 Conti）内部チャットの漏洩（p.45）

4 月
White Dev 115（別名 BlackBasta）登場。その後 Blue Cronus へ派生（p.46）

5 月
オーストラリア選挙をテーマにしたおとりを用いた、ScanBox による標的攻撃（p.25）

6 月
Red Dev 32 が PlugX から ShadowPad に移行、他の脅威アクターに加わる（p.22）

7 月
サイバー犯罪フォーラムで Brute Ratel レッドチームツールが支持を集める（p.53）

8 月
Black Alicanto、Microsoft Software Installer を用いておとりを多様化（p.32）

9 月
2022 年ランサムウェアリークサイトの被害組織が急増（p.42）

10 月
Yellow Dev 32、イランの抗議者にモバイルマルウェアを展開（p.29）

11 月
例年同時期と比較してランサムウェアリーク件数減少（p.42）

12 月
Blue Callisto、より多くのウクライナ支持組織にフィッシング（p.15）

Log4Shell の影響

2021 年 12 月に明るみとなった Log4Shell（CVE-2021-44228)は、Apache Log4j というソフトウェアの一部バージョン [5]の重大な脆弱性であり、これによって世界中の組織は混乱の中 2022 年を迎えることとなった。Apache Log4j は汎用性のあるソフトウェアであったため、さまざまなセクターや国の事業体が、Log4Shell の脆弱性開示に対して対応を迫られた [6]。しかも、脆弱性が明らかになった直後に、この脆弱性の悪用方法を示した概念実証（PoC）が自由に利用可能になった。あらゆるタイプの攻撃者が、この脆弱性の影響を受けるシステム上でコードを遠隔実行可能な状態となり、事態の緊急度はより高まったのである。組織は自環境内の Log4j インスタンスの発見に奔走し、Apache 財団もパッチ開発を急いだが、脆弱性発表から数時間のうちに、脅威アクターはこの機会を悪用し始めた [7]。

Log4Shell の悪用を検出

シンプルかつ広範囲にわたるネットワーク内の検出方法は、公開サーバーへの全インバウンドトラフィックを検査して「${jndi: -」という文字列または「${」のすぐ後に「jndi」が続くものを検索し、いくつかの一般的な回避テクニックを検討することである。

2021 年 12 月末までに、Apache 財団は、Log4Shell に対応する多数のアップデートをリリースした。国際的なセキュリティコミュニティやさまざまな政府機関も、人気のあるソフトウェアのどのバージョンにセキュリティ修正が施されているか、依然として注意が必要なのはどのソフトウェアなのか、といった点について情報を提供した [8,9]。こうした協力的な取り組みが奏功したこともあって事態の収束につながったが、脅威アクターは 2022 年全体にわたって Log4Shell および最初の修正実施後に発覚した Log4j に関連する脆弱性（CVE-2021-45046、CVE-2021-45105）を悪用していたことが判明している。

Log4Shell の公表以来、何十もの脅威アクターが、さまざまなセクターにおいて、諜報または金銭目的でこの脆弱性を悪用してきた [10]。2022 年における一例を挙げると、Log4Shell の公表から 8 カ月

---

[5] *Note:* When originally discovered, Log4Shell impacted Apache Log4j versions 2.0-beta9 to 2.14.1, and subsequent releases spawned additional vulnerabilities, remediated by version 2.17.0. *Source:* 'Alert AA21-356A - Mitigating Log4Shell and Other Log4j-Related Vulnerabilities', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa21-356a (23rd December 2021)

[6] *CTO-QRT-20211210-01A - Active scanning of CVE-2021-44228*

[7] 'Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation', Microsoft, https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/ (11th December 2021)

[8] 'Apache Log4j Vulnerability Guidance', CISA, https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance (December 2021)

[9] 'Alert: Apache Log4j vulnerabilities', NCSC, https://www.ncsc.gov.uk/news/apache-log4j-vulnerability (10th December 2021)

[10] 'Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation', Microsoft, https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/ (11th December 2021)

後、Yellow Nix（別名 MuddyWater、MERCURY）[11]が、IT サポート・管理製品である SysAid の脆弱性を悪用し、イスラエルの組織にアクセスしたことが、Microsoft の報告で明らかになった [12]。未対策の Log4j インスタンスは依然として悪用されているが、CVE-2022-41040 や CVE-2022-41082（総称して ProxyNotShell として知られている）を含む、他の有名な脆弱性 [13]と同様に、Log4Shell の日常的な悪用が広がっている可能性がある [14]。

2022 年には多くの脆弱性が公開されたが、Apache Log4j ソフトウェアの汎用性、影響を受けるシステムの特定の困難さ、脆弱なシステムをスキャンしてアップデートやパッチが適用されていないシステムを見つけ出して悪用し続ける脅威アクターにより、Log4Shell の重大性が最も際立った 1 年となった。Log4Shell の影響は、仮に防御者の優れた対応と国際的なセキュリティコミュニティの協力的な取り組みがなされなければ、はるかに酷い状況に陥ったと思われる。

11 *Note:* We documented one such example in *CTO-TIB-20221007-01A - Yellow Nix with a new access trick, alongside PowerShell scripts*.

12 'MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations', Microsoft, https://www.microsoft.com/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations/ (25th August 2022)

13 'Alert AA22-117A - 2021 Top Routinely Exploited Vulnerabilities', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-117a (27th April 2022)

14 *CTO-QRT-20221003-01A - ProxyNotShell*

ロシアによるウクライナ侵攻

2022 年 2 月 24 日、ロシアがウクライナへの侵攻を開始し、空爆とミサイル攻撃によりウクライナのインフラ設備を襲った [15]。この侵攻までに、ロシア政府の攻撃的な主張は何カ月にもわたりエスカレートしていた。また、2014 年のロシアによるクリミア半島併合や、ウクライナ東部地域における、ロシア政府の支援による自称ルハンスク人・ドネツク人民共和国の事実上の分離など、ウクライナの領土保全は長年侵害されてきた。また、この侵攻により、北大西洋条約機構（NATO）への加盟申請が発生するなど、2022 年を通じてより広範な地政学的影響をもたらす展開となった [16]。

ウクライナは過去 10 年にわたり、ロシアを拠点とする脅威アクターから執拗に標的とされてきた。特に、2015～2016 年には、ウクライナの電力網に対して無数のサイバー攻撃がなされた。Blue Echidna（別名 Sandworm）による NotPetya 攻撃は、当初ウクライナの金融管理アプリケーションに対するランサムウェアと考えられていたが、後に破壊的ワイパー型マルウェアであることが判明し、標的となったソフトウェアを使用していた企業はウクライナにとどまらず壊滅的影響を受けた [17]。

2022 年 1 月にロシアのワイパーがウクライナの標的の間で広がり始める中、NotPetya の記憶はウクライナに重くのしかかり、侵攻の最初の数カ月間も続いたものの、ウクライナおよび他国政府、セキュリティ業界のパートナーの努力により、その影響は抑えられ、予想よりもはるかに限定的であった [18]。特に、ロシアを拠点とする脅威アクターは、侵攻開始から 5 日間、ウクライナ国防省および国内最大の民間銀行である PrivatBank を集中的に狙った [19]。NotPetya の際と同様に、世界中の多くが、サイバー活動が紛争地域を越えて大規模に広がっていく可能性を危惧したものの、それが 2022 年末までに実現することはなかった。

---

15 *CTO-SIB-20220224-01A - Tensions escalate into invasion*

16 *CTO-SIB-20221102-01A - NATO expansion - Finland and Sweden's changing cyber threat landscape*

17 *CTO-SIB-20220127-01A - Russia and Ukraine: on the brink*

18 'ESET Research jointly presents Industroyer2 at Black Hat USA with Ukrainian government representative', ESET, https://www.eset.com/int/about/newsroom/press-releases/events/eset-research-jointly-presents-industroyer2-at-black-hat-usa-with-ukrainian-government-representativ/ (25th August 2022)

19 'Ukraine defence ministry website, banks, knocked offline', Reuters, https://www.reuters.com/world/europe/ukraine-reports-cyber-attack-defence-ministry-website-banks-tass-2022-02-15/ (15th February 2022)

2022 年 1 月

ロシア、White Ursia に関与した 14 人を逮捕（p.16）
PwC が Blue Dev 7 と関連付けているワイパーの解析（p.12）
Blue Otso フィッシング活動の解析（p.16）
DDoS 代行（DDoS-for–hire）サービスとして Blue Kurama が浮上（p.19）
ウクライナのセキュリティサービスに届いた爆弾予告メールの解析（p.11）

2022 年 2 月

ロシアによるウクライナ侵攻開始（p.8）
Viasat 衛星ネットワークへの攻撃（p.11）
Hermetic ワイパーの解析（p.12）
さまざまな対応を見せる犯罪者（いずれかに加担／中立を表明）（p.16）
ロシアへの制裁措置として一部ロシア金融機関を SWIFT から排除（p.10）

2022 年 3 月

CaddyWiper と ControlZero ワイパーの解析（p.12-13）
Blue Callisto・Blue Dev 4 フィッシング活動の解析（p.15-16）
Blue Cronus 内部チャットのリーク（p.17、45）

2022 年 4 月

StarWiper の解析（p.13）
Blue Echidna が CaddyWiper と使用した Industroyer 亜種および Blue Athena が実行した CaddyWiper 亜種の開示（p.11）
Blue Callisto のインフラ解析（p.15）

2022 年半ば

Dark Crystal RAT の分析（p.18）
Blue Kurama、DDoS 攻撃を継続（p.19）
Blue Kurama、GreyAres から攻撃を受けたとの噂（p.19）

2022 年末

Blue Kurama による DDoS 攻撃の継続（p.19）
Blue Otso によるフィッシングの継続（p.16）
Blue Lelantos の活動は年間を通じて休止状態（p.17）

例外的に一部のウクライナ国外の組織に影響を与える事例もあったものの、全体として、ロシアを拠点とする脅威アクターは目前の紛争地域における妨害活動に集中していた。ただし、ロシアを拠点とする脅威アクターによるより幅広いフィッシング活動は、世界中の国々や組織を標的として行われ、ウクライナに関連した内容をおとりに用いた事例も見られた。

以下のセクションでは、妨害工作、フィッシング工作、サイバー犯罪を行う脅威アクターやそのテクニックの共通部分など、戦争に至るまでと戦争突入後におけるサイバー脅威アクターやその活動に関する、注目すべき事象や傾向を詳述する。

脅威アクターによる活動の影響を予想していた多くの国家機関は、Blue Athena（別名 APT28、FANCY BEAR）や Blue Kitsune（別名 APT29、COZY BEAR）などの脅威アクターの主要ツール、戦

術・技術・手順（TTP）に幅広く対応する軽減策についてアドバイスを発表した [20,21]。民間部門もこうした取り組みに貢献し、Mandiant[22]とDragos[23]の例では、集団的に運用・制御テクノロジー（OT）システムを標的とした破壊的手法を明らかにし、防御者を支援してみせた。

西側諸国による制裁措置と対応

ロシアのウクライナ侵攻に対して、西側諸国では一連の制裁措置が取られ、市民から非難の声も上がった。こうした措置は、ロシアに経済的影響をもたらした。ウラジミール・プーチン大統領や高位の政治家・官僚などの個人や組織に対して、さまざまな制裁が課されたのである。侵攻開始直後、一部のロシア系金融機関は、グローバルの主要決済メッセージシステムであるSWIFTのネットワークから排除された [24,25]。EU加盟国、英国、米国その他の国々は、サプライチェーンの制限などのかたちでロシアに対する制裁をさらに強め、多数の海外ブランドが、倫理的配慮や市民感情を理由に、ロシアでの事業活動の一時停止または撤退を決定した [26]。

一部の戦略的セクターにおいて、これらの制裁はロシアの重要部品やテクノロジーへのアクセスに打撃を与えることとなり、ロシアは以後、代替部品や不正なサプライチェーンの利用といった代替策を模索し始めている。ロシアがこの戦争を長期化させ、孤立を深めていく中で、PwC は、ロシアを拠点とする諜報目的の脅威アクターは、経済諜報活動による国内生産能力の支援や、ウクライナへの連帯を表明した組織・国家に対する報復へと方針を変更していくと予想している [27]。

本レポートの「今後の展望」セクションにおいて、こうしたシナリオがいかに現実のものとなるかや、具体的なセクターや国々への影響について検討している。

---

20 'NCSC advises organisations to act following Russia's attack on Ukraine', NCSC, https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences (18th March 2022)

21 'Alert AA22-110A - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (20th April 2022)

22 'INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems', Mandiant, https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool (13th April 2022)

23 'PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems', Dragos, https://hub.dragos.com/whitepaper/chernovite-pipedream (13th April 2022)

24 'Joint Statement on Further Restrictive Economic Measures', The White House, https://www.whitehouse.gov/briefing-room/statements- releases/2022/02/26/joint-statement-on-further-restrictive-economic-measures/ (26th February 2022)

25 *CTO-SIB-20220228-01A - Implications of isolation*

26 *CTO-SIB-20220825-01A - Sanctions and sectoral impact*

27 *CTO-SIB-20220825-01A - Sanctions and sectoral impact*

妨害工作と重複

ウクライナにおけるロシアの侵攻においては、情報工作からウクライナの情報通信システムを弱体化させることを目的とした破壊工作まで、さまざまな妨害活動が一貫して確認された。2022 年 2 月に発生した Viasat 衛星通信ネットワークへのサイバー攻撃は、ロシアを拠点とした活動であり、ロシアの攻撃開始と同時期に開始された。これは、サイバー脅威アクターが軍による物理的攻撃を戦術的に支援した顕著な例であり、より長期的な戦略的意味合いを持つものである [28,29,30, 31]。

侵攻に先立つ 2022 年 1 月下旬から 2 月、ウクライナのセキュリティサービスに届いた爆弾予告メールのサンプルを PwC で解析したが、これらはウクライナにおける日々の活動を妨害することを目的とした、ロシアを拠点とする脅威アクターが発信したものと評価している [32]。2022 年 2 月下旬以降、こうした情報操作は、ソーシャルメディア上で顕著に見られるように、さまざまなチャネルにおいて、親ロシア派と親ウクライナ派双方の主張に説得力を持たせるべく、拡大の一途にある [33]。侵略以降のサイバーによる情報操作を含むネット上の活動は、ハクティビズムの復活タイミングと合致していた。

ワイパー型マルウェア

ウクライナへの侵攻が続く中、ロシアを拠点とする多くの脅威アクターが、ウクライナ企業に対して破壊的なマルウェアを展開した [34]。PwC による入手可能なサンプルの分析や、セキュリティ業界の他社が発表した調査から、ロシアを拠点とする複数の脅威アクター間でコードが重複している事例およびコードを共有している可能性を示す指標が見つかった。例えば、2022 年 4 月、リサーチャーは PwC が Blue Echidna として追跡調査している脅威アクターによる活動を確認し、Industroyer の亜種が CaddyWiper サンプルとともにウクライナのエネルギー組織を標的として使用されていることが判明した [35,36]。また、Mandiant のリサーチャーは、PwC が Blue Athena として追跡調査している脅威アクターが、CaddyWiper の亜種をウクライナの組織に対して実行したと示した [37]。ロシア政府がウクライナへの攻撃を中心とした戦略的優先事項を掲げていることを考えると、集団間の争いやセキュリティ・インテリジェンスサービス間の歴史的な対立にもかかわらず、ロシアを拠点とする脅威アクターがマルウェアや能力を互いに共有する、あるいは情報交換している可能性は高いと思われる。

---

28 *CTO-WTU-20220513-01A - Ukraine Weekly Report*

29 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union', European Council, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high- representative-on-behalf-of-the-european-union/ (10th May 2022)

30 'Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion', UK Government, https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion (10th May 2022)

31 'Attribution of Russia's Malicious Cyber Activity Against Ukraine', US Department of State, https://www.state.gov/attribution-of-russias- malicious-cyber-activity-against-ukraine/ (10th May 2022)

32 *CTO-QRT-20220224-01A - Wiping and disruption in Ukraine*

33 *CTO-WTU-20220311-01A - Ukraine Weekly Report*

34 'Wipermania: An All You Can Wipe Buffet', Trellix, https://www.trellix.com/en-us/about/newsroom/stories/research/wipermania-an-all-you-can-wipe-buffet.html (15th November 2022)

35 'Industroyer2: Industroyer reloaded', ESET, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (12th April 2022)

36 *CTO-WTU-20220414-01A - Ukraine Weekly Report*

37 'GRU: Rise of the (Telegram) Mini0ns', Mandiant, https://www.mandiant.com/resources/blog/gru-rise-telegram-minions (23rd September 2022)

PwC による情報の可視化・収集に基づき、以下のワイパーを分析した。

WhisperGate ワイパー

侵攻に先立つ 2022 年 1 月 15 日、Microsoft は WhisperGate として追跡調査している破壊的マルウェアに関するレポートを発表した [38]。これは、PwC が Blue Dev.7 と関連付けているマルウェアである。WhisperGate は、マスター・ブート・レコード（MBR）の上書きとファイル破損段階で構成される、複数の攻撃段階を組み合わせたものである [39]。WhisperGate が最初に発見された際、その挙動や設計から当初はランサムウェアと思われた。しかし、従来の金銭目的のランサムウェアと異なり、その破損プロセスは不可逆的なものであった。つまり、脅迫ではなく妨害目的のマルウェアということである。さらに、WhisperGate の主な標的は、ウクライナ政府組織およびウクライナ政府にサービスを提供しているテック企業少なくとも 1 社であった。

Hermetic ワイパー

ロシアによる侵攻と時を同じくして、PwC では最初のレポート公開後に Hermetic ワイパーを分析した。このワイパーは、ウクライナのインフラを標的として、攻撃が成功した場合には、感染したコンピュータのパーティションを消去して操作不能にするものである。このバイナリは、EaseUS Partition ファイルをドロップしてワイプ活動を行うが、Windows のアプリケーション・プログラミング・インターフェース（API）を使用してファイルをワイプすることも可能である [40]。

CaddyWiper

2022 年 3 月半ば、セキュリティリサーチャーがウクライナの環境で CaddyWiper が実行されているのを発見した [41]。このワイパーは、端末がプライマリドメインコントローラーでない場合、そのシステム内のファイルを消去し、最終的には、マッピングされた全ての物理ドライブのファイルを消去する機能が含まれていた。PwC は、CaddyWiper の背後にいる脅威アクターは、おそらく Portable Executable (PE)内の Rich ヘッダを操作して、本来の開発フィンガープリントを隠蔽したと評価している [42]。他のセキュリティリサーチャーは、CaddyWiper を、Olympic Destroyer などにおいて Rich ヘッダを操作することで知られる脅威アクターとして PwC が追跡調査している Blue Echidna と関連付けている [43]。

---

38 'Destructive malware targeting Ukrainian organizations', Microsoft, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (15th January 2022)

39 *CTO-TIB-20220121-01A - The WhisperGate Wiper*

40 *CTO-QRT-20220224-01A - Wiping and disruption in Ukraine*

41 @ESETResearch, Twitter, https://twitter.com/esetresearch/status/1503436420886712321 (14th March 2022)

42 *CTO-QRT-20220315-03A - CaddyWiper hits Ukraine*

43 'The devil's in the rich header', Kaspersky, https://securelist.com/the-devils-in-the-rich-header/84348/ (8th March 2018)

ControlZero ワイパー

2022 年 3 月半ば、PwC はファイルの削除に NtFsControlFile API を利用していることから 4 番目のワイパーを ControlZero（別名 DoubleZero）[44]と命名し、これがウクライナのネットワーク上で破壊活動に用いられていた可能性があると評価した。PwC の分析では、ControlZero は影響を受けたシステムからレジストリキーを削除することが確認された。そのシステムは最終的に、重要なシステムリソースが変更されたため再起動を促した [45]。PwC の観察によれば、これはさらなる破壊を引き起こすためにレジストリキーを削除する 2022 年最初のワイパーであった。

StarWiper

2022 年 4 月、PwC は、StarWiper（別名 ACIDRAIN）[46]と名付けた別のワイパーを解析した。そのワイパーは MIPS（Microprocessor without Interlocked Pipeline Stages）アーキテクチャを前提としていたため、デスクトップデバイスではなく組み込みデバイスを標的としたものと思われる。このワイパーは、ウクライナ人を蔑称するロシア語のファイル名を使用していたため、PwC は、可能性は高くないもののロシアのウクライナ侵攻との関連性を疑っている。StarWiper が、実際にロシアを拠点とする脅威アクターの「ワイパー武器庫」の中からウクライナに対して展開されたものだった場合、破壊的マルウェアが、従来のようなデスクトップデバイスから組み込みデバイスへと標的を変化させていることを示すものである [47]。

[44] 'CERT-UA#4243 - Кібератака на українські підприємства з використанням програми-деструктора DoubleZero', Computer Emergency Response Team of Ukraine (CERT-UA), https://cert.gov.ua/article/38088 (22nd March 2022)

[45] *CTO-QRT-20220222-02A - ControlZero added to the wiper list*

[46] 'AcidRain | A Modern Wiper Rains Down on Europe', Sentinel One, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ (31st March 2022)

[47] *CTO-TIB-20220405-01A - StarWiper*

PwC が分析したワイパー（MITRE ATT&CK）

ロシアのウクライナ侵攻に関連して PwC は 5 つのワイパー（WhisperGate、Hermetic、CaddyWiper、ControlZero、StarWiper）を分析し、それぞれが採用した戦術（内側の円）とテクニック（外側の円）を MITRE ATT&CK のフレームワーク上にマッピングした。

以下の円では、PwC の脅威インテリジェンスレポートおよび検出規則で対応した、これらの戦術とテクニックの検出範囲を視覚化している。各色は異なる戦術とそれぞれのテクニックを表し、各ラベルの横には、PwC 保有の該当する検出規則および／またはレポートの数を示している。ダークグレイの 5 つのテクニックは、PwC が守備範囲としていない領域を示している。脅威に用いられる戦術とテクニックのマッピングは、どのように可視化しても、防御者が守備範囲のギャップや弱点を特定するのに役立つだろう。さらに、組織のリスク評価と合わせて、検出バックログの優先順位付けに用いることも可能である。

フィッシング活動

ロシアを拠点とする脅威アクターは、侵攻に至るまでも侵攻後も、ウクライナの組織その他を標的として、幅広いフィッシング活動を行った。こうした活動は主にウクライナ政府・軍を標的としていたが、ロシアを拠点とする脅威アクターは、より幅広い対象を標的としており、その一部については情報開示により暴露された。ロシアを拠点とする脅威アクターはそうした情報開示への対応でも素早い動きを見せ、民間・政府のセキュリティ組織両方から追われている状況にあって、素早く適応して効果的な活動を継続する能力を示した。例えば、2022 年 3 月初旬、PwC が Blue Athena として追跡調査している脅威アクターに関わるインフラ情報を Google TAG[48]が開示したわずか 1 日後、当該脅威アクターは以前のフィッシングサイトから複製したコードを再利用して、新たなフィッシングドメインを作成したのである [49]。

ロシアを拠点とする脅威アクターによるフィッシング活動の別例として、Blue Callisto（別名 Callisto Group）は、ウクライナのある流通・配送会社を標的とした。この会社は、商業的活動に加えて、ウクライナへの人道支援物資運搬も行っていた。Blue Callisto は、欧米の組織に対しても認証情報の窃取キャンペーンを仕掛けるなど、おそらくロシア政府の意向を受けたと思われるそのダイナミックな活動内容が際立っていた [50]。2022 年 12 月、PwC は Blue Callisto がウクライナ人道支援物資の提供からウクライナにおけるロシアの活動調査まで、さまざまなかたちの支援を提供するその他組織も標的としたことのエビデンスを特定した [51] 。

Blue Callisto のインフラ追跡

2022 年 4 月、PwC は Blue Callisto（別名 Callisto Group）のドメインを分析した結果、共通のインフラパターンを発見し、同インフラのネットワークがさらに広がりを見せていることが明らかになった。この脅威アクターはおそらく、このインフラを利用して、ウクライナ軍をテーマとしたフィッシングキャンペーンを実施した可能性が高いと評価している [52]。2022 年 9 月には、Blue Callisto のさらなる追跡テクニックと、このアクターが米国内の研究施設に関心を示していることを突き止めた [53] 。

Blue Callisto の詳細について 2022 年に投稿したブログ記事

また PwC は Blue Dev 4（別名 Ghostwriter、UNC1151）の分析過程で、脅威アクターに関連している可能性が高いと評価している Word 形式ドキュメントを特定した。ファイル名に Ghostwriter のリファレンスが含まれていたためである。このドキュメントには、ウクライナ軍に関連する個人名、組織名、電子メールアドレスリストが含まれており、そのリストには Blue Dev 4 が関心を寄せる標的が含まれ

[48] 'An update on the threat landscape', Google TAG, https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/ (7th March 2022)
[49] *CTO-TIB-20220411-01A - Blue Athena 2022 phishing part 2*
[50] *CTO-SIB-20220908-01A - Ukraine Threat Update - August 2022*
[51] *CTO-SRT-20221213-01A - Blue Callisto targets Ukraine-linked organisations*
[52] *CTO-TIB-20220511-01A - Tracking Callisto infrastructure*
[53] *CTO-TIB-20220913-02A - Blue Callisto still phishing*

ている可能性が高いと評価している。リストには、ウクライナの軍服・機器・装備品を扱う店舗の Web サイトオーナー、ザポリジシア地方に拠点を置くウクライナ海軍 A1965 部隊、国内防衛機関に所属する複数のリサーチャー、ヴィニツィア地方のウクライナ予備役が含まれていた [54]。Blue Dev 4 による標的設定のアトリビューションより、さまざまな被害者への幅広い無差別的な標的設定から、特定の標的に被害を与えようと執拗かつ継続的に行うものまで、さまざまなアプローチを取っていることが判明した。

また、2022 年 1 月に見られた Blue Otso（別名 Gameredon Group）のフィッシング活動を分析した。侵攻前夜、ロシアとウクライナの間で緊張が高まる中、Blue Otso はスピアフィッシング活動において、武器化したドキュメント内にセベロドネツク（ウクライナの都市）やクリミアをおとりとして使用し、自己解凍アーカイブと UltraVNC バイナリに誘導した。セベロドネツク、クリミアともに地政学上の重要地点である。前者は、ロシアの庇護を受けた分離主義派 LPR が支配していた領土に接するルハンスク州に位置する戦略都市であり、後者は 2014 年以降、ロシアによる併合下にある [55]。2022 年後半、Blue Otso は、2020 年の活動時に PwC が特定した電子メールを使用して再びドメインを登録した。このドメインはウクライナの国家特殊通信・情報保護局をテーマとするものであったが、ドメインは以前の Blue Otso 活動と比べて異なる形式であった。2022 年まで、Blue Otso は、特定のテーマを有さないワードリストを使用した自動化プロセスによってドメイン登録を行っていたと考えられる [56]。また、Blue Otso は、自動化された活動だけでなく、別途、手動による活動も継続していた模様である。2022 年、Blue Otso のインフラ管理は多様化し、よりダイナミックなものとなり、コマンド＆コントロール（C2）ドメインは、新たな IP アドレスに対応すべく毎日変更されていた。

サイバー犯罪への防戦態勢

ロシアのウクライナ侵攻により、東欧のサイバー犯罪者がこの戦争にどのようなスタンスをとるのか、特にどちら側につくのか、新たに注目が集まった。侵攻に先立ち、2022 年 1 月中旬、ロシア政府は、REvil または Sodinokibi として知られるランサムウェアのアフィリエイトプログラムを掌握する脅威アクター、White Ursia への関与の疑いで 14 名を逮捕したと発表した。この発表により、一部のサイバー犯罪者は標的を再考することとなった。逮捕者のうち少なくとも 1 名は、2021 年 5 月に発生した White Apep（別名 DarkSide、BlackMatter）による米 Colonial Pipeline へのランサムウェア攻撃にも関与していると指摘されている [57]。2022 年 2 月のロシアによるウクライナ侵攻後、サイバー犯罪者の間で、ロシアへの制裁措置によって不正な活動による脅迫、資金洗浄、現金化能力に影響が出ることへの懸念が高まったものの [58]、全体的には、従来と変わらずサイバー犯罪は続いた。

---

54 *CTO-QRT-20220303-01A - Blue Dev 4 phishing operations in 2022*

55 *CTO-TIB-20220203-01A - Blue Otso retains Ukraine interest*

56 'ACTNIUM targets Ukrainian organizations', Microsoft, https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/ (4th February 2022)

57 *CTO-SIB-20220211-01A - White Ursia, from Unknown to under the bus*

58 *CTO-SIB-20220915-02A - Tales from the crypto*

著名なサイバー犯罪組織を効果的に抑制する制裁措置

2021 年、バンキング型トロイの木馬である Dridex や、BitPaymer、DoppelPaymer、Grief、Wasted Locker といったランサムウェアシステムを用いる脅威アクター、Blue Lelantos（別名 Evil Corp）は、ランサムウェア活動のリブランドを複数回試みた。この脅威アクターに対する米国の制裁措置に呼応して、保険会社およびランサムウェア専門交渉者によって「ブラックリスト」入りしたためである。Blue Lelantos は、2022 年にはより抜本的な活動の方向転換を余儀なくされていることから、PwC は以下の見解に基づき、こうしたリブランドの試みは失敗に終わった可能性が高いと評価している：

- かつて Evil Corp の主力であった Dridex による活動が縮小した
- 2022 年には、既存の Blue Lelantos ランサムウェア亜種の新たなリブランドは観察されなかった
- 他のセキュリティリサーチャーは、Blue Lelantos の一部がライバルのランサムウェアスキームに登録しようとしたことを報告している [59]

かつて悪名高いサイバー犯罪組織であった Blue Lelantos の活動が 2022 年を通じて休止したことから、少なくともこの事例では、制裁とテイクダウン [60] が、知名度の高いサイバー犯罪活動に大きな打撃を加える有効手段であることが示された。

2022 年 2 月、Blue Cronus によるランサムウェア Conti は、ロシアのウクライナ侵攻への支持を宣言し、反ロシア諸国の重要インフラを標的にするという脅迫をリークサイトに直接投稿した。一方、他のサイバー犯罪脅威アクターである White Janus（別名 LockBit）や White Dev 101（別名 ALPHV-ng、BlackCat）は、自身の動機が純粋に金銭目的であることを強調し、戦争に関してある程度の中立性を表明した [61]。イデオロギー的なスタンスの違いにかかわらず、ロシアを拠点とするランサムウェアの脅威アクターは、ロシア政府から協力を受け、あるいは強要され、ロシアを支援する活動を行う立場にある可能性が高いと PwC では評価している。

[59] 'To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions', Mandiant, https://www.mandiant.com/resources/blog/unc2165-shifts-to-evade-sanctions (June 2022)

[60] 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)

[61] *CTO-SIB-20220301-01A - Cyber criminal and hacktivist response*

ウクライナにおける Dark Crystal RAT の活動

ロシアのウクライナ侵攻開始以来、金銭目的やスパイ活動を目的とするさまざまな脅威アクターが、標的環境への足がかりを得るためのテーマとしてこの侵攻を利用してきた。ある攻撃では、Dark Crystal RAT（金銭的な動機による活動で通常見られるリモートアクセス型トロイの木馬（RAT））が用いられた。関連する悪意ある Excel ファイルには、ウクライナ国家緊急事態省に関わる情報およびマクロが含まれており、ウクライナ政府関連組織を標的とするために使用された可能性が高い[62]。Dark Crystal RAT を用いた脅威アクターは、その後、ロシア協力者に関連した、ウクライナをテーマにした別のおとり文書で復帰し、その文書により、金銭目的の脅威アクターと関連付けられることの多い別のマルウェア亜種である WarZone RAT を実行した。

Dark Crystal RAT の検出

URI（Uniform Resource Identifier）

\.php\?type=__ds_setdata&__ds_setdata_user=[a-f0-9]{40}&__ds_setdata_ext=[a-f0-9]{32}&__ds_setdata_data=

\.php\?type=__ds_getdata&__ds_getdata_user=[a-f0-9]{40}&__ds_getdata_ext=[a-f0-9]{32}&__ds_getdata_key=[a-f0-9]{32}$

COMSurrogate

Dark Crystal RAT は、ユーザーが権限昇格でログオンすると、タスク COMSurrogate を起動する（MITRE ATT&CK T1053.005 - Scheduled Task/Job: Scheduled Task）[63]

また、b64 エンコードされた powershell コマンドを実行し、以下の検出トリガーとなる（MITRE ATT&CK T1140 - Deobfuscate/Decode Files or Information および T1059.001 - Command and Scripting Interpreter：PowerShell）：
[0934]-[evasion]-[m]-powershell_executing_base64_encoded_commands
[0942]-[execution]-[m]-powershell_with_abbreviated_noprofile_switch
[0931]-[execution]-[m]-powershell_with_abbreviated_executionpolicy_bypass_switch

金銭目的の脅威アクターが侵攻に関わるストーリーを用いる、あるいは回避する中で、ハクティビズムに影響を受けた脅威アクターと対話者も現れ始め、親ロシア派と親ウクライナ派の情報操作合戦は一層複雑な様相を示している。例えば、PwC が Grey Ares として追跡調査している Anonymous 集団や、IT Army of Ukraine[64]、Network Battalion 65（別名 NB65）に属する自称親ウクライナ派のハ

[62] *CTO-TIB-20220616-01A - Opaque Dark Crystal RAT activity in Ukraine*
[63] *CTO-TIB-20220616-01A - Opaque Dark Crystal RAT activity in Ukraine*
[64] *CTO-SIB-20220301-01A - Cyber criminal and hacktivist response*

クティビストアカウントが登場した。[65]また、PwC が Blue Kurama[66] として追跡調査している親ロシア派ハクティビスト集団は、リトアニアの主要インフラ、ノルウェーの著名な公共・民間機関 [67]、ラトビア議会、エストニアの公共 Web サイト [68]に対する複数の分散型サービス妨害（DDoS）攻撃でその名をはせた。Blue Kurama の活動は、ロシアの行動に批判的で、紛争地域外に位置する公共・民間組織を DDoS の標的としていたため、2022 年に注目を集めた。ただし、同キャンペーンは、広く報道された一方で、効果としては、他の種類のサイバー攻撃に比べてその影響は大きくなかった [69]。

Blue Kurama 騒動

Blue Kurama（別名 Killnet）は、ウクライナ侵攻中に出現した、親ロシア派または親ウクライナ派の利益を支持するさまざまな「愛国主義的ハッキンググループ」の一例に過ぎない。Blue Kurama は特にロシアを支持する姿勢を示しており [70]、ロシアの国益に反すると考えられる国（ルーマニア [71]、イタリア [72]、リトアニア、ノルウェー[73]、米国 [74] など）から、主にウクライナの公共・民間組織、特に重要インフラや防衛に関連する組織への DDoS 攻撃を行った。Blue Kurama は当初、2022 年 1 月に DDoS 代行サービス「DDoS-for-hire」として、ロシアに拠点を置く、ロシア国籍を自称する個人（オンライン上のニックネームは「Killmilk」）により設立された。その後、代行型から自ら標的を定め攻撃するようになるにつれ、この脅威アクターは主にロシア語の Telegram チャネルを通じてその活動と勧誘を活発化させた。多くの公開フォーラムで、Blue Kurama は 2022 年に Mirai ボットネットを使用して DDoS 攻撃を行ったことが報告されている。2022 年 5 月、Blue Kurama は Grey Ares（別名 Anonymous）が仕掛けたとされる攻撃を受けた [75]。

全体として、Blue Kurama による攻撃は、成功したとしてもその大半が短期間のものであり、重大かつ継続的な影響をもたらすものではなかった。しかし、この脅威アクターの攻撃と意図は、大きな破壊につながる可能性を秘めたものであり、今後侵攻が継続した場合や他の紛争が発生した場合には、こうしたハクティビズム活動が増加する可能性があるという注意喚起となる。

---

[65] *CTO-SIB-202220707-01A - Ukraine Threat Update - June 2022*
[66] *CTO-TIB-20221208-02A - Not cool Killnet*
[67] *CTO-SIB-202220707-01A - Ukraine Threat Update - June 2022*
[68] *CTO-SIB-20220908-01A - Ukraine Threat Update - August 2022*
[69] *CTO-TIB-20221208-02A - Not cool Killnet*
[70] *CTO-TIB-20221208-02A - Not cool Killnet*
[71] *CTO-WTU-20220505-01A - Ulraine Weekly Report*
[72] *CTO-WTU-20220513-01A - Ulraine Weekly Report*
[73] *CTO-SIB-20220707-01A - Ukraine Threat Update - June 2022*
[74] *CTO-SIB-20220804-01A - Ukraine Threat Update - July 2022*
[75] *CTO-WTU-20220526-01A - Ulraine Weekly Report*

中国を拠点とする脅威アクターによる活動の最適化

2022 年を通じて、脅威アクターは共有ネットワーク、インフラ、能力を中心に合体し、多くの場合、これまでよりも合理的で拡張性があり、技術的にも洗練された活動を行うようになった。PwC もこうした傾向を数年前から分析しているが [76, 77] 、2022 年には、obfuscation-as-a-service（難読化サービス）プロキシネットワークを含む共有エクスプロイトとツールの急増が観察された。PwC による脅威アクターの標的パターン分析ではさらに、脅威アクターがデジタルサプライチェーンやハイテク部門への侵害、特に通信セクターの組織を引き続き主な標的とするだけでなく、特定の国を標的とした活動も行っていたことが明らかになった。

これらの標的は目新しいものではないが、中国を拠点とする脅威アクターは、その活動を最適化するとともに共有プロキシリソースを活用するようになっており、アトリビューション、インシデント対応、被害評価に関する従来型手法に挑んでいる。

さらに、2021 年後半から、複数の脅威アクターがマルウェアのペイロードを難読化する事例が多数確認されたが、これは検出を回避し、分析を妨害するために用いられた可能性が非常に高いと考えられる。特に、Red Lich（別名 Mustang Panda、Temp.Hex、TA416）は、欧州の企業を標的としたキャンペーンにおいて、ローダーと内部の PlugX ペイロードの両方に LLVM ベースの難読化を使用していた。LLVM やその他の難読化手法の使用は新しいものではないが、これらは従来、ローダーコンポーネントにのみ適用され、ペイロード自体には適用されてこなかったものである。

この進化は、YARA シグネチャや静的・動的解析ツールを用いた人手での分析により従来は検知できた未知のペイロードについて識別して、リバースエンジニアリングする試みをさらに困難にする。カスタムツールや特注ツールにこのような保護レイヤーを追加することで、攻撃者は防御側が改善を図ったとしても、キャンペーンの寿命を延ばすことが可能となる。

個々の脅威アクターがカスタムマルウェアに難読化を採用しているような活動レベルにおいて、また脅威アクターに提供されたマルウェアがクォーターマスターによって容易にパッケージ化または難読化されているような開発者レベルにおいて、難読化とペイロード保護という傾向は継続し、高度化していくと予想される。

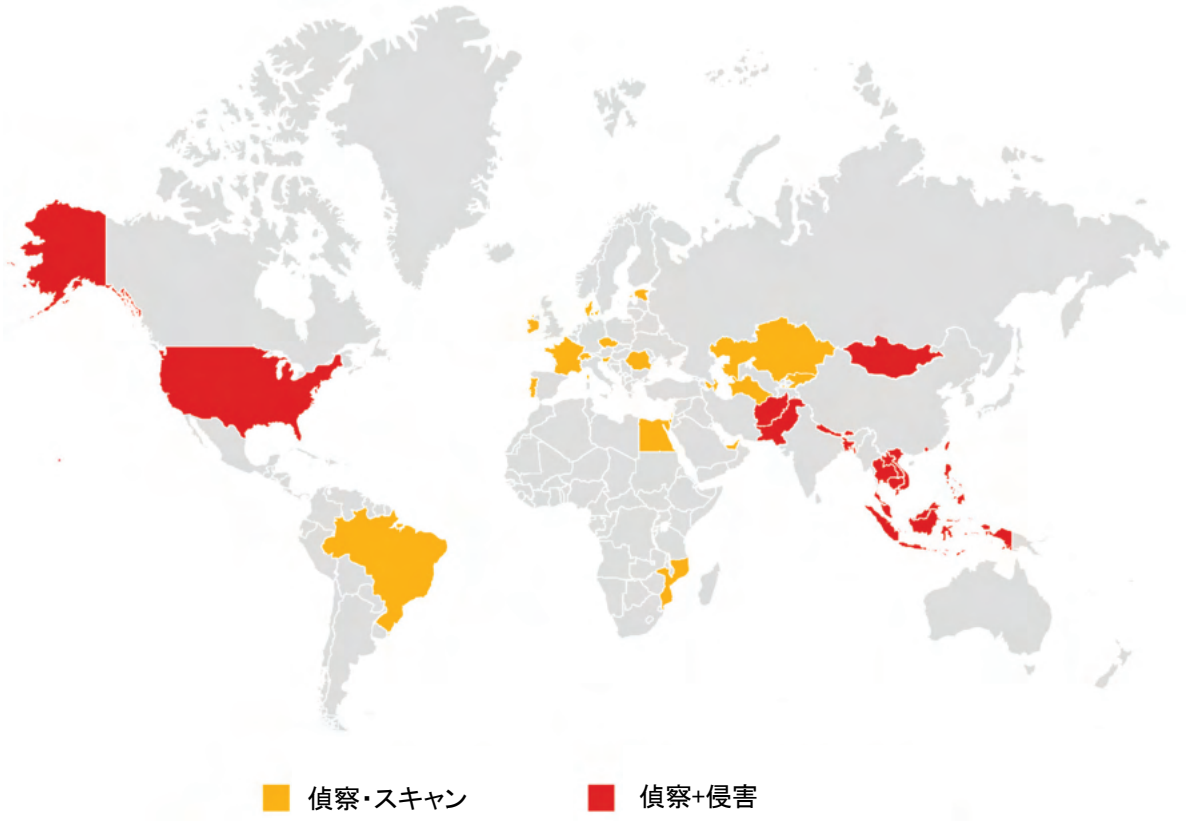
[76] 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence, https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf (17th December 2020)

[77] 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)

Winntiと連動した世界規模の脅威：Red Scylla

2022年8月、PwCはRed Dev 10として追跡調査していた活動にRed Scylla（別名CHROMIUM、ControlX、Earth Lusca、Aquatic Panda）を割り当てた[78]。その主な理由は、一連のインフラとテクニックに顕著な特徴が見られると判断したためである[79]。Red Scyllaは、2022年に最大の猛威を振るった中国を拠点とする脅威アクターであり、その世界規模の標的設定や最適化された活動ペース、洗練度から、PwCはRed Scyllaを中国発の最も活発な脅威アクターと見ている。

2022年におけるRed Scyllaの標的



PwCは、Red Scyllaが脆弱性をスキャンし、オープンソースツールのAcunetix[80]を使用するとともに、ShadowPadやPlugXなどのこれら脅威アクターの間で一般的に共有されているカスタムバックドアとツールの両方を含む、侵害後に悪用する多様なツールセットを導入していることを確認した。2021年以降、PwCはShadowPad[81]のユーザーとしてRed Scyllaを追跡調査してきた。Red Scyllaは主に、PwCが ScatterBee[82]と名付けたカスタム難読化手法（コントロールフロー難読化、ガードレール、ランタイムパッチを使用）によりフォレンジック分析を妨害している。世界中のさまざまなセク

[78] Please see *Appendix B – Threat actor reference* for more information about our naming convention.
[79] *CTO-TIB-20220825-01A - Red Scylla: A Winnti-Linked Global Threat*
[80] *CTO-TIB-20220621-01A - Red Dev 10 - Acunetix Scanning*
[81] 'Chasing Shadows: A deep dive into the latest obfuscation methods being used by ShadowPad', PwC Threat Intelligence, https://www.pwc.co.uk/issues/cyber-security-services/research/chasing-shadows.html (8th December 2021)
[82] *CTO-TIB-20211021-01A - Chasing shadows*

ターの組織を標的としており、偵察活動から急速に進展し、被害ネットワークにアクセスし、侵入の初期段階でマルウェアを展開することで、被害環境における足場を広げようとしているものと見られる。

昨年、ShadowPad を展開した脅威アクターは Red Scylla だけではない。2022 年を通じて、ShadowPad は、このマルウェアファミリーとすでに関連付けられた脅威アクター間で使用されており、これを用いた活動クラスターも新たに特定されている。ShadowPad C2 インフラを追跡調査中、PwC は関連するインフラ管理に基づく新たなクラスターを特定した。これは現在、Red Dev 32 として追跡調査中である [83]。PwC はこの脅威アクターについて、2022 年 6 月に PlugX から ShadowPad に移行し、インフラを操作してニセの Microsoft Secure Sockets Layer（SSL）証明書を提供した可能性が高いと評価している。2022 年の後半には、Red Scylla の ORB（オペレーション・リレー・ボックス）が、Red Dev 32 の ShadowPad C2 のテスト活動に使用されているなど、Red Dev 32 と Red Scylla が重複している証拠が確認された。PwC は、この 2 つの脅威アクターが何らかのかたちで組織的関連性を有している可能性が高いと評価している。2022 年 10 月、PwC はさらに、ShadowPad のインフラを Red Dev 14 と関連付けた。複数の ShadowPad C2 ホストが、中東の政府機関から窃取された自己署名証明書を提供していたのである [84]。

TTP の共通点に対する防御

中国を拠点とする脅威アクターの間でこのような TTP の共通点があることから、防御者には、アーカイブファイルを標的とする LNK ファイルや補足コマンドライン（MITRE ATT&CK T1204.002 - User Execution: Malicious File）を監視することが推奨される。さらに、乗っ取られるアプリケーションはさまざまであるが、ダイナミック・リンク・ライブラリ（DLL）のサイドローディング（T1574.002 - Hijack Execution Flow: DLL Side-Loading）は引き続き、これらの脅威アクターによる感染において一貫して見られるテクニックとなっている。

共有プロキシネットワーク：RedRelay

2022 年を通じて、PwC は、2021 年に特定し、複数の脅威アクターによって使用されているプロキシネットワーク、RedRelay に関する調査を継続した。これらの脅威アクターは、過去数年間に共有プロキシネットワークに移行し始めており、そのような共有された秘密ネットワークは、公共または民間組織によってツールが提供、販売、共有されるクォーターマスター方式で運営されている可能性が高いと PwC は評価している。プロキシネットワークの特徴として、マルチホップのプロキシや暗号化チャネルによる通信の円滑化などがあり、従来の調査手法では分析やアトリビューションが困難となっている。プロキシネットワークはまた、脅威アクターが運営する数百台の仮想プライベートサーバー（VPS）と侵害されたデバイスの組み合わせにより構築される。

一例として、PwC は Red Vulture（別名 APT15、APT25、Ke3chang）による RedRelay の利用を分析した。Red Vulture は、2021 年から 2022 年初頭にかけて、RedRelay インフラのうち特定のクラ

[83] *CTO-TIB-20220913-01A - Red Dev 32*
[84] *CTO-TIB-20221005-01A - Not to worry; I have a certificate of authority*

スターを使用していたが、2022 年 3 月にはこのクラスターを処分して再構築し、欧州政府、汎欧州機関および国際組織に対する偵察・エクスプロイト活動を再開した。こうした変化は、Red Vulture の積極的な「運用上のセキュリティ（OPSEC）」対策を示すとともに、2022 年 2 月に観察された RedRelay インフラ管理手法の広範な変化を反映したものである [85]。

国別の標的

2022 年 1 月、PwC は Red Orthrus（別名 Keyboy、TA428、Tropic Trooper）に帰属する C2 ドメインと通信するマルウェアを分析した。このマルウェアは、オープンソースで nccTrojan として知られている RAT の 64 ビット版であった [86]。これらの nccTrojan サンプルにおける C2 ドメインのおとりテーマは、ロシアの防衛および製造セクターのニセ組織と見られる。さらに、nccTrojan ドメインをホストするインフラからさらに目を移すと、ロシアをテーマにしたドメインと Red Orthrus インフラの間でさらにクロスオーバーしていることが判明した。ある段階で、これらのドメインは全てロシアを拠点とする IP アドレスでホストされており、PwC は、脅威アクターが C2 トラフィックを標的に対して無害に見せるために、意図的にこれを構成した可能性が高いと評価している [87]。これらは、ウクライナ侵攻に先立ち、ロシア軍が動員された際の情報収集活動であった可能性が高いと PwC は評価している。

Red Phoenix（別名 APT27、Emissary Panda、LuckyMouse）は、2022 年を通じて常に活発な脅威アクターであった。2022 年 1 月、ドイツの連邦憲法擁護庁（BfV）はブログ [88] を公開し、この脅威アクターの活動や、Red Phoenix がドイツ企業を標的としていることに関する技術的な詳細情報を提供した。Red Phoenix に起因する長年のカスタムマルウェアファミリーである HyperBro および FOCUSFJORD[89] に関連するインフラやマルウェアを追跡調査した結果、2022 年の活動の大部分は、南シナ海地域を拠点とする組織を標的としていたことが分かった。

---

[85] *CTO-TIB-20220523-02A - Rampant Reconnaissance Redux*

[86] 'China-linked TA428 Continues to Target Russia and Mongolia IT Companies', Recorded Future, https://www.recordedfuture.com/china-linked-ta428-threat-group (17th March 2021)

[87] *CTO-QRT-20220315-01A - Red Orthrus targets Russia*

[88] 'Cyber attack campaign against German commercial companies', BfV, https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2022/2022-01-26-cyberbrief.html (26th January 2022)

[89] 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence, https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf (17th December 2020)

注目を集めた Red Phoenix

HyperBro

HyperBro バックドアは、長い間 Red Phoenix（別名 APT27、Emissary Panda、LuckyMouse）と関連付けられてきた。この脅威アクターは、正規のバイナリを使用して悪意ある DLL をサイドロードし、被害端末に HyperBro をドロップするという、Red Phoenix が 2015 年から採用しているテクニックを用いている。HyperBro マルウェアの特徴として、中国に拠点を置くモバイルインターネット企業である Cheetah Mobile Inc.の署名証明書が用いられている点が挙げられる。また、C2 インフラストラクチャは、一貫した反応を引き出すだけでなく、443 番ポートに SHA-1 ハッシュ値 44b9d089cf734d2478165a8539b23aed51887f7d の SSL 証明書を必ずホストしている。これまでのオンラインポートスキャンデータは、少なくとも 2019 年 6 月以降、アクティブな HyperBro サーバーの間でこうした特性が共通していることを示唆している [90]。

FOCUSFJORD

2022 年には、ユニークな難読化コード Shikata Ga Nai を含む複数の新しい FOCUSFJORD サンプルが確認されており、コンパイルのタイムスタンプは 2022 年 6 月以降となっている。これらの最近のサンプルに関連する C2 ドメインは全て、「.me」というトップレベルドメイン（TLD）を含む傾向があった。

その他のツール使用

上記に加えて、2022 年 8 月におけるオープンソースの報告では、中国のインスタントメッセージングアプリである MiMi が、Red Phoenix へのリンクとともに、rshell バックドアの ELF および Mac 亜種を取得するために使用されていたことが詳細に報告されている [91]。その後、PwC はさらなる rshell マルウェアのサンプルを特定し、一部の事例では、既知の HyperBro C2 インフラとの重複をベースに、Red Phoenix が関連インフラを制御していた可能性が高いと評価している [92]。また調査中には、HyperBro の C2 サーバーが Cobalt Strike 証明書を同時にホストしているのを発見し、一方で別の HyperBro サーバーが Fast Reverse Proxy（FRP）を同時にホストしていた [93]。

また、2022 年 1 月には、Red Lich（別名 Mustang Panda、Temp.Hex、TA416）による可能性が高いと PwC が評価しているキャンペーンに関して、地域面での標的の大きな変化について追跡調査を開始した。2020 年以降、Red Lich は、南アジアや東アジア、そして国際的な非政府組織（NGO）から政府機関まで幅広い被害者を標的としていたのに対し、このキャンペーンは、欧州の政府機関や外交機関に的を絞ったものだった。少なくとも 2022 年 1 月から 2022 年 3 月下旬、欧州に的を絞った同

[90] *CTO-TIB-20221102-01A - Rising from the hashes*

[91] 'LuckyMouse uses a backdoored Electron app to target MacOS', Sekoia, https://blog.sekoia.io/luckymouse-uses-a-backdoored-electron-app-to-target-macos/ (12th August 2022)

[92] *CTO-TIB-20221102-01A - Rising from the hashes*

[93] *CTO-TIB-20221102-01A - Rising from the hashes*

キャンペーンの第 1 段階において、Red Lich は RAR または ZIP アーカイブを用いており、タイトルには欧州問題、特定の中欧諸国、ウクライナにおけるロシアの侵攻に関連したテーマが用いられていた。

こうしたアーカイブには、被害者におとり文書をダウンロードさせる正規の実行ファイルの他、PlugX 用の Trident ローダー、無害の実行ファイル、サイドロードされる悪意ある DLL、DAT リソースにエンコードされた PlugX のサンプルも含まれていた [94]。2022 年 3 月下旬から 2022 年 10 月下旬にかけて、Red Lich は欧州企業を標的とした TTP を更新した。これは、おそらく検出回避のためであり、また、キャンペーンが公になったことへの対応とも考えられる [95]。この脅威アクターは、被害端末で PlugX を実行するための Trident ローダーを起動させる、悪意ある LNK ファイルを含む圧縮アーカイブの使用に軸足を移した。同キャンペーンの第 2 段階において、Red Lich はマルウェアに難読化および解析防止策をさらに追加した（LLVM 制御フローの平坦化など）。同キャンペーンを通じて、Red Lich は主に外交に関わる東欧・中欧政府機関や、ベルギーに拠点を置く大使館や超国家組織を標的にしていた。

脅威アクターの間で共有され、注目を集めている活動に用いられている能力の一例として、PwC は Proofpoint[96] とともに、2022 年 4 月から 2022 年 6 月まで続いた、諜報目的の ScanBox キャンペーンについて分析を行った。ScanBox は、中国を拠点とする脅威アクターの間で独自に共有されている Web 偵察とエクスプロイトのフレームワークで、少なくとも 2014 年から散発的に用いられてきた。2022 年のキャンペーンは世界規模で展開されたが、とりわけ、アジア太平洋地域の組織、オーストラリアの政府機関やメディア、グローバルの重工業メーカーを含む南シナ海で資本を有する企業や国に集中していた。PwC は、同キャンペーンを Red Ladon（別名 TA423、APT40、Leviathan）によるものと考えている。Red Ladon は、2018 年にも ScanBox を使用していた。2018 年、2022 年の両キャンペーンにおいて、この脅威アクターは、国政選挙にまつわるおとりを作成し、最新情報をテーマにした悪意ある Web サイトを開設して標的を引き寄せた。2022 年のキャンペーンの場合、Red Ladon は、オーストラリアのニュースメディアを偽装した管理 Web サイトに、英国に拠点を置くニュース組織から 2022 年 5 月のオーストラリア選挙に関する見出しをそのまま並べていたのである [97]。

関連の脅威アクター Red Dev 26 については、「Virus Bulletin 2022」でより詳しく説明している。

94 *CTO-QRT-20220302-01A - Red Lich eyes Europe*

95 'Mustang Panda's Hodur: Old tricks, new Korplug variant', ESET, https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/ (23rd March 2022)

96 'Rising Tide: Chasing the Currents of Espionage in the South China Sea', Proofpoint, https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea (30th August 2022)

97 *CTO-TIB-20220829-01A - Rising Tide*

通信セクターへの執着

通信事業者を標的とする脅威アクターの事例は何年も前から確認されてきたが、同セクターに対する 2022 年の活動を調査した結果、複数の脅威アクターがさらなる最適化を図っていることが分かった [98] 。

通信事業者への侵入は、国家間、企業間、政府間の安全なコミュニケーションを毀損し、世界中の外交、社会、企業の規範を脅かすという意味で、極めて重大な問題である。

2022 年 8 月、PwC は、脅威アクターの明確な TTP、偵察活動、C2 インフラおよび通信を特定した後、Red Dev 4（別名 GALLIUM）として以前追跡調査していた脅威アクターを Red Moros に割り当てた。2022 年を通じて、Red Moros は世界中の通信事業者や政府機関、また多くの学術機関を積極的に標的とした。Red Moros の活動を可視化した結果、この脅威アクターはオープンソースの SoftEther 仮想プライベートネットワーク（VPN）ソフトウェアを攻撃目的として、またインフラ構築の一部として使用していることが判明した。また、PwC はオープンソースで PingPull として知られているマルウェアファミリーの亜種を確認したが、これは China Chopper マルウェアの進化版と推測される、と評価している [99]。

2021 年に初めて登場した [100] Red Menshen は、2022 年を通じて通信・物流セクターを標的として活動を継続した。最も広く使用されているマルウェアファミリーの 1 つである BPFDoor が公開され、2022 年 8 月には、長期的に稼働していた多数の BPFDoor 感染が組織的に削除されたものの、Red Menshen が過去の被害組織や新たな標的組織のシステムにアクセスしている様子が引き続き確認されている [101]。

これらの脅威については、「TROOPERS22」の概要で詳述している。

98 'U/OO/160405-22: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices', US government, https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF (7th June 2022)

99 *CTO-TIB-20220823-02A - Red Moros' Reconnaissance*

100 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)

101 'Tinker Telco Soldier Spy', PwC Threat Intelligence, https://troopers.de/troopers22/talks/7cv8pz/ (29th June 2022)

イランの内的・外的課題

2022 年を通じて、イランを拠点とする脅威アクターは、中東、欧州、北米の被害組織に対してスパイ活動を目的とする攻撃を続け、一部ではワイパー、ランサムウェア、「ハック＆リーク」攻撃を含む破壊攻撃を強化した。

PwC は、スパイ防止策の失敗や国内情勢不安、報復作戦の必要性の認識から、イランを拠点とする脅威アクターが、国内・地域をさらに標的とするようになった点も確認した。

制裁措置とサイバー活動のイネーブラー

2022 年におけるイランの違反行為に対する欧米の対応の多くは、イラン政権への追加制裁措置というかたちを取った。イランは、石油化学製品の販売促進を目的とする制裁回避ネットワークへの関与／ウクライナで用いられる無人航空機（UAV）と武器のロシアへの販売／抗議者・政治的反体制派への弾圧、インターネット検閲、人権侵害／攻撃的サイバー活動という、主要な不正活動 4 分野に対して米国による制裁を受けた [102]。イランが経済的・外交的な孤立を続ける中、イランを拠点とする脅威アクターは、制裁や政権に対する公式の非難に直接的・間接的に関連するセクターや地域を標的とした。2022 年、PwC によるイランの攻撃的サイバー活動の分析は、Najee Technology や Ravin Academy など PwC が分析対象とした組織に米国が制裁を課したことによって、裏付けられたものもあった。

2022 年 9 月、SECNERD（正式名称 Najee Technology）は、ランサムウェア活動に関与しているとして米国政府が制裁したイランの「イスラム革命防衛隊（IRGC）」関連団体のリストに加えられた [103]。2022 年初頭から、PwC はサイバーセキュリティのリソースを提供すると称するペルシャ語 Web サイト SECNERD に関連するインフラの追跡調査を開始した [104]。その結果、SECNERD と Yellow Dev 24（別名 DEV-0270、Nemesis Kitten）の間で、インフラの重複が見られた。その後、SECNERD の背後にある企業を追跡調査したところ、IRGC、「ホメイニ・イマームの命令の実行（EIKO）」と称する組織、その他の制裁対象企業などの、イラン政府機関と関連があることが分かった [105]。

2022 年 10 月、米国政府は、イランのサイバー活動やデモ隊への弾圧に対して、複数のイラン人、情報機関、また Ravin Academy など表立った NGO に制裁を課した [106]。Ravin Academy の設立は 2019 年 11 月、一連のリーク情報により共同設立者がイラン情報セキュリティ省（MOIS）に所属して

102 'Iran Sanctions', US Department of State, https://www.state.gov/iran-sanctions/ (23rd November 2022)

103 'Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity', US Department of the Treasury, https://home.treasury.gov/news/press-releases/jy0948 (14th September 2022)

104 http://secnerd[.]ir, WayBackMachine (Archive), https://web.archive.org/web/20220223151704/http://secnerd.ir (6th April 2022)

105 *CTO-TIB-20220517-01A - Get some better OPSEC nerd*

106 Treasury Sanctions Iranian Officials and Entities Responsible for Ongoing Crackdown on Protests and Internet Censorship', US Department of the Treasury, https://home.treasury.gov/news/press-releases/jy1048 (26th October 2022)

いることが明らかになった直後のことである。Ravin Academy に関する PwC の分析では、さらに Yellow Nix との関連性、および Ravin Academy と Yellow Maero（別名 APT34）の間の専門的関連性が明らかになった [107]。

Yellow Nix については、2022 年のブログ記事で詳述している。

妨害攻撃

2022 年 7 月、MOIS とつながった複数の脅威アクターが、アルバニア政府のシステムに対して妨害攻撃を行ったことが確認された [108]。これには、ワイパーやランサムウェアを展開する前に偵察や事前準備を行った形跡もある [109]。この攻撃は、アルバニアがイランの反体制組織であるモジャヘディネ・ハルグ（MEK）を受け入れていることが原因であることはほぼ間違いないと PwC は評価している。同攻撃によるアルバニアとイランの外交的な影響は大きく、アルバニアはイランとの国交を断絶した。アルバニア政府はさらに NATO 条約第 5 条の発動を検討したが、最終的にはイランとの対立をこれ以上悪化させないという判断を下した。PwC は、これらの攻撃と、2022 年 1 月に MEK とのつながりを理由に米国を拠点とする組織に対して行われた攻撃の間に類似性を見出している [110]。これは、PwC が Yellow Dev 19（別名 Emennet Pasargad）として追跡する IRGC と連携した脅威アクターによって実行されたものである [111]。

アルバニアへの攻撃において、イランを拠点とする脅威アクター[112]は 、アルバニア政府のシステム上に 14 カ月もの長期にわたってとどまっており、大打撃を与えるために大規模な事前準備を行ったことがうかがえる。この大規模な活動により、脅威アクターの永続性と、イランを拠点とする脅威アクターが標的に対してスパイ行為と妨害行為の両方を採用する傾向が浮き彫りとなった。脅威アクターは、パッチが適用されていない SharePoint サーバーを悪用して初期アクセスを行い、Web シェルをドロッ

---

107 *CTO-SIB-20220121-01A - Advanced persistent teacher*

108 *Note: Microsoft assesses multiple Iranian threat actors participated in this attack under four different clusters of activity which we associate with Yellow Maero (a.k.a. APT34), Yellow Dev 9 (a.k.a. Lyceum, Hexane) and Yellow Dev 31 (a.k.a. DEV-0842). Source: 'Microsoft investigates Iranian attacks against the Albanian government', Microsoft, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/ (8th September 2022)*

109 'Alert AA22-264A - Iranian State Actors Conduct Cyber Operations Against the Government of Albania', US Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/uscert/ncas/alerts/aa22-264a (21st September 2022)

110 'PIN 20221020-001 - Iranian Cyber Group Emennet Pasargad Conducting Hack-and-Leak Operations Using False-Flag Persons', US Federal Bureau of Investigation (FBI), https://www.ic3.gov/Media/News/2022/221020.pdf (20th October 2022)

111 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)

112 *Note: Microsoft assesses multiple Iranian threat actors participated in this attack under four different clusters of activity which we associate with Yellow Maero (a.k.a. APT34), Yellow Dev 9 (a.k.a. Lyceum, Hexane) and Yellow Dev 31 (a.k.a. DEV-0842). Source: 'Microsoft investigates Iranian attacks against the Albanian government', Microsoft, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/ (8th September 2022)*

プした後、リモートデスクトップソフトウェアの AnyDesk を用いてラテラルムーブメントを行った。そして、Microsoft Exchange へのビルトイン・ロール・グループを使用して 権限を昇格させた。その後、エンドポイント防御を無効化し、ワイパーとランサムウェアの両方を展開する直前、脅威アクターはこれらのロール権限を活用して、特別ツールを用いて電子メールを流出させたのである [113]。

イランを拠点とする脅威アクターは、他の組織に対する「ハック＆リーク」または「ロック＆リーク」活動も継続しており、2021 年には、Moses Staff として知られる脅威アクターがイスラエルのさまざまなセクターに対して「ロック＆リーク」活動を展開したことが分かっている [114]。2022 年後半には、Abraham's Ax という非常に似た脅威アクターが出現し、サウジアラビア内務省のシステムにアクセスし、反西側と反イスラエルのメッセージをソーシャルメディアに投稿したと主張している [115]。Moses Staff と Abraham's Ax の手口（modus operandi）はほぼ同一であり、ネットワークインフラの重複も確認されていることから、2 つの脅威アクターが密接に連携していることがうかがえる [116]。

国内・反体制派の標的

PwC の分析から、Yellow Garuda（別名 Charming Kitten、APT42、PHOSPHORUS）のようなイランを拠点とする脅威アクターは、国内および反体制派を集中的に狙う傾向が年間を通じて見られたことが分かった。Yellow Garuda は、イラン国内だけでなく、海外でもペルシャ語を話す人、特に学生、活動家、過激派と称される人々を主な標的とした。PwC は、2021 年 9 月から 2022 年 6 月の間に発生した活動の重複を分析し、Yellow Garuda が CVE-2021-40444 と CVE-2022-30190 を使用して Microsoft ドキュメントを武器化したことを示した。コンパイル時間に応じて、Yellow Garuda はこれらのエクスプロイトを公開後 1 週間以内に用いることが可能であり、防衛側は、効果的な検出および軽減策を講じる余裕がほとんどなかったのである [117]。

2022 年 9 月、ヒジャブ法に抵触するとして逮捕されたクルド系イラン人女性、マフサ・アミニの死亡を発端とするイラン国内の抗議活動中 [118]、イランを拠点とする脅威アクターは、活動家、反体制派、抗議者といった国内の人々に焦点を当て続けてきた。広範な抗議運動が勃発しても、イランを拠点とする脅威アクターは、政府、防衛、通信、エネルギーセクターの組織など、イラン政権にとって優先度の高い組織にも焦点を当て続けていた [119]。同時に、イランの国内サーベイランス組織は、サードパーティのイネーブラーや、民間のモバイル端末に展開されるマルウェアなどを通じて、国内の標的への

113 *CTO-TIB-20220916-01A - Iran-based APTs attack Albania*

114 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)

115 'Abraham's Ax Likely Linked to Moses Staff', Secureworks, https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff (26th January 2023)

116 'Iranian Hacking Group Abraham's Ax claims hack on Saudi Ministry of Interior', Cyberwarzone, https://cyberwarzone.com/abraham-ax-saudi-ministry-interior-cyberattack/ (November 2022)

117 *CTO-TIB-20220728-01A - Bye Follina*

118 'UN rights chief says 'full-fledged' crisis underway in Iran amid crackdown on protesters', CNN, https://www.cnn.com/2022/11/24/middleeast/iran-protests-un-human-rights-council-intl/index.html (24th November 2022)

119 'Alert AA22-055A - Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-055a (24th February 2022)

監視を継続した [120]。Yellow Dev 32 は、2022 年 10 月にデモ参加者の携帯電話に L3MON という Android マルウェアを展開し、国内標的に焦点を当てたグループの 1 つである [121] 。

セクター別・地域別ターゲティングの傾向

2022 年に見られたイランを拠点とする脅威アクターに関するもう 1 つの傾向は、欧州と中東の海運、物流、海事、重要インフラに関連するセクターを重点的に標的にしていた、という点である。少なくとも 2022 年 5 月以降、Yellow Liderc（別名 Tortoiseshell、CURIUM）は、海運、船舶、物流分野で活動する公式 Web サイト上に JavaScript を埋め込んでいた [122]。このスクリプトは、ユーザーの位置情報、デバイス情報、閲覧のタイムスタンプを取得することで、Web サイト訪問者のフィンガープリントを取得する。これと同時に、この脅威アクターは、悪意あるスクリプトに感染した Web サイトを装ったタイポスクワッティングドメインを登録した。PwC は、Yellow Liderc がこれらのタイポスクワッティングドメインをユーザーのフィンガープリントデータと組み合わせて使用し、カスタマイズされたスピアフィッシング攻撃を開始した可能性が高いと評価している。この活動の一部は、オープンソースで報告された同様の標的と一致しており、同報告では、2020 年から 2022 年にかけて脅威アクターがイスラエルの海運組織を標的にした方法が詳述されている [123]。さらに、この活動の多くは、2022 年 5 月に米国政府の要請により地中海で押収された船舶のように、イラン産原油を輸送するタンカーの押収に関連している可能性が高いと評価している [124]。

2022 年初頭、PwC は、Yellow Garuda がトルコの核問題や米国の海運港など、さまざまなテーマをおとりとして利用している事例を確認した。PwC はまた、Yellow Garuda が中東の幅広い地域を標的にこうしたおとりを作成した可能性について、また、同活動はエネルギーセクターの組織に的を絞ったキャンペーンではなかった可能性について検討した。少なくとも 1 つの米国港湾関連のおとり文書は、受取人が指定されたレターのフォーマットであったため、標的とされた可能性が高い [125]。

PwC はまた、2022 年 1 月にオープンソースで公開された関連インフラの分析を通じて、2019 年に初めて見られた、同様の TTP を使用してジャーナリストやシンクタンク、リサーチャーを標的とする Yellow Garuda の活動を引き続き観察した [126]。PwC は、このインフラを Yellow Garuda のものと評価し、米国、イスラエル、アラブ首長国連邦に拠点を置くメディア組織やシンクタンクを詐称するドメインを特定した。さらに分析した結果、標的となったシンクタンクやジャーナリストは、中東の外交政策、核交渉、その他イラン政権に関連する戦略的利益の専門家として注目を集めている、または通常そうしたトピックに関与していることが判明した。また、Google や Microsoft のアカウントになりすましたドメインや、Yellow Garuda の典型的な被害者像に沿った国内の標的も確認された [127]。

---

120 *CTO-TIB-20221206-01A - A sour L3MON and a FurBall*

121 *CTO-TIB-20221206-01A - A sour L3MON and a FurBall*

122 *CTO-TIB-20221208-01A - Yellow Liderc ships its scripts*

123 'Suspected Iranian Actor Targeting Israeli Shipping, Healthcare, Government and Energy Sectors', Mandiant, https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping (17th August 2022)

124 'Iranian oil tanker's cargo seized in Greece after US request', AP News, https://apnews.com/article/russia-ukraine-politics-united-states-68af0db11c5c03e89049da0629ef4d85 (26th May 2022)

125 *CTO-TIB-20220308-01A - Charming Kitten's Turkish delight*

126 'Shady Network of Fake Mossad Job Sites Targets Iranian Spies', The Daily Beast, https://www.thedailybeast.com/shady-network-of-fake- mossad-job-sites-target-iranian-spies (24th January 2022)

127 *CTO-TIB-20220302-01A - A busy bird that Yellow Garuda*

Yellow Garuda については、2022 年のブログ記事で詳述している。

2022 年、イランを拠点とする脅威アクターは、イスラエルを拠点とする組織を引き続き標的としていた。ある例では、PwC は Yellow Nix に関連する GitHub アカウントを分析し、その後、同アカウントのリポジトリ内に C2 IP アドレスを含むスクリプトを特定した。PwC は、このインフラを Yellow Nix のものと評価し、イスラエルとトルコの組織を標的にするために使用された可能性が高いとした [128]。また別の例では、Yellow Nix は 2022 年 11 月、Syncro と呼ばれる市販のリモート管理ツールを用いてイスラエルの複数の保険会社を標的とした [129]。

Yellow Liderc に関するインシデント対応事例

2022 年初頭、脅威インテリジェンスチームは、Yellow Liderc（別名 Tortoiseshell、TA456）に狙われた欧州のエンジニアリング・製造組織に関する PwC の広範なインシデント対応策を支援した。被害組織から提供された実行ファイルのサンプルの分析を通じて、脅威アクターが進化したツールと技術を採用していることが判明した。こうした変化は、Yellow Liderc が検出を回避し、被害組織ネットワーク内での持続性を維持すべく、活動のセキュリティを強化しようとしていることを示していると考えられる。

支援においては、オープンソースで提供されているツールである PyArmor で難読化された 3 つの Python スクリプトの機能と、被害組織と Yellow Liderc サーバー間のネットワークトラフィックを分析した。その結果、C2 通信が 2022 年 1 月初旬には始まっており、少なくとも 4 カ月間継続していたことが判明した。高度に難読化されたサンプルは、専用のメールボックスに安全なメッセージングプロトコルで通信しており、これらは全て Yellow Liderc が活動のセキュリティを強化していることを示している [130]。

活動セキュリティの低さや既知のインフラやツールの使用などの特徴から、イランを拠点とする脅威アクターを発見する事例はよくあるが、今回のインシデントは、目的意識の高い脅威アクターと、従来評価の行動や限界を超えて進化するその能力を過小評価してはならないことを強く示すものである。脅威アクターの目的や TTP に関する深い知識により、PwC はインシデント対応に優先順位を付け、被害組織に有意義な背景情報を提供し、今後の計画策定に貢献することができた。

[128] *CTO-TIB-20220210-01A - Smooth Operator*
[129] *CTO-TIB-20221206-02A - Let's Syncro up with Yellow Nix*
[130] *CTO-TIB-20220628-02A - Three varieties of Liderc*

他地域のケーススタディ

このセクションでは、洗練度や目的がさまざまに異なる他の脅威アクターを紹介する。

例年通り、2022 年の脅威アクターの活動は現実世界の事象と一致し、地政学的状況を反映しており、多くの場合、政治や国家の戦略目標や優先順位との相関性が見られた。

金銭目的のブラックバッグ（侵入）活動

2022 年を通じて、北朝鮮を拠点とする脅威アクターの活動に関する PwC の調査では、主に、金融サービス部門の組織や暗号通貨関連企業 [131]、その他多数のセクターにわたる金銭目的の攻撃など、これまで見られた傾向や TTP、被害組織について補強を進めた。2022 年に観察された標的パターンに基づき、PwC は、北朝鮮を拠点とする脅威アクターが引き続き政府の代わりに金銭的窃取のタスクに対応し続ける可能性が高い、と評価している。

2022 年は、暗号通貨だけでなくベンチャーキャピタルやスタートアップ組織を標的にした、金銭目的の Black Alicanto（別名 COPERNICIUM、DangerousPassword、CryptoMimic、CryptoCore、Operation SnatchCrypto）や Black Dev 2（別名 Operation Gold Hunting、 Operation SnatchCrypto）による活発な活動が引き続き観察された。Black Dev 2 は Black Alicanto と関連している可能性が高いと PwC は評価しており、2021 年以降、両アクターは求職をテーマにしたおとり文書で被害組織を狙い、暗号通貨空間でのベンチャーキャピタル調達の機会も狙っている [132]。Black Alicanto は、2022 年半ばから後半にかけて、悪意ある LNK ファイルを使用する従来の方法とは異なり、Microsoft Software Installer（MSI）を使用して、被害組織のシステムへの初期アクセスおよびインストールを行っていた。

Black Artemis（別名 Lazarus Group、Hidden Cobra、ZINC）は、2022 年を通じて複数のキャンペーンを実施し、非常に活発な活動を継続している。この脅威アクターは、オープンソースで Operation Dream Job、Operation Interception として知られ、PwC が ShowState として追跡調査しているキャンペーンを、オープンソースで BLINDINGCAN として知られているマルウェアファミリーを用いて継続した [133]。Black Artemis が、それぞれ少なくとも 2018 年と 2014 年から展開されている BLINDINGCAN や DTrack などのマルウェアを継続して使用していることから、新たなツールを武器として装備することに加えて既存のコードベースも放棄せず開発するという、この脅威アクターの傾向がうかがえる。

131 *CTO-SIB-20220915-02A - Tales from the crypto*
132 *CTO-TUS-20220616-01A - Threats under the Spotlight - May 2022*
133 *CTO-TIB-20220812-01A - Black Artemis' dream job hunt*

Black Artemis は、防衛・軍事組織を標的としたスパイ活動も継続し、ツールセットの大幅な追加を行い、YamaBot や MagicRAT といったマルウェアファミリーを導入した。この脅威がエネルギーセクターを標的にしていることを示す業界レポート [134, 135]は特に注目を集めており、Black Artemis のその他の活動に関する PwC の可視性を補完する材料となっている。

PwC 韓国からの知見

2022 年後半、PwC 韓国は、韓国語で「幽霊」を意味する GWISIN を自称するランサムウェアの脅威アクターが、韓国内の組織を標的にしているとのアラートを受けた。この脅威アクターは、広く採用されている国内セキュリティシステムやセキュリティ認証、法執行機関など国内の環境について熟知していると思われる。この脅威アクターは、その名のとおり防御的な回避テクニックを採用し、被害組織からコマンドを送信し、データを抜き取るべくWebの脆弱性とWebシェルを組み合わせて用いていた。

変化のない Orange

2022 年を通じて、インドを拠点とする脅威アクターは、2021 年から既知の TTP を採用し、比較的高い活動ペースを維持している。パキスタンを拠点とする政府機関や国防機関が、インドを拠点とする脅威アクターによって、前年に使用されたものと同じマルウェアで大規模に標的とされていることが確認された一方で、注目すべき新しい標的や TTP もいくつか確認された。Orange Yali（別名 BITTER）[136]、Orange Kala（別名 DONOT）など、同地域の他国に拠点を置く組織にも標的を広げたと思しき脅威アクターもあり、Orange Chandi（別名 SideWinder）は、2020 年と 2021 年に使用した長年の TTP とは攻撃プロセスを変えている。

2022 年、同地域の政治的事象に沿った新たな標的活動のエビデンスが得られたが [137]、インドを拠点とする脅威アクターは、より高度な技術を実装する代わりに、主に攻撃プロセス内のツールを変更した。例えば、インドを拠点とする脅威アクターがキャンペーンにおいて、2021 年同様、汎用 RAT を使用した事例もいくつか見られた [138]。

134 'Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets', Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage (27th April 2022)

135 'DTrack activity targeting Europe and Latin America', Kaspersky, https://securelist.com/dtrack-targeting-europe-latin-america/107798/ (15th November 2022)

136 *CTO-TUS-20221027-01A - Threats under the Spotlight - September 2022*

137 *CTO-SIB-20220915-01A - APAC-origin forecast - Q2 2022 developments*

138 *CTO-TIB-20210112-01A - Orange Kala enters the Warzone*

応募の必要なし：求職をテーマにしたおとりを用いる高度な持続的脅威

新型コロナウイルス感染症（COVID-19）の流行により、多くの労働者が自分のキャリアを見直すようになった。脅威アクターは、2022 年を通じて、金銭・諜報両方の目的において戦略的目標を達成すべく、こうした状況を利用した。北朝鮮やイランを拠点とする脅威アクターは、有名企業の社員を標的にした試みにおいて特に大胆で、ソーシャルエンジニアリングを用いて、そうした社員に電子メールやソーシャルメディアを介して近づき、信頼関係を築いてから、企業ネットワークへの初期アクセスを図ろうとした [139]。

- **北朝鮮を拠点とする脅威アクターと金銭目的によるキャンペーン**：
  求人活動は、北朝鮮を拠点とする脅威アクターによる長年のパターンである。2022 年のキャンペーンでは、Black Artemis（別名 Lazarus Group、Hidden Cobra、ZINC）が、有名企業の採用担当者や人事担当者を装うなど、さまざまなソーシャルメディア上の人物像を仕立て上げ、標的をソーシャルエンジニアリングした。また、Black Artemis は、有名な就職支援会社の偽装 Web サイトを開設し、ブラウザのエクスプロイトを武器に、標的の端末にマルウェアを仕込んだ。別の方法では、LinkedIn、WhatsApp、電子メールで個人に接触した後、脅威アクターは標的を説得し、仕事で使用しているシステムの悪意ある文書を開かせようとした。そうした文書を開くと、リモートテンプレートインジェクションや悪意あるマクロによって、組織のネットワーク上にマルウェアが埋め込まれた状態でダウンロードされる。少なくとも 2022 年 7 月以降、Black Artemis は、有名テック系企業で募集している職務の説明や候補者の評価を装って、圧縮アーカイブに含まれる EXE ファイル [140] や ISO ファイル [141] を標的に開かせることに軸足を移している。別の例では、少なくとも 2022 年 8 月以降、Black Alicanto（別名 COPERNICIUM、DangerousPassword、CryptoMimic、CryptoCore、Operation SnatchCrypto）は、おそらく初期アクセステクニックの多様化を図るために、同様のキャンペーンで悪意あるおとりファイルとして試験的に MSI ファイルを用いた。

- **スパイ活動を目的にキャンペーンを採用する、イラン拠点の脅威アクター**：
  Yellow Dev 13（別名 BOHRIUM、TA455）は、Meta[142] と Microsoft によるテイクダウンにもかかわらず、LinkedIn、Facebook、Instagram、Twitter などさまざまなソーシャルメディアで実在する企業や架空の企業の採用担当者を装った [143]。Yellow Dev 13 は、人工知能（AI）が生成したさまざまな写真をプロフィールに使用し、少なくとも 1 人の実在する個人になりすまして活動していた。

---

139 'Talent Need Not Apply Tradecraft and Objectives of Job-themed APT Social Engineering', PwC Threat Intelligence, https://i.blackhat.com/USA-22/Thursday/US-22-Wikoff-Talent-Need-Not-Apply.pdf (11th August 2022)

140 *CTO-TIB-20220812-01A - Black Artemis' dream job hunt*

141 'It's Time to PuTTY! DPRK Job Opportunity Phishing via WhatsApp', Mandiant, https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing (14th September 2022)

142 'Meta Quarterly Adversarial Threat Report: Q1 2022', Meta, https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf (April 2022)

143 'Microsoft Corporation, A Washington corporation, Plaintiff, v. John Does 1-2, Controlling a computer network and thereby injuring plaintiff and its customers：Ex Parte temporary restraining order and order to show cause re preliminary injunction', Microsoft, https://news.microsoft.com/wp-content/uploads/prod/sites/358/2022/06/Doc.-No.-16-Ex-parte-TRO-SEALED.pdf (27th May 2022)

Yellow Dev 13 は、少なくとも ApplyTalents と CareersFinders という、2 つのニセの人材紹介会社サイトも運営し [144]、いずれも、英国を拠点とする人材紹介会社を装った、同じニセチームと連絡先を用いていた。少なくとも 1 つの事例では、脅威アクターは、適性試験やライブチャットサポート機能など、求職者向け評価プラットフォーム全体を偽装する悪意ある実行ファイルを構築し、バックグラウンドで ApplyTalents ドメインに接続するようにした。このプラットフォームでは、リサーチャーによる分析を回避するために、脅威アクターの提供と思しき認証情報の入力が必要であったが、PwC は、Yellow Dev 13 が諜報目的で個人または組織を侵害しようとしていた可能性が高いと評価している。

詳しくは、BlackHat USA 2022 における PwC の講演「Talent Need Not Apply」を参照のこと。

White Dev 21 について

2022 年、White Dev 21（別名 WIRTE）は、ヨルダン、パレスチナ、シリア、レバノンなど、中東全域でさまざまな被害組織を標的に活動を継続した。2022 年 9 月における攻撃グループから、White Dev 21 は地政学的なおとり文句を多用し、湾岸協力会議に関するテーマやアラブの金融サービス、政府組織に関する情報を活用していることが判明した。この脅威アクターは、2022 年、同地域の主要セクターや団体を執拗に標的とする手法を示した [145]。

White Tur の興味深い展開

2022 年 1 月、PwC は、少なくとも 2017 年から 2021 年にかけてバルカン地域内の組織を標的として、PwC が White Tur として追跡調査している脅威アクターに関するブログを発表した。公開後もこの脅威アクターは活動を続け [146]、ボスニア・ヘルツェゴビナおよびセルビアに関連するテーマを用いて、同地域内の組織を狙い続けた。さらに、PwC が 2022 年 1 月から 2022 年 4 月にかけて作成された一連の HTML アプリケーション（HTA）スクリプトを特定した結果、White Tur の TTP が変化したことが示唆された。この一連の HTA スクリプトでは、脅威アクターは WebDAV プロトコルを使用して、悪意あるペイロードを被害組織の端末に転送していた [147]。

White Tur については、2022 年のブログ記事と SANS CTI Summit 2022 の「Threat Actor of in-Turest」講演で詳しく説明している。

144 *CTO-TIB-20220121-02A - Talent need not apply to this career finder*

145 *CTO-TUS-20221027-01A - Threats under the Spotlight - September 2022*

146 'Threat actor of in-Tur-est', PwC Threat Intelligence, https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/threat-actor-of-in-tur-est.html (27th January 2022)

147 *CTO-TIB-20221012-03A - White Tur's WebDAV adventures*

White Tur TTP の詳細

HTA ファイルは、有名な live-off-the-land バイナリ（別名 LOLBin）である mshta.exe によって解釈・実行され、脅威アクターによって頻繁に悪用されている。HTA ファイルは、ブラウザの制約を受けずに HTML でスクリプトを起動することが可能になるため、攻撃者は悪意ある JavaScript や VBScript の実行をプロキシするなどの目的で悪用している。そのため、mshta.exe プロセス周りに焦点を当てた検出コントロールを行う必要がある（例：mshta.exe が遠隔地から HTA ファイルを呼び出する、あるいは特定の拡張子のファイルをディスクに書き込むなどの検出）。

White Tur は、WebDAV プロトコルを使用して実行ファイルをディスクにコピーする際、継続的に実行できるようスタートアップフォルダに置かれた。エンタープライズの環境においてスタートアップフォルダに書き込まれた全てのファイルを監視することは困難であるが、脅威アクターによる悪用の頻度を考えると、疑わしいファイル作成を特定する検出コントロールを行う必要がある。このディレクトリの異常なアクティビティやグローバルにユニークなファイルに基づく検出ロジックは、この種のアクティビティを検出する可能性が高いが、この種の分析は全ての検出ツールで利用できるわけではない。まずは、LOLBin または一般的な悪意ある実行可能ファイルがこの場所にファイルを書き込んでいないか監視することから始めるのがよいだろう。

White Dev 140 に何が起こったか

PwC における 2022 年の調査プロジェクトの 1 つにおいて、White Dev 140 によるものと思われる不可解な行動パターンが見られた。White Dev 140 は、2022 年にウクライナの組織に関心を寄せており、この点はロシアを拠点とする脅威アクターの標的と同様であったが、以下に示すさまざまなセクターにも関心を示していたことが、この脅威アクターの目的に関する PwC の初期評価が混乱する一因となった [148]。

- 食品輸出業者、スーパーマーケット、小売業者
- ウクライナ・ドニプロ市、ピアティカトキー地区などの地域政府機関
- ウクライナの原子力機関である Energoatom
- ガス会社
- 金属・電子デバイス製造工場
- 物流会社、個人宅配業者

2022 年に確認した White Dev 140 活動の指標例：

```
https[:]//product808[.]godaddysites[.]com/purchase-order
https[:]//support-domaill[.]godaddysites[.]com/ukr
https[:]//shipping8[.]godaddysites[.]com/dhl
```

[148] *CTO-TIB-20221209-02A - Phishing trips to Ukraine*

https[:]//servicesagreement[.]godaddysites[.]com/update
https[:]//support-ukr[.]godaddysites[.]com/log-in

PwC は、2022 年 5 月に White Dev 140 のスピアフィッシング活動を初めて確認した。この脅威アクターは、ウクライナ政府にもライセンス供給を行っている国内ソフトウェア再販業者を標的としていた [149]。スピアフィッシングの電子メールには、ウクライナで電子メールに使用されている人気のインターネットポータル、UKR[.]net に関するテーマが含まれていた。この電子メールには、ウクライナ語で以下のメッセージが記載された PDF が添付されていた:

ユーザー様
このメッセージは非常に重要です。当社の記録上、ユーザー様のアカウントが更新されていません。
【注意】確認されない場合、当該アカウントはまもなく無効となります。

このメッセージを受信されたユーザー様は、直ちにアカウントの更新を行ってください。
@UKR メールチーム

当時のスピアフィッシング活動の TTP は、広範なフィッシングキャンペーンを展開していた Blue Athena が使用していたものと類似していた: [150, 151]

- フィッシングのリンク先を含む、UKR[.]net のテーマを使用した PDF 添付ファイル
- 無料ホスティングプロバイダーの活用
- 標的
- メール文面

スピアフィッシングメールには、URL のフィッシングリンク先が貼られた PDF 添付ファイルが含まれていた。

https[:]//ukrverifikaciyaakkaunta[.]godaddysites[.]com/privacy-policy

2022 年 10 月、別の White Dev 140 スピアフィッシングメールでは、ウクライナのドメインを標的とし、メールには DHL のテーマが使われていたが、フィッシングリンク先には Deutsche Post の URL が使用されていた。フィッシング URL は

https[:]//deutschepost[.]godaddysites[.]com/login

149 *CTO-QRT-20220601-01A - More phishing attempts against Ukraine*
150 *CTO-QRT-20220326-01A - Blue Athena Phishing Part 1*
151 'Update on cyber activity in Eastern Europe', Google, https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/
(3rd May 2022)

スピアフィッシングメールに関するテクニカルデータを分析したところ、以前分析した 2022 年 5 月および 2022 年 10 月のフィッシングとの類似性が認められた。追加サンプルからは、一貫したパターンが見つかり、さらなるフィッシングの特定に至った。

カスタマイズ対応？

2022 年 9 月、中国の「国家コンピュータウイルス緊急対応センター（CVERC）」は、米国家安全保障局（NSA）の Tailored Access Operations（TAO）と呼ばれるグループが、一連のツールを使って中国の大学に対して攻撃を開始したと報告した [152]。そして、その一部は Shadow Brokers として知られる個人とグループの両方が以前に別々にリークしたツール名と同じ名称であった [153]。2022 年 9 月のレポートには、この攻撃疑惑の指標、機関、その他の特徴は記載されていなかった。

PwC ブラジルからの知見

2022 年、PwC ブラジルは、ブラジルを拠点とする脅威アクターが、少なくとも 5 年以上前から存在し、ブラジル国民に関する機密情報を検索可能な Data Broker Panels と呼ばれる Web インターフェイスを商業化し、利用していることを分析した。これらの脅威アクターは、パネルへのアクセス権を通常月額プランで販売し、その情報をサイバー犯罪者がソーシャルエンジニアリングや詐欺へ悪用できるようにしていた。

152 'Chinese reports uncover details of cyber attacks by U.S. security agency', Xinhua, https://english.news.cn/20220913/71f9b72993614795b4d8ff554c99ef9b/c.html (13th September 2022)
153 'Shadow Brokers leaks show U.S. spies successfully hacked Russian, Iranian targets', CyberScoop, https://www.cyberscoop.com/nsa-shadow-brokers-leaks-iran-russia-optimusprime-stoicsurgeon/ (18th April 2017)

サイバー犯罪エコシステムの変化

2022 年は サイバー犯罪のエコシステム全体において、注目に値する展開が見られた。例えば、デジタル版「スマッシュ＆グラブ」とも言える「ハック＆リーク」活動に「ビッグゲームハンティング」的要素を加えた、つまり、知名度と悪名を追求しつつ、注目度や価値が高いと思われる標的を厳選するといった動きを見せる脅威アクターが現れた。

しかし、サイバー犯罪のエコシステムの変化を主に支えているのは、窃取、脅迫、詐欺などばらまき型のエクスプロイト攻撃を用いる、従前からの金銭目的の脅威アクターの存在であり、市場の大部分を占めているのはランサムウェア攻撃である。

2022 年、ランサムウェアの脅威アクターは、脅迫被害組織に圧力をかけ、内部関係者のリクルートをより大胆に行った。PwC はこうした傾向について、脅威アクターがランサムウェアブランドをさらに細分化し、リソースを奪い合い、防御力やレジリエンスの組織的向上に対応していく中で、2023 年により顕著になると予測している。東欧を拠点とするサイバー犯罪と脅威アクターが交差するポイントであることから、本レポートでは、ロシアのウクライナ侵攻に関連した具体的動向を取り上げた（ロシアによウクライナ侵攻：サイバー犯罪への防戦態勢）。

ランサムウェアの動向

かつて、サイバー犯罪の脅威環境を破壊するものと考えられていたランサムウェアは、ここ数年、組織に対する脅威として常に圧倒的な存在となっている。ランサムウェアの普及が続いているのは、ランサムウェア・アズ・ア・サービス（RaaS）の運用によるところが大きく、この永続的なモデルは PwC のレポート**「サイバー脅威：2021 年を振り返る」**で詳述している [154]。

154 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)

2022 年、ランサムウェアの脅威環境に関しては、2021 年の傾向と同程度のリークサイト被害が確認された。しかし、ランサムウェアブランド数は、脅威環境を示す指標としては適切ではないと思われる。というのも、ランサムウェアのブランドは急速に変化し、ブランドの変更も珍しくないためである。

今後、ランサムウェアの活動全体の状況を追跡調査するためのより適切なデータポイントは、ランサムウェア脅威アクター間の TTP 重複だと判断している。

典型的なランサムウェア・アズ・ア・サービス（RaaS）で観察される TTP

リークサイト解析

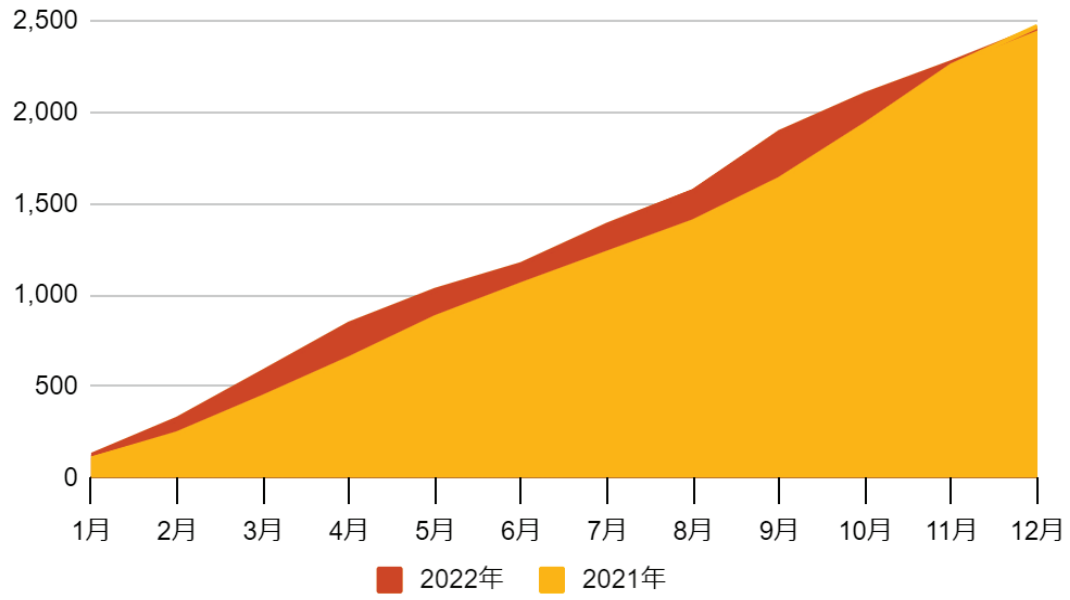
2022 年、PwC が追跡したランサムウェア流出サイトに投稿された被害組織の総数は 2,462 で、2021 年の 2,471 に比べて若干減少し（1%以内）、2020 年の 1,330 からほぼ倍増している。2020 年から 2021 年にかけてランサムウェア流出サイトの被害組織が一貫して増加する一方で、流出サイトの被害組織総数は 2021 年から 2022 年にかけて横ばいとなった。

2022 年、ウクライナにおけるロシアの侵攻、ランサムウェア脅威アクターに対する法執行機関の活動、暗号通貨の変動、著名ランサムウェアグループの内部流出や対立など、ランサムウェアのエコシステムに大きな課題が発生し、2021 年と 2022 年の漏洩サイト被害組織の数は、おそらくこの活動の「最高水位」であると評価している [155]。

リークサイトの活動 vs より広範なランサムウェア脅威活動

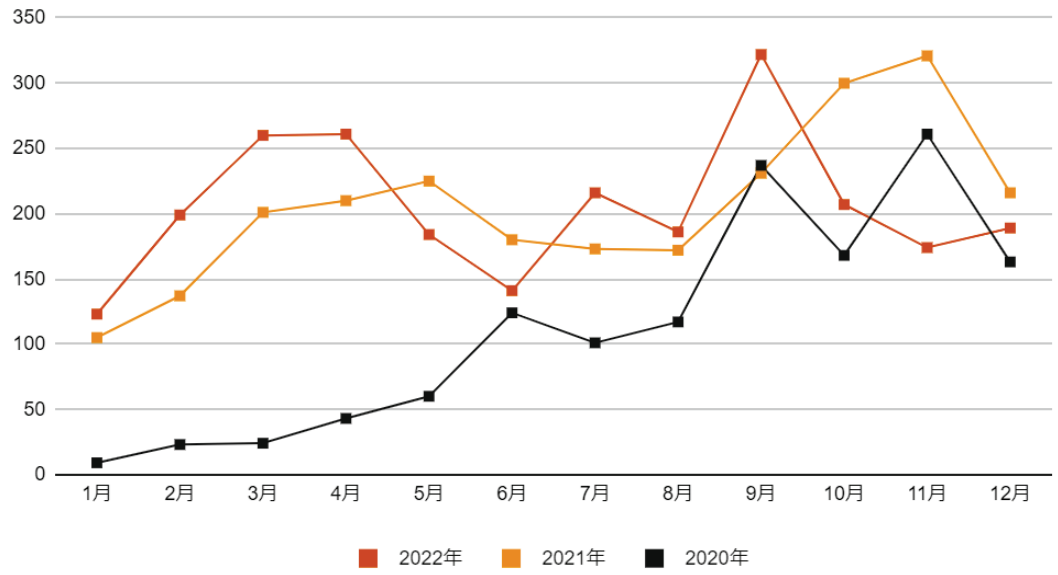
リークサイトの活動を追跡調査することで、ランサムウェアの脅威の状況を具体的に把握することができるものの、リークサイトではランサムウェアの活動の全体像を把握することは不可能である。そのため、特にリークサイトを設けずに活動する脅威アクターや、リークサイトに投稿されない、あるいは公開されていない被害組織に関する分析を引き続き実施している。

1 年を通じたリークサイト被害組織の投稿数（2021 年～2022 年）



[155] *CTO-SRT-20230118-01A - Ransomware report for December 2022*

毎月のリークサイト被害組織の投稿数 （2020 年～2022 年）



PwC は、ランサムウェア攻撃を、ばらまき型攻撃であり、広範囲かつ無差別な感染によって可能になる攻撃と分類している。それでも、2022 年、比較的多くのリークサイト被害組織が発生した複数のセクターが観察された。特に、2022 年にランサムウェアの流出サイトに投稿された被害組織の上位 5 セクターは、製造（15%）、建設（10%）、プロフェッショナルサービス（9%）、テクノロジー（8%）、小売（8%）であった。

その理由として、これらのセクターでは業務停止による被害額が高額になると考えられていることや、これらのセクターに課される情報セキュリティ規制のレベルが比較的低いことなどが考えられる。こうした傾向に加えて、ランサムウェア攻撃は、2022 年に政府、通信、運輸、エネルギー、教育など他のセクターに属する組織にも大きな影響を与えた。

大部分を占める White Janus

2022 年のリークサイト活動の分析では、White Janus（別名 LockBit）が年間を通じて数の面で他を圧倒し、2021 年のリークサイト活動でランサムウェア群をリードしていた Blue Cronus の 2021 年ペースを瞬く間に抜き去った。2022 年 6 月、White Janus は LockBit 3.0 RaaS プログラムを発表し、2022 年後半にその活動とリークのペースを一層強化した。PwC は、White Janus が 2022 年 6 月の大半を LockBit 3.0 のベータテストに費やしたため、2022 年前半において他の脅威アクターのリークサイト活動と比較して、そのリークサイトに投稿された被害組織数が顕著に減少したものと評価している [156]。2022 年 12 月末までに、White Janus は、2021 年に脅威アクターが投稿した被害組織数（460）と比べて、2022 年合計で 907 の被害組織をリークサイトに投稿した [157]。

[156] *CTO-QRT-20220804-03A - White Janus changes the Locks*
[157] *CTO-SRT-20230118-01A - Ransomware report for December 2022*

2022 年 6 月に LockBit 3.0 が初めてリリースされた際、PwC は、今や消滅した BlackMatter RaaS 活動における主要なランサムウェアバイナリとして使われていたマルウェアとコードベースが重複していることを確認した。PwC はこれらの重複（当初は開封機能で発見された）について分析し、LockBit 3.0 は、特定の国別コードの言語チェック、暗号化の実装、解析対策テクニックなど、BlackMatter とほぼ同じものと判断した [158]。2 つの技術的な重複は十分に大きく、PwC は、他のリサーチャーとともに、この類似性は BlackMatter のコードベースを White Janus が調達したことによる可能性が高いと判断した [159]。この点については、2022 年 7 月に報告されたインタビューにおける White Janus 広報担当者の発言で確認された [160]。

BlackCat として BlackMatter を見る

2022 年において、BlackMatter と能力で重複が見られる脅威アクターは、White Janus（別名 LockBit）だけではなかった。2021 年 12 月に現れたランサムウェア脅威アクターALPHV-ng は、そのロゴからオープンソースの多くの人々が BlackCat というブランド名で呼ぶようになった。PwC は、White Dev 101 としてこの脅威アクターを追跡調査し始め、すぐに BlackMatter とのつながりを特定した [161]。BlackMatter と White Dev 101 のバイナリの間にある重要なコードの重複に基づき、PwC は、BlackMatter の開発者が 2021 年 11 月、BlackMatter 運営停止後に ALPHV-ng ブランドを立ち上げるため活動を進化させた可能性が非常に高い、と評価している [162]。

2022 年を通じて被害組織数が 907 に達した White Janus が、ランサムウェア流出サイトの活動をほぼ独占したが、White Dev 101 の被害組織数が 228 と 2 番目に多く、これに続いて、Blue Cronus（別名 Conti）が 177、White Dev 115（別名 BlackBasta）が 139 という結果となった [163]。

ランサムウェアに関する PwC の調査については、SANS Ransomware Summit 2022 における PwC の講演「The R Word: Retelling the Recent Rise and Resurgence of Resilient RaaS Operators」でより詳しく説明している。

158 *CTO-TIB-20220916-02A - LockBit evolves…sort of*

159 'LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities', Trend Micro, https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html (25th July 2022)

160 'RHC interviews LockBit 3.0. "The main thing is not to start a nuclear war"', Red Hot Cyber, https://www.redhotcyber.com/en/post/rhc-interviews-lockbit-3-0-the-main-thing-is-not-to-start-a-nuclear-war/ (26th July 2022)

161 *CTO-TIB-20220121-03A - White Dev 101 does not Rust on its laurels*

162 'The R Word: Retelling the Recent Rise and Resurgence of Resilient Ransomware-as-a-Service Operators', PwC Threat Intelligence, https://www.youtube.com/watch?v=pZ3tyhL61rI (2nd August 2022)

163 *CTO-SRT-20230118-01A - Ransomware report for December 2022*

LockBit 3.0 のリリース後の 2022 年 9 月、White Janus は、White Janus の 3.0 暗号化ツールである LockBit Black のビルダーを「不満を抱いているとされる内部関係者」によって流出させられるなど、自らも情報漏洩に見舞われた [164]。PwC はこのビルダーを独自にテストし、動作する LockBit 3.0 バイナリと有効な復号ツールを生成することを確認した。また、このバイナリは LockBit 3.0 と BlackMatter の両方の PwC 検出ルールをトリガーした [165]。LockBit 3.0 ビルダーが入手可能になったことで、ランサムウェアに乗り出す洗練されていない脅威アクター、またはアトリビューションを回避しようとするより広範な脅威アクターの参入障壁が下がったことはほぼ間違いない。2022 年 10 月以降、White Janus の活動ペースが低下しているが、これは上述の LockBit 3.0 ビルダーの流出の影響である可能性が高いと PwC は評価している。

2022 年には、成功した熟練の経験豊富な個人が、解散する RaaS 活動から、サイバー犯罪のエコシステム内の他の機会へと移るパターンも見られた。

過去数年間、この領域が成熟した結果、個人がある RaaS 活動から他の RaaS 活動へと移る際、知識や専門能力を持ち出すという、企業のような事例が展開されることとなった。ランサムウェアグループの出現、分裂、再ブランド化に伴い、そうした個人の行動の影響が明らかになっている。LockBit 3.0 の登場はこのパターンに合致しておらず、技術やコードベースが再利用される、または完全に取得されるという RaaS モデルの新たな変化を示している可能性が高いと評価している [166]。

常に進化するランサムウェアの脅威に対して効果的な防御を行うには、2 つの側面からのアプローチが必要である。組織は、対ランサムウェア準備フレームワークを活用して、ある特定の脅威だけにとらわれない戦略を構築する必要がある。同時に、組織は、既知の脅威の土台となる先行者やコードベースについての理解を深め、検出と軽減措置を効率化する機会を創出する必要がある。

RaaS プログラム：望まれない専門化

2022 年には、複数のランサムウェア脅威アクターが RaaS プログラムをさらに専門化させている。これが意味するのは、脅威環境が過飽和状態を迎え、脅威アクターが競合を出し抜くために新しい戦術を採用するよう求められていること、また、セキュリティ対策や対応策を強化しつつある被害組織を恐喝・強要する新たな方法を求めている、ということである。

164 LockBit ransomware builder leaked online by “angry developer”’, Bleeping Computer, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-builder-leaked-online-by-angry-developer-/ (21st September 2022)

165 *CTO-SRT-20221019-01A - Ransomware report for September 2022*

166 *CTO-TIB-20220916-02A - LockBit evolves…sort of*

脆弱性報奨プログラムと検索可能なデータベース

2022 年 9 月、White Janus（別名 LockBit）は、脆弱性報奨プログラムの最初の報酬を発表した（50,000 米ドル相当とされている）。発見された脆弱性は、脅威アクターのランサムウェアによって暗号化されたファイルの復号を可能にするものであった [167]。2022 年半ばまでに、White Janus と White Dev 101（別名 ALPHV-ng、BlackCat）の両アクターは、リークサイトに検索機能を追加し、訪問者が被害組織データを検索できるようにした [168]。

ランサムウェアの交渉における高圧的戦術

Conti ブランドによって流出した通信の分析により、脅威アクターが被害組織またはその代理人との直接のコミュニケーションを活かして交渉を行う、高圧的でありながら成熟した活動が明らかになった。これらのリーク情報は、PwC が Blue Cronus として追跡調査している脅威アクターが Conti や Emotet を含むランサムウェア活動を安定的に継続している理由を理解する上でも役立った。PwC の分析から、ランサムウェアの被害組織に対して、以下のような戦術が用いられていることが分かった：

- Conti ブランドのスタッフが、被害組織データの公開予定日までの残り時間（カウントダウンタイマー）について頻繁に言及する
- 非公開のブログ記事で、被害組織のデータやファイルディレクトリの設定などを記し、侵害の「証拠」を示す
- 交渉なしで迅速に身代金を支払った被害組織には割引する、と勧める
- 身代金の支払額と窃取されたデータの価値と修復費用を見積もり、比較データを被害組織に示す
- 被害組織のクライアント、パートナー、投資家とコンタクトを取ると脅す [169]

Blue Cronus の活動と最新情報

ロシアがウクライナに侵攻した翌日の 2022 年 2 月 25 日、Conti ランサムウェアグループの背後にあって以前 PwC が White Onibi として追跡調査した脅威アクターである Blue Cronus が、ロシアの行動を支持する公的声明を発表した。その後、2022 年 2 月 27 日から 2022 年 3 月 2 日にかけて、ある Twitter アカウントが Blue Cronus の活動に関する内部データを次々と公開し、2020 年 6 月まで遡ってアーカイブした 10 万件以上のインスタントメッセンジャー通信を通じて、前例のないレベルの詳細や内部工作を明らかにした。これらの通信を調査し、脅威アクターの活動を分析した結果、脅威アクターである White Magician（別名 TrickBot、Bazar、Anchor）、White Onibi（別名 Conti、Ryuk）、White Taranis（別名 Emotet）は、本質的に同一犯罪組織を構成する組織であり、PwC は 2022 年 3 月 Blue Cronus とした [170]。

[167] *CTO-SRT-20221019-01A - Ransomware report for September 2022*

[168] 'Experts concerned about ransomware groups creating searchable databases of victim data', Recorded Future, https://therecord.media/experts-concerned-about-ransomware-groups-creating-searchable-databases-of-victim-data/ (14th July 2022)

[169] *CTO-SIB-20220324-01A - Negotiation tactics and internal dynamics*

[170] *CTO-QRT-2022-20220315-02A - In the leak midwinter*

Blue Cronus の活動に関するこれらの開示とその後の評価は、Conti ブランドの明らかな段階的廃止と解消を示しているにもかかわらず、脅威アクターの動きを鈍化させることはなかった。2022 年 4 月、PwC が White Dev 115 として追跡調査しているランサムウェアの脅威アクターである BlackBasta は、ロシア語のサイバー犯罪フォーラム「Exploit」と「XSS」に投稿して活動を開始した。Blue Cronus が配信メカニズムとして Qakbot を使用したことに加え、White Dev 115 も被害組織のネットワークへの初期アクセス時に一貫して Qakbot を使用していた。PwC は、White Dev 115 がランサムウェア亜種 Blue Cronus のポートフォリオの一部である可能性が非常に高いと評価している [171]。

先行者の規模拡大

サイバー犯罪者は、特に業界全体規模で実装されるセキュリティ強化策に対応する際、最もアジャイルかつ前向きに進化する脅威アクターであり、これは 2022 年の前触れ的な活動にも見てとれた。

2022 年 7 月、Microsoft がインターネットからダウンロードした Microsoft Office 文書のマクロをデフォルトでブロックするというポリシーを打ち出したことで、一部のサイバー犯罪者が反応したことが、この年の注目すべき傾向として挙げられ [172]、このレポートでも詳しく説明している（「攻撃に関する知見と傾向：マクロがなければ問題なし？」）。Bumblebee（別名 Blue Cronus）、IcedID（別名 White Khione）、Qakbot（別名 White Horoja）の背後にいる脅威アクターは、2022 年に Microsoft が実施した変更に対抗するための回避策を開発し、よりカスタムメイドで完全に高度な攻撃プロセスを生み出したのである。このプロセスでは、ISO ファイルと LNK ファイルを組み合わせ、被害組織の端末にマルウェアローダーをドロップして実行するための複数の段階が設けられている [173]。

Bumblebee

2022 年前半、TrickBot と BazarLoader に代わるものとして Blue Cronus が開発した Bumblebee と呼ばれる初期段階のマルウェアローダーが出現した。Bumblebee には高度な仮想化対策テクニックが組み込まれており、Metasploit や Cobalt Strike などのポストエクスプロイトキットを配信する機能を備え、すぐにランサムウェア攻撃で多用されるようになった。Bumblebee は、ほぼフィッシング攻撃によって配信され、被害組織の目から合法的に映るようにメールのスレッドを乗っ取り、請求書や会議の議題、被害組織から回答を引き出すためのその他文書を装って配信されることが多い。また、このメールには被害組織の「個人パスワード」が記載されており、パスワードで保護された悪意ある ZIP アーカイブや ISO ファイルを開くよう、被害組織をさらに誘い込む。被害組織が悪意あるファイルを開くと、Bumblebee が LNK ファイルを通じて被害組織の端末にロードされる [174]。

---

171 *CTO-SIB-20221222-01A - Blue Cronus and Black Basta*

172 'Macros from the internet will be blocked by default in Office', Microsoft, https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked (11 October 2022)

173 *CTO-TIB-20221014-01A - ISO-lemnly swear, that we are up to no good*

174 *CTO-TIB-20220729-02A - New Queen of the APIary*

IcedID

IcedID は、PwC が White Khione によるものと評価している、バンキング型トロイの木馬からマルウェア配信システムになったもので、被害組織のシステムまたはネットワークへの最初のエントリポイントとして、多くの脅威アクターによって使用されている。2022 年、Microsoft によるマクロのデフォルト無効化を受けて、White Khione は IcedID を更新し、マクロを含む悪意ある Excel スプレッドシートの使用から ISO ファイルの使用に移行した。これらのファイルは、White Khione の有名な Fake Legal Threat フィッシングキャンペーンとの組み合わせにより、ペイロードを配信するために一貫して使用されてきた。

Qakbot

Qakbot（別名 Qbot、Pinkslipbot）は、PwC が White Horoja として追跡調査している脅威アクターによって管理されており、2007 年から用いられている。バンキング型トロイの木馬として誕生した Qakbot は、2021 年に、ローダー機能、カスタムパッカー、アンチ・サンドボックス・フェイルセーフ、アンチ・デバッグ・テクニックを誇る、完全モジュール型のマルウェアツールキットへと進化し始めた。Qakbot は、現在もあらゆる種類のおとり文句を利用したフィッシング攻撃によって配信されているが、2022 年には、マクロ化 Office ファイルの使用から、悪意ある MSI に埋め込まれパスワード保護された ZIP アーカイブにパッケージするかたちで配信されるようになった [175]。

Blue Cronus による White Taranis の再生

White Taranis（別名 Emotet）は、2021 年後半に Blue Cronus によって再生され、再び姿を現した。2022 年前半における White Taranis の活動は、C2 インフラ、スパムエンジンおよびシステム偵察能力のアップグレード実施に伴う一時的な中断を挟みつつも、安定的に進んだ [176]。Blue Cronus は、ペイメントカード認証情報の収集機能を含む、いくつかの旧機能も復活させた [177]。Blue Cronus「stable」の他のメンバーと同様に、Conti ランサムウェアの運用停止は White Taranis のキャンペーンに直ちに影響を与えることはなかったが、2022 年 7 月中旬までに White Taranis の活動が突然停止し、2022 年 11 月初旬まで休眠状態となった。スパムキャンペーンは 2022 年 11 月に本格的に再開され、ペイロードは、被害組織の端末上で White Taranis のバイナリをダウンロードして実行するマクロを含む、悪意ある Microsoft 文書で構成されていた。

Microsoft がマクロのデフォルト設定を変更した後、Blue Cronus は、受信者に悪意ある添付ファイルをテンプレートフォルダにコピーさせ、その場所から文書を開くように指示することで、この保護を回避しようとした。この操作により、悪意あるドキュメントから Mark of the Web（MotW）フラグが削除され、一度開いたファイルは「保護されたビュー」で開かれなくなり、マクロが実行されて Emotet バイナリのインストールが可能となった [178]。脅威アクターがこの手法を続けるか、Blue Cronus が Bumblebee や IcedID の配信に使用している手法に切り替えるかは、まだ不明である。

---

175 *CTO-TIB-20220525-01A - Duck, Duck, Bot: Qakbot evolves!*
176 *CTO-TIB-20221104-01A - More modules, More Problems*
177 *CTO-QRT-20220728-01A - You can't keep a good botnet down*
178 *CTO-QRT-20221103-01A - Emotet resumes operations*

Bumblebee、Qakbot、IcedID のキャンペーンでよく見られるテクニックの検出方法

これらのローダーを配信することで、脅威アクターは効果的な攻撃ルートへと収束していき、キャンペーンごとのわずかなバリエーションが見られるのみとなった。こうしたバリエーションにかかわらず、これらの攻撃パスは互いに交差するポイントがある。このポイントこそ、PwC が検出し、悪意ある活動の可能性を示す証拠をピンポイントで示すことができる部分である。

脅威アクターは、Microsoft OneDrive や Google Drive へのリンクを配信し、アーカイブファイルをダウンロードするようユーザーを誘導することが確認されている。これらのドメインは、ほとんどの組織で許可リストに登録されているため、この方法は有効である。また、HTML スマグリングと呼ばれる手法で、悪意ある HTML ファイルをユーザーに配信し、そのファイルを開くよう促す場合もある。HTML ファイルには難読化されたペイロードが埋め込まれており、JavaScript を使用してブラウザがこれをアセンブルしてユーザーの端末に書き込む。ユーザーが 1 つの HTML ファイルを電子メール添付で受領したというログがあれば、その後にブラウザで HTML ファイルが実行されると、当該ファイルがユーザーのダウンロードディレクトリに起因する場合に、連鎖的な検出が可能である。

前述のように、パスワードで保護されたアーカイブは、脅威アクターの間でよく用いられる。組織がアーカイブツールを分析し、復号に関連するコマンドラインパラメータを抽出すれば、暗号化されたアーカイブをディスクに解凍するユーザーに対して情報検出の構築が可能である。このようなアーカイブには ISO ファイルが含まれていることが多く、マウントされると、ペイロードの実行を促す起動引数を持つショートカットファイルが表示される。また、DLL ペイロードの使用も一般的になってきているため、脅威アクターはペイロード実行に rundll32.exe などのシステムバイナリを悪用することを検討している。「C ドライブ」以外で DLL を起動する rundll32.exe の検出は、一般的にロバストであるため、攻撃者は rundll32.exe の正規コピーを送り、同じ動作を実行しようとする。これを検出するために、組織は System32 ディレクトリの外での実行を探すか、名前が変更されている場合は、プロセス名がないバイナリに固有のコマンドライン引数の検出を行うことができる。

実行時、ペイロードが Windows Defender の機能を無効にし、直ちに自らのために除外項目を追加しようとすることが確認された。このような挙動パターンに対応するため、ペイロードがこれらの強制的な設定変更を実施するために行うレジストリ変更について、定義を行った。

ハッカー、詐欺集団、窃盗集団

2022 年、サイバー犯罪者は Microsoft のデフォルトマクロ設定に対抗すべく迅速な変化を図ったが、他の脅威アクターも多要素認証（MFA）を回避するための戦術において常にアジャイルな姿勢を取っている。脅威アクターが MFA 保護に遭遇する機会が増えているため、MFA 消耗作戦、修正を施

した認証情報の窃取機能、強化されたフィッシング・アズ・ア・サービス（PHaaS）提供など、MFA バイパス機能に対する需要も高まっている。

この点については、本レポートの後半「攻撃に関する知見と傾向：MFA の増加、回避策の増加」で詳述している：

LAPSUS$ の判定

PwC が White Dev 111（別名 LAPSUS$ Group）として追跡調査している窃盗恐喝グループは、2022 年に Samsung、NVIDIA、Microsoft などの大企業への攻撃で注目を集め、Okta、Uber、Rockstar に侵入したと主張して国際的にも有名になった。White Dev 111 は、ソーシャルエンジニアリングや MFA 消耗作戦など、セキュリティの人的要素を狙った攻撃を行い、「スマッシュ＆グラブ」戦術を用いて、有名な組織を標的にしていた [179]。White Dev 111 は、2021 年 12 月にブラジル保健省への侵入に成功した後、初めて表舞台に登場した [180]。同省への侵入で 50TB 分のデータを盗んだと主張している。White Dev 111 は Telegram チャネルで被害組織を宣伝し、そのチャネルを利用して、複数の大手テック、ゲーム、通信組織の「従業員／内部関係者」の募集広告を掲載し、会社の「VPN または Citrix」ログインへのアクセスを要求した [181]。

多くの国が White Dev 111（別名 LAPSUS$ Group）の活動に関与したとされる 10 代の若者を逮捕しているが [182, 183, 184]、脅威アクターの TTP と目的は、世界中の組織にとって依然として懸念材料である。

嘘吐き、イカサマ師、インフォスティーラー

2022 年、認証情報を窃取するマルウェアはアンダーグラウンド経済で流行り、RedLine [185]、Raccoon [186]、Vidar [187] といったシステムが、認証情報侵害市場を独占した。これらの情報窃取マルウェア開発者（別名インフォスティーラー）が、組織のセキュリティ環境保護のために MFA を導入する組織が急増する中で、ツールの調整を図ったことが大きな要因である。

---

179 *CTO-QRT-20220920-01A - Uber and Rockstar breaches*

180 'Brazil health ministry website hit by hackers, vaccination data targets', Reuters, https://www.reuters.com/technology/brazils-health-ministry-website-hit-by-hacker-attack-systems-down-2021-12-10/ (10th December 2022)

181 *CTO-TIB-20220406-01A - LAPSUS$ Group has entered the chat*

182 'Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal', BBC News, https://www.bbc.com/news/technology-60864283 (24th March 2022)

183 'UK police arrest teenager suspected of Uber, GTA 6 hacks', TechCrunch, https://techcrunch.com/2022/09/26/london-police-arrest-uber-rockstar/ (26th September 2022)

184 'PF prende brasileiro suspeito de integrar organização criminosa internacional', Brazilian Ministry of Justice and Public Security, https://www.gov.br/pf/pt-br/assuntos/noticias/2022/10/pf-prende-brasileiro-suspeito-de-integrar-organizacao-criminosa-internacional (19th October 2022)

185 *CTO-TIB-202209-01A - The Rise of RedLine*

186 *CTO-TIB-20220914-02A - Raccoon Stealer 2.0*

187 *CTO-TIB-20230113-01A - Vidar Stealer*

2022 年を通じて、認証情報窃取マルウェアの開発者は、セッションクッキーを吸い上げる機能を追加・強化し、特定の状況下で MFA を容易に回避することが可能になった。

2022 年 3 月、Raccoon Stealer は突然活動を停止した。マルウェア開発者の報告によれば、ウクライナでロシアの侵攻によりリーダーが死亡したためという [188]。2022 年半ばまでに、Raccoon Stealer の開発者は、こうした大きな出来事にもかかわらず、強化した機能を誇る Raccoon Stealer の新バージョンの開発を継続すると犯罪者顧客層に約束していたが、2022 年 10 月、米国政府は、開発者のリーダーはウクライナ人で、ウクライナでは殺害されておらず、2022 年 3 月にオランダ警察に逮捕されたと発表した。その後 Raccoon Stealer インフラは国際法執行機関の協働的取り組みにより解体されて、開発者は活動のリローンチを余儀なくされた [189]。

凄まじいフィッシング

2022 年、サイバー犯罪者は、巧妙なメッセージと一要素認証からなる、絶対確実なフィッシング戦術に頼り続けた。また、フィッシングメールの作成・配信やフィッシング作成のためのインフラやツールを提供する Glitch や Gophish といった、主にセキュリティ実務者を対象とした無償のサービスを利用する脅威アクターも多く見られた。また、フィッシング攻撃を行う脅威アクターは、政府機関や法執行機関になりすますことへの躊躇が皆無である様子に変わりはない。有名な詐欺師である Ramon Abbas（別名 HushPuppi）の逮捕を機に、米国司法省の犯罪被害者対策室（Office of Victims of Crime）を騙り、標的からさらに情報を奪おうとしたり、個人の金融情報の窃取を図ろうとしたりした脅威アクターの事例もあった [190]。

不具合にとどまらない

フィッシング攻撃を行うためのインフラ構築・維持は、費用と労力を要する作業である。また、ホスティングプロバイダーによってインフラがダウンしたり、Web ブラウザによってブロックされたりするなど、脅威アクターにとって特にフラストレーションが溜まることになる。そのため、脅威アクターは、フィッシングの運用に、無料かつ使いやすいプラットフォームやサービスを求めている。Glitch は、西アフリカを拠点とするビジネスメール侵害（BEC）の脅威アクターが使用した、無料で使用できるクラウドベースのソフトウェア開発プラットフォームの 1 つであった。Glitch のプラットフォームには無料版があり、ユーザーは Glitch が提供するホスト名でパブリックな Web アプリケーションを迅速に展開することができる。脅威アクターは Glitch と LogoKit として知られる古いフィッシングキットを組み合わせて、ニセの電子メールのログイン

188 *CTO-TIB-20220914-02A - Raccoon Stealer Returns.*

189 'United States of America v. Mark Sokolovsky', US Department of Justice, https://www.justice.gov/usao-wdtx/page/file/1546626/download (26th September 2022)

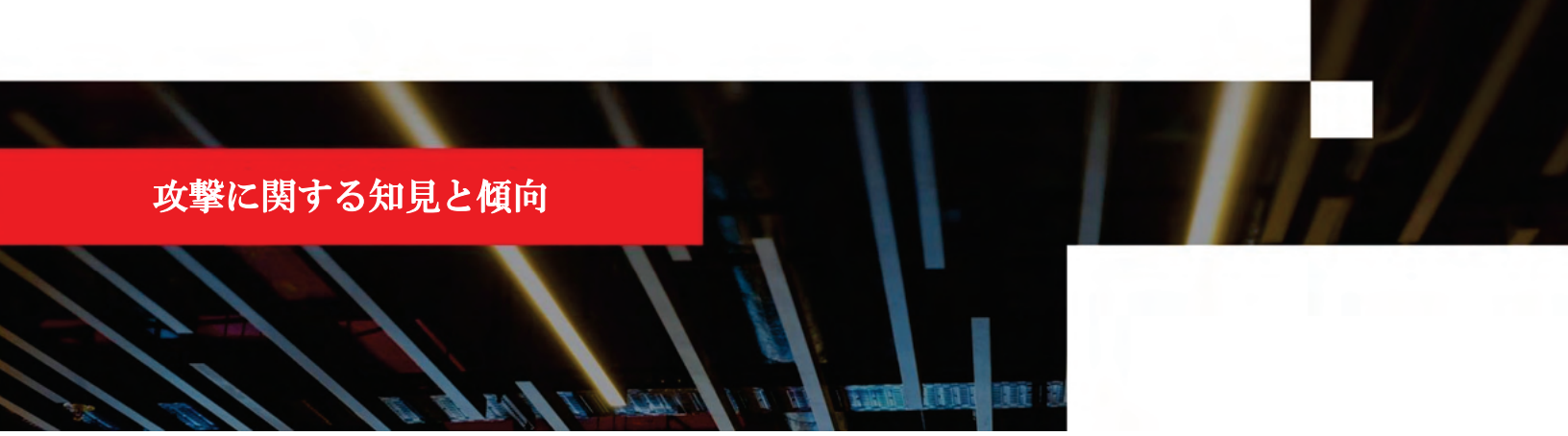
190 'Nigerian Man Sentenced to Over 11 Years in Federal Prison for Conspiring to Launder Tens of Millions of Dollars from Online Scams', US Department of Justice, https://www.justice.gov/usao-cdca/pr/nigerian-man-sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions (7th November 2022)

を作成し、ユーザーの認証情報を取得、これを被害組織のネットワークにアクセスするために使用した[191]。

2022 年には、EvilProxy、Caffeine、Robin Banks ツールキットなど、需要の高い機能や特徴を提供する新しいプロバイダーが複数登場した。EvilProxy は 2022 年半ばに登場し、フィッシング被害組織と企業のログインポータルの間の中間者（AitM）として動作し、サイバー犯罪者にフィッシングキャンペーン配信をカスタマイズして自動化する GUI を備える。また、全ての使用料も低額である。EvilProxy は、MFA を回避するための認証情報とクッキーの盗用機能の両方を促進し、Google、Microsoft、LinkedIn などの大企業のサインオンポータルやその他のサービスを侵害する能力を宣伝している。

EvilProxy のポイント＆クリックによる簡単操作は、サイバー犯罪のエコシステム内で成長を遂げている市場における一製品であり、オンデマンドおよび使用料ベースの機能開発を促進するとともに、さまざまな脅威アクターが攻撃に関与する参入ハードルを一層引き下げている。

[191] *CTO-SIB-20220811-01A - A glitch in the BEC system*



攻撃に関する知見と傾向

2022 年を通じて、新しいテクノロジーや共通の脆弱性が攻撃者と防御者の間に浸透し、それぞれが相手の優位に立とうと模索する中、深層防御の必要性が浮き彫りとなった。攻撃者は、より高度なツールやフレームワークを活用して攻撃を行うようになり、また、防御者が実装するセキュリティ対策を凌ぐために TTP の修正を図った。このような変化は、リモート・デスクトップ・プロトコル（RDP）の露出したインスタンスや、MFA で保護されていないシステムを悪用するなど、従来の方法の継続的使用と相まって、脅威を生み出している。

ツール・フレームワーク

2022 年を通じて、ツールやフレームワークの事例が数多く業界全体で議論され、追跡調査された。また、正規のレッドチームと悪意ある攻撃者の間で、これらがどのように使用されているかに関して認識が高まっていることが確認された。

こうしたフレームワークは急速な進化を遂げており、防御側にとって課題ではあるが、同時に、検出の機会をもたらすものでもある。場合によっては、防御者が特定のフレームワークの使用を検出した場合、同一または類似のアプローチで、他のフレームワークの検出に至る可能性もある。

2022 年に業界全体で有名になったフレームワークもある中で、Cobalt Strike は引き続き、幅広い脅威アクターによって使用され、最も悪用されたポストエクスプロイトフレームワークであった。特定のフレームワークの使用を単独で検出することは、防御側にとって依然として課題であり、今後数年間はより困難さを増す可能性が高い。

Cobalt Strike の検出

Cobalt Strike のデフォルト設定はよく知られており、例えば、ドメイン名に.stage.を使用するデフォルト DNS C2 など、検出しやすい。以下のネットワーク検出ルールでは、通常aaa.stage.*というクエリで始まる標準的な形式を検索する。

ネットワーク

```
alert dns any any -> any any (msg:"[PwC] Generic - CobaltStrike - DNS query for
.stage."; \
   dns_query; content:".stage."; \
   pcre:"/^[a-z]{3}\.stage\.[0-9]+\.(?:[a-z0-9-]+\.)+[a-z]{2,4}$/"; \
   classtype:domain-c2; \
   metadata:copyright,Copyright PwC Threat Intelligence 2017; metadata:tlp green; \
   metadata:confidence Medium; metadata:efficacy Medium; \
   metadata:mitre,T1071/004; \    metadata:author RM; metadata:created 2020-07-07; \
   sid:200100001; rev:2020070701;)
```

Brute Ratel

Brute Ratel は商用 C2 フレームワークとして複数の脅威アクターによって使用されたため、2022年をかけて知名度が向上していった[192]。昨年、Brute Ratel のさまざまなバージョンが流出し、クラックされたが、このフレームワークは簡単にカスタマイズして拡張可能である。デフォルトでは、EDR（Endpoint Detection and Response）/AV（Antivirus）のアンフック、さまざまな C2 メカニズム、API の間接実行など、検出回避に利用可能なさまざまな機能を有している。

192 'When Pentest Tools Go Brutal: Red-Teaming Tool Being Abused by Malicious Actors', Palo Alto Unit 42, https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/ (5th July 2022)

Brute Ratel の検出

防御者として、**Brute Ratel** の検出を可能にするさまざまなデフォルトがあり、例えば YARA を使用したメモリ上／ディスク上の **Brute Ratel** や、デフォルトの SSL 証明書やドメインを特徴とするネットワークトラフィックを検出できる。

YARA

```
rule Brute_Ratel_PE_Badger_API_Loading_Routine : Heuristic_and_General
{
   meta:
      description = "Detects Brute Ratel Badger payloads (PE and DLL) based on a unique routine used to
dynamically load APIs"
      TLP = "AMBER"
      author = "PwC Threat Intelligence"
      copyright = "Copyright PwCIL 2022 (C)"
      created_date = "2022-09-29"
      modified_date = "2022-09-29"
      revision = "0"
      hash = "4de333f164d70b59849c3aa12a9c95cdcbecae3023386ee08c15b38874260941"
      hash = "dc71c5721fa6b3148a3a0564931dc063d03694ca57aa61e8c2532b5a565b2548"
      hash = "ef803ea871c974623ceb678548c938826b683c857adc85a6bf8af34c8b61fc52"

   strings:
      // 8B5324       MOV EDX,DWORD PTR [RBX+24]
      // 4D01DB        ADD R11,R11
      // 8B431C       MOV EAX,DWORD PTR [RBX+1C]
      // 4D01D3       ADD R11,R10
      // 410FB71413    MOVZX EDX,WORD PTR [R11+RDX]
      // 498D1492      LEA RDX,[R10+RDX*4]
      // 8B0402       MOV EAX,DWORD PTR [RDX+RAX]
      // 4C01D0       ADD RAX,R10
      $ = {8B53244D01DB8B431C4D01D3410FB71413498D14928B04024C01D0}

   condition:
      all of them
}
```

ネットワーク

```
alert dns any any -> any any (msg:"[PwC] Generic - Brute Ratel - C2 node evasionlabs[.]com in DNS
query"; \
   dns.query; \
   content:".evasionlabs.com"; endswith; \
   threshold: type limit, track by_src, count 1, seconds 3600; \
   classtype:domain-c2; \
   metadata:copyright,Copyright PwC Threat Intelligence 2022; \
   metadata:tlp green; metadata:confidence High; metadata:efficacy Low; \
   metadata:mitre,T1071/004; \
   metadata:author RM; metadata:created 2022-09-29; \
   sid:222092910; rev:2022092901;)
```

Sliver

Brute Ratel とは異なり、Sliver はオープンソースのフレームワークであるため、利用者はフレームワークをより容易にカスタマイズ可能である。Sliver は、mTLS（mutual Transport Layer Security）や Wireguard を含むさまざまな C2 メカニズムをサポートしており、またビーコン・オブジェクト・ファイル（BOF）をサポートしていることから、Cobalt Strike プラグインを再利用することも可能である。

Sliver の検出

mTLS の設定はハードコーディングされており、JARM のフィンガープリントは一貫している（28d28d00028d00043d28d43d47390d982d099a542ccbc90628951062）。防御者が HTTPS トラフィックを検出できる場合、サーバーの応答ヘッダは、HTTP リクエスト形式同様、一貫性があることを指す。また、Wireguard のトラフィックは、ネットワークトラフィックの中で非常に特定・検出しやすい。

YARA

```
rule Sliver_Protobuf_Symbol : Heuristic_and_General
{
   meta:
      description = "Detects symbol in Sliver implants (PE, ELF, Mach-O and shellcode) referencing a
custom protobuf module"
      TLP = "AMBER"
      author = "PwC Threat Intelligence"
      copyright = "Copyright PwCIL 2022 (C)"
      created_date = "2022-10-18"
      modified_date = "2022-10-18"
      revision = "0"
      hash = "41cf473fe535b932c68e9f295680fe228cde0094a8bac70ccb68c21aaff22188"
      hash = "c12c33111b41bf2be458004d532f1255fd734057d2c7bf59e0877e31dbedfd4e"
      hash = "3b4c57e04422825609bc70dfa5bf741cded6961df87369b530c45720eee828fd"
      hash = "4c668595d6767e9cdb68f875aab9d4d39ae0ff94d94e76dc301eb336f1d74096"
      reference = "https://github.com/BishopFox/sliver"

   strings:
      $ = ".sliverpb."

   condition:
      // Note, you can remove these file signature checks to wider the rule further
      (
         // PE
         uint16(0) == 0x5A4D or
         // Shellcode
         uint32be(0) == 0x4883e4f0 or
         // Mach-O
         uint32be(0) == 0xcffaedfe or
         // ELF
         uint32be(0) == 0x7f454c46
      ) and
      any of them
}
```

ネットワーク

```
alert udp any any -> any any (msg:"[PwC] Policy - Tunnelling - Wireguard VPN client handshake";
flow:from_client; dsize:148; \
    content:"|01 00 00 00|"; startswith; \
    content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; endswith; \
    flowbits:set,PwC.Policy.Tunnelling.Wireguard; target:src_ip; \
    reference:md5,b82a587befc34c0db00eed5c4117d88d343b8b895f03fc409a55d9240cf9fde1; \
    classtype:pup-activity; \
    metadata:copyright,Copyright PwC Threat Intelligence 2022; metadata:tlp green; \
    metadata:confidence High; metadata:efficacy Low; \
    metadata:mitre,T1133; \
    metadata:author RM; metadata:created 2022-05-04; \
    sid:222050432; rev:2022050401;)
```

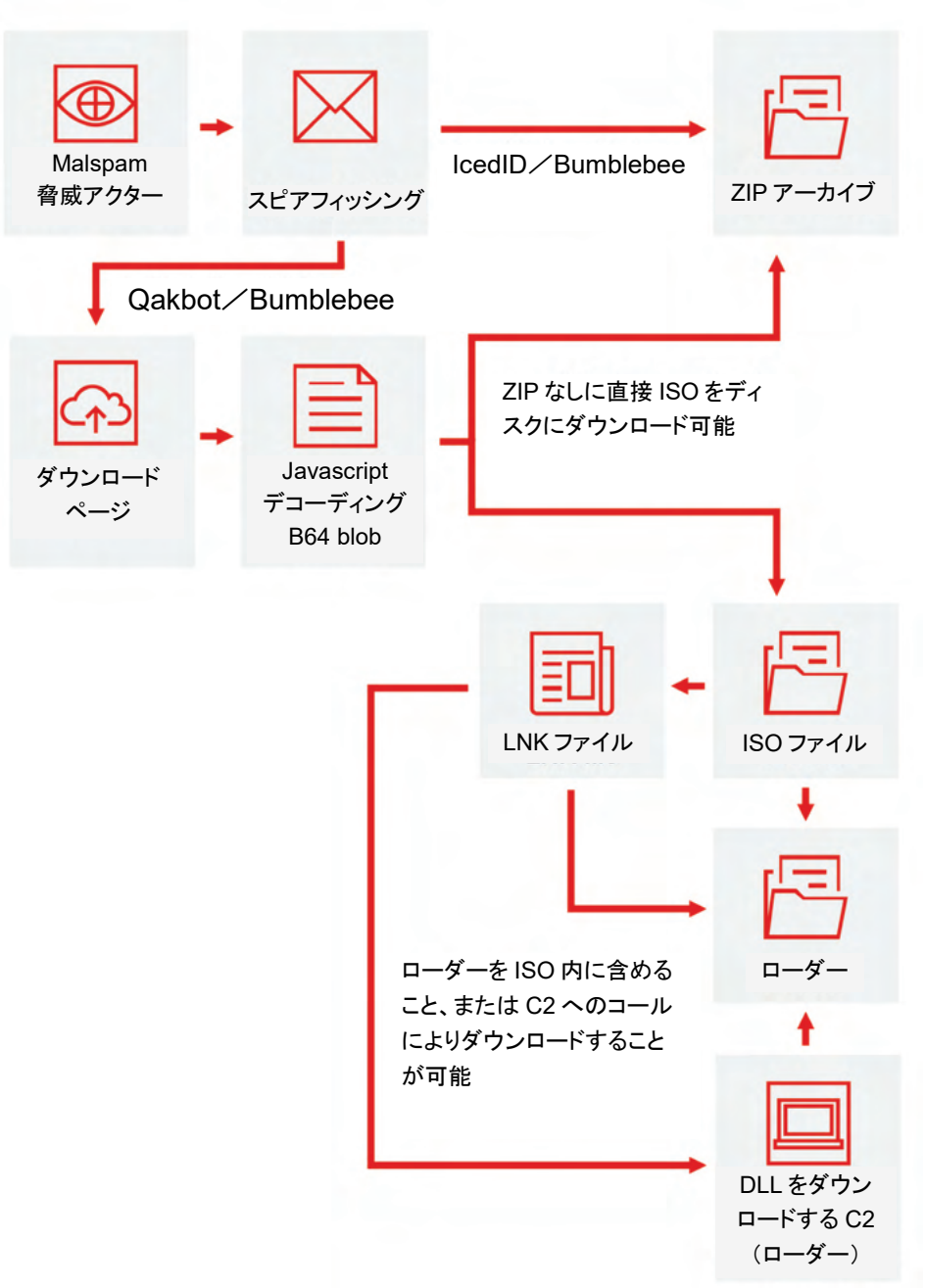
マクロがなければ問題なし？

脅威アクターはこれまで、フィッシングメールに添付された悪意あるドキュメントを用いるなど、被害組織に送るマルウェアの実行の際、主にマクロ機能を利用してきた。悪意あるファイルが被害組織の介入なしにマクロを自動実行する機能を持たないため、脅威アクターは、被害組織の操作やシステムによる防御をできるだけ回避しつつ他の自己実行型手法に頼らざるを得なかったのである。PwC は、Microsoft による 2022 年のアップデートで Mark of the Web（MotW）がデフォルト設定で無効になったことにより [193]、脅威アクターが、マクロ実行に頼る悪意ある文書を用いた組織への標的攻撃手法の見直しを迫られたことを確認した。さらに、リソース、洗練度、目的などさまざまに異なる脅威アクターは、標的への初期アクセス方法としてマクロ以外の方法を模索しているものと見られ、その証左として以下の感染経路が確認されている：

- ISO ファイル（事実上アーカイブファイルとして機能する）を使用して悪意あるペイロードを配信
- LNK（ショートカット）ファイルを使用して、正規のドキュメントを装った（実際には悪意ある）ペイロードを実行

193 'Macros from the internet will be blocked by default in Office', Microsoft, https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked (11th October 2022)

ISO + LNK ファイルによる感染チェーンの例



悪意ある恐れのある ISO ファイルや LNK ファイルの検出

ISO ファイルは、物理的なディスクイメージの複製という正当な目的で使用される。マルウェアを含む ISO ファイルを検出するには、正規の ISO ファイルのプロファイルを踏まえた上で、ベースラインからの逸脱を探す必要がある。例えば、企業環境では、ISO ファイルはソフトウェアの大規模なインストール作業のために管理者アカウントによって扱われる事例がある。この点を念頭に置き、標準ユーザーアカウントで作成された ISO ファイルや、サイズの小さい ISO ファイルに対して検出を行うことができる。また、ISO ファイルをディスクに書き込む、よく悪用されるアプリケーションのシグネチャも可能である。この動作の検出に関して特に注意すべきアプリケーションは、フィッシングの主要な手段である事例が多い、電子メールクライアントと Web ブラウザなどである。

アーカイブ内から ISO ファイルを開くと一時ファイルがディスク上に作成されるため、このファイル作成イベントからのアラートにより、攻撃の初期段階を検出することができる。これと同じメカニズムで、アーカイブ内の LNK ファイルを検出することも可能である。多くの組織では、アーカイブ内の LNK ファイルはある程度の頻度で発生する可能性があるため、インシデントの確認にはアラートを他の行動と関連付ける必要があるものの、LNK ファイルは脅威アクターにより多く使用されることから、組織によっては、そうした関連付け自体がさらなる分析の機会となる。

MFA の増加、回避策の増加

特権アクセスや ID・アクセスマネジメント（IAM）に MFA を採用する組織が増える中、脅威アクターは、被害組織に対する MFA 消耗攻撃を採用した White Dev 111 の事例に見られるようなソーシャルエンジニアリングから、サイバー犯罪者やより高度な脅威アクターが用いるマルウェアに組み込まれるレベルの技術的検出回避テクニックへと移行している。

例えば、PwC が 2022 年に発生したインシデント対応事例で分析した脅威アクターBlue Dev 5（別名 NOBELIUM）が挙げられるが、この脅威アクターは、被害組織の Microsoft Azure Active Directory（AD）環境にアクセスするために、休止アカウントを悪用して MFA による保護を回避していたことが分かった。Blue Dev 5 は、有効な認証情報を使用してアカウント認証をパスしたが、この休止アカウントは被害組織が MFA を導入する前に作成されたものだった。Blue Dev 5 は、侵害アカウントを使用して、新しい MFA 方式のソフトウェア OATH トークンを登録した [194]。

194 *CTO-QRT-20220720-01A - Blue Dev 5 - MFA Evasion using dormant accounts*

Blue Dev 5（別名 NOBELIUM）による MFA 回避インシデントの教訓

このインシデントの分析には、2022 年 7 月に見られた以下の Blue Dev 5 関連侵害指標（IoC）が含まれ、過去ログからの検索や検出アラートへの追加が可能であった：

- 198.244.224[.]89[195]

PwC は、少なくとも 14 日間ログインしていないユーザーに対して、MFA 登録の検出設定を推奨する。これにより、本インシデントで説明したようなアクティビティを検出することができる。

また、Microsoft のクラウド環境では、ナンバー照合などの安全な認証方法で MFA を実施し、Microsoft Azure AD Incident Response PowerShell Module が提供する以下のコマンドを使用して、現在 MFA が登録されていないアカウントを積極的に特定することを推奨する：

- Get-AzureADIRMfaAuthMethodAnalysis[196]

クラウドを標的に

被害組織に侵害するために、クラウド環境を標的とする脅威アクターが増加している。これはおそらく、組織がクラウドテクノロジーの統合化を進めていることへの対応であり、脅威アクターは脆弱性や設定ミスを利用して膨大なデータのロックを解除できるようになった。2022 年初頭、PwC は Blue Dev 5 に関する別のインシデントに対応したが、この事例では、脅威アクターがクラウド・サービス・プロバイダー（CSP）を侵害することで、被害組織のクラウド環境への初期アクセスを獲得していた [197]。この CSP は、被害組織の Microsoft Azure AD と O365 テナントの代理管理者（Delegated Administrator[198]）権限を持っており、脅威アクターは、被害組織の Microsoft クラウド環境への実質的な管理アクセスを得ることができた。

このアクセスを利用して、Blue Dev 5 はバックアップアプリケーションが使用する Azure AD Service Principal[199] にパスワード認証情報を追加し、脅威アクターは正規のバックアップアプリケーションと同じ権限で被害環境にログインできるようになった。Blue Dev 5 は、これらの認証情報を使用してバックアップアプリケーションとして認証し、Exchange Web Service（EWS）[200] クラウド API を Exchange Online（O365）に呼び出した。バックアップアプリケーションの権限により、被害組織の全 O365 ユー

195 *CTO-QRT-20220720-01A - Blue Dev 5 - MFA Evasion using dormant accounts*

196 'Azure AD Incident Response PowerShell Module', Microsoft, https://github.com/AzureAD/Azure-AD-Incident-Response-PowerShell-Module

197 'What is a cloud service provider', Microsoft, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-cloud-provider/

198 'Delegated admin privileges in Azure AD', Microsoft, https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-delegated-administration-primer (12th March 2023)

199 'Application and service principal objects in Azure Active Directory', Microsoft, https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals (15th December 2022)

200 'Explore the EWS Managed API, EWS, and web services in Exchange', Microsoft, https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/explore-the-ews-managed-api-ews-and-web-services-in-exchange (13th June 2022)

ザーアカウントのメールにアクセスし、流出させることが可能になったのである。Blue Dev 5 はその後、同じ被害組織への活動においてこれらの手法をミラーリングし、別の CSP も侵害した [201]。

Blue Dev 5（別名 NOBELIUM）による CSP 侵害インシデントの教訓

このインシデントで分析された以下の IoC は、もはや使用されていないと PwC は評価しているが、過去のログの検索やアラートを支援するために提供している：

- 193.8.172[.]208 - 2021 年 7 月から 2021 年 8 月まで確認
- 18.130.157[.]66 - 2021 年 7 月に確認
- 18.169.208[.]15 - 2022 年 1 月から 2022 年 2 月まで確認
- 79.143.87[.]14 - 2022 年 3 月頃確認 [202]

さらに、この事例への対応を通じて、PwC は、Blue Dev 5 や、同様の TTP を利用する他の脅威アクターに対して Microsoft Azure AD および O365 環境を堅牢化するための一連の推奨事項を策定した：

- MSP（マネージド・サービス・プロバイダー）やその他のサードパーティとのパートナー関係から代理管理者権限を削除するか、または、詳細代理管理者権限（Granular Delegated Administrator Privileges）[203] を使用して、厳密に必要な場合にのみ、サードパーティに時間制限管理アクセスを許可する
- 全てのユーザーに対して強力な MFA 方法を設定する（ナンバー照合によるプッシュ通知など）[204]
- Azure AD と O365 のログを、既存の SIEM または新しい Microsoft Sentinel にオンボードする
- Azure AD および O365 の侵害によく使われる手法の検出ルールを設定する
- Azure AD と O365 の特権アカウントの使用を監査し、セキュリティを確保する
- Azure AD サービスプリンシパル、アプリケーションの認証情報、機密性の高い権限を監査し、その継続的な使用を監視する
- 条件付きアクセスルール [205] を使用して、機密性の高いサービスプリンシパルへのログインを IP アドレスの許可リストに制限し、サービスプリンシパルを保護する [206]

インシデント対応事例から得られたその他の知見

本レポートですでに取り上げたインシデント対応事例に加え、PwC ではより広範なデータセットを分析し、さらなる傾向や知見を得た。2022 年、PwC が分析したインシデント対応事例の 63%は、金銭

201 *CTO-TIB-20220429-01A - Bearing down on the Clouds*

202 *CTO-TIB-20220429-01A - Bearing down on the Clouds*

203 'Introduction to granular delegated admin privileges (GDAP)', Microsoft, https://docs.microsoft.com/en-us/partner-center/gdap-introduction (8th August 2022)

204 'How to use number matching in multifactor authentication (MFA) notifications (Preview) - Authentication Methods Policy', Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match (30th November 2022)

205 'Conditional Access for workload identities preview', Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/conditionalaccess/workload-identity (21st November 2022)

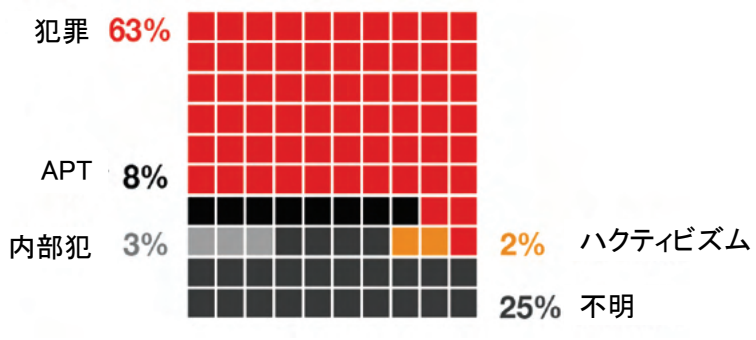
206 *CTO-TIB-20220429-01A - Bearing down on the Clouds*

目的の脅威アクターによる攻撃であり、その約半数はランサムウェア攻撃によるものだった。2022 年に分析したランサムウェア事例のうち、被害を受けた上位 3 セクターは製造、建設、小売で、2022 年におけるランサムウェア流出サイトデータに見られた全般的な傾向と一致している。

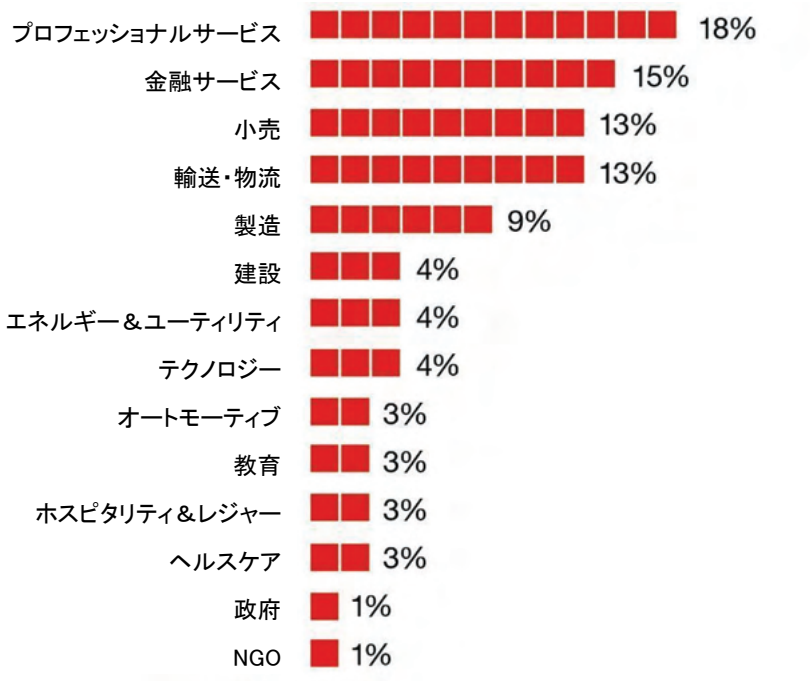
2022 年に分析したインシデント対応事例のうち、被害を受けた上位 5 セクターは、プロフェッショナルサービス、金融サービス、輸送・物流、小売、製造であった。

2022 年に分析した事例のうち、約 4 分の 1 についてはその目的を確認できず、2021 年に目的不明として分類した事例の割合（7.5%）より高くなっている。これは、侵入ライフサイクルの早期段階で検出と対応策が取られたためと思われるが、2022 年には、脅威アクターが共有機能・ツールを使用し、TTP を強化する傾向が見られたことにも関連しているとも考えられる。

2022 年、脅威アクター分類別に分析したインシデント対応事例



2022 年、セクター別に分析したインシデント対応事例

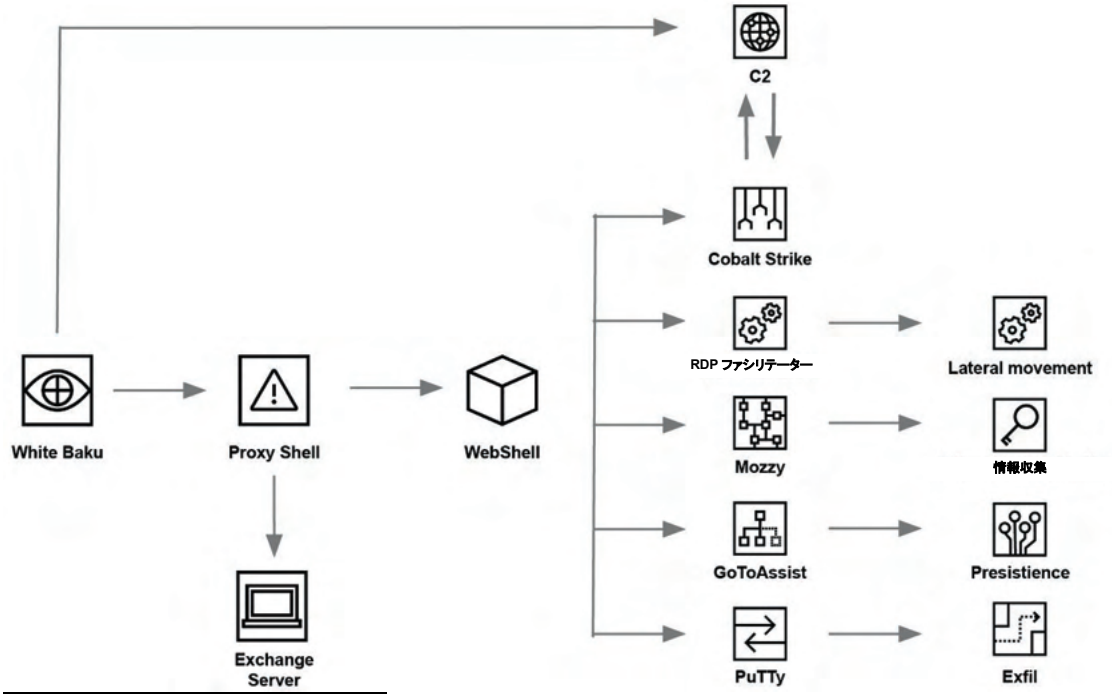


組織は、セキュリティスタック全体からできるだけ多くのテレメトリを記録・維持することが必須である。これは、過去のネットワークメタデータやホストの活動を確認することで、その時点では検出されなかった攻撃の影響をインシデント対応者が理解するのに役立つためである。キーログやテレメトリのデータ量は比較的少なく、長期的なアーカイブ型の保存に適している。

White Baku ケーススタディ

2022 年 3 月、PwC は、Cuba ランサムウェアの背後に存在する脅威アクター、White Baku が関与するインシデントに対応した [207]。White Baku は、ProxyShell の脆弱性を悪用して Microsoft Exchange サーバーに Web シェルをドロップすることで被害組織への初期アクセスを獲得しており、これは同脅威アクターによるものとして公に報告された他のランサムウェアインシデントとも一致している。White Baku はその後、Cobalt Strike を C2 およびラテラルムーブメントに活用し、被害組織の EDR に関する情報を収集するために設計されたカスタムマルウェアである Mozzy と、RDP を進めるためのバックドアの構成に用いられるマルウェアである RDP Facilitator を展開した。被害組織のネットワークにおける足場を強化するため、White Baku はリモートサポートツールである GoToAssist をインストールした。また、情報収集・流出のためにファイル圧縮アプリケーションとして WinRAR を、ファイル転送とデータ流出のために PuTTY Secure Copy（PSCP）をインストールし、システムを暗号化する前に被害組織からファイルを窃取できるようにした。そして最後に、White Baku は最終的なランサムウェアの展開に PsExec を使用した。

White Baku の侵入チェーン



[207] *CTO-TIB-20220608-01A - White Baku grabs a foothold*

ProxyShell を含む White Baku（別名 Cuba）によるインシデントの教訓

PwC は、White Baku によるインシデントについて複数の側面から分析し、攻撃チェーンのいくつかの段階と潜在的な検出および軽減策について知見を得た。

- *初期アクセス*：ProxyShell のような Web サーバープロセスから生成される異常なプロセスや、Web サーバープロセスから発信される異常なファイル書き込みを検出することは、一般的な Web シェルの活動を特定する上で重要な戦略である。これは多くの場合、攻撃者がネットワークにアクセスする最初のポイントであり、その後、攻撃者は被害組織の環境をより詳しく探ることになる。防御者は、ネットワーク発見に関連する子プロセスおよびコマンドを検索することで、Web サーバー上のこのような疑わしい活動を表面化させることができる。MITRE ATT&CK T1505.003 - Server Software Component：Web Shell.

- *永続性*：リモートアクセスツール（GoToAssist など）のインストールを監視することが非常に重要である。これは、簡単に検出可能であるという理由だけでなく、通常、攻撃の初期段階でリモートデスクトップツールが展開されるためである。許可リストのポリシーによって承認されるリモート管理ツールを理解することで、このポリシーから外れる一般的なリモート管理ツールの検出ルールを作成できる。熟練の攻撃者が承認されたリモート管理ツールをインストールする場合も、ユーザー空間でのインストールや予期しないアカウントによるインストールなど、異常なインストールを特定する検出策が構築可能である。一部のツールは、特定のコマンドラインフラグを持つインストーラを利用しているため、インストールの監視に加え、防御者はインストールプロセスの特定のコマンドラインを調査することができる。例えば、インストールが行われていることをユーザーが確認できないようにするサイレントフラグ（すなわち、インストールユーザーインターフェイス（UI）を使用しない場合）や、リモートサポートツールとしては珍しくスタートアップにユーティリティを追加するフラグなどがある。MITRE ATT&CK T1219 - Remote Access Software

- *ラテラルムーブメント*：PsExec は、ランサムウェアアクターの間で非常に広く使用されているツールである。リモート管理を目的とするもので、Server Message Block（SMB）を介してリモートシステム上でコードを実行することができ、ランサムウェアの伝播に最適なツールである。PsExec が承認された管理ツールでない場合、防御者は PsExec の実行を監視することができる。正規の実行を行うユーザーには、代替となるリモート管理手段を指示すればよい。PsExec は攻撃者によって頻繁に名称が変更されるため、標準的なプロセス名がない場合に、特別なコマンドラインパラメータやエンドユーザーライセンス契約（EULA）の承諾に関連するレジストリアーティファクトを探す行動は、多くの場合、攻撃者が検出を回避しようとしていることの明らかな証拠となる。PsExec がネットワーク上の管理者によって広く使用されている場合、PsExec の活動が疑わしいものか識別するために、より複雑なロジックを導入する必要がある。PsExec は、Metasploit や Cobalt Strike のようなポストエクスプロイトツールのラテラルムーブメント機能としても構築されており、それぞれ微妙に異なる方法で PsExec を実装して

いる。各ポストエクスプロイトツールによって実行されるリモートサービスプロセスを監視するために、検出機能を構築する必要がある。防御者は、正規表現を使用して、これらのツールがオペレーションに挿入しようとするランダム性を捕捉する必要がある。MITRE ATT&CK T1021.002 – Remote Services：SMB/Windows Admin Shares

- *収集*：WinRAR などの圧縮ツールは完全に合法的なものであるが、サイバー犯罪脅威アクターや高度な持続的脅威アクターにも使用されている点を忘れてはならない。このようなツールがインターネットからダウンロードされたり、%TEMP%などの特定のフォルダにインストールされたりするのを検出することは、レビューのフラグ立てが可能な疑わしい活動を特定する、有用なヒューリスティック手法に成り得る。 MITRE ATT&CK T1560.001: Archive Collected Data：Archive via Utility

- *流出*：上記の収集に用いられる圧縮ツールと同様に、PuTTY Secure Copy（PSCP）など正規のファイル転送ツールを介してデータの流出を行うアクターの活動は、しばしば正規の活動と判別が付きづらい場合がある。このような流出活動を正規のファイル転送活動と区別する方法として、当該環境において異常な発信データ転送の発信元、発信先およびデータ量について具体的に警告することが有用となる場合がある。さらに、エンドポイントシグネチャを作成して、組織のポリシーに反するファイル転送ツールを検出することも可能である。これと同様に、既知の問題ないファイル転送ツールと同じ動作を示すプロセスであっても、異常なプロセス名を使用している場合は、エンドポイントシグネチャを通じて警告することが可能である。MITRE ATT&CK T1048.002 - Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

Black Artemis ケーススタディ

2022 年後半、PwC は、Black Artemis のサブグループとして追跡調査している、北朝鮮を拠点とする脅威アクターである Andariel（別名 Stonefly、Silent Chollima）による、化学セクター組織への長期的かつ永続的な侵入に対応した。この脅威アクターは、被害組織の環境に永続的にアクセスし、最初の侵害から 2 カ月後、少なくとも 1 回はネットワークに戻り、さらなる活動を行った。被害組織の性質、テーマに関する専門知識、インシデント対応中に発見された証拠から、PwC は、この侵入はスパイ活動を目的とするものであり、被害組織の知的財産や独自の知見を標的としていた可能性が高い、と評価している。

PwC が残された証拠を検証した結果、被害組織の環境への最初の侵入は、Log4Shell に脆弱なインターネット接続サーバーを Andariel が悪用して行われた可能性が高いことが分かった。ネットワークへの初期アクセス後、Andariel は DTrack バックドア用の実行ローダー[208] を複数のホスト上に展開し、Autorun キーの設定やスタートアップサービスの作成など、さまざまな方法で永続性を確立したが、バックドア自体はメモリ内でのみ実行された。

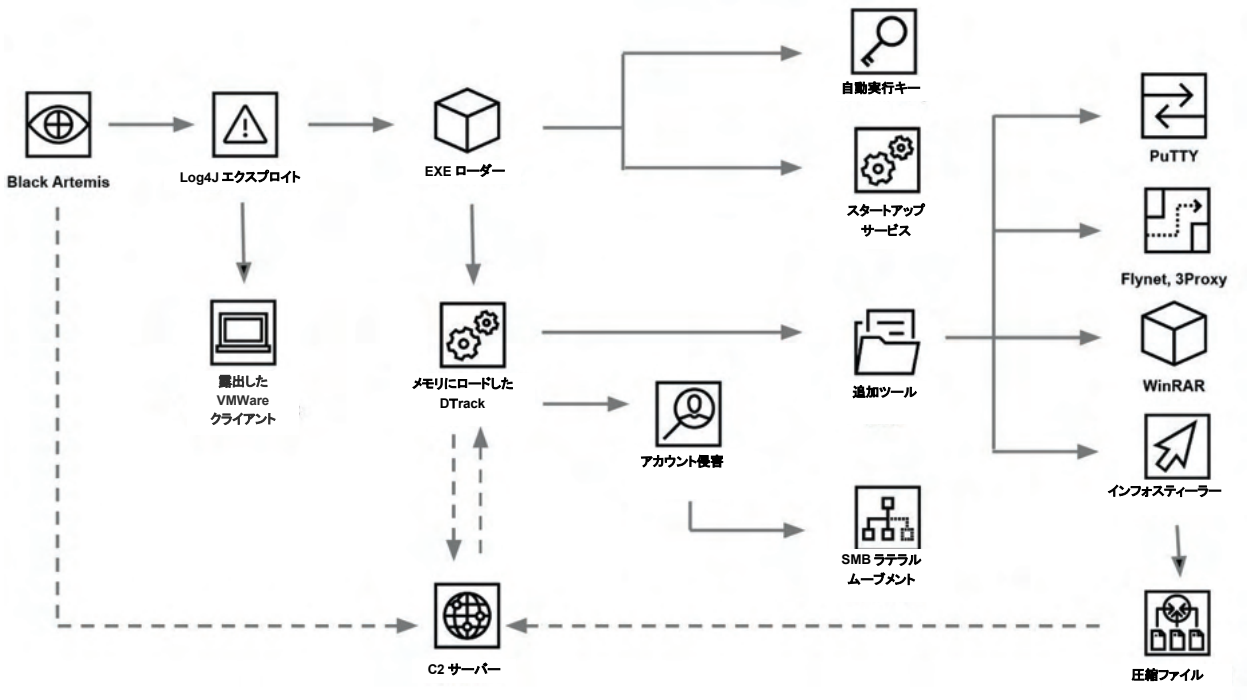
208 'Dtrack activity targeting Europe and Latin America', Kaspersky, https://securelist.com/dtrack-targeting-europe-latin-america/107798/ (15th November 2022)

その後、Andariel は、追加のツールをディスクにドロップした:

- 正規の PuTTY クライアント
- Windows 用 PuTTY Secure Shell Protocol（SSH）/Telnet クライアントの特定の旧バージョンをソースからコンパイルしてカスタムビルドしたもの
- 主に、Windows 用のオープンソースの Go TCP/UDP プロキシングツールである Flynet と組み合わせて使用
- 少なくとも 1 つの事例では、Andariel はオープンソースのプロキシユーティリティである 3Proxy もドロップ

これらのツールには、被害組織環境のアンチウイルス機能関連に偽装したファイル名が付けられていた。PwC は、Andariel がこれらのツールを使用して、被害組織のネットワークに出入りするトラフィックをサーバーに送っていた可能性が高いと評価している。これは、Cisco Talos がインシデント対応中に他の被害組織ネットワークで遭遇した Andariel による他の活動とも一致している [209]。これは、脅威アクターが侵入全体にわたり、非常に明確かつ一貫したプレイブックを持っていることを示唆している。

Black Artemis 侵入チェーン



209 'Lazarus and the tale of three RATs', Cisco Talos, https://blog.talosintelligence.com/lazarus-three-rats/ (8th September 2022)

Andariel はさらに、ローカル管理者からドメイン管理者まで複数のアカウントを侵害した。PwC は、SMB 接続によりホストを踏み台とするなどして、脅威アクターがネットワーク上でラテラルムーブメントを行った証拠を確認した。この脅威アクターは、複数のホストで特定のバージョンの WinRAR をドロップし、DTrack ローダーを含む圧縮アーカイブを解凍して実行し、現実的な確率でファイルを圧縮して流出させるために使用した。また、Andariel は、DTrack の活動に関する Symantec のブログ記事の内容と一致するカスタムインフォスティーラーを使用し、特にファイルサーバーに展開していたことを示す証拠も見つかった [210]。

DTrack を含む Andariel によるインシデントの教訓

このインシデントで確認された、Andariel が行う侵入チェーンには、いくつか検出と軽減が可能なポイントが存在する。この事例を前述の White Baku の事例と比較する際、攻撃段階の類似性が複数見られることを考慮することが重要であり、これによって脅威アクター間で広く使われているテクニックに対する防御の重要性がさらに強まる。

- *初期アクセス*: 上記の White Baku ケーススタディにおける本セクションを参照。MITRE ATT&CK T1505.003 - Server Software Component: Web Shell

- *永続性*: 脅威アクターは、レジストリキーやサービスなど、よく知られた永続化メカニズムを引き続き使用している。これらは、脅威アクターによる設定も容易であるが、その検出や監視も同様であり、作成時だけでなく、環境の通常セキュリティハイジーン（hygene）チェック時にも確認できる。レジストリキーやサービスのような項目は、組織環境の合法的かつノーマルな部分であって、脅威アクターの手により、期待されるソフトウェアやタスクに紛れ込むように設定することも可能である一方で、自動実行手法の作成または変更を監視する検出ルールを作成することも可能である。MITRE ATT&CK T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder, T1543.003 - Create or Modify System Process: Windows Service

- *ラテラルムーブメント*: 上記の White Baku ケーススタディにおける本セクションを参照。MITRE ATT&CK T1021.002 - Remote Services: SMB/Windows Admin Shares

- *収集*: 繰り返しになるが、WinRAR などの圧縮ツールは完全に合法的なものであり、サイバー犯罪脅威アクターや高度な持続的脅威アクターにも使用されている点が重要である。このようなツールがインターネットからダウンロードされたり、%TEMP%などの特定のフォルダにインストールされたりするのを検出することは、レビューのフラグ立てが可能な疑わしい活動を特定する、有用なヒューリスティック手法に成り得る。MITRE ATT&CK T1560.001 - Archive Collected Data: Archive via Utility

[210] 'Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets', Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage (27th April 2022)

- *流出:*White Baku と同様に、Andariel もデータ流出を目的としてファイル転送ツールを利用しており、その防御策は本ケーススタディで詳述している。さらに、この脅威アクターは、正規のネットワークプロキシツールも利用しており、これについても同様の指摘が該当する。つまり、防御者はこのような活動が環境のベースライン特性から逸脱していないか確認する必要がある。しかし、ネットワークトラフィックのサーバー送信に関する正式なシナリオは、通常、より限定的であるため、White Baku よりも、若干厳密な特定が可能となる場合がある。MITRE ATT&CK T1048.002 - Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol, T1090.001 - Proxy: Internal Proxy

今後の展望

さまざまな脅威アクターが進化を続け、セキュリティメカニズムを回避する TTP を採用する中、PwC は 2023 年のサイバー環境について、ID と特権アクセス能力を標的とした脅威が大勢を占めると予想している。また、諜報活動を目的とする脅威アクターは、デジタルサプライチェーンを標的とし、アクセス活動のためにゼロデイを悪用するケースが増加するだろう。

脅威アクターは、クォーターマスターの調整により活動し、汎用または共有ツール、フレームワーク、マルウェアを用いており、PwC はこれらの機能の商用市場が進化し、より広く採用されるようになると予想している。この進化を示す指標としては、ゼロデイ市場の拡大や、NSO Group（Grey Anqa）[211] などエクスプロイトを備蓄する商業的脅威アクターなどが挙げられる。このような進化により、通常はリソース不足である、あるいは十分に活用されていなかった新興勢力から、より多くの諜報目的の脅威アクターが出現する可能性がある。

特に、クォーターマスターの傾向に関する予想としては、諜報目的の脅威アクターが難読化サービスプロキシネットワークへの投資を増やすと見ている。また、脆弱な IoT 機器や SOHO 機器は引き続き、こうしたネットワークの商用プロバイダーにより運用されるエクスプロイト・詐欺システムの主要な標的となると予想される。

サイバー犯罪エコシステム全体が飽和状態にあることから、PwC は、サイバー犯罪者が引き続き、収益化した犯罪サービスの深さ・幅において変化していくと予想している。また、2022 年に注目を集めた「スマッシュ＆グラブ」攻撃は、金銭目的、ハクティビズムの両方において、2023 年も同様の活動を後押しすると見ている。また、ソフトウェアライブラリの脆弱性も、この 1 年間、脅威アクターにとってエクスプロイトの焦点となる可能性があるだろう。

最後に、イランを拠点とする脅威アクターによる妨害能力の開発と展開を調査する中で、PwC は今後も、「ハック＆リーク」攻撃、 ワイパーの使用、産業制御システム（ICS）に対する長年の破壊工作、そしてデータ改変型の攻撃も含み得るようなテクニックの進化が続くと予想している。

211 We previously shared information about this threat actor in 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022).

2023 年に予想される脅威アクター別の標的

ロシアによるウクライナ侵攻が長期化し、多くの国々との外交関係が悪化していることから、ロシアを拠点とする脅威アクターによる、ウクライナへの支援やロシアからの離脱を見せた／表明した組織やセクターを標的とした攻撃は一層増えていくと PwC は予想している。また、侵攻が続く中、ロシアを拠点とする脅威アクターは、物流、輸送、製造セクターおよび、ロシアがサプライチェーンに大きな課題を抱えている他セクターを標的としていくと思われる（例えば産業スパイ活動など）。そして、長年にわたるスパイ活動の一環として、政府、防衛、および関連組織にも、引き続き関心を示していくだろう。

特に 2022 年には米国が中国への制裁措置を課したことから、PwC は、中国を拠点とする脅威アクターが半導体産業やハイテク部門を一層標的として狙っていくと予想している [212]。さらに、この地域の地政学的緊張により、こうした脅威アクターによる標的活動が増加するものと思われる。2022 年後半に中国全土で発生した抗議活動を考えると、国内サーベイランス活動を支援するために脅威アクターがどのように対応するか注目される。

イランを拠点とする脅威アクターは、イラン政権に関連するセクターや、イランの戦略的利益の発展に関わるセクターを引き続き標的とするだろう。イランを拠点とする脅威アクターはまた、イスラエル、サウジアラビア、米国を拠点とする海外組織を引き続き標的とする一方で、国内の標的や反体制派に対する標的についてもこれまで同様のペースを継続すると予想される。

2022 年、ロシアによる侵攻の最中に米国が「ウクライナ支援」目的の攻撃的サイバー活動を行ったことを認めたように、米国をはじめとする西側諸国の行動は引き続き、地政学的な問題を反映した、足並みの揃ったものになると予想される [213]。

212 *CTO-SIB-20221117-01A - US export controls on semiconductors*

213 'US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command', Sky News, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (1st June 2022)

PwC のサイバーセキュリティ

本レポートで詳述した脅威について、より詳しい情報をご希望の方は、jp_cons-threatintelligence@pwc.com までお気軽にお問い合わせください。

PwC は、サイバーセキュリティ分野のリーダーとして、また強力なグローバルのデリバリー能力を有し、クライアントが直面するセキュリティおよびリスク課題に対応できるネットワークとして、業界アナリストから世界的に評価されています。

PwC は、マネージド・サイバー・ディフェンス（MSD）、レッドチーム演習、インシデント対応、脅威インテリジェンスなどのサービスにおけるニッチな技術専門知識までカバーする、サイバー防御の最前線から得た専門知識を武器に、役員会レベルのセキュリティ戦略およびアドバイザリーコンサルティングサービスを提供しています。

PwC は、戦略的思考、強力な技術力、複雑な業務の遂行を、卓越したクライアントサービスと組み合わせる能力によって、他社との差別化を図っています。独自の研究およびセキュリティ関連インテリジェンス、技術専門知識、サイバーリスクに対する深い理解により、クライアントが新たな課題や機会に自信を持って適応していくのに必要な道筋を見出す支援を行います。

PwC は、セキュリティマネジメント、脅威の検出と監視、脅威インテリジェンス、セキュリティアーキテクチャとコンサルティング、行動変革、法規制面のアドバイスに関する専門知識を有するスペシャリストチームを擁し、最も大切なものを守るクライアントの取り組みを支えます。

PwC は、専門能力を駆使して、高度なサイバー攻撃の阻止、検出、対応を図るクライアントを支援するために必要なサービスを提供します。これには、データ漏洩、ランサムウェア攻撃、産業スパイ活動、通常高度な持続的脅威（APT）と呼ばれる行為を含む標的型の侵入などの危機的事象が含まれます。PwC の脅威インテリジェンス調査は、PwC の全てのセキュリティサービスを支えるものであり、世界各地の公的・民間部門の組織において、ネットワークの保護、状況認識、戦略情報の提供に利用されています。

付属資料

付属資料 A:手法

年間を通じて、PwC はクライアントやステークホルダー、セキュリティ業界専門家と協力し、インテリジェンス要求の検証や改善を行い、PwC ならではの可視化、カスタマイズツール、技能、分析の取り組みを、実用的なインテリジェンスとしてクライントに提供している。本レポートは、2022 年に展開した PwC の分析を抜粋してまとめたものである。PwC 独自の機能、商用ツールやオープンソースへのアクセスに加え、インシデント対応案件やその他の業務において、PwC グローバルネットワークの各メンバーファームと密接に連携している。以下に挙げる PwC のメンバーファームから、業務を通じて得られた知見の提供を受け、充実した分析を行うことができた:オーストラリア、オーストリア、ブラジル、カナダ、チェコ共和国、ドイツ、香港、インドネシア、イタリア、マレーシア、オランダ、ニュージーランド、韓国、英国、米国、ベトナム。

推定に関する表現

推定的または確率的な表現(「~だろう」「ほぼ確実」など)の解釈はさまざまであり、誤解を避けるため、本レポートでは、PwC の評価に対する信頼度を示す際に以下の定性的用語を使用している。特に断りのない限り、PwC の評価は統計的分析に基づくものではない。

定性的用語	対応する確率
程遠い、可能性が非常に低い	10%未満
ありそうにない、可能性は低い	10-25%
現実的確率である	26-50%
有力、可能性が高い	51-75%
非常に有力、可能性が非常に高い	76-90%
ほぼ確実	91%以上

付属資料 B:脅威アクターリファレンスでは、脅威アクターの命名規則に関する方法論と、脅威アクターの目的と能力の定義方法について説明している。

付属資料 D:防御者インデックスでは、検出・軽減方法について、追加の定義と説明を行っている。

付属資料 B：脅威アクターリファレンス

PwC は世界中のさまざまな脅威アクターを追跡調査しているが、まず、その脅威アクターの拠点に関する評価を示す色をもとにした命名規則を適用している。PwC は、評価中の脅威に対して White という色を指定している。また、以下の表は、色のマッピングの一部を示したものである。色に続いて、神話上の人物名を割り当て、脅威アクターのユニークな名称を定める。既知の組織に割り当てられない活動を観察した場合、さらなる開発と分析を進めるために、脅威アクターに dev set という名称を付け、分析の結果、アトリビューション評価が得られた場合は、当該 dev set に名称セットを割り当てる場合もある。PwC の調査と他の組織の調査の間にアトリビューションの重複が見られる場合、それぞれの脅威アクターの名前を付与する。

脅威アクターに関する主な用語・フレーズ

サイバー犯罪アズ・ア・サービスの提供：本レポートに含まれる以下のような対価を支払うことで利用可能なサイバー犯罪サービスを開発・宣伝すること：

- アクセス・アズ・ア・サービス（AaaS）：主に企業向けネットワークへのアクセスに対して顧客に課金する犯罪サービスの提供。このタイプのサービスは、次の 2 つのカテゴリーに分けられる：
  - イニシャル・アクセス・ブローカー（IAB）：リモート・デスクトップ・プロトコル（RDP）や仮想プライベートネットワーク（VPN）など、インターネット上で公開されたインフラへのログイン認証情報を顧客に販売するサイバー犯罪者
  - マルウェア・デリバリー・システム：Emotet 経由の White Taranis や Qakbot 経由の White Horoja など、顧客のマルウェアを二次ペイロードとして侵害ホストにアップロードする犯罪サービス—p.45-48

- DDoS 代行（DDoS-for–hire）：サイバー犯罪者が不正組織に料金を支払い、DDoS 攻撃を行ってもらう犯罪サービス。DDoS 代行組織としてスタートした Blue Kurama（別名 Killnet）などがある—p.19
- フィッシング・アズ・ア・サービス（PHaaS）：サイバー犯罪者が、EvilProxy、Caffeine、Robin Banks ツールキットなどの不正なフィッシング組織に料金を支払い、フィッシングメールを送信する犯罪サービス—p.48、50-51
- ランサムウェア・アズ・ア・サービス（RaaS）：ランサムウェアを開発し活動全体のブランディングを行うオペレーターと、ランサムウェアを攻撃に利用するアフィリエイターによる、ランサムウェアプログラムのモデル—p.39-46

データブローカー：本レポートでは、被害組織から窃取した機密情報の収集、集約、アクセスの販売を行う不正事業者を指す— p.38

スパイ目的の脅威アクター：「高度な持続的脅威」（APT）と呼ばれることもあるこれらの脅威アクターは、通常、情報収集要件に応えるべくアクセスや情報を求め、その支援者に経済的または政治的な利益を提供する— p.61（PwC が分析したインシデント対応事例における高度な知見）

金銭目的の脅威アクター：これらの脅威アクターは、サイバー犯罪者の目的が単に自分たちの活動で金銭を得ることであるため、対象を問わず攻撃できる。これらの脅威アクターの技術的洗練度には大きな幅があり、TTP セットも大幅に異なる— p.39-51、61

ハクティビズム：ハクティビストは、世間的な知名度を上げ、自分たちの活動に対する周囲の認識を高めることを目的として攻撃を行う。これは通常、サービス妨害（DoS）攻撃や Web サイトの改ざんなど、サービスの妨害により行われる— p.1、11、18-19、61、68

内部関係者／内部犯：組織のネットワーク、システム、データへのアクセスを許可されている／許可されていた、現職員／元職員、請負業者、その他のビジネスパートナーであって、そのアクセス権限を意図的に悪用して組織のデータまたはシステムを侵害する者—p.39、44、49、61

オペレーショナルセキュリティ（OPSEC）：日常業務と資産を保護し、妨害、無効化（preempted）、アトリビューションされないようにするために実施される手段— p.23、31

プロキシネットワーク：本レポートでは、RedRelay のような、脅威アクターが活動を遂行するために使用する匿名化されたネットワークまたはその他の難読化された中継システムを指す—p.2、20、22-23、68

クォーターマスター：ツール、能力、フレームワークの開発、提供、仲介により、脅威アクターの活動を可能にする組織— p.20、22、68

妨害目的の脅威アクター：データやシステムの完全性を毀損、破壊、またはその他の方法で妨害することを目的とする妨害者—p.1-2、8、11-14、28-29、68-69

ツール、戦術・技術・手順（TTP）：TTP とは、脅威アクターの行動を指す。付属資料 D：防御者インデックスでは、本レポートで引用された TTP の例についてクイックリファレンスを提供している。

本レポートで取り上げた脅威アクター

- Abraham’s Ax—p.29
- Black Artemis のサブグループ Andariel（別名 Stonefly、Silent Chollima）—p.64-67
- ビジネスメール侵害（BEC）脅威アクター—p.50
- Black Alicanto（別名 COPERNICIUM、DangerousPassword、CryptoMimic、CryptoCore、Operation SnatchCrypto）—p.32、34

- White Horoja：akbot の背後に存在する脅威アクター—p.46-47
- White Janus（別名 LockBit）—p.17、42-45
- White Khione：IcedID の背後に存在する脅威アクター—p.46-47
- White Taranis（別名 Emotet）：Emotet の背後に存在し、Blue Cronus と関連する脅威アクター—p.47-48
- White Tur—p.35-36
- Yellow Dev 9（別名 Lyceum、Hexane）—p.28（脚注）
- Yellow Dev 13（別名 BOHRIUM、TA455）—p.34-35
- Yellow Dev 19（別名 Emennet Pasargad）—p.28
- Yellow Dev 24（別名 DEV-0270、Nemesis Kitten）—p.27
- Yellow Dev 31（別名 DEV-0842）—p.28（脚注）
- Yellow Dev 32—p.30
- Yellow Garuda（別名 Charming Kitten、APT42、PHOSPHORUS）—p.29-30
- Yellow Liderc（別名 Tortoiseshell、CURIUM）—p.30-31
- Yellow Maero（別名 APT34）—p.28（脚注）
- Yellow Nix（別名 MuddyWater、MERCURY）—p.6、28、31

付属資料 C:エグゼクティブコンパニオン

PwC の「第 26 回世界 CEO 意識調査」において、CEO が今後 5 年間のリスク上位に挙げたのは、サイバーセキュリティと地政学的紛争であった。2022 年、ウクライナ紛争の激化、持続的かつハイペースなランサムウェア活動、政治的・犯罪的利益を求める妨害を背景に、サイバー脅威アクターはセキュリティ対策をかいくぐろうと自らの行動を適応・改変し続けている。脅威環境が変化し、リスクが増大する一方で、PwC の「Global Digital Trust Insights 2023 年版」調査では、サイバーセキュリティの改善とリスク軽減に向けた持続的かつ累積的な投資の最大化を果たすためには、最高情報セキュリティ責任者(CISO)、C-suite、取締役会の協力が極めて重要であることが明らかになった。

PwC の脅威インテリジェンスは、2022 年の脅威に焦点を当てた調査および新たなサイバー問題を特定・評価する積極的な取り組みから、以下の主要なサイバーリスクを特定した。

1. **脅威アクターの活動に反映された地政学的問題—p.1-2、68-69**
    - ロシアのウクライナ侵攻で見られたような、戦争・紛争における従来の戦術を補完するものとして、脅威アクターがサイバー能力を広範囲に使用した(p.8-19)。
    - 中国を拠点とする脅威アクターは、従来の標的に対する活動の難解化能力を高め、ウクライナ侵攻や国際社会の反応に関連する情報に強い関心を示した(p.20-26)。
    - イランを拠点とする脅威アクターは、反体制派への標的をエスカレートさせ、バルカン半島における政治的武器としてサイバーを使用する意思を示した(p.27-31)。
    - 北朝鮮を拠点とする脅威アクターは引き続き、収益を上げ、制裁の影響を相殺すべく、金融サービスや暗号通貨を標的とした(p.32-34)。
    - 米国サイバーセキュリティ・社会基盤安全保障庁(CISA)や英国の国家サイバーセキュリティセンター(NCSC)などのサイバー当局が、地政学的緊張の高まりに伴い組織が巻き添えを食らう可能性を警告したこともあり、多くの国が国家レベルでサイバーレジリエンス向上に向けた取り組みの優先度を引き上げた(p.9-10)。

2. **ランサムウェアの進化と展望—p.39-48**
    - ランサムウェアは、全世界の大半の組織にとって主要なサイバー脅威である状況に変わりはない。脅威アクターはビジネスモデルを専門化し、製造、建設、小売などの高価値セクターに対して 24 時間 365 日止むことのない活動を行うようになっている(p.41-42、44-45)。
    - 脅威アクターの関心対象は、地方自治体を含む中小規模の組織にも広がり、軽減・修復のために多額の費用が発生する事態となっており、またリークサイト上で攻撃や破壊が公表されている(p.41-42)。
    - ランサムウェアグループと主要な脅威アクターは 2022 年を通じて分裂とリブランディングを続け、ランサムウェア・アズ・ア・サービス(RaaS)はビジネスモデルとして一層人気を博している(p.39-46)。

3. **妨害活動のエスカレート—p.1-2、68-69**
    - ロシアを拠点とする脅威アクターは、ウクライナを拠点とする組織に対して複数の形式による破壊的マルウェアを展開し、2023 年においても同様と予想される（p.1、11-14）。
    - イランを拠点とする脅威アクターは、アルバニア政府内組織に対して妨害攻撃を行った。これらの活動が成功を収めたことは、イランを拠点とする脅威アクターだけでなく、妨害を目的とした能力を有する他の脅威アクターも、将来的に攻撃的なサイバー手段によって戦略的影響力の行使を図る傾向が高まっていくことを予想させるものである（p.2、28-29、68-69）。

4. **多要素認証（MFA）の迂回／回避と消耗—p.49-52、58-60**
    - 脅威アクターは、クラウド環境を含む企業環境に自由にアクセスする能力を最大化するために、複数の形態の MFA を含む強化されたセキュリティ制御に適応して回避する能力、ソーシャルエンジニアリング（p.49）、認証情報窃取ツール（p.49-50）を調整する能力を発揮した（p.58-59）。
    - 企業環境において、特に特権アクセスアカウントで MFA の使用を怠ったことが、2022 年に観察された一部のランサムウェア攻撃やその他のサイバー犯罪の侵害の成功要因となった。MFA は、犯罪者が正式なユーザー名とパスワードを取得していても、ネットワークへのリモートアクセスを大幅に困難化する（p.50）。

5. **デジタル ID と特権アクセスの標的化—p.1、58-60、68**
    - ID と特権アクセスの保護は、組織の環境とデータを保護する上で最も優先すべき事項である。
    - 2022 年、脅威アクターは、初期アクセスを実現するために高度なソーシャルエンジニアリングを用いて、デジタル ID を侵害することに重点を置いていた（p.49）。
    - また、脅威アクターは、ネットワークへ初期アクセスするために、ユーザーの認証情報やその他の情報を吸い上げるインフォスティーラーを使用していた（p.49-51）。

6. **標的とされたクラウド環境—p.59-60**
    - 多くの組織がクラウドに移行し、その環境から得られるセキュリティ強化というメリットを享受する一方で、脅威アクターはクラウドサービスを侵害するための新しいツールの開発や知識の取得に心血を注いだ（p.58-60）。
    - 脅威アクターが主に ID、サービス、アプリケーション・プログラミング・インターフェース（API）を悪用するため、クラウドベースの環境とサービスを標的とした攻撃への対応には、他とは異なるアプローチが求められる（p.59-60）。また、2023 年にはソフトウェアライブラリの脆弱性が攻撃の焦点となる可能性が高い（p.68）。
    - 2022 年に支援したインシデント対応事例をもとに、PwC はクラウド環境の堅牢化に関するいくつかの提言を作成した（p.59-60）。

極めて高度な技術を有する脅威アクターが、スパイ活動や知的財産の窃取対象組織への侵害に必要となる規模のアクセスを実現しようとする中、今後一層、顧客ネットワークへ

の特権アクセスを有するクラウドサービス、マネージドサービス、ID・アクセスマネジメント（IAM）プロバイダーが狙われるだろう（p.68）。

本レポートのその他の付属資料には、PwC の手法、本文中で説明されるさまざまな脅威、防御者に関連する情報の照合インデックスに関する詳細情報を記載している。また、「今後の展望」のセクションでは前向きの知見を掲載するとともに、以下のセクター[214]および業界に影響を与えるインシデントについても触れている。

- オートモーティブ - p.61
- 化学 - p.64
- 建設 - p.42、61
  - エンジニアリング - p.31
- 重要インフラ - p.17、19、30
- 防衛 - p.8、19、23、29、33、69
  - 防衛組織 - p.16
  - 軍事 - p.15、32
  - 軍事をテーマにした標的 - p.15
  - 研究施設 - p.15
  - サプライヤー - p.16
- 反体制派 - p.27、29、69
  - アクティビスト - p.29
  - 抗議者 - p.27、29-30、69
- 教育・研究-p.42、61
  - 学術界、リサーチャー- p.16、26、30、39
  - 学生 - p.29
  - シンクタンク - p.30
- エネルギー、ユーティリティ、資源 - p.29-30、33、42、61
  - 原子力発電 - p.30、36
  - 石油・ガス - p.30、36
  - 電力グリッド - p.8
- エンタテイメントとゲーム - p.49
- 金融サービス - p.2、32、35、63
  - 暗号通貨と分散型金融（DeFi） - p.2、32、35、41
  - 商業銀行 - p.8、17、47
  - 財務管理ソフトウェア - p.8
  - 保険会社 - p.17、31
  - ベンチャーキャピタル - p.32
- 食品輸出業者、スーパーマーケット、小売 - p.36、61
- 政府 - p.1-2、6、8-19、22-37、42、50、61、69
  - 通信サービス - p.11、16
  - コンピュータ緊急対応 - p.13（脚注）、p.38
  - 外交団体 - p.24-26
  - 選挙をテーマにした標的 - p.25
  - 緊急時サービス - p.18
  - 政府システム - p.28-29
  - 法執行とセキュリティ - p.11、33、50
  - 議会 - p.19
  - 公共サービス - p.19、49
  - 地域・地方自治体 - p.36
  - 被害組織サービスをテーマにした標的 - p.50
- ヘルスケア - p.49、61
- 政府間組織（IGO） - p.8、28
- 製造 - p.23、25、31、36、42、60-61
  - 半導体産業 - p.49、69
- 海事 - p.30
  - 港湾をテーマにした標的 - p.30
- メディア - p.25、30
  - ジャーナリスト - p.30
  - ニュースをテーマにした標的 - p.25
- 非政府組織（NGO）-p.15、24、28、61
- 業務テクノロジー - p.10
  - 産業用制御システム（ICS） - p.69
- プロフェッショナルサービス - p.42、61
  - 人材をテーマにした標的 - p.34-35
  - 就職活動をテーマにした標的 - p.34-35
  - 採用をテーマにした標的 - p.34-35
- 小売 - p.36、42、61
- テクノロジー - p.12、20、34、42、49、61、69
  - 人工知能（AI） - p.34
  - クラウドコンピューティング・環境 - p.1、50、59-60
  - デジタルサプライチェーン - p.20、68

214 *CTO-SIB-20230223-01A - Sector shifts and insights - 2022*

PwC の脅威インテリジェンスチームのその他記事など：

- 2022 年に公開したブログ記事
- BlackHat USA 2022 での講演
- SANS CTI Summit 2022 での講演
- SANS Ransomware Summit 2022 での講演
- Virus Bulletin 2022 での講演

付属資料 D：防御者インデックス

脅威アクターの傾向を先取りし、脅威アクターの変化を可視化し、クライアント向けに検出・軽減戦略を開発するために、PwC は以下の主要な柱を活用し、検出能力の土台としている：

1. **エンドポイント**：今日の分散型、クラウドネイティブ環境では、仮想サーバー、物理サーバー、ノートパソコン、モバイルデバイスなど、エンドポイントにおいて効果的に検出することが、防御者にとって最も重要なポジションの 1 つである。

2. **ネットワーク**：トランスポート・レイヤー・セキュリティ（TLS）は依然として課題ではあるものの、ほぼ全てのマルウェアが C2 通信にインターネットを使用している。全てのネットワークトラフィックを可視化することで、攻撃者がエンドポイントでの検出を回避した場合や検出ツールのないエンドポイントを侵害した場合でも、通常、C2 活動を検出できる。内部ネットワークの可視化は、ラテラルムーブメントの検出と追跡調査にも役立つ。

3. **セキュリティ情報・イベントマネジメント（SIEM）／セキュリティオーケストレーション、自動化および対応（SOAR）**：全ての検出イベントを一元的に把握することで、防御者はより高いレベルで相関を図り、さらなる検出を行うことができる。また、うまくいけばノイズの中からシグナルを見つけることができるのと同様に、活動状況をより幅広くまとめることができる。SOAR プラットフォームは修復の自動化を可能にするものであり、ランサムウェアが動作し、一刻も早い対応が求められる場合に特に有用である。

4. **YARA:** リアルタイムの検出にはほとんど使用されることはないが、YARA は疑わしいバイナリの解析やメモリのスキャンに非常に役立つ。また、YARA を使用することで、侵入やキャンペーン分析の一環として、疑わしいサンプルやクラスタアーティファクトの優先順位付けを支援するルールを作成することができる。

脅威アクターによる特定の活動を高い信頼度で検出すること、同時に脅威アクターのわずかな動きやその他の行動の変化も見逃さないよう、より全般的にその行動を検出することにより、深層防御をさらに強化することができる。

FIRST22 における YARA ワークショップの詳細

本レポートで取り上げた共通脆弱性・暴露（CVE）

- CVE-2021-40444 - p.29
- CVE-2021-44228（別名 Log4Shell） – p.1、6-7、64
- CVE-2021-45046 - p.6
- CVE-2021-45105 -p.6
- CVE-2022-30190 - p.29
- CVE-2022-41040、CVE-2022-41082（総称 ProxyNotShell） - p.7

脅威アクターの TTP の主要テーマ・例

*攻撃に関する知見と傾向 - p.52

Adversary-in-the-middle（AitM）：MITRE ATT&CK T1557 - Adversary-in-the-Middle で説明。本レポートでは EvilProxy を例として挙げている— p.51

ビッグゲームハンティング：本レポートにおいて、「ビッグゲームハンティング」攻撃とは、脅威アクターが知名度の高い、あるいは価値が高いと思われる標的を選ぶことを指す—p.39

JavaScript によるブラウザフィンガープリント：ユーザーが感染した Web サイトを閲覧した際に、脅威アクターがユーザーやデバイスの情報を取得するために用いる手法（Yellow Liderc の例）—p.30

クラウド環境の標的：本レポートでは、Blue Dev 5（別名 NOBELIUM）によるクラウド環境の標的に関する詳細と、これらの事例を踏まえた PwC 推奨の堅牢化策をまとめている—p.58-60

サイバー犯罪フォーラム（Exploit、XSS の例）—p.6

デリバリーステム：インハウスのマルウェアインストールサービスを提供する、あるいは悪意あるペイロードを侵害されたホストにデリバリーするために外部パートナーに課金するアクセス・アズ・ア・サービス活動。例として、Qakbot、IcedID、Bumblebee など—p.46-48

二重恐喝：本レポートでは、脅威アクターが被害組織のネットワークに侵入し、ネットワークを暗号化した後、ネットワークへのアクセス回復を餌に被害組織を恐喝した上で、さらに被害組織から窃取したデータを販売または漏洩すると脅して再び恐喝すること—p.39、40（典型的な攻撃の連鎖を示す図）

ダイナミック・リンク・ライブラリ（DLL）のサイドローディング：T1574.002 - Hijack Execution Flow: DLL Side-Loading で説明。本レポートでは ShadowPad を例として挙げている—p.22

ハック＆リーク／ロック＆リーク：「ハック＆リーク」または「ロック＆リーク」攻撃は、脅威アクターがネットワークに侵入し、ネットワークを暗号化し、被害組織から盗んだデータを漏洩する活動—p.2、27、29、39、68

HTML スマグリング： 悪意ある HTML ファイルをユーザーに配信し、HTML 内に難読化されたペイロードを埋め込んで、JavaScript を使って解読して配信—p.48

インシデント対応の動向—p.60-61

情報窃取（別名インフォスティーラー）—p.49-50、66、76

ISO（光ディスクイメージ）ファイル：アーカイブファイルとして機能するファイル形式で、悪意あるペイロードを配信するために脅威アクターが使用する—p.34、46-48、56-58

検出ロジック・方法

[215] 'Macros from the internet will be blocked by default in Office', Microsoft, https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked (11th October 2022)

インシデント対応などのケーススタディから得た知見

MITRE ATT&CK リファレンス

機能およびマルウェアに関する全てのリファレンス

- 3Proxy - p.65
- AnyDesk - p.29
- BlackMatter - p.16、43-44
- BLINDINGCAN - p.32
- BPFDoor - p.26
- Bumblebee - p.46-48
- Caffeine - p.51
- China Chopper - p.26
- Cobalt Strike - p.1、24、47、52-53、55、62-63
- Dark Crystal RAT - p.18
- Dridex - p.17
- DTrack - p.32、64、66
- Emotet - p.45-48
- EvilProxy - p.51
- FOCUSFJORD - p.23-24
- Flynet - p.65
- Glitch - p.50
- Gophish - p.50
- GoToAssist - p.62-63
- HyperBro - p.23-24
- IcedID - p.46-48
- L3MON - p.30
- LogoKit - p.50
- MagicRAT - p.33
- Metasploit - p.46、63
- Mirai - p.19
- Mozzy - p.62
- nccTrojan RAT - p.23
- PingPull - p.26
- PlugX - p.20、22、25
- ProxyShell - p.62-63
- PsExec - p.62-63
- PuTTY Secure Copy（PSCP） - p.62、64
- PyArmor - p.31
- Qakbot - p.46-48
- Raccoon Stealer - p.49-50
- RDP Facilitator - p.62
- RedLine Stealer - p.49
- RedRelay - p.2、22-23
- Robin Banks - p.51
- rshell - p.24
- ScanBox - p.2、25
- ScatterBee - p.22
- ShadowPad - p.2、21-22
- Sliver - p.55-56
- Syncro - p.31
- Vidar Stealer - p.49
- WinRAR - p.62、64、66
- YamaBot - p.33

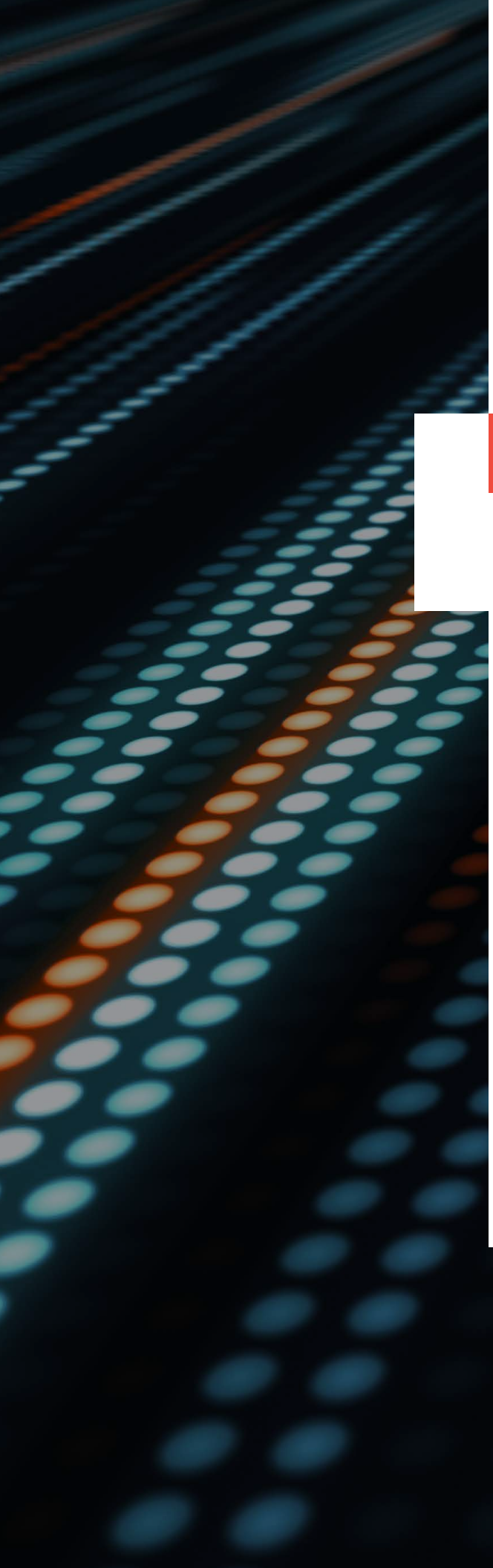
日本のお問い合わせ先

PwC Japan グループ
https://www.pwc.com/jp/ja/contact.html

PwC コンサルティング合同会社
サイバーセキュリティ&プライバシー

林 和洋
リーダー
上席執行役員 パートナー

村上 純一
マネージングディレクター



pwc

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約11,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界152カ国に及ぶグローバルネットワークに約328,000人のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細は www.pwc.com をご覧ください。

本報告書は、PwCメンバーファームが2023年4月に発行した『Cyber Threats 2022: A Year in Retrospect』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
オリジナル（英語版）はこちらからダウンロードできます。 https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html

日本語版発刊年月：2023年9月　管理番号：I202304-05