サイバー脅威：2021年を振り返る

www.pwc.com/jp

pwc

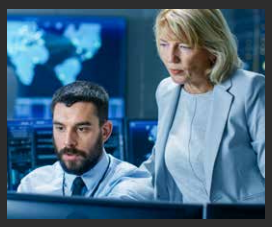
日本語版発行にあたって

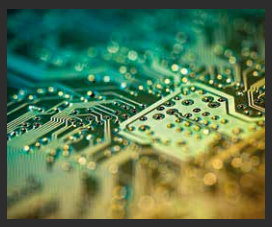
近年、米中対立を中心とした地政学リスクの高まり、新型コロナウイルス感染症（COVID-19）による行動様式の変容、デジタル技術の普及に伴うビジネス環境の変化といったさまざまな要素が相互に影響しあい、社会の不確実性が高まっています。サイバー脅威もITの世界に留まらず、こうした現実社会と呼応する形で国・企業・個人に対して顕在化しています。

PwCのグローバル脅威インテリジェンスチームでは、2020年から「Year In Retrospect」として1年間のサイバー脅威を総括し、サイバー脅威の動向、その変化の予測に関する示唆を公開しています。これには、日本を含む各国・地域で確認された具体的なサイバー攻撃の被害やその分析結果を含みます。

本レポートが、国内はもちろん、海外の拠点におけるサイバー脅威の状況を理解し、今後のサイバー脅威および必要となるセキュリティ対策を予測する上での一助として活用いただければ幸いです。

目次





はじめに

2021年、勢いと影響力を増したランサムウェアは、地域や業界を問わず、組織が直面する最も顕著なサイバーセキュリティ脅威としてその地位を確固たるものにした。

PwCは、世界154カ国に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生かして、優れた（そして重要な）脅威インテリジェンス情報をクライアントに提供している。PwCが実施する調査は、PwCの全てのセキュリティサービスを支えるものであり、世界各地の公共・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る。本レポートは、安全なデジタル社会の構築を支援する貢献の一環として、2021年にPwCが観察した包括的およびテーマ別のトレンドをまとめたものである。

アフィリエイトプログラムやランサムウェア・アズ・ア・サービス（RaaS）スキームは、サイバー犯罪の脅威をさらに高め、教育機関、慈善団体、公共サービス、重要インフラがしばしば無差別に標的とされるなど、これまで見えていなかった影響が顕在化している。このようなスキームは、金銭的インセンティブや、組織の評判を餌にした取引、さらには実行犯に対して段階的な侵入のためのプレイブックをリソースとして提供するなど、侵害から利益を生み出すパイプラインを合理化したものである。同時に、このスキームは、マルウェア配信システム（TrickBot、IcedID、QakBotなど）、ランサムウェアのアフィリエイト（関係組織）を募集するアンダーグラウンドフォーラム、アクセス・アズ・ア・サービス（AaaS）市場など、ランサムウェアを取り巻くサイバー犯罪エコシステムとの相互関係を強化し続けている。

2020年のトレンドは、もっぱら新型コロナウイルス感染症（COVID-19）の世界的感染拡大とそのサイバー空間への影響だったが、2021年の大きなトレンドは、サイバー能力の拡大であった。ゼロデイ脆弱性がサイバーセキュリティに関する話題の中心となり、その研究、開示、悪用にまつわる問題が世間の注目を集めた。こうした問題は特に、無差別的な標的設定や国家安全保障の問題に関連して、あらゆる動機と能力を持つ脅威アクター（サイバー空間に脅威をもたらす攻撃主体）がProxyLogonやLog4Shellといった有名な脆弱性の悪用したため、このような事態が発生した。

このようなゼロデイ攻撃の乱用は、他の2つの現象とも相互に関連している。すなわち、「デジタルクォーターマスターがサイバー脅威の状況にもたらす影響（商業クォーターマスターによる影響も含む）」、そして「民間人を標的とするサーベイランス活動」である。インテリジェンス収集活動は、地政学的な事象に応じて行われることがほとんどだった。しかし2021年には、過去に類を見ないレベルで、特定の国の戦略的利益に沿った目的を追求する新たな活動集団が確認された。その中には、これまでサイバー攻撃の活動が見られなかった国を拠点としている可能性が高い脅威アクターもあった。

本レポートの分析は、オーストラリア、イタリア、ドイツ、オランダ、スウェーデン、英国、米国にわたるPwC脅威インテリジェンス（Threat Intelligence）部門が実施したものである。さまざまな脅威アクターによるサイバー攻撃や標的に関するPwCの内部情報データ、世界各地のPwCのインシデント対応業務やマネージド脅威ハンティングサービスから得られた情報、および一般公開情報に基づいている。

パーフェクトストーム：ゼロデイ、クォーターマスター、サーベイランス

「ゼロデイ」の1年

ゼロデイ脆弱性およびその調査と開示は、これまでにもサイバー・セキュリティ・コミュニティにおいて関心を集めてきたトピックである。しかし2021年には、高度な標的型攻撃や脆弱性の大規模攻撃など複数の注目すべき事象が発生したこともあり、このトピックが再び戦略的・戦術的な議論の前面に浮上し、世間の注目も高まった。

このセクションでは、「ゼロデイ」を克服できない脅威として扱うのではなく、この現象の戦略的背景を説明する。

デイ・バイ・（ゼロ）デイ：ゼロデイをめぐる状況の戦略面から概観

ゼロデイに関する議論は、ゼロデイを回避することの困難さについて語られることが多い。また、こうした議論は「ゼロデイ防御は一層困難になる恐れがある」という前提認識に基づいている。2021年には、SolarWindsの事案をきっかけとしたサプライチェーン攻撃や（Colonial Pipeline社などのへの攻撃に続く）ランサムウェアなど、注目度を集めた話題とともに、ゼロデイに関する報道が広く行われるようになった。また、2021年は、1年間で開示されたゼロデイの数が最も多く、2020年の数字のほぼ2倍となった[1]。この急増の背景は単純なものではなく、おそらく以下のような複数の要因が重なった結果と思われる。

- **より公然とした国家安全保障に関連する要因：**ゼロデイ脆弱性は長年悪用されてきたが、2021年には「ゼロデイ外交」、つまり国家安全保障レベルでのゼロデイ攻撃に関する議論が政治の場で行われるようになった。その一例として、ドイツで新たに選出された連立政権は、ゼロデイの「ITセキュリティと市民権との非常に重大な関係」を理由として、政府によるゼロデイの購入を解禁する政治声明を発表した[2]。また、中国サイバースペース管理局（CAC）は、国内の脆弱性開示に関する新しい法律を発表した[3]。この新法はベンダーにも適用され、ベンダーはあらゆる脆弱性を適時に軽減し、修正プログラムと合わせて顧客に速やかに開示することを保証しなければならず、民間組織には、脆弱性調査に対して奨励金を支払う脆弱性報奨金制度（bug bounty program）の設立を奨励している。
- **ゼロデイに対する市場の拡大：**この数年、個人のセキュリティリサーチャーからゼロデイ犯罪ブローカー、さらにはHacking Team、FinFisher、NSO Group、Candiruといった民間の諜報組織まで、数多くのプレーヤーが脆弱性研究分野に参入している。特に、攻撃ブローカーと民間組織がゼロデイの開発と取引に関して最も注目を集めている。
- **これまでにないインセンティブの増加：**現在では、脆弱性リサーチャーがエクスプロイト開発成果を競い合い、金銭的な報酬を得る手段が増えつつある。Tianfu CupやPwn2Ownのような合法的なものもあれば、ロシア語ダークウェブフォーラム[4]に端を発するオフェンシブセキュリティの研究コンテストのような非合法なものもある。こうした活動がオフェンシブセキュリティ分野に根付いているため、防御側は、GoogleのProject Zero[5]のように、特定と開示を目的とした、独自のエクスプロイト開発作業にリソースを割いて対応する必要がある。
- **サードパーティー感染への再注目：**さまざまな動機を持つ脅威アクターが、サプライチェーンを構成する組織を標的とするようになり、多くの場合、一度に複数の標的にアクセスできるようになった。こうした状況を背景に、電子メールサーバーやナレッジ・マネジメント・ソフトウェアなど広く使われているビジネステクノロジーの脆弱性調査にリソースが投じられている。これにより、当然ながら発見されるゼロデイの数も増加し、開示によって（ベンダーの修正プログラムや勧告を伴う場合でも）、まさにその脆弱性を悪用しようとする試みも増加したのである。

結局のところ、ゼロデイを防ぐことは、ソフトウェア開発者やベンダーはもちろん、その顧客層にとっても決してたやすいことではない。しかし、顧客や防衛者は、侵入後の行動や活動に対する検知と対応に重点を置き、導入できる機能や対策を軽視してはならない。堅牢なコア・セキュリティハイジーンと組み合わせることで初めて、堅固な検出・対応機能は新たなゼロデイが組織にもたらし得る影響を抑えることが可能になる。

クォーターマスターによる活動の概要

脅威アクターがどのようにツールを調達・供給するかは、脅威アクターの能力や新たな標的を求める能力にも影響を与える可能性がある。「デジタルクォーターマスター」という概念自体は、サイバー運用において新しいものではないが、その重要性はますます高まっている。クォーターマスターとは、従来、軍事部隊に技術提供を行う役割と関連付けられてきた。そのため、デジタルクォーターマスターは、高度な持続的脅威（APT）アクターが、一部の脅威アクター間でしか共有されていない機能にアクセスする組織、あるいはツールを配布して使用できるようにする役割の中央組織から、そうしたツールを取得する組織、として捉えられることが多い。

しかしPwCは、これに加えて、スパイウェア、ゼロデイ攻撃および関連機能などの攻撃的セキュリティソリューションを（それらを運用する）組織に販売する企業を「商業クォーターマスター」と定義している。従来のクォーターマスターは、自国の脅威アクターにツールを提供するのみである場合が多いが、商業クォーターマスターの場合、クライアントとなるアクターは、自国だけでなく複数の国を拠点とする場合もある。

APTクォーターマスター

常に証明できるわけではないが、複数のAPTグループが同じデジタルクォーターマスターの下で活動している、または同じデジタルクォーターマスターから援助を受けている、という仮説は、さまざまな脅威アクターについて排除できないだろう。2021年、PwCは引き続き、複数がグループの共有している能力（マルウェア、技術、攻撃など）の観察、インフラの重複（指令サーバー（C2）で観察された同一パターンまたは他の脅威アクターによるドメイン／IPの再利用など）などを通じて、こうした現象の観察を続けた。

Shadowsとプロキシ：中国を拠点とする脅威アクターがツールを共有

中国を拠点とする脅威アクターの間では、ツールやテクニックが継続的に共有されている。中国を拠点とする脅威アクターの全てがツールを共有して同じツールにアクセスできるわけではないが、クォーターマスターによる調整（後のセクションで詳述）が、活動のアトリビューションを複雑にしていることに変わりはない。例えば、同じ種類のマルウェア（PlugX、PoisonIvy、ShadowPad、Quarian、Winntiバックドアなど）が、中国国内の複数の脅威アクターによって使用されており、2021年にProxyLogon事件で明らかになったように、一部の脅威アクターは攻撃手法も共有している。

これらの脅威アクター全てが、以下に詳述する共有ツールを利用していることが確認されているわけではないが、これらは本セクションで説明するトレンドの典型例である。

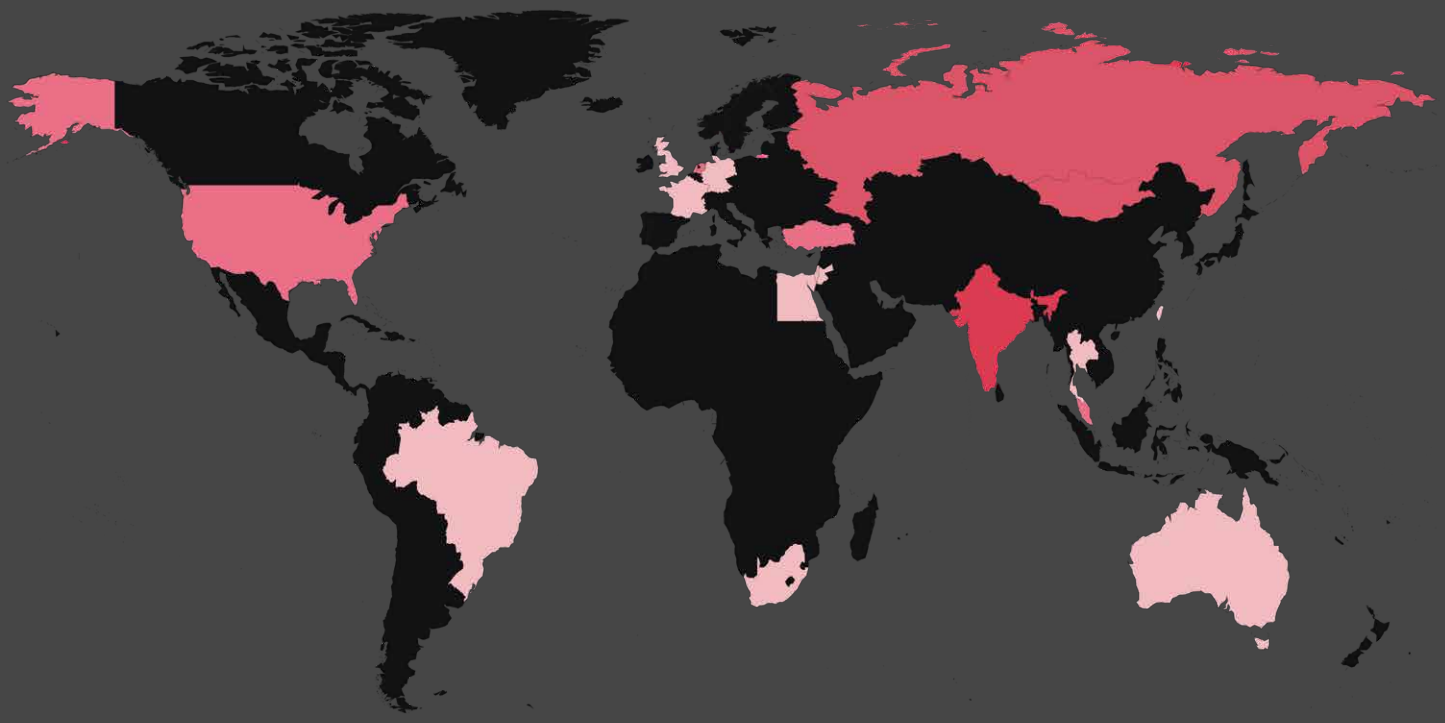
ShadowPadとScatterbee

ShadowPadは、脅威アクターによって埋め込まれた機能をカスタマイズすることが可能なモジュール型バックドアである。PwCが確認したShadowPad のサンプルには、後段のモジュールセットを調整するルートモジュールがあり、これには、脅威アクターが必要とする機能に応じてカスタマイズ可能なプラグインモジュールが含まれている。プラグインにより、HTTPまたはTCPを介したC2通信、キーロギング、スクリーンショット収集、ポートマッピング、システム情報収集などの機能を有効にすることができる[6]。

2021年、「標準型」ShadowPadのサンプルを追跡調査する中で、PwCがScatterbeeと呼ぶ新たな変種を特定・分析した。これは、ShadowPadサンプルを独自の手法により難読化したものである[7]。おそらく標的のネットワーク上で極力検出されないよう、ScatterBee のパッキングメカニズムは、制御フローの難読化、文字列エンコーディング、動的API解決、複数の解析対策技術およびシェルコードのデコーディング／デクリプティングを実装している。PwCは、1名ないし複数のShadowPadユーザーがScatterBeeにアクセスし、Adobe Flashアップデートファイルの配信に使用されるサイトへの「水飲み場型攻撃」を通じて、これらの悪意あるペイロードの一部を送り込んでいる可能性が非常に高いと評価している。また、ScatterBeeペイロードの大半は、PwCがRed Dev 10（別名：Earth Lusca）として追跡調査している脅威アクターに直接関連付けることができ、航空宇宙・防衛分野の組織を標的として使用されてきたと評価している。

PwCは、ShadowPadが、少なくとも中国を拠点とする11の脅威アクターによって使用されている可能性が高いと評価している[8]。ShadowPadインフラの特定のサブセットを分析した結果、インドを拠点とする電気通信業界および石油・ガス業界の事業者から、国際人道支援組織の東アジア支部に至るまで、幅広い被害者が特定された。

図表1：2021年12月までに観察されたShadowPad被害者の地理的分布



出所：PwC

Microsoft Exchangeを「エクスチェンジ」：ProxyLogon

2021年初頭、Red Dev 13（別名：HAFNIUM）はMicrosoft Exchangeの脆弱性に攻撃を開始し、これは「ProxyLogon」と総称されるようになった[9、10、11]。ProxyLogonをめぐる初期の活動はもっぱらHAFNIUMに関連したものであったが、2021年2月末から3月初頭にかけて（これらのキャンペーンが初めて明るみになった時期に近いがそれよりも前のタイミングである）、中国を拠点とする複数の脅威アクターが同じ脆弱性に攻撃を開始し、大規模なものから細かく標的を絞ったものまで、さまざまな活動を展開した。

すでに述べたように、これらの脅威アクターがツールを共有することは珍しいことではない。しかし、Microsoft Exchangeの脆弱性パッチが適用されるまでの間にこれほど迅速に攻撃が共有されたことはなかった。

複数のAPTにわたり活動するイランの開発者

脅威アクターは通常、その能力、インフラ、標的、通常の戦術、技術および手順（TTP）によって識別される。しかし、複数の脅威アクターにわたるキャンペーンの背後に潜む開発者やオペレーターの存在によって、こうした分析やアトリビューションが混乱する場合がある。

このようなケースは、イランを拠点とする脅威アクターに時折見受けられる。例えば、PwCがYellow Liderc（別名：Tortoiseshell、TA456）によるフィッシングキャンペーンを調査した結果、高等教育機関を標的とした一連の悪意あるPDF文書が確認された。この標的は、本来であればYellow Lidercの標的とは合致しないが[12]、Yellow Garuda（別名：Charming Kitten、APT35、PHOSPHORUS、TA453、ITG18）の標的と合致している。PwCは以前、これら2つの脅威の間にインフラの重複があることを指摘し、Yellow LidercがYellow Garudaの分派であるという仮説を提起した[13]。これらの脅威アクター間の複数の類似点に基づき、PwCは2021年中にオペレーターがこの2つの間を移行していたという可能性が現実的であると評価している。

商業クォーターマスター

商業クォーターマスターは、CyberRootやBellTroXのような、いわゆるハッカー代行（Hack-for-Hire）業者とは異なる[14]。ハッキング代行業者が、報酬を支払うクライアントに代わって実際のハッキング行為を行うのに対して、商業クォーターマスターは、クライアントが支払う分のツールを提供するのみであり、実際にツールを用いてハッキングを行うのはクライアント自身である。商業クォーターマスターの初期例としては、Hacking TeamやFinFisherが挙げられるが、いずれも世間から大きな反発を受け、その後、ブランド名の変更や倒産を余儀なくされた。こうした企業の活動による損失例があるにもかかわらず、PwCは、脅威アクター、特にサーベイランスを行う企業が、いまだに商業クォーターマスターとその能力を活用しているケースを確認している[15]。

最近になってNSO GroupやCandiruのような商業クォーターマスターに対して世間の目が向けられたことで、比較的秘密裏に拡大を続けてきたこの業界に対する知見が得られた。それは、サイバーセキュリティの専門家や潜在的な被害者にとって、以下のような意味を有する。

- 商業クォーターマスターに頼らず、また高度な攻撃を行うことができない脅威アクターは、特定することが困難である。
- 国家が最新のマルウェアを用いて企業、政府機関、またはその職員など民間と公共部門の両方を標的にすることが可能になる。
- これらのツールが、ジャーナリスト、活動家、市民社会を標的に乱用される可能性がある。

さらに、商業クォーターマスターが開発したツールは、政府関係者や民間企業の役員を含む幅広い標的に対して使用されていることはほぼ間違いなく、この種の脅威アクターが自分たちの脅威プロファイルには適合しない、と考えている組織は注意が必要である。

厳しさを増す監視の目：サーベイランスと市民社会

民間人を標的としたサーベイランスは、攻撃ブローカーやサーベイランス・ソフトウェア・ベンダーの台頭による武装化であれ、クォーターマスターの調整による強化であれ、あるいは国家が支援するグループによる実行であれ、全ての人々にとって安全なデジタル社会の実現に大きな脅威をもたらす行為である。マイノリティ、公民権活動家、反体制派、政治家、ジャーナリスト、そしてより幅広い一般市民が、こうした国家主導のスパイ活動の標的になるケースが多く見られる。また、市民社会の標的には、NGO、社会運動、連合、宗教組織など、共通の利害を有する組織も含まれる場合がよくある。

サーベイランス活動はしばしば特定の対象者に焦点を当てるが、そうした対象者が関わる組織が被害者となることもある。その場合、組織は本来の標的である個人にアクセスするための踏み台とされる。こうしたケースは、市民社会への脅威を万人共通の問題として説明する上で有用だろう。

サーベイランスの強化：ハッキング代行業者から商業クォーターマスターまで

Candiru

2021年7月、Citizen Lab[16]、Microsoft[17]、Google[18]は、程度の差こそあれ、Candiruという名前の商業クォーターマスターの存在を明らかにし、PwCはこれをGrey Mazzikim（別名：SOURGUM）として追跡調査してきた。Microsoftによると、この脅威アクターのスパイウェアは、100人以上の標的に対して展開されたとされている。2021年にPwCが追跡調査したキャンペーンに関連する複数のドメインは、明らかに人権活動家およびジャーナリストを標的にしていること示していた。また、他のドメインは、エネルギー輸出や政府機関などにより国家の戦略的利益に沿った標的であった。Grey Mazzikimが販売するスパイウェアは非常に高度で、iPhone、Android、Mac、PC、クラウドアカウントに感染し、秘密裏に状況を把握することが可能である[19]。一旦スパイウェアに感染すると、Gmail、Skype、Telegram、Facebookを含む多くのアプリやアカウントから被害者の個人データを流出させ、閲覧履歴やパスワードを取得することが可能である[20]。また、標的のWebカメラやマイクをオンにすることやスクリーンショットを撮影することも可能と思われる。

Candiruは世界中の複数の脅威アクターにツールを提供するサプライヤーであり、これらの攻撃の複雑さと規模は非常に広範囲に及ぶ。PwCは、これらの脅威を最大限にカバーし分類するため、CandiruをGrey Mazzikimとして追跡調査しており、現在少なくとも4つの異なる脅威アクター（「WhiteDev87」「WhiteDev88」「White Dev 16」「Gray Turul」）からなるその顧客を、可能な限り個別に調査している[21]。標的は多岐にわたるが、特に欧州と中東に焦点が当てられている。

NSO Group

PwCがGrey Anqaとして追跡調査しているNSO Groupは、2010年に設立された。同社は、Pegasusと呼ばれるスパイウェアで最も広く知られているが、携帯電話用の位置情報ソフトウェアやデータ分析システムなど、その他の製品も幅広く提供している。同社が提供する主なサービスと製品は、モバイル機器とネットワークに特化している。Pegasusは、FORCEDENTRYとして知られる最も高度な攻撃を含むゼロクリックおよびゼロデイ攻撃によって、一般的なモバイルOSの最新バージョンに感染することが知られている[22,23]。

NSOは、Pegasusスパイウェアを国家に販売し、最終的に国家がそのツールで市民社会をサーベイランスしていたということで幾度も話題となった。

Grey AnqaとGrey Mazzikimには多くの類似点がある。同じ国で活動する同じタイプの企業で、採用人材層も顧客層も同じである。どちらのケースでも、脅威アクターは攻撃的な能力を簡単に購入可能であり、国際的な規模で市民社会を標的にするのに使われてきた高度なツールを脅威アクターが行使できるようになる産業であることが明らかになっている。

プラグを引き抜く：商業クォーターマスターへの反応

2021年は、商業クォーターマスターは世間の目にさらされ、また複数の国において法廷の場に引きずり出された。例えば、米国のテクノロジー企業数社は、自社の顧客基盤を代表して商用スパイウェアプロバイダーに対して訴訟を起こし、場合によっては、被告が企業のハードウェアやソフトウェアにアクセスすることを制限するよう求めている。2021年には、国家レベルで初めて商業クォーターマスターに焦点を当てた行動も見られた。米国商務省が、NSOグループとCandiruを「米国の国家安全保障または外交政策の利益に反する」行動をとる危険性が高いとして、Entities List（取引制限リスト）に掲載したのである[24]。

こうした活動の最初の成果として、イスラエル政府は、国内セキュリティ企業がサーベイランス・攻撃用ハッキングツールを販売できる国家リストを3分の2に制限するなどの措置を取った。先に強調したように、商業クォーターマスターは世界の複数の国で活動しており、欧州[25、26]や米国[27]でも数多くのブローカーが活動していることに注意する必要がある。

商業クォーターマスターが今後も存続する可能性が高いということは、新たな課題をもたらすことになる。国家が、比較的容易に自国の能力を高度な持続的脅威のレベルにまで高めるような特注の高度な攻撃ツールを購入できてしまうのである。商業クォーターマスターが最先端の技術を有しているということ、またそれに見合う研究開発予算があるということは、高い運用セキュリティ標準を維持しつつ新たなツールを提供する能力があることを意味する。これらによって、脅威アクターは、商業クォーターマスターが世間の目にさらされるようになっても、自らの活動を継続することが可能なのである。

執拗な高度監視者：APTサーベイランス活動

Red Dev Redemption

Red Dev 3（別名：DeepCliff、RedAlpha）は、少なくとも2015年から活動している脅威アクターであり、2018年にCitizenLabによって特定のコミュニティを標的にしていることが初めて公開情報の中で暴露された[28]。そして2021年、Red Dev 3が世界規模でさまざまな標的層を狙ったクレデンシャル・フィッシング・ページをホストする数百のドメインを設定したことが確認された[29]。

Red Dev 3のドメイン命名規則は一般的なメールサービスプロバイダーを模倣しており、脅威アクターが標的組織における特定のメールサービスのログイン画面を詐称する場合もある[30]。

Red Dev 3は、ディアスポラ（移民）や反体制派に人気のあるニュースメディア、Amnesty Internationalなど難民や市民・人権に焦点を当てたNGO、シンクタンクや政策研究所なども標的にして、なりすましを行った。

2021年4月以降、PwCは脅威アクターの標的が市民社会から少なくとも5カ国の外務省および複数の政治団体を含む政府機関に広がっていることを確認した[31]。しかし同時に、脅威アクターは、センシティブな政治的・社会的トピックに関連して、個別の市民や脆弱なコミュニティを大胆かつ執拗に狙い続けていた。

Red Nueの新たな行動

2017年から活動しているRed Nue（別名：ReverseWindow）は、マルチプラットフォームのLootRATバックドアを使用することで知られている[32]。LootRATには、Windows[33]およびMacintosh[34]向けの亜種（公開情報ではDemstyとして報告されている）、さらにSpyDealerとして知られるAndroid向け亜種がある[35]。Red Nueは、少なくとも2019年以降、WinDealer[37]として知られる別のWindowsバックドア[36]も使用しており、中国のディアスポラコミュニティ向けの中国ニュースサイトにおいて、水飲み場型攻撃の一環として標的へのキャンペーンを展開した。

2021年、脅威アクターはLootRATを用いた活動を繰り返し、バックドアのLinuxバージョンを展開したことが確認された[38]。このバックドアの新しいサンプルでは、バイナリのコメントセクションが削除されており、これはおそらく脅威アクターに関する分析と理解をより困難にするためであったと思われる。このキャンペーンで観察された全ての被害者は、アジアを拠点としており、シミュレーションソフトを提供するテクノロジー企業が含まれていた。

「商業クォーターマスターが最先端の技術を有しているということ、またそれに見合う研究開発予算があるということは、高い運用セキュリティ標準を維持しつつ新たなツールを提供する能力があることを意味し、これらによって、エンドユーザーとなる脅威アクターは、商業クォーターマスターが世間の目にさらされるようになっても、自らの活動を継続することが可能なのである」

Red Nueの被害地域は、主にアジアの一部地域であった。この脅威アクターは、LootRatのMacOS版であるDemstyを使用して、個人や大学を標的にしている。例えば、SpyDealer（LootRATのAndroid版）は、WeChat、Facebook、WhatsApp、Skype、Sina Weibo、Tencent Weibo、Oupeng Browserなど40以上のモバイル通信アプリから情報を窃取する機能を有しており、これらのアプリケーションの多くは中国で広く使用されているものである。

中東・北アフリカを標的とするWhite Dev 75

White Dev 75は、少なくとも2015年から活動しており、PwCは、この脅威アクターが諜報活動を目的としている可能性が高いと判断している。観察された被害者は主に市民社会のメンバーであり、政治的な話題に関連して狙われている可能性が高い。White Dev 75は現在も、中東および北アフリカ全域のジャーナリスト、反体制派、および政治的に関与する個人のメールアカウントを侵害する上で非常に大きな効果を上げている[39,40,41]。

White Dev 75は、少なくとも2021年4月から10月にかけて、中東諸国の外務省になりすましたドメインなど、過去のキャンペーンで観察された戦術や手順と一致する数十もの新しいフィッシングドメインを登録した。White Dev 75は、多要素認証（MFA）を回避し、信憑性のあるソーシャルエンジニアリング技術を活用することができるため、特に効果的である。White Dev 75がよく用いるフィッシングメールは、ログインに異常があることを知らせる偽のセキュリティアラートである。この脅威アクターは、OAuthを攻撃してMFAやパスワードを一斉に回避することも確認されている[42]。OAuthは、パスワードを共有することなくサードパーティーのサービス認証を可能にする一般的なアプリケーションである。観察されたWhite Dev 75のTTPは、特に高度なものではないが、市民社会に対してこれらの戦術を実行することが有効であることを示すものである。

40 種類以上：SpyDealer（Android版LootRAT）が情報を取得できるアプリの数

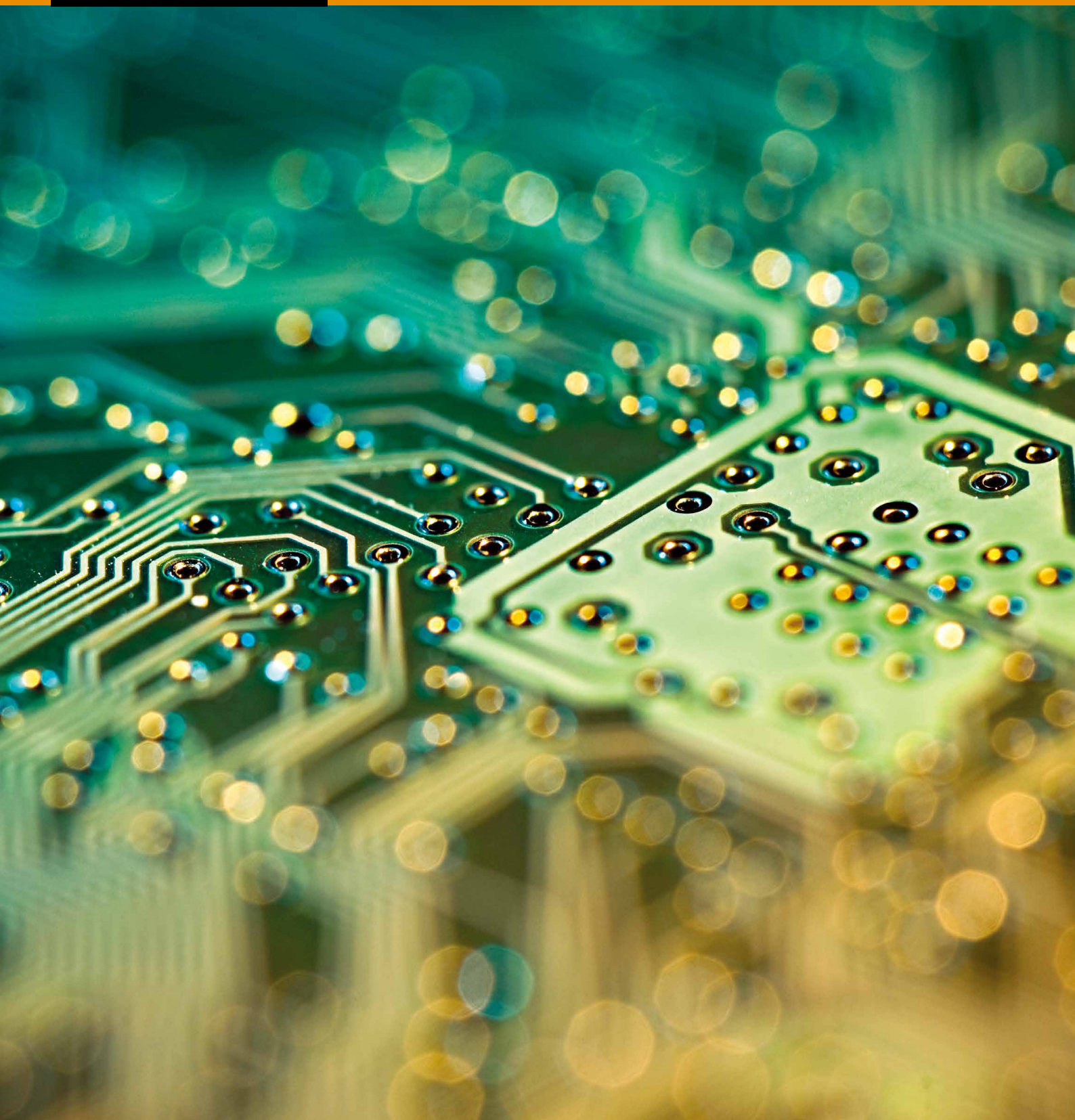
Yellow Garudaの国内サーベイランス

Yellow Garuda（別名：Charming Kitten、PHOSPHORUS、ITG18）は、少なくとも2012年から活動しているイランを拠点とする多才な脅威アクターである。2021年を通じて、非常に活発にそのサーベイランス能力を発揮してきた。

PwCは、Yellow Garudaが被害者のTelegramアカウントからデータを抽出するために、標的型の国内サーベイランスキャンペーンを行った証拠を発見した[43]。その証拠として、流出したメッセージ、メディアファイル、グループメンバーの詳細、および被害者の連絡先などが含まれていた。PwCが入手したデータおよび被害者のアカウントからデータを流出させるために使用された脅威アクター独自のTelegramのデータ抽出ツールのコピーから、2021年9月から10月にかけて、脅威アクターが少なくとも6名のイラン人を攻撃していたことがわかっている。PwCはまた、7人目の国内被害者のサーベイランスに関して、脅威アクター自身が書いた運用レポートも発見した。この被害者のデータはより広範囲に及ぶもので、モバイルマルウェアによって流出した可能性が高いものだった。

Yellow Garudaのツールセットにモバイルマルウェアが加わったことは、公開されたフォーラムで報告されており[44]、これは、2021年初頭に既知のYellow Garudaインフラに複数のリンクを有するAndroidマルウェアサンプルに対して行ったPwC独自の分析とも相関している[45]。このサンプルは、メッセージアプリのWhatsAppを装っており、音声や動画の録音、写真撮影、連絡先、位置情報、SMSへのアクセス、通話開始などの機能が備わっていた。その機能とコードベースは、イラン国民を標的とするために使用されたとされる2018年の旧型Androidマルウェアのサンプルと類似しており、Yellow Garudaが以前からこの機能を有していた可能性が高いことを示している。

サイバー犯罪



ランサムウェア

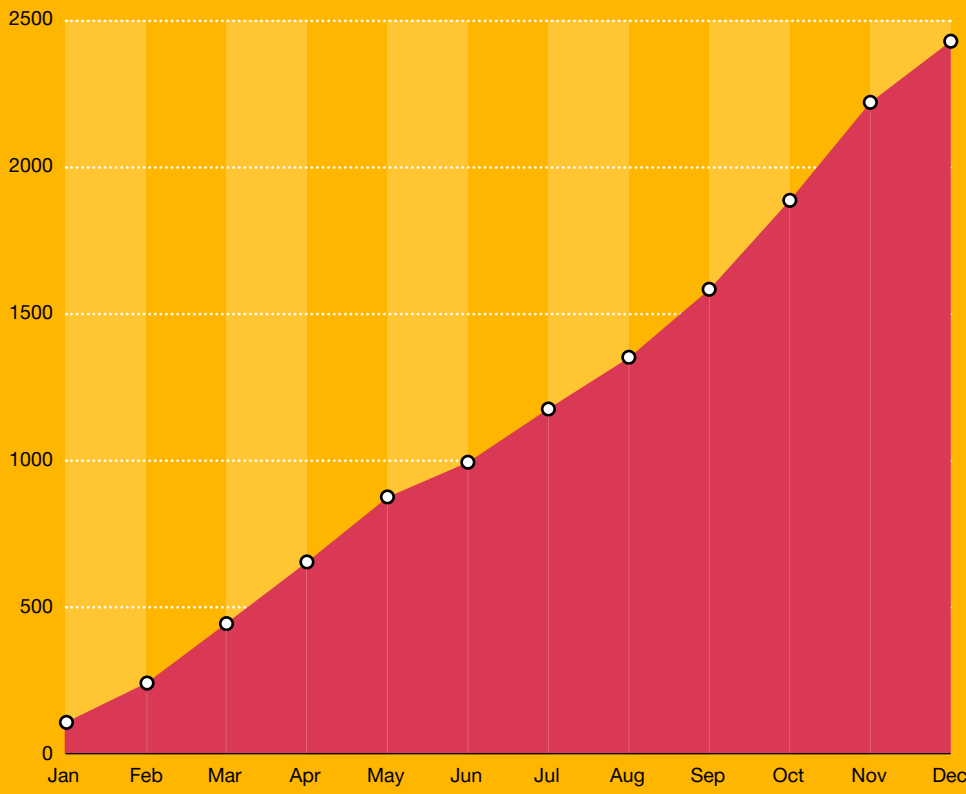
2021年においても、ランサムウェアは多くの組織が直面した最も重大なサイバー脅威であった。こうした傾向が続いている背後にある要因もこれまでと同様であり、その多くは以下の観察にあるようにより増幅している。

- ランサムウェアの運用に携わる脅威アクターの数は、ランサムウェア・アズ・ア・サービス（RaaS）やアフィリエイトスキームの台頭を背景に増加した。
- 公に報告された攻撃のペースと頻度がほぼ倍増した。
- 盗んだデータの流出または流出による脅迫は、著名な脅威アクターの大多数にとって標準的手順となり、データの暗号化によって引き起こされる事業の混乱という危機に、プライバシー、規制、評判のリスクが加わった。

ランサムウェアは金銭的な動機によるものが圧倒的に多いが、政治的な動機による意図的な破壊攻撃のケースも少ないながら存在する。

2020年、約1,300のランサムウェアの被害組織から、リークサイトにデータが流出した。これが2021年にはほぼ倍増し、2,435の組織が被害を受けた。

図表2：2021年のランサムウェア流出件数の推移



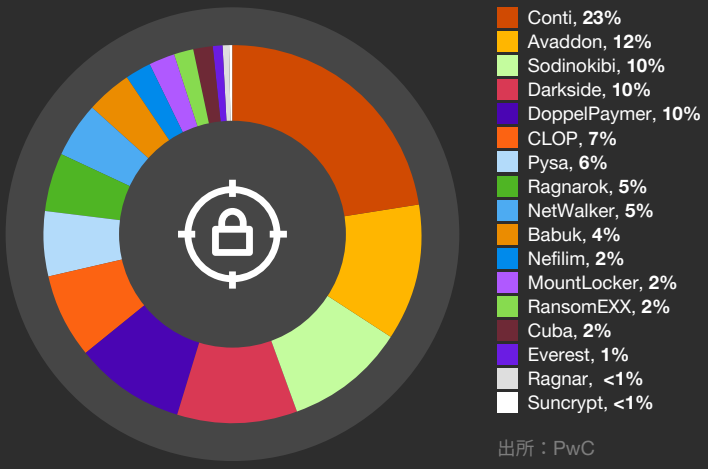
昨年の約2倍にあたる

2,435

の組織が被害を受けてリークサイトにデータが流出。

出所：PwC

図表3：ランサムウェアのインシデント数：2021年第1四半期

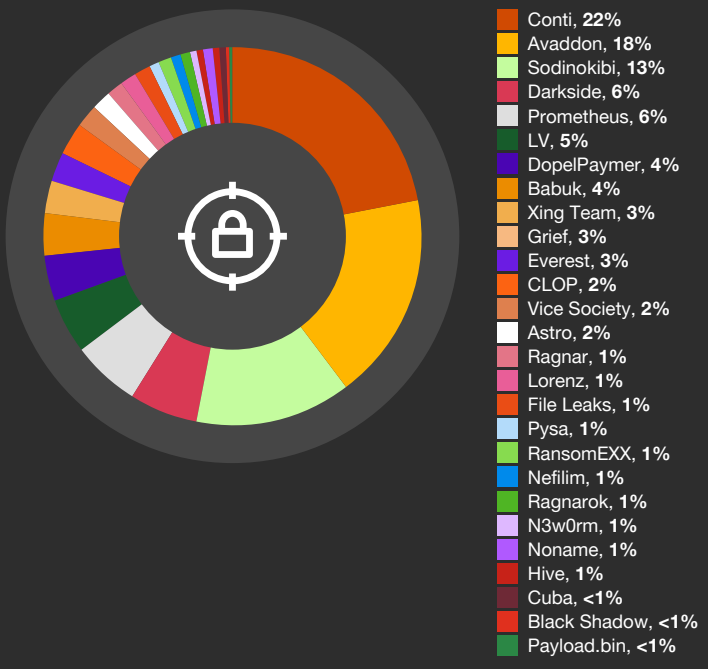


出所：PwC

ランサムウェア運用に関わる脅威アクターの数は変動しており、後のセクションで詳述するように、著名な脅威アクターが活動を休止するケース、完全に活動を停止するケース、活動休止を経て新しいブランド名で登場するケースもある。例えば、2021年第1四半期にPwCは、17の脅威アクターが約440の組織のデータを漏洩したことを確認したが、これらの攻撃の65%は、わずか5社の脅威アクターによるものであった。

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

図表4：ランサムウェアのインシデント数：2021年第2四半期



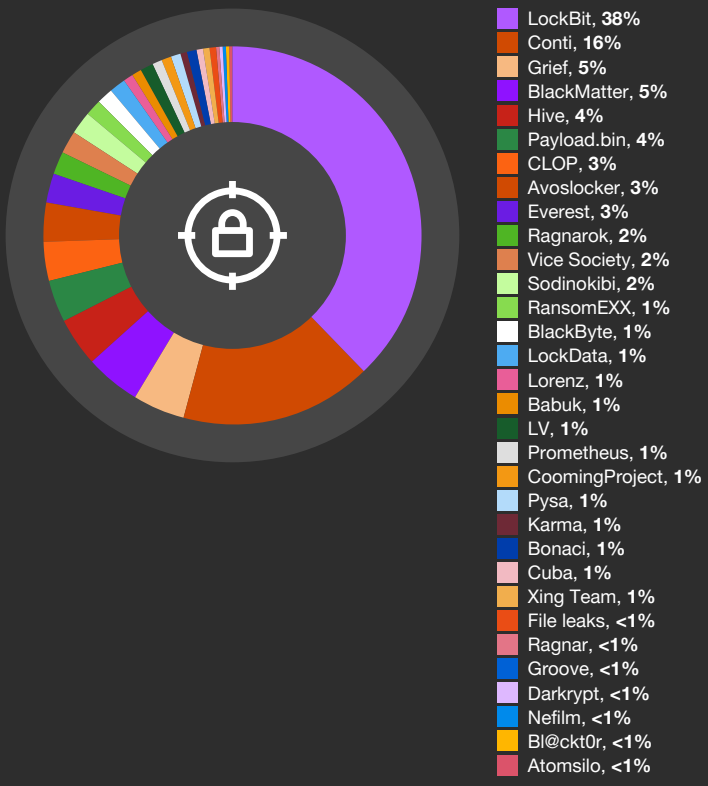
出所：PwC

2021年第2四半期、ランサムウェアの運用が観察された脅威アクターの数は27に増え、それに対応する被害組織の数も500を超えた。しかし、その活動はこれまで同様、少数のランサムウェアファミリーが大半を占め、インシデントの約60%がわずか4つのランサムウェア運用によるものである。

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

2021年第2四半期にDoppelPaymerの運用が目に見えて減少したのは、Griefと呼ばれるランサムウェアの亜種を導入する前に、脅威アクターが運用の「リブランディング」を図ったためと思われる。

図表5：ランサムウェアのインシデント数：2021年第3四半期



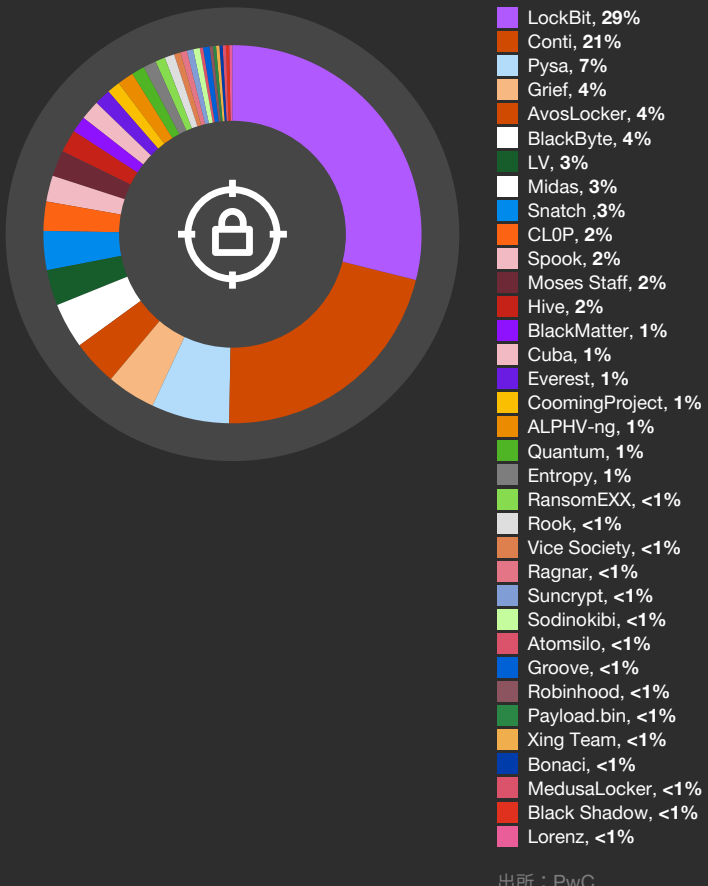
出所：PwC

2021年第3四半期までに、ランサムウェア市場に大きな変化が起こり始めていた。これらは、アフィリエイトプログラムが主なリクルートメントサイトから追放されたことや、注目を集めた攻撃の後、一部が自主的に解散したためである。しかし、この時期においてランサムウェア市場に影響を与えた最も重要な事象は、2021年7月にWhite Janus（別名：LockBit）がLockBit 2.0として再登場したことであった。LockBitのオリジナルのアフィリエイトプログラムは、2020年後半から活動を停止しており、White Janusがランサムウェアを作成し直した2021年7月まで、犯罪フォーラムのRAMP（Russian Anonymous Marketplace）に再登場することはなかったのである[46]。

この脅威アクターは急速なペースで活動を確立し、第3四半期に観察されたインシデントの約40%を占めた。これは、第2四半期末または第3四半期初頭に閉鎖された他のランサムウェアのスキームからアフィリエイトを引き取った結果と思われる。第3四半期には、32の脅威アクターがデータを流出させ、約600の被害組織を出したが、インシデントの64%は、やはりわずか4つのランサムウェアによるものであった。

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

図表6：ランサムウェアのインシデント数2021年第4四半期



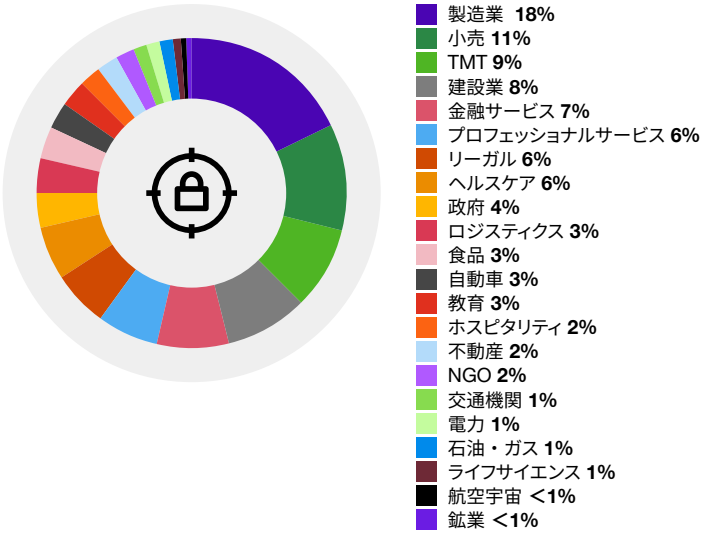
出所：PwC

2021年第4四半期は、攻撃のペースが上がり、約850件の被害がインシデントの観察集計結果に追加された。前四半期と同様に、データをリークする脅威アクターの数が再び増加し、第4四半期中に35のリークサイトが活動を行った。LockBitとContiが引き続き優勢で、観察されたインシデントの64%は、わずか5つの脅威アクターによるものであった。

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

Pysaの活動が急増したのは、11月10日にデータ流出が発生したためであるが、これは、Pysaの活動が急増したというよりも、脅威アクターが、標的からしばしば無視される流出サイトをアップデートしたことによるものである可能性が高い。

図表7：2021年の分野別ランサムウェアのインシデント数



出所：PwC

分野別内訳

ランサムウェア活動は、多くの場合、組織の経済分野には関心を払っていないものの、COVID-19の流行以降、多くの脅威アクターが、病院やその他のヘルスケア施設を標的としないことを公言している（完全に遵守しているわけではない）。脅威アクターが標的を定める場合、その注目ポイントは単純に組織の規模（エンドポイント数）、地理的位置（カナダ、EU、米国、英国に重点）、収益である[47]。2020年と同様、攻撃を受けなかった分野は皆無であったが、一部の分野が他に比べて頻繁に攻撃を受けており、上位6分野で全インシデントの 60%を占める結果となった：

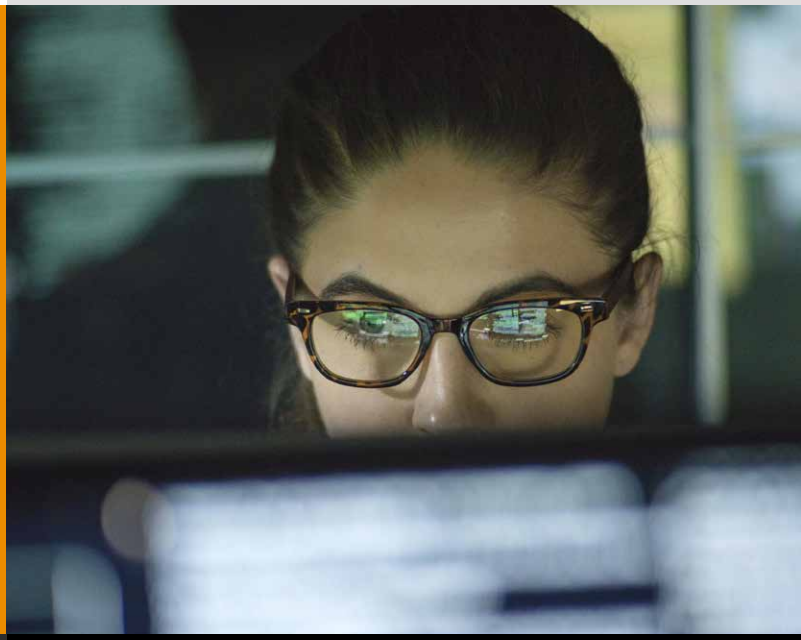
- 製造業 – 18%
- 小売・消費財 – 11%
- テクノロジー – 9%
- 建設業 – 8%
- 金融サービス – 7%
- プロフェッショナルサービス – 6%

2020年のランサムウェアインシデントのうち、同じ上位6分野が全体の66%を占めている。

これらの分野が、脅威アクターによって特に狙われているという証拠は見当たらない。しかし、ヘルスケア分野を除いた場合、これら6つの分野は、米国における売上高上位6分野とほぼ一致する[48]。White Onibiをはじめとする活動的な脅威アクターにとって、初期アクセスに成功した後、攻撃活動を継続するか判断する上で、被害者の収益は重要な要素となっている。これが、分野別の被害組織分布に何らかの影響を及ぼしている可能性がある。

60%

6分野（製造、小売・消費財、技術、建設、金融サービス、プロフェッショナルサービス）で発生したインシデントの全体に占める割合



インシデント対応ケーススタディ：

HSE

アイルランド共和国の保健サービス委員会（HSE）は、2021年5月にHSEのITシステムを混乱させたConti攻撃に関するレポート作成をPwCに委託した。HSEは、2021年12月10日に同レポートを公開し、このようなインシデント後の「完全開示」を行った世界初の事例のひとつとなった[49]。

2021年5月14日、ランサムウェアContiが3,500台以上のワークステーションと2,800台のHSEサーバーで起動し、アイルランド国内の医療サービスに広範囲かつ長期間にわたる混乱をもたらした。一部の医療機関では電子システム経由による患者データへのアクセスや予約が不可能になった。攻撃の発端は2021年3月にさかのぼる。あるユーザーが、電子メールで配信された悪意ある添付ファイルを開封してしまったのだ、ネットワークへの初期アクセス達成から攻撃後の活動まで、大きな時間差が生じた。これは、最初の侵害がアクセス・アズ・ア・サービス（AaaS）運用によって行われ、その後Contiが侵害されたエンドポイントを制御して攻撃を進めた結果と思われる。

Contiは「人間が操作する」ランサムウェアであり、ネットワークを通じて自動的に伝播し、あらゆるインフラを無差別に暗号化するマルウェアとは異なり、手動でバッチコマンドを実行することにより展開される。Contiの操作は、ネットワーク内でのラテラルムーブメントや権限昇格を容易にするCobalt Strikeの展開、Mimikatzを含むその他のツールを用いた管理者レベルのアカウントとシステム（特にActive Directory）の特定や侵害、ファイル暗号化に先立つデータ流出など、脅威アクターに関連する既知のTTP（戦術、技術、および手順）に従って行われた。Contiが被害者のコアIT資産だけでなく医療システムにも及んでいた場合、この攻撃の影響はさらに深刻化した恐れがある。今回のインシデントの規模と影響をもたらした要因の多くは、HSEという組織に限ったものではない。このレポートは、全ての組織が同様のサイバー攻撃に備え、その被害を軽減し、回復するために検討すべき教訓を明らかにしている。

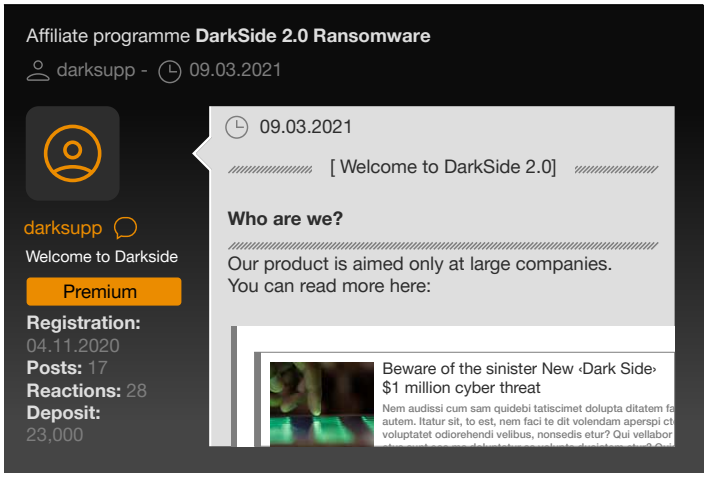
アフィリエイトプログラム

前年同様、2021年もアフィリエイトプログラムがランサムウェアの運用規模やペースを支える原動力となった。一般的に、ランサムウェアのアフィリエイトプログラムは、特定の種類のランサムウェアへのアクセスを利益分配ベースで提供する。このスキームでは、White Ursiaのような主要な脅威アクターがマルウェアの開発と管理に責任を持ち、攻撃を役割とする関連組織にアクセス権を提供する。被害者から得た資金は、事前に合意された利益分配に関する取り決めに従い、ランサムウェア運営組織とその関連組織の間で分配される。これにより、ネットワーク侵入や攻撃のスキルを有する脅威アクターは自らの手では容易に開発できないランサムウェアやマネタイズ能力が得られ、参入障壁も下がる。

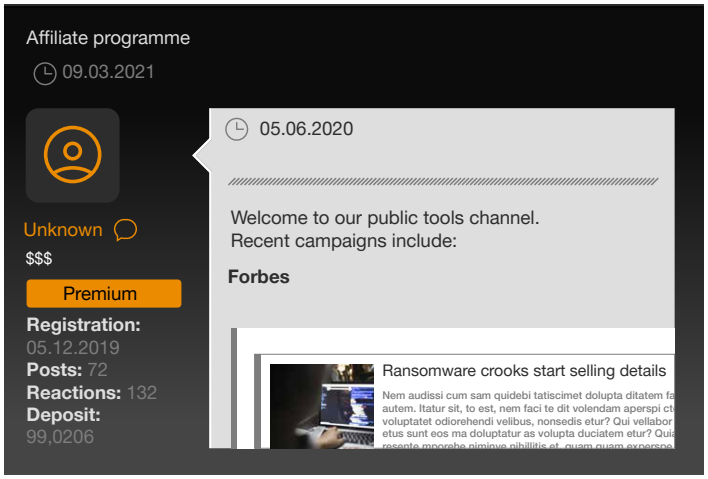
DarkSide、REvil、LockBitなど、有名なランサムウェアの多くは、ランサムウェアのアフィリエイトスキーム（Партнёрская программа）をオープンに運営している。他にも、Contiなど、最終目的を明確にせずに「ペネトレーションテスター（pentester）」として採用したケースも有る。アフィリエイトプログラムは、主にロシア語圏の犯罪フォーラム「Exploit」、「XSS」などで推進された。アフィリエイト（адвертов）の数と質が多くのランサムウェアが生み出す収益の決定的要因であるため、競合するスキーム間の競争は激化している。脅威アクターは、次のような方法で自らのプロファイルを高めている。

- 自らのフォーラムのアカウントに多額の暗号通貨を入金し、スキームの経済的な成功を示す
- メディアのインタビューに応じて活動の成功と収益を宣伝する。その多くが関連組織の募集場所でもある犯罪者フォーラムで好意的に伝えられた
- 自らの活動に関するメディア記事へのリンクを掲載する
- 採用する組織に他よりも優れた利益分配の仕組みを提供する
- 競合他社に対する技術的な優位性を主張する

図表8：DarkSideの関係組織募集広告



図表9：REvil



図表10：LockBit 2.0の広告－競合するスキームに対する技術性能の優位性を主張

Encryption speed comparative table for some ransomware - 02.08.2021

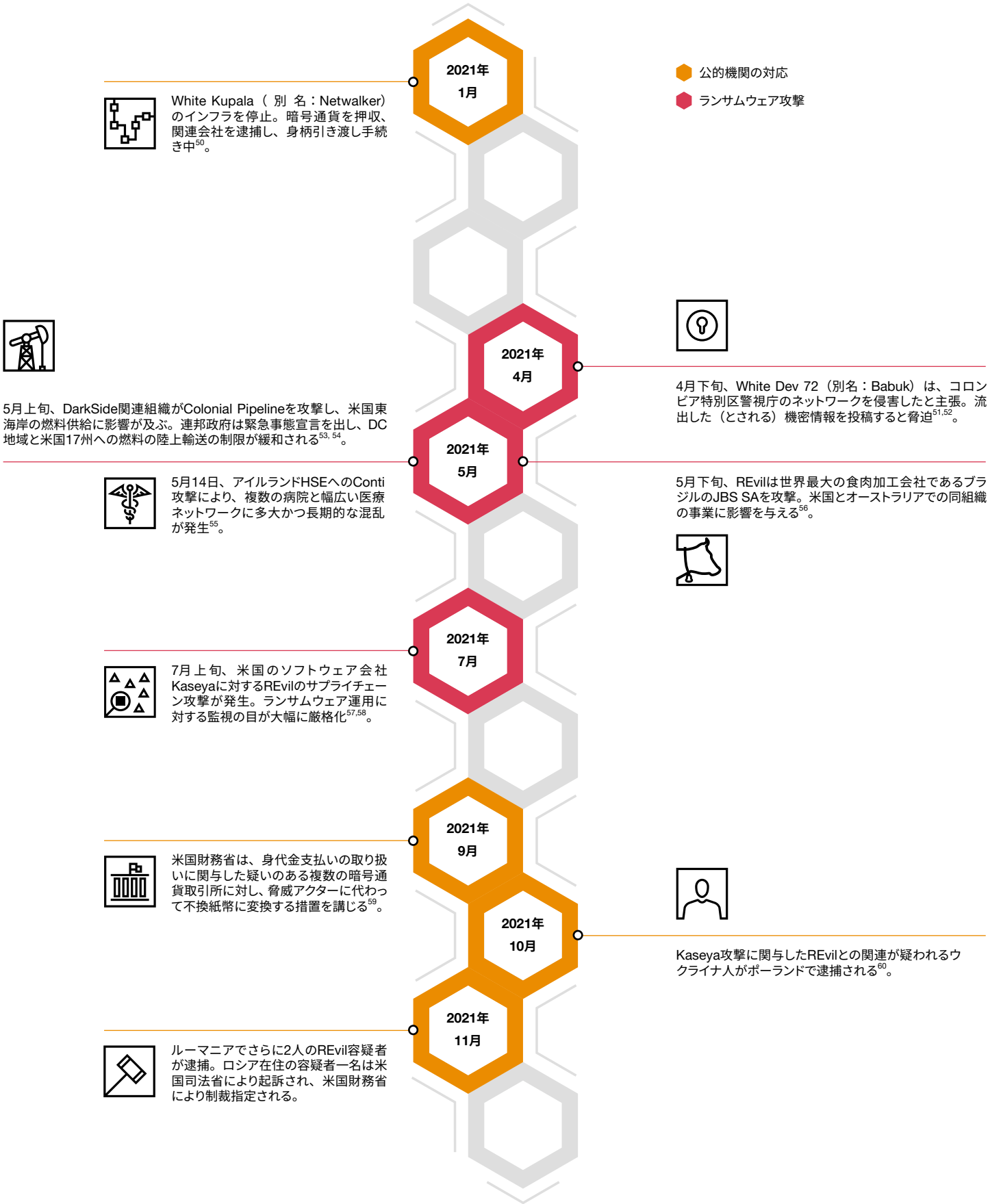
PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797

政治問題化：法律と規制への対応

2021年前半に主に米国の組織が被害を受けた一連の事件により、ランサムウェアの注目度が大きく高まった。

図表11：注目を集めたランサムウェア攻撃と公共機関の対応の年表



アフィリエイトスキームの大量排除

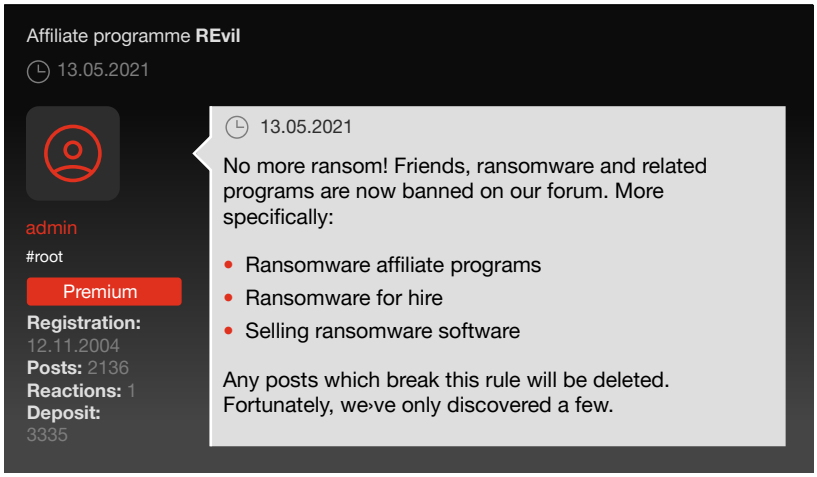
Colonial Pipelineインシデントを主なきっかけとして、ランサムウェアシステムに対する注目と圧力が高まり、アフィリエイトスキームに直ちに影響を与えた。5月14日、犯罪フォーラム「XSS」の管理者が、以下のような書き込みを削除した。

- アフィリエイトスキームの募集
- ランサムウェアのレンタル
- ロッカー（ランサムウェア）ソフトの販売

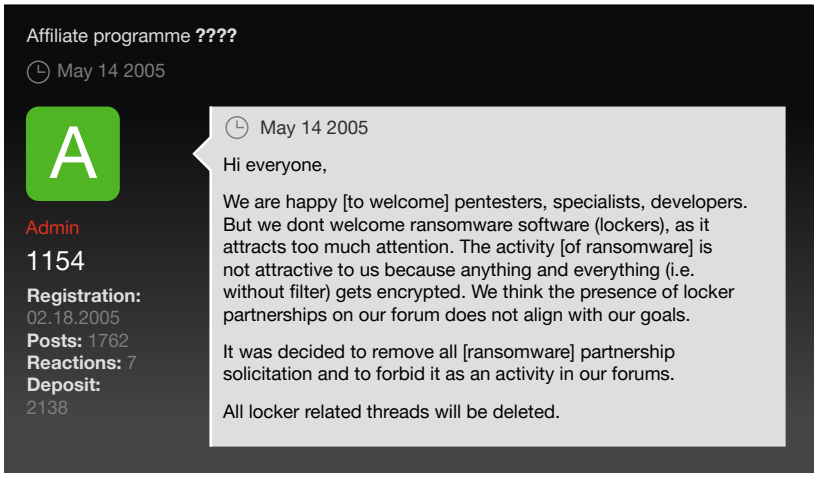
削除理由について管理者はいくつかの理由を挙げているが、重要なポイントは、ランサムウェアは「危険で有害であり地政学や国家による攻撃と結び付いている」ことだった。アフィリエイトスキームが運営されていたもうひとつの主要フォーラムである「Exploit」も、同様の理由を挙げてこうした動きに追従した[61]。

アフィリエイトスキームの禁止（ban）は、ランサムウェア脅威アクターのフォーラムからの排除にまでは至らなかったものの、一部は撤退を余儀なくされた。例えば、White Ursiaは、REvilアフィリエイトスキームを閉鎖し、「非公開にする」と発表し、その後、フォーラムのメンバーシップを完全にキャンセルした。White Apepは、「DarkSide」ランサムウェア運用を終了すると発表し、マルウェアの復号キーを公開した[62]。しかし、White Janus（別名：LockBit）を含む他の組織は、メンバーシップを維持し、関係組織の募集活動をリークサイトに移すのみであった。

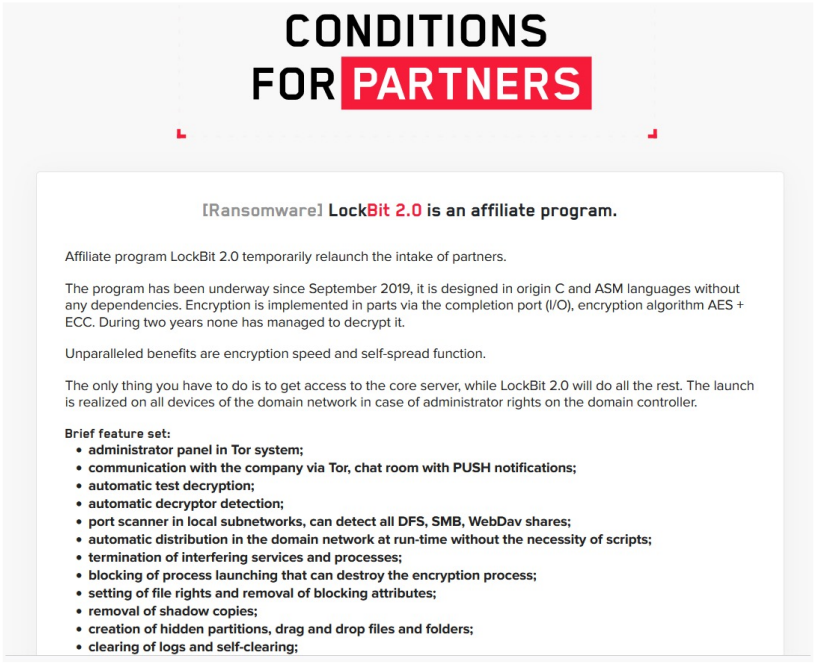
図表12：「XSS」管理者がサイト上でのランサムウェアの活動を禁止する



図表13：同様の措置を講じた「Exploit」管理者

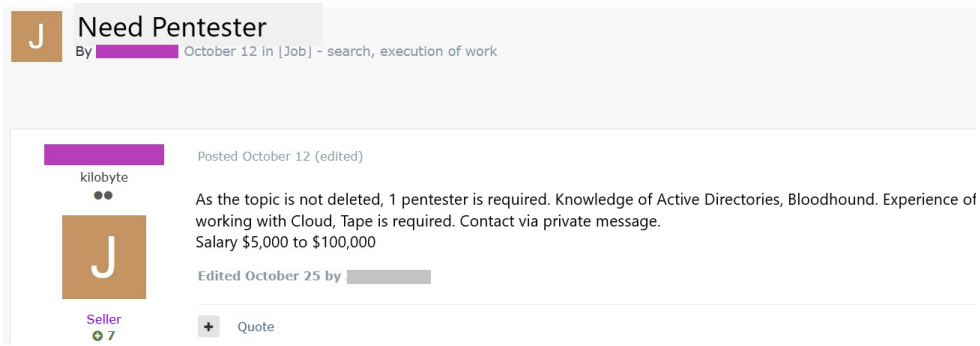


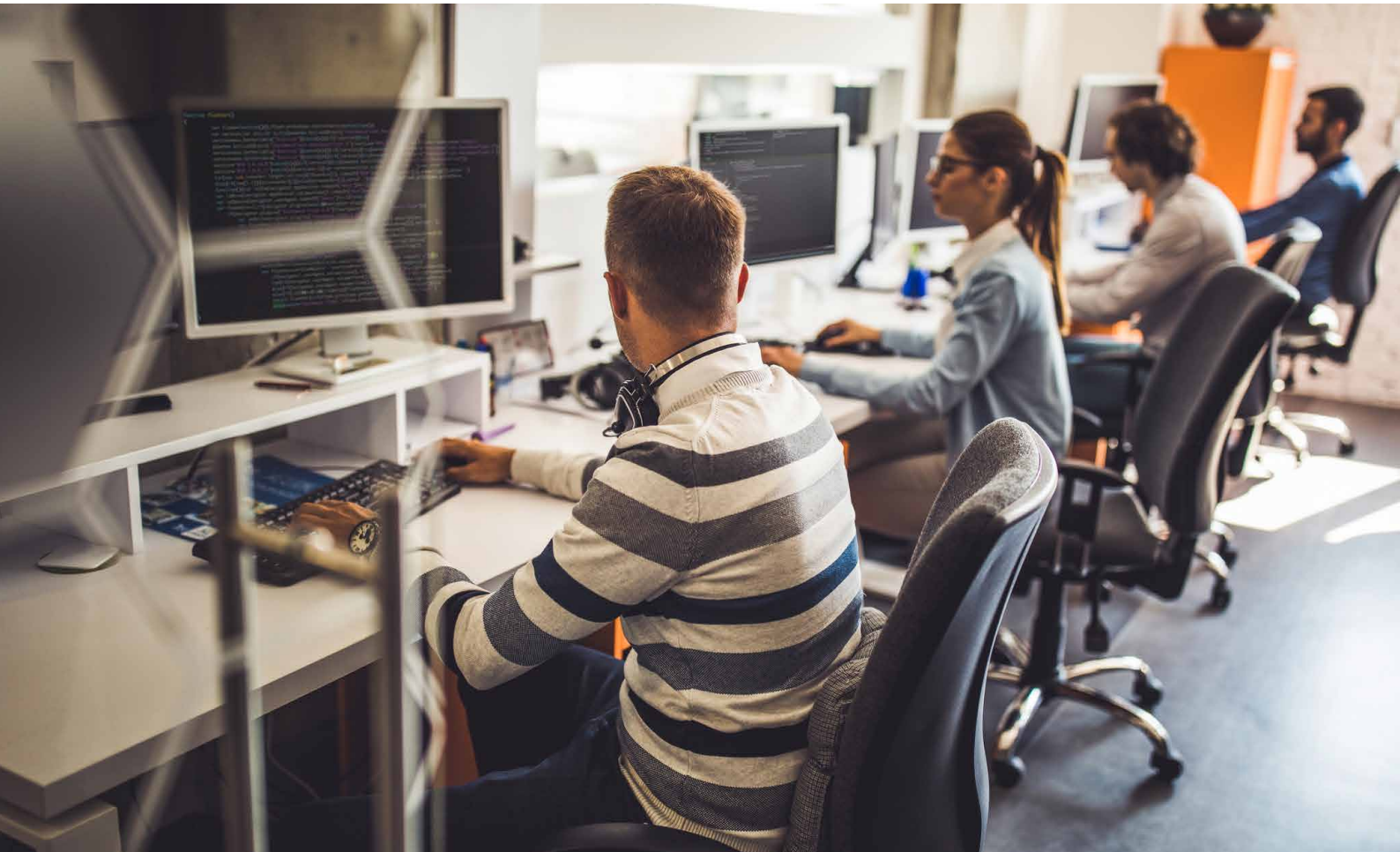
図表14：White Janusリークサイトにおける関連組織の募集広告



あからさまな募集が禁止された一方で、「ペンテスター」の募集は、犯罪フォーラム「Exploit」や「XSS」の「求職中」や「フリーランス」などのセクションに掲載されており、ほとんど影響を受けることなく継続していた。広告には、ランサムウェア運用のために募集が行われていることは明言されていなかったものの、多くの募集職種の職務記述書の内容は、以前のアフィリエイトスキームの募集時のものと類似していた。

図表15：正体不明の脅威アクターによるペンテスターの募集広告

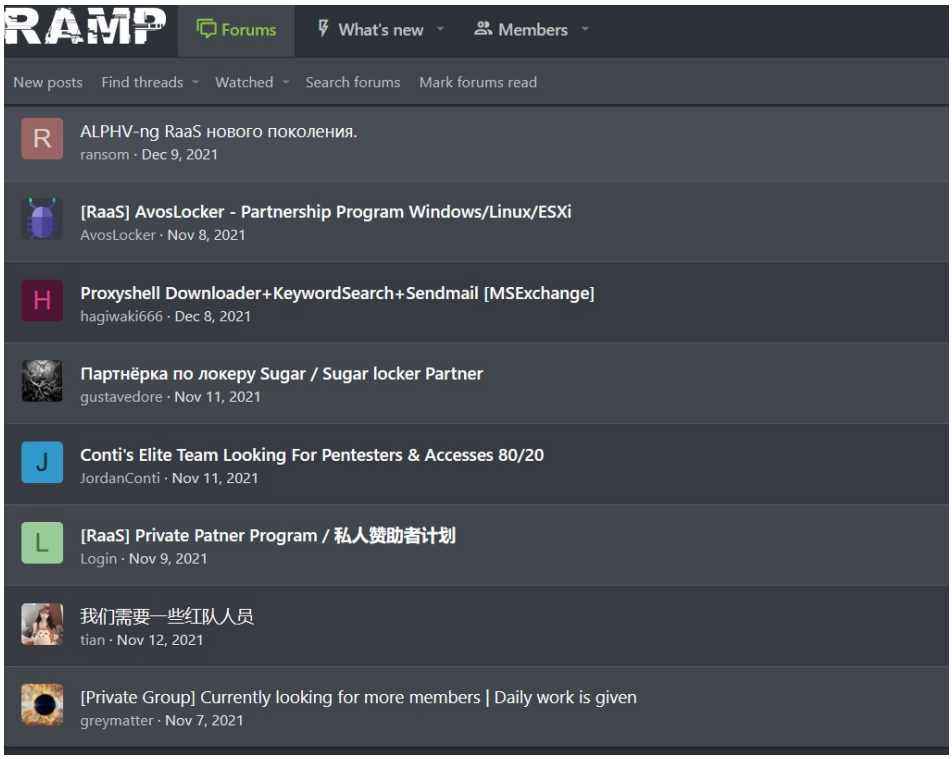




RAMP（Russian Anonymous Marketplace）の立ち上げ

7月中旬、アフィリエイトプログラムの募集が禁止されたことを受け、ランサムウェア運用やアフィリエイトプログラムのニーズに対応することを目的とした犯罪フォーラムが立ち上げられた。このサイトは当初、White Dev 72（別名：Babuk）が以前リークサイトに使用していたダークウェブのアドレスで運営され、ロシア語で麻薬の販売に関与していた以前のダークウェブサイトへの目配せかRAMPと名乗った。同フォーラムには、RaaSスキーム専用のセクションがあり、ペンテスターや企業ネットワークへのアクセスを募集する広告が掲載されている。現在、RAMPで活動している主なランサムウェアには、Conti、AvosLocker、BlackCatなどがある。

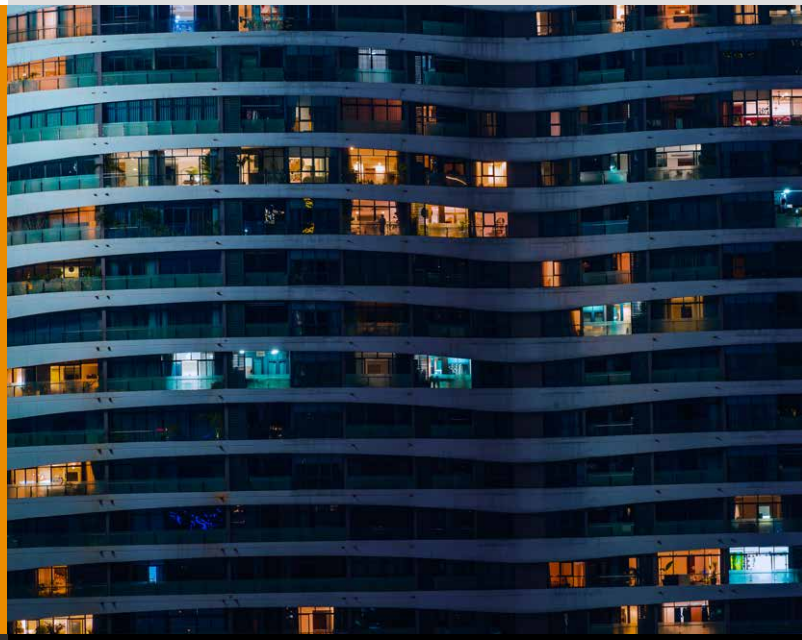
図表16：RAMPフォーラムにおける関連組織の募集広告



ランサムウェアのリブランディング

法的・政治的圧力の高まりに伴うもうひとつの影響として、2021年、近年で最高レベルのランサムウェアのリブランディングが見られた。ランサムウェアのリブランディングには、主に3つの利点がある。

- サイバー犯罪の脅威アクターにとって、何らかの失敗を犯した後でもプログラムを「リブート」できる可能性が生まれる（例えば、ランサムウェアの暗号化ルーチンに欠陥がみつかり、暗号化されたファイルの復号ツールを公開する羽目になった後）。
- 大規模なキャンペーンを行った後、高まった注目度を下げる機会が生まれる。
- 脅威アクターが攻撃元の発覚を阻止または遅延させることができる。



インシデント対応ケーススタディ：

新しい仕事は誰が？ランサムウェア運用者がアフィリエイトスキームを変える

2021年2月、PwCのインシデント対応チームは、フランスに拠点を置く農業関連組織を狙ったSodinokibi／Revil攻撃に対応した。この攻撃は1月中旬に始まり、フィッシングメールを介して同社の従業員に届けられた悪質な添付ファイルにより、被害者のワークステーションにQakBotがインストールされた。

初期アクセスに成功した後、脅威アクターはCobalt Strikeを展開し、被害者環境での影響力を強化した。そして、Windowsのリモートデスクトッププロトコル（RDP）を利用して、LSASSの認証情報にアクセスし、ネットワーク内でラテラルムーブメントを行った。この脅威アクターは、BITSジョブ、PowerShell、コマンドラインインタラクションを組み合わせて、ペイロードをインストールおよび実行し、ネットワークのフィンガープリントによる通信先のOSやデバイスの推測を行った。クラウドストレージ上のコンテンツを管理するために使用されるオープンソースソフトウェアであるRCloneを使用して、被害者のローカルストレージとクラウドストレージからデータを取得し、ランサムウェアを起動させた。

脅威アクターは、最終的にSodinokibi／REvilランサムウェアを展開したが、被害者環境内での動作は、PwCがWhite Samyaza（別名：Egregor、Prolock）として追跡調査している別のランサムウェアプログラム関係組織が採用していることが知られている技術により近いものであった。例えば、QakBotは、REvilの感染につながることも確認されているが[63]、むしろWhite Samyazaの活動とより強く結びついていた[64]。コマンドラインツールであるRCloneは、Egregor／Prolock運用者に頻繁に使用されており、特にこのユーティリティは、被害者の環境に不自然でないように「svchost.exe」という名前に変更されていた[65]。また、インシデント対応中に観察されたランサムウェアのファイルには、被害組織の名称が用いられていた。この命名方式は、Egregorランサムウェアに特有のもので、Sodinokibi／Revilランサムウェア（ランダムな命名方式でファイル名を付けることが多い）には通常見られない特徴である。

私たちが調査した証拠によれば、White Samyazaの関係組織がWhite Ursiaに移り、White Samyazaの関連組織によく見られるTTPを用いて Sodinokibi／REvilを展開した可能性が現実的であると評価している。

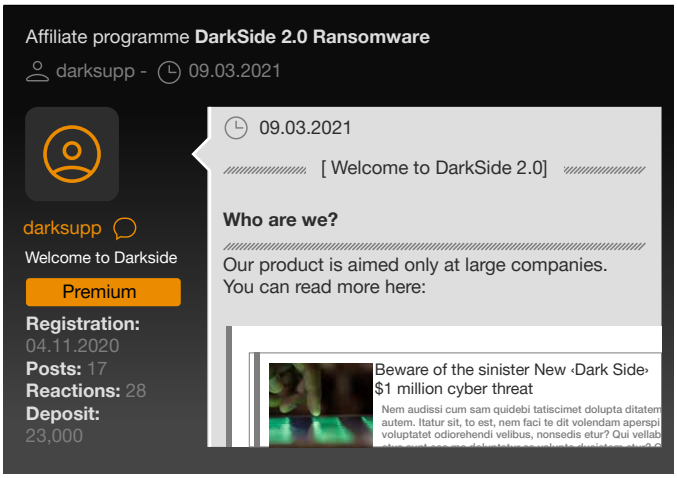
Blue Lelantos

2019年12月、ロシアを拠点とする犯罪集団「Evil Corp」（PwCではBlue Lelantosとして追跡調査）のメンバーが米国当局に起訴され、制裁対象に指定された[66]。Evil Corpの活動は2020年を通して続いたが、同グループに変化が生じたことが同年末には明らかになり、2021年を迎えて一層顕著になった。Evil Corpの主要なランサムウェアシステムのひとつであるWastedLocker[67]の検出は、2020年後半にはほとんど見られなくなった。しかしWastedLockerの運用は、相次ぐリブランディングを経て、2021年も継続された。2020年後半、WastedLockerによる身代金を要求するレターと同様のレターが、3月にはHadesランサムウェアおよびPhoenix Cryptolocker、6月にはPayloadbin、10月にはMacawで発見され始めた[68]。同様に、Evil Corpの悪名高き二重脅迫型ランサムウェアDoppelPaymer[69]は5月に事実上活動を停止し、同月、最後の被害者がそのリークサイトに追加された。6月には、GriefまたはPayorGriefと名乗る新たなランサムウェアが出現し、当初から被害者データをリークサイトに掲載するようになった。Griefのサンプルを分析したところ、DoppelPaymerとの間にコーディング上の類似点が多く見受けられた。大きな変更点としては、身代金の支払いに暗号通貨Moneroを使用している点が挙げられる。PwCは、GriefがEvil Corpによる新たなリブランディングによるものであり、これが最後である可能性は低いと評価している[70]。

2021年にEvil Corpが相次いでリブランディングを行った理由について直接的な証拠はないものの、PwCは、米国当局による同グループの制裁対象指定の結果である可能性が高いと判断している。

- 他の大部分のランサムウェアと同様、被害者の大半は米国である。
- 制裁対象組織に身代金を支払うまたは支払いを促す組織は米国の制裁措置に抵触する可能性があるため、支払いを行う可能性は低い。
- WastedLockerとDoppelPaymerのリブランディングにより、少なくとも短期的には、ランサムウェアのインシデントを制裁対象組織に責任を負わせることがより困難になった。
- 新たなランサムウェアの亜種をゼロから作成するのではなく、既存のコードをリブランディングすることで、Evil Corpの機会費用とランサムウェア運用を維持するために必要な時間を削減することが可能となる。

図表17：「Welcome to Darkside 2.0」告知投稿



White Apep

PwCがWhite Apepとして追跡調査しているDarkSide（別名：BlackMatter）は、少なくとも2020年8月から運営されており、2021年末時点ですでに2回のリブランディングが行われていた。1回目は、DarkSideのアフィリエイトプログラムが開始された2カ月後の2021年1月で、これはセキュリティ企業のBitdefenderがDarkSideによるファイルの復元を可能にする復号ツール[71]を公式に発表した時期である。White Apepの活動は一旦休止したが（その間、おそらく脅威アクターがアップデートを行ったと思われる）、結局、2021年3月9日に「DarkSide 2.0」という新たなブランドのもとで再開された。これはアフィリエイトプログラムのリローンチを伴い、既存のツールによる復号を防ぐよう設計されたランサムウェアのアップデート版を特長とするものであった[72]。

DarkSideの関連組織のひとつが、2021年に観察された中で最も被害が大きいインシデント、すなわち米国Colonial Pipelineへの攻撃を5月7日に成功させたのは、この最初のリブランディング後であった。この攻撃により、米国東海岸の燃料のほぼ半分を供給する5,500マイルのパイプラインの操業が停止する事態となった。米国政府によるDarkSideへの注目の高まりと、その後のインフラの撤去により、脅威アクターは5月中旬に活動停止を発表した[73]。

White Apepの2回目のリブランディングは7月下旬、BlackMatterと名付けられた新しいRaaSシステムという形で行われた。この新しいランサムウェアは、全てではないもののコードの一部をDarkSide 2.0と共有しており、これには、権限昇格、被害者のフィンガープリンティング、ネットワーキング機能を実装したコードルーチンが含まれていた[74]。

法的機関からの圧力が強まった結果、White Apepは2021年11月に再びランサムウェアの舞台から去ることを発表した。この決定を受けて、米国司法省は、このグループに関する潜在的情報に対して1,000万USドルの報奨金を支払うことを発表した[75]。2021年末、White Apepの活動は依然として停止状態にある。しかし、White Apepのランサムウェアと全体的な運用が何度も変化していることを考えると、PwCは今回の活動停止について、組織はこのまま潜伏した後リブランディングして再登場する可能性が現実的であると評価している。また、現在PwCがWhite Dev 101として追跡調査しているALPHV-ng（別名：BlackCat）が、さらに別のリブランドであるという状況証拠もある。2021年12月9日、RAMPで脅威アクターのアフィリエイトスキームが開始され、PwCのインシデント対応チームは、以前BlackMatterスキームに属していた特定の関係組織が行った複数のBlackCatインシデントに対応している。

White Ursia

White Ursiaは、2021年上半期に最も活発であったランサムウェアの脅威アクターのひとつである。表に出ている活動としては、「Exploit」では「UNKN、「XSS」では「Unknown」というオンライン名を名乗り、インタビューやREvilのアフィリエイトプログラムの宣伝などを行い、高い知名度を維持した。KaseyaとJBSの攻撃でより厳しい監視対象となった後、White Ursiaへの圧力が高まり、2021年に初のオフラインでの活動を開始した。「UNKN」は、5月に「XSS」と「Exploit」からアフィリエイトプログラムが追放されたことを受けて、すでに休業する決定を発表していた。White Ursiaによる漏洩した被害者データの公開に使われたリークサイト「Happy Blog」は、7月中旬にオフラインとなり、同時に身代金支払用インフラも停止した。7月4日以降、REvilの運営は停止し、「UNKN」は「XSS」や「Exploit」にコメントを投稿しなくなった。REvilの支払用インフラが停止したこと、また、「UNKN」が姿を消したことにより、この脅威アクターの評判は損なわれた。

9月、「Exploit」上では「REvil」「XSS」上では「0_neday」と名乗る新たなペルソナが登場し、「UNKN」の失踪後、バックアップからREvilの操作を復元することができたと発表している。White Ursiaは、9月10日から10月14日の間に6人の被害者のデータを掲載し、その後、再びサイトが停止した（今回はおそらく永久に停止と思われる）。「0_neday」は、脅威アクター個人を標的としたと思われるサイバー攻撃を受けた結果、REvilインフラのコントロールを失ったと主張し、潜伏することを決定していた。2022年1月14日、ロシア連邦保安庁（FSB）は、REvil活動の捜査に関連して、14人の容疑者を拘束し、25の施設を捜索したことを発表した[76]。少なくともその一部が2022年初頭に逮捕されたものの、2022年1月の係る措置に先立って、REvil活動の一部要素がロシア当局によって破壊されていたことは現実的にありうると思われる。「XSS」の複数の犯罪的脅威アクターが、「UNKN」が7月に失踪したことやその後のWeb上での沈黙はFSBの活動によるものと主張しているが、これらの主張を検証することは不可能である。

サプライチェーン侵害：もはや「ニューノーマル」

サプライチェーン攻撃は、これまで長い間、複数の脅威アクターにとって手慣れた手法であった。従来は国家が支援する脅威アクターと関連付けられていたが、金銭的動機による脅威アクターも、こうした攻撃に成功している。2021年初頭、ランサムウェア「CL0P」を用いた脅威アクターWhite Austaras（別名：TA505）は、レガシーファイル転送ソフトウェア「Accellion FTA」を使用していた複数の組織への侵害に成功した。White Austarasは25人弱の被害者からデータを流出させ、身代金を支払わない場合はCL0Pのリークサイトに公開すると脅迫した[77,78]。

2021年7月、White Ursiaは、ネットワークおよびITマネジメントソフトウェアを専門とする米国企業Kaseyaの顧客である複数の組織に対して、同社のVSAソフトウェアを悪用して悪意あるペイロードを送り、侵害した。この攻撃はAccellionの事件よりもはるかに大規模で、1,400もの組織がREvil／Sodinokibiランサムウェアの影響を受けた[79]。

配信とアクセス

配信システム

マルウェア配信システムは、ランサムウェア脅威アクターに不可欠なものであることが証明されている。これは、悪意あるペイロードを格納するために特別に設計されたソフトウェアの一部であり、脅威アクターが標的のシステムやネットワークに最初に侵入するために、ドロップするものである。既存のプレーヤーと新規参入者の両方がランサムウェア分野で活発な活動を見せた2021年、サイバー犯罪の脅威アクターは、マルウェア配信市場において、複数のオプションの中から、自分たちの活動にとって最も安定して信頼性の高いものを選択することができた。

Emotet

PwCがWhite Taranisとして追跡調査しているEmotetは、最も有名かつ長期間稼働しているマルウェア配信システムのひとつである。2021年初頭、国際的法機関により、「Operation LadyBird」と名付けられたEmotetのボットネットインフラがテイクダウンされた。この作戦では、EmotetのC2システムに使用されていた700台以上のデバイスが押収され、ウクライナでは逮捕者も出た[80,81]。これにより、2021年、脅威アクターはかなりの期間、悪質なスパムメールやスピアフィッシングのメールキャンペーンを実施することができなくなった。

しかし、11月中旬、PwCがWhite Magicianとして追跡調査しているグループが運用するバンキング型トロイの木馬Trickbotが、Trickbotに感染した端末に悪意あるEmotetバイナリを配信し、メモリ内で実行しているのが観察された。これは、Emotetのコマンド&コントロールインフラを復元するために、脅威アクターが行ったと思われる。この手法は、2020年10月のTrickbotテイクダウン後に、Trickbotバイナリの配信を支援する手段としてEmotetが使用されたWhite Taranis関連の活動と一致するものである。

Emotetバイナリの配信とそのコマンド&コントロールインフラの復活と並行して、2つの新しいスパム配信ボットネットサーバーEpoch4とEpoch 5が導入された。これにより、White Taranisが以前から感染に使用していたEpoch 1、Epoch 2、Epoch 3という3つのボットネットサーバーに新たな2つが加わったのである。また、ネットワークトラフィックの暗号化に使用されるEmotetの暗号化機能や、通信プロトコルのさらなる更新も確認された[82]。Emotetのシステムにこれらが加わったことで、White Taranisが重要な機能を利用できるようになったこと、また、引き続き組織に脅威を与え得ることが明らかになった。

2021年の大部分の期間、Emotetが使用不能であったため、その顧客ベースのかなりの割合が、他のマルウェア配信システムに目を向けざるを得なくなった。2021年には、Buerloader、Bazar、SquirrelWaffle、IcedIDといったマルウェア配信システムの活動が大幅に増加したが、これは、テイクダウンでEmotetが不在となった隙間をついたものと思われる。

IcedIDよりもコールド

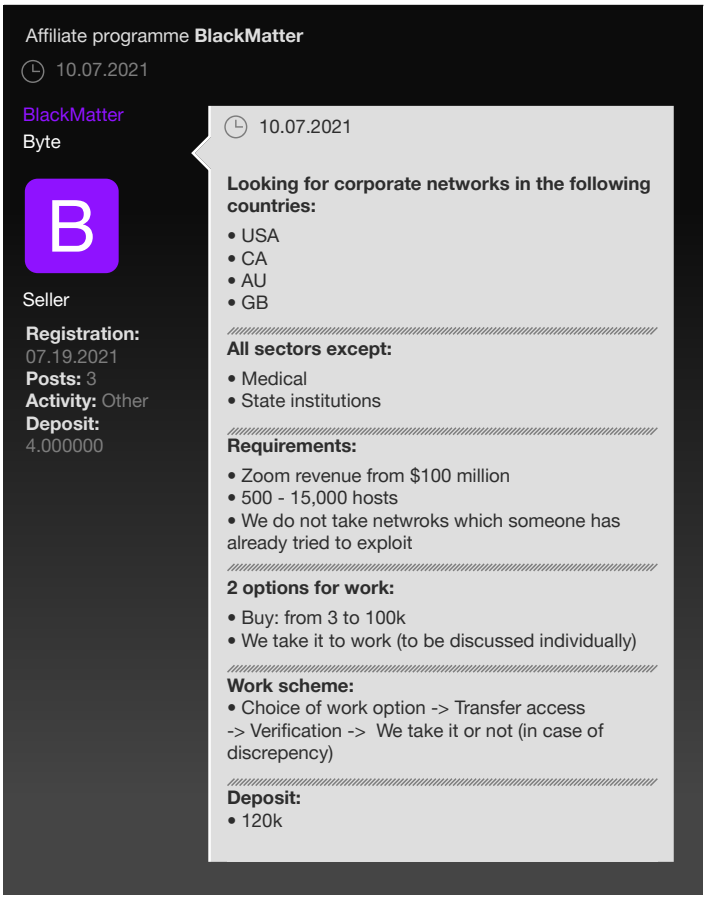
PwCがWhite Khioneとして追跡調査している脅威アクターは、ContiやSodinokibi／Revilなどの有名なランサムウェアシステムに関連するマルウェア配信システムであるIcedID（別名：Bokbot）の背後に存在する。2017年に初めて確認されたIcedIDは、もともと金融情報を窃取することが可能なバンキング型トロイの木馬として開発された。しかし、他のバンキング型トロイの木馬と同様に、IcedIDはその後、ネットワークへのリモートアクセスを提供するために設計されたモジュール型マルウェアとして再利用され、後にAaaSモデルの一部として他のユーザーに販売されることになった83。2021年、IcedIDは、Emotetが不在の中、その能力を高め、最も一貫したマルウェア配信システムのひとつであることを証明した。IcedIDのコア機能は、一貫した電子メールスパムキャンペーンにあり、感染の連鎖を開始するために使用される。IcedIDはさらに、リモートコードの実行やウェブブラウザへのインジェクションなどの機能も備えており、財務情報の抽出を目的とした中間者攻撃を実行することも可能である。ただし、IcedIDは通常、Cobalt Strikeのようなさらに高度なペイロードを展開するために使用されることが多い。

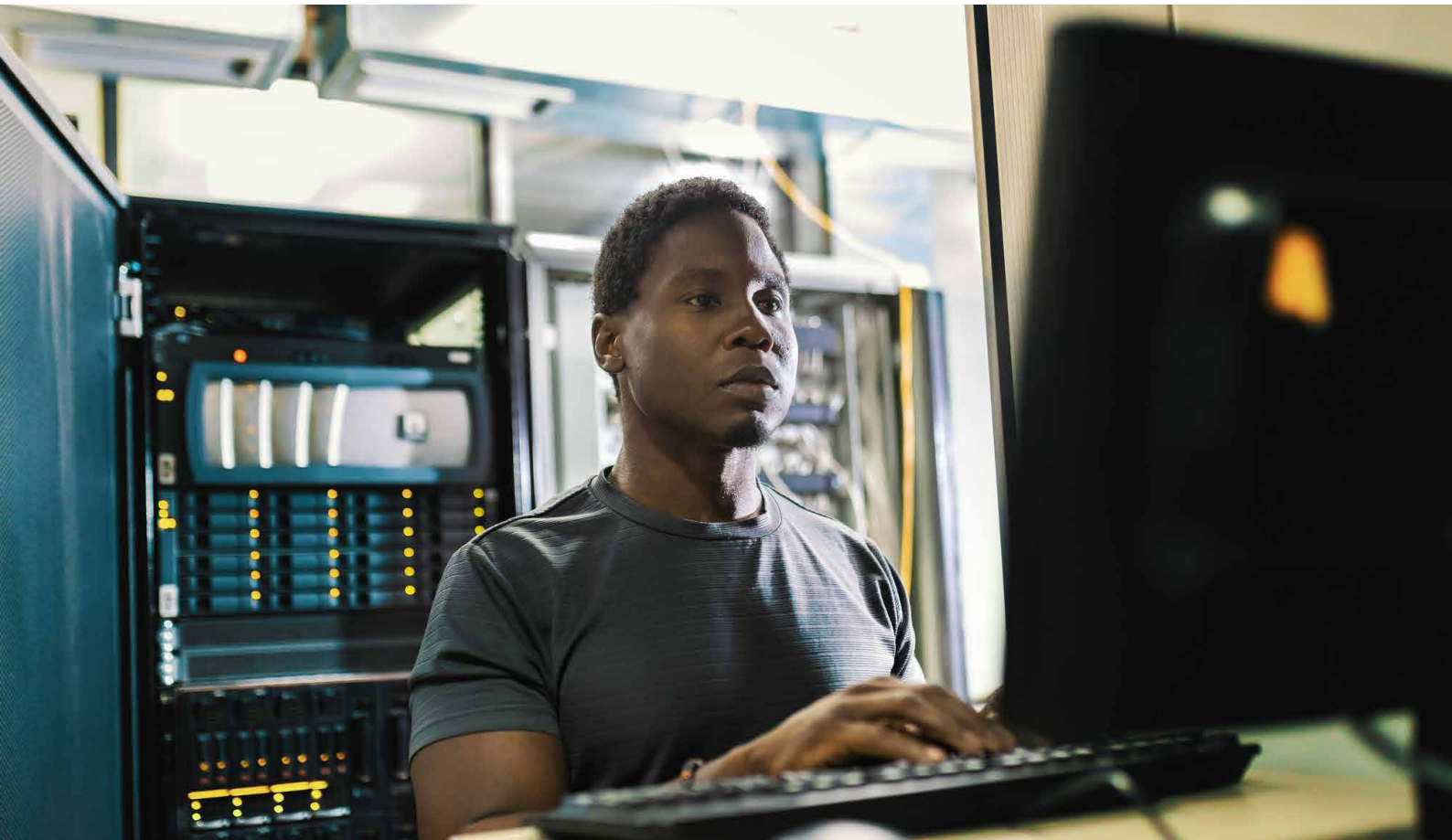
アクセス・アズ・ア・サービス（AaaS）

EmotetやIcedIDのような配信システムは、多くのサイバー犯罪の脅威アクターにとって、常に初期アクセスに選ばれてきた。しかし、その可用性とアクセス性は信頼性に欠けることがあり、一部のシステムは強制的にオフラインにされたり、マルウェア配信サービスにアクセスするために長期間にわたる関係が必要とされる場合もある。こうした理由から、2021年にはアクセス・アズ・ア・サービス（AaaS）取引市場が成長する余地が生まれた。この取引市場では通常、RDPやVPNによるアクセスやWebシェルという形で、さまざまな組織や分野から侵害を受けたホストへのアクセスを売買することが可能である。「Exploit」や「XSS」といったロシア語の各種犯罪フォーラムや、OdinやMagBoといった専用取引市場が、アクセスリストの宣伝に利用されている[84]。

AaaSの普及の最大の要因は、新たな脅威アクターにとって参入障壁が低くなる、という点である。AaaSを活用することで、脅威アクターは認証情報を収集するために複雑な侵入や広範なフィッシングキャンペーンに骨を折る必要性がない。AaaSでは、最初の侵入がすでに完了しているため、購入者はそのまま侵入後の活動やランサムウェアの展開に移行することが可能である。2021年、PwCは、ランサムウェアを多用する脅威アクターまたはその関連組織が、初期アクセス手段としてAaaSを利用しているのを確認した（Janus＜別名：Lockbit2.0＞やWhite Apep＜別名：BlackMatter、DarkSide＞など）。

図表18：「Exploit」フォーラムで企業ネットワークへのアクセスを探る White Apep





地域別活動

このセクションでは、特定の地域に拠点を置き、情報収集活動（政治的・国家戦略目標を支援するもの）から金銭的動機による活動まで、脅威アクターが行った標的型、ばらまき型両方の活動について説明する。2020年と同様に、サイバー脅威の状況は地政学的状況と一致しており、現実世界の事象がスパイ活動や破壊活動を動機とする作戦に同様の影響をもたらし続けていることが確認された。

アジア太平洋

生き残るための困難な道

北朝鮮において、指導者である金正恩氏の政治的信条の中心をなすのは、国家財政を重視した核戦力の継続的開発である。サイバー作戦は、国際的な制裁措置を回避し、戦略的目標を達成するために北朝鮮が取る主要な手段のひとつである可能性が高い。特に暗号通貨は、北朝鮮の政権にとって重要な収入源であり、北朝鮮を拠点とする複数の脅威アクターが、少なくとも2017年以降、暗号通貨、特に暗号通貨取引所に関わる組織や個人を標的としている[85]。

ビットコインは銀、サイバー攻撃は金：北朝鮮を拠点とする新たな脅威アクター

2021年、PwCは、北朝鮮を拠点とする脅威アクターによって行われた可能性が高く、また、国際的な規模で暗号通貨や金融分野を扱う事業者を標的とした2つの主要攻撃グループを観察した。当初、PwCは2つの攻撃グループをBlack Alicanto（別名：Dangerous Password、LeeryTurtle、CryptoMimic、CryptoCore、Operation SnatchCrypto）[86、87]、Black Dev 2（別名：Operation Gold Hunting, Operation SnatchCrypto）として、別々に追跡調査していたが、それらの能力、インフラ、および標的層の重複から、最終的に、Black AlicantoとBlack Dev 2は北朝鮮に拠点を置く同一の脅威アクターである可能性が高いと評価した。さらにPwCは、この脅威アクターについて、Black Artemis（別名：Lazarus Group、HIDDEN COBRA）の金銭的動機によるサブグループBluenoroffの発展型である可能性が非常に高いと見ている。

以下では、Black AlicantoとBlack Dev 2をそれぞれ概説し、2つの攻撃グループに関連する異なるTTPの概要を説明する。

Black Alicanto

Black Alicantoは金銭的な動機の攻撃グループであり、少なくとも2018年以降、金融サービス業界の暗号通貨組織・団体を標的に活動している。この脅威アクターは、しばしば昇進やボーナスに関する内容のおとり文書を使用して標的にペイロードを開かせるように誘導していたが、2021年9月から12月にかけて、Black Alicantoが Goldman Sachs、JP Morgan、Commerz AG、SALT Lending、Blockchain Intelligence Groupなどの金融・暗号通貨分野企業の職務記述書を示すおとり文書を使っていたことも観察された[88]。

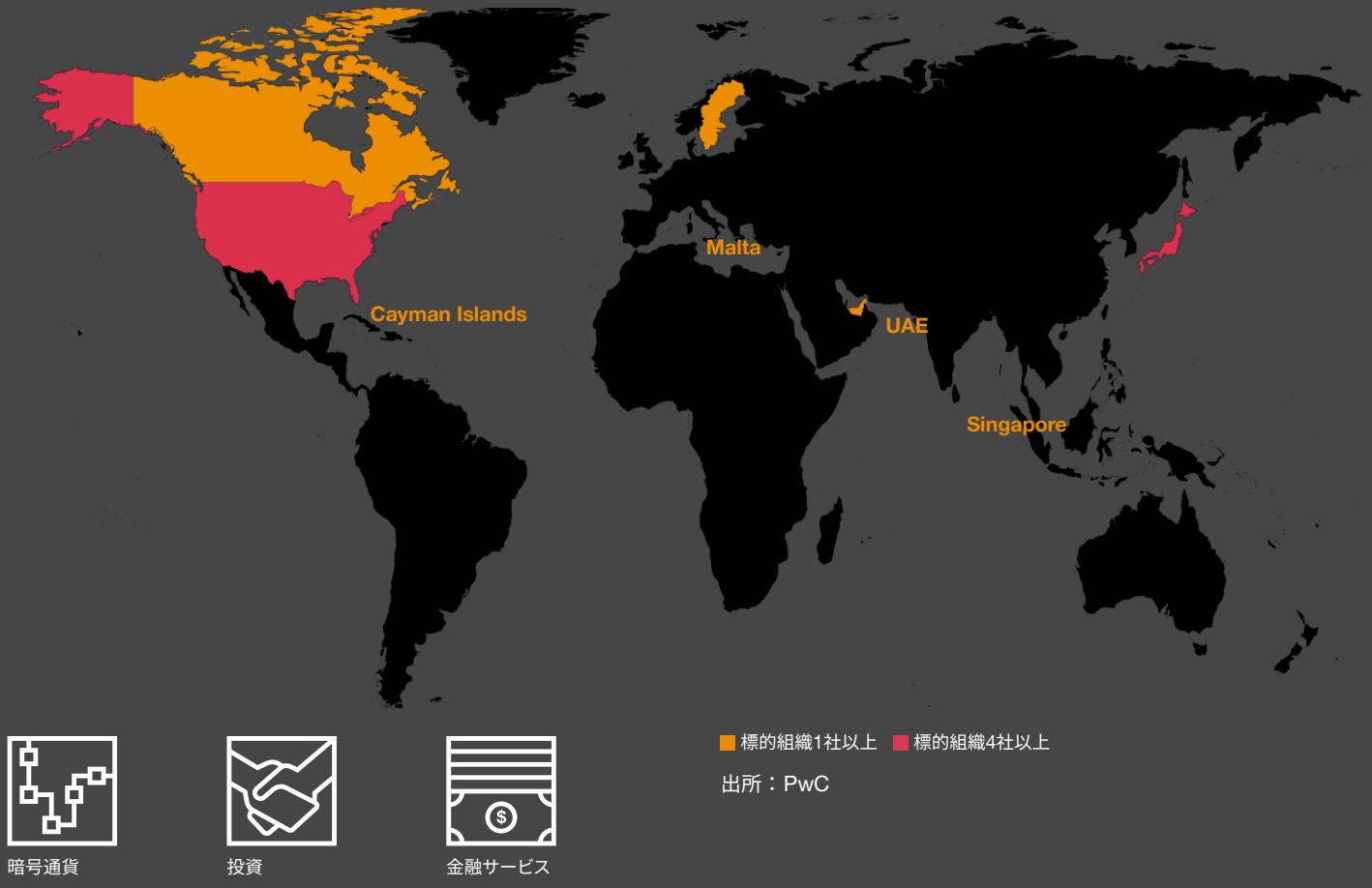
Black Alicantoはまず、アーカイブファイルを添付したスピアフィッシングメールを標的に送信する。これらのメールには通常、2つの拡張子を持つ文書（WordやPDF文書を装った.LNKファイル）や、パスワードで保護されたおとり文書、Password.txt.lnkという不正なLNKファイルなどが含まれている。このリンクファイルは、Bit.lyの短縮URLを悪用して、脅威アクターが登録したドメインから悪意あるスクリプトをダウンロードするよう標的を誘導する。Black Alicantoは、セキュリティリサーチャーではなく、実際の標的のみがペイロードを受け取るよう慎重に確認した上で、ペイロードを手動で展開する。

このようなペイロードのひとつが、Black Alicantoが特に関心のある被害者のシステムに手動で展開するリモートアクセス型トロイの木馬（RAT）msoRAT[89,90]である。。msoRATは、BlueNoroffが長年使用してきたバックドアを進化させたものである[91,92]。

Black Dev 2

少なくとも2020年8月以降、PwCは、当初Black Dev 2[93]と呼んでいた攻撃グループを追跡調査してきた。Black Dev 2は、暗号通貨やフィンテック分野の組織、および暗号通貨やテクノロジー関連のベンチャー企業に出資しているベンチャーキャピタル（VC）を主な標的としている。

図表19：Black Dev 2の標的となった組織の地理的分布



Black Dev 2に関連した侵入では、VCのプレゼンテーションや企業の売り込み、あるいは機密保持契約などの内容のおとり文書が一般的であった。こうしたおとり文書は、脅威アクターが登録したドメインから、悪意あるリモートテンプレートを取得する。リモートテンプレートのマクロは、さらにペイロードをダウンロードし、別の実行中のプロセスに注入する。このペイロードは、通常、バックドアと被害者のプロファイリング機能を備えた悪意あるダイナミックリンクライブラリー（DLL）である。

Black Dev 2が作成した悪意ある文書の作成時刻と最終更新時刻を時系列に並べたところ、午前8時頃から始まり、途中1～2時間の昼食時間をはさんで、午後6時頃まで続く平均的な勤務日のパターンと一致していることがわかった。また、北朝鮮のタイムゾーンであるGMT+9とも一致している。

PwCはまた、Black Dev 2がBlack Alicantoによって使用された他のmsoRATのC2サーバーと重複するインフラで、msoRATの亜種と思われるマルウェアファミリーを使用していることを観察した[94]。Black Dev 2とBlack Alicantoで採用された侵入チェーンおよびインフラ設定の類似性、また被害状況の共通性から、PwCは、Black Dev 2とBlack Alicantoは北朝鮮に拠点を置く同一の脅威アクターであり、Bluenoroffの発展型である可能性が高いと評価した。

補完的ミッション

北朝鮮を拠点とする既存の脅威アクターは、政権への資金供給を継続する必要性に加え、北朝鮮の戦略目標に沿った標的を追求し続けている。

Black Banshee

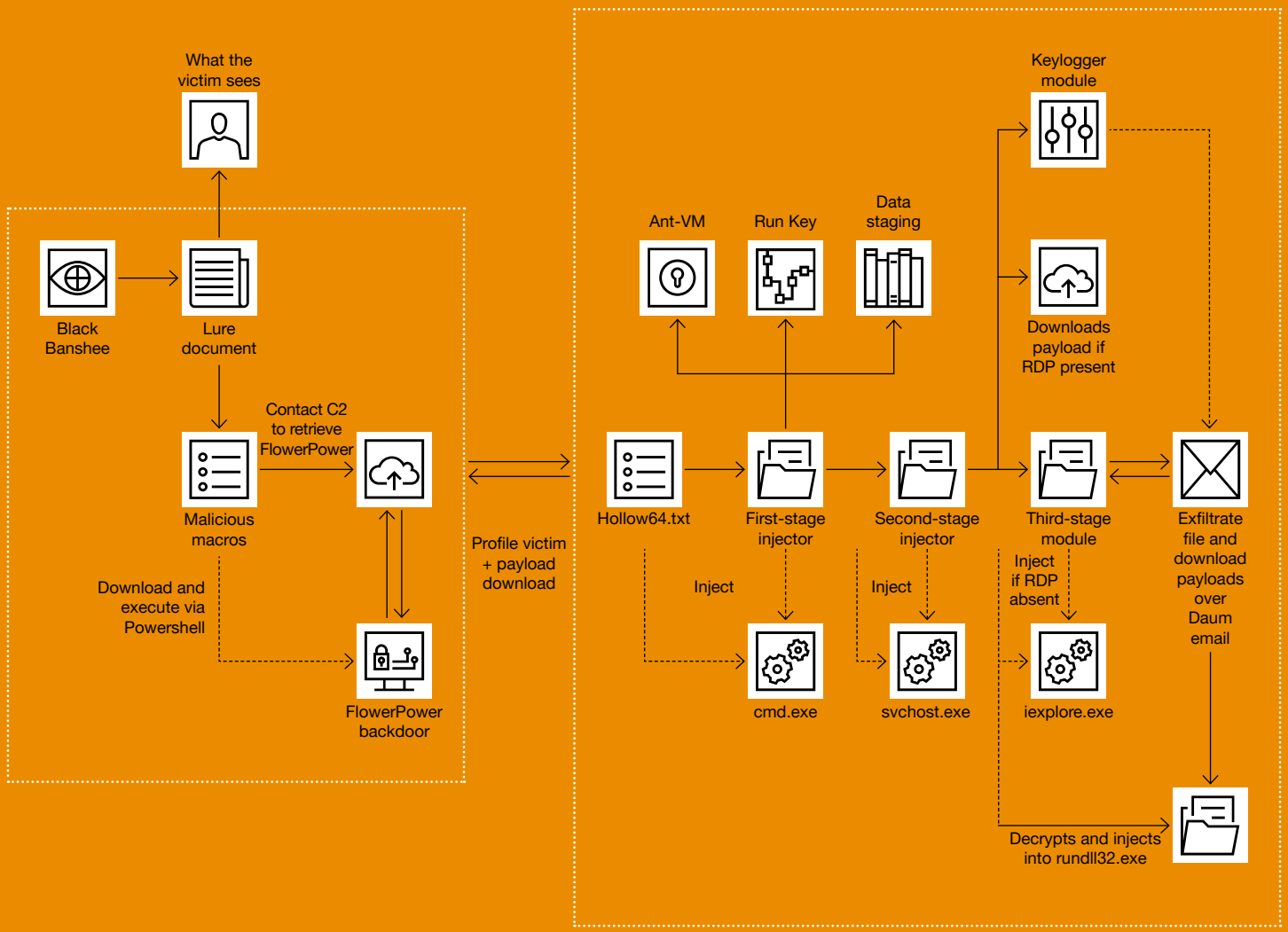
2021年、Black Banshee（別名：Kimsuky、Velvet Chollima）の中心的な関心分野は以下のとおりであり、この脅威アクターのこれまでの標的と一致したものであった。

- 政府・公共機関
- シンクタンクを含む外交・政策系
- 研究学術組織（特に原子力研究と国際政策分野）
- 防衛・航空宇宙
- 核関連
- 北朝鮮に関連して活動するジャーナリストやNGOのような市民社会団体、および宗教団体などの特定の集団

BravePrinceのアップデート

PwCは、2021年、Black Bansheeがこれらの優先的な標的に焦点を合わせつつ、北朝鮮の戦略目標に沿った標的を追求するべくこれまでのツールを刷新していることを確認した。例えば、バックドアであるBravePrinceのアップデート版を開発し、韓国の標的に対して使用した[95]。BravePrinceバックドアは、被害者のプロファイリング、キーロガー、および情報収集機能を備えたツールであり、韓国の電子メールサービス「Daum」を介して被害者のデータを送出する。また、このバックドアは、Black Bansheeが関心を持つ特定のファイルを送出することができるようになっていることから、オペレーターがバックドアを直接操作しているというだけでなく、脅威アクターが関心を持つ特定の標的に絞ってバックドアを展開していることが想定される。このキャンペーンは、韓国の組織・団体に焦点を当て、北朝鮮、中国、ロシア、そして米国との関係における韓国のスタンスについて、外交、政治、軍事的情報を得ることを目的としていたと考えられる。また、2021年11月[96]に発表されたこのキャンペーンに関する最新情報では、航空燃料など特定分野の科学研究に加えて、航空宇宙・防衛材料などを標的としていることが詳述されている。

図表20：BravePrinceバックドアを含むBlack Bansheeの侵入チェーンのステップ



BabySharkに向けた核政策

Black Bansheeはまた、2021年[97]の大半においてBabySharkキャンペーンを継続し、これまで同様、核、政策、外交関連のトピックに焦点を当てた。PwCは、2021年8月以降にBlack Bansheeが侵害した少なくとも8人の被害者を特定し、通知を行っている。この中には、外交官、アジア太平洋地域に焦点を当てたシンクタンクの現職・元上級アナリスト、アジア太平洋の歴史、政策、防衛に焦点を当てた上級リサーチャー、そして朝鮮半島に焦点を当てたNGO職員が含まれている。これらの標的層は国連を含む超国家的組織で働く個人を標的にし始めた脅威のアクターを、PwCが初めて観察した時期である少なくとも2018年後半以降の、Black Bansheeによるキャンペーンとも一致している。

Black Artemis

Black Artemis（別名：HIDDEN COBRA、Lazarus Group）は、PwCがShowStateとして追跡調査中のキャンペーンの一環として、航空宇宙・防衛業界を重点的に標的にしていた[98]。このキャンペーンは2021年まで続き、航空宇宙・防衛の求人情報を偽ったソーシャルエンジニアリングの手法を用いたスピアフィッシング文書を用いて、エンジニアリング・製造系企業に拡大した[99]。

2021年にBlack Artemisが行った韓国の組織を狙った別のキャンペーンでも、初期アクセスにマクロを仕込んだ悪意ある文書が使用されていた。しかし、この一連の侵入では、マクロは、アンチウイルスソフトウェアによる静的検出を困難にするために、悪意あるデータを含むPNG画像の圧縮ファイルをディスクにドロップしていた。その後、マクロはこのPNG画像をBMPファイルに変換し、mshta.exeを介して実行する。埋め込まれた実行可能ファイルのペイロードは、PwCがPaintJob[100]と呼ぶマルウェアファミリーで、その暗号化ルーチンは、Black Artemisのサブグループ Andarielに属する有名なRAT、Dtrackのものと類似している。

Black Artemisは、この一年間、オフェンシブセキュリティのリサーチャーや脆弱性リサーチャーも執拗に標的にしていた。2021年1月、Google[101]とMicrosoft[102]は、セキュリティリサーチャーを装ったTwitterのプロフィールや、LinkedIn、Telegram、Discord、Keybaseのアカウントを用いた、数カ月に及ぶソーシャルエンジニアリングキャンペーンを報告した。Black Artemisは、脆弱性調査プロジェクトに協力すると偽って標的に接触する。そして、Comebackerドロッパーを実行する悪質なコードを埋め込んだVisual Studioのプロジェクトファイルを送りつけ、最終的にKlackringバックドアのインストールに誘導するという手口をとっている。

この脅威アクターは、水飲み場型攻撃をかけるセキュリティブログを運営しており、標的となるセキュリティリサーチャーとの会話の中で、このブログへ誘導するケースもあった。標的がこのサイトを訪問すると、Chromeのゼロデイ脆弱性を悪用する攻撃により、悪意あるサービスがインメモリバックドアとともに端末にインストールされる。これにより、Black Artemisは、セキュリティリサーチャーのシステムへのアクセスを取得および悪用し、関心のあるオフェンシブセキュリティの研究を特定し、窃取することが可能となる。

Black Artemisは、中国語で書かれた悪意ある誘い文句で、中国のオフェンシブセキュリティのリサーチャーを標的にした活動を並行して行っている[103]。セキュリティリサーチャーを狙った不正行為には、サイバーセキュリティの研究、特に脆弱性解析とエクスプロイト開発に用いられている逆アセンブルソフトウェアであるIDA Pro[104]のトロイの木馬化バージョンも含まれている。

中国を拠点とする脅威アクターの活動

事前計画

中国を拠点とする脅威アクターの活動は、引き続き顕著に観察されている。これらの脅威アクターの中には、Red Djinnのように、半導体、AI、ヘルスケア（遺伝子研究やバイオテクノロジーを含む）、量子コンピューティング、宇宙・海洋・極地探査といった特定の産業分野に着目している組織もある[105]。また、Red Kelpieのように、非常に広範な標的を狙ったり、場合によっては、他組織による実行を支援したりするケースもある。

経済的な戦略目標だけでなく、公共部門を標的としたスパイ活動も引き続き確認されており、「Red Vulture（別名：Ke3chang、APT15、APT25、NICKEL）」や「Red Keres（別名：APT31、ZIRCONIUM）」は、こうした標的を狙うグループの主要な例として挙げられる。

Red Djinn

Red Djinn（別名：BlackTech、Mobwork、Palmerworm）としてPwCが追跡調査している中国を拠点とする脅威アクターは2021年も活動を続け、既知のツール（PLEADやTSCookieなど）と新たなツール（Consock、FlagPro、SpiderRATなど）を使用している。

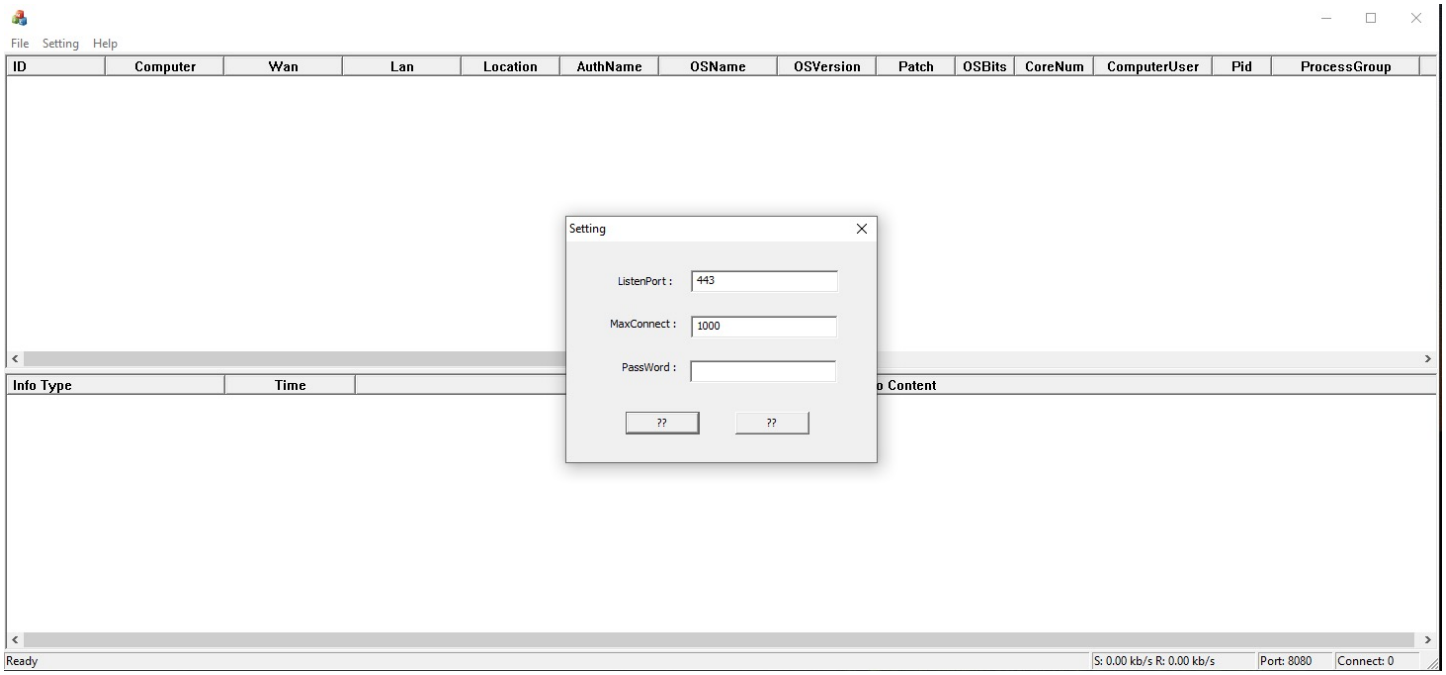
2021年初頭には、PLEADおよびTSCookieと呼ばれるマルウェアファミリーを使用した一連のRed Djinnのキャンペーンが観察された。これらのキャンペーンは、アジアの一部を拠点とする組織を標的としており、IT・通信企業も含まれていた。脅威アクターは、クラウドやVPNサービスに偽装したドメインを登録しており、使用するマルウェアファミリーには、製造・エンジニアリング分野を標的にしていることを示すと思われるキャンペーンIDも含まれていた。

New Djinn

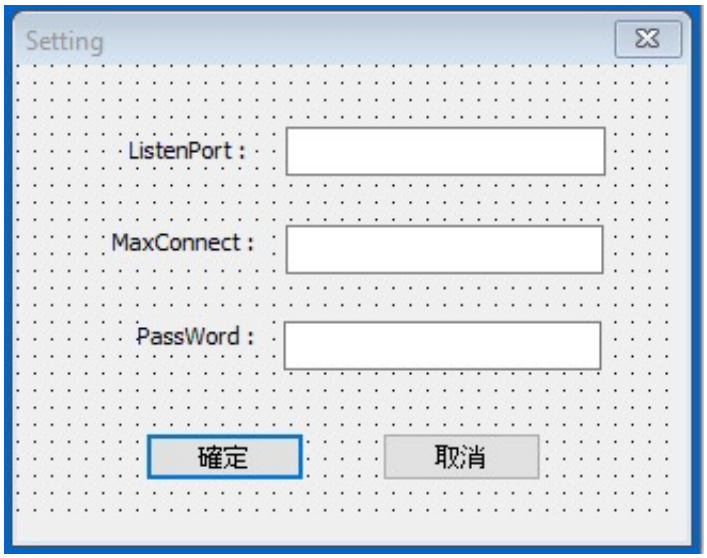
Red Djinnは、歴史的に一貫してアジア地域の経済大国を標的としてきたが、以前には、この脅威アクターによるより広範な標的も確認されている。例えば、Red Djinnは以前、マネージドサービスプロバイダー（MSP）の海外子会社を標的にして、MSPのメインネットワークでラテラルムーブメントを行う「アイランドホッピング」攻撃を実行した。

Red Djinn（別名：Gh0stTimes）に関連する、Gh0stRATをカスタムした亜種Consock[106,107]の追跡調査を通じて、PwCはこのマルウェアの管理システムを特定することができた。

図表21：Red DjinnのマルウェアConsockの管理システムであるTimes.exe



図表22：Times.exeはもともと中国語システム用に設計された



また、脅威アクターがConsockおよび、PwCがFlagproと名付けた新たなマルウェアの両方を送り込むために使用したスピアフィッシングの手口も確認されている[108]。PwCは、Red Djinnが東アジアと南アジアで事業を展開する日本のITサービスプロバイダーおよびソフトウェア開発企業の子会社を標的とする際にFlagproを使用した可能性が非常に高いと評価している。

このキャンペーンを分析したところ、Red Djinnが使用している可能性が高いと評価される一連の攻撃スクリプトが確認された。メタデータによると、攻撃スクリプトの一部は、Seebugなどの一般公開されている脆弱性データベースから取得または転用されたものである可能性が高いことが判明した。これらのフォルダーには、Red Djinnが国際的な規模で脆弱なシステムの偵察を行っていたことを示唆するデータも含まれていた。さらに、CitrixやMikrotik製の機器に対する攻撃コードも確認されたが、それらはまだ開発中のものと思われる109。また、2021年3月のProxyLogonを悪用する脆弱性攻撃や、PwCがSpiderRATと呼ぶ新しいバックドアを展開するRed Djinnの活動も確認された[110,111]。

Red Vulture

Red Vultureは、2021年を通じて活動のペースを高めた。PwCは、Red Vultureが2021年を通じて、以下の分野のさまざまな組織に対して定期的に偵察を行うのを観察した。

- 政府
- 航空宇宙・防衛
- 教育
- NGO

こうした偵察は、主に脅威アクターが、標的組織のWebサイトおよびVPNや電子メールのようなネットワークの境界に位置するサービスを探索することで行われた。脅威アクターがインターネットに面したインフラの脆弱性を大量にスキャンしているという証拠もある[112]。2021年、Red Vultureが標的組織への攻撃に成功したのは、多くの場合、ネットワークの境界に位置する認証システム（VPNなど）に対する攻撃を多用したためである。

観察された偵察活動は、外務省（MFA）を標的としたものが中心で、一貫して欧州と南米に焦点が当てられていた[113,114,115]。

Red Keres

2021年初頭、ドイツ連邦憲法保護局（BfV）は、Red Keresが欧州各地の「省庁や当局、政治団体、財団」を含む機関を標的にしている、と報告した[116]。

BfVが開示したRed Keresのインフラを分析したところ、少なくとも2020年12月から2021年2月にかけて、この脅威アクターが東南アジア諸国政府の外務省のメールサーバーに侵入し、直接アクセスしていた可能性を示唆する証拠も確認された[117]。同じ頃、別の東南アジアの国の国防省のメールサーバーでも同様の活動が確認された。

2021年末、フランスの国立情報セキュリティ機関（ANSSI）は、Red KeresのTTPに関する詳細なレポートを発表した。このレポートでは、1000台を超えるスモールオフィス／ホームオフィス（SOHO）ルーターを含む、この脅威アクターの多層的な匿名化のためのインフラの設定について詳述されている。PwCは、2021年を通して、中国を拠点とするその他複数の脅威アクターがSOHOルーターを使用していることを観測している。また、Red Keresが被害者への初期アクセスを試みる際に展開するさまざまなテクニックも取り上げており、スピアフィッシングから総当たり攻撃、有効な認証情報の悪用、ProxyLogonやVPN製品に対する脆弱性攻撃など、そのテクニックは多岐にわたっている。

Red Kelpie

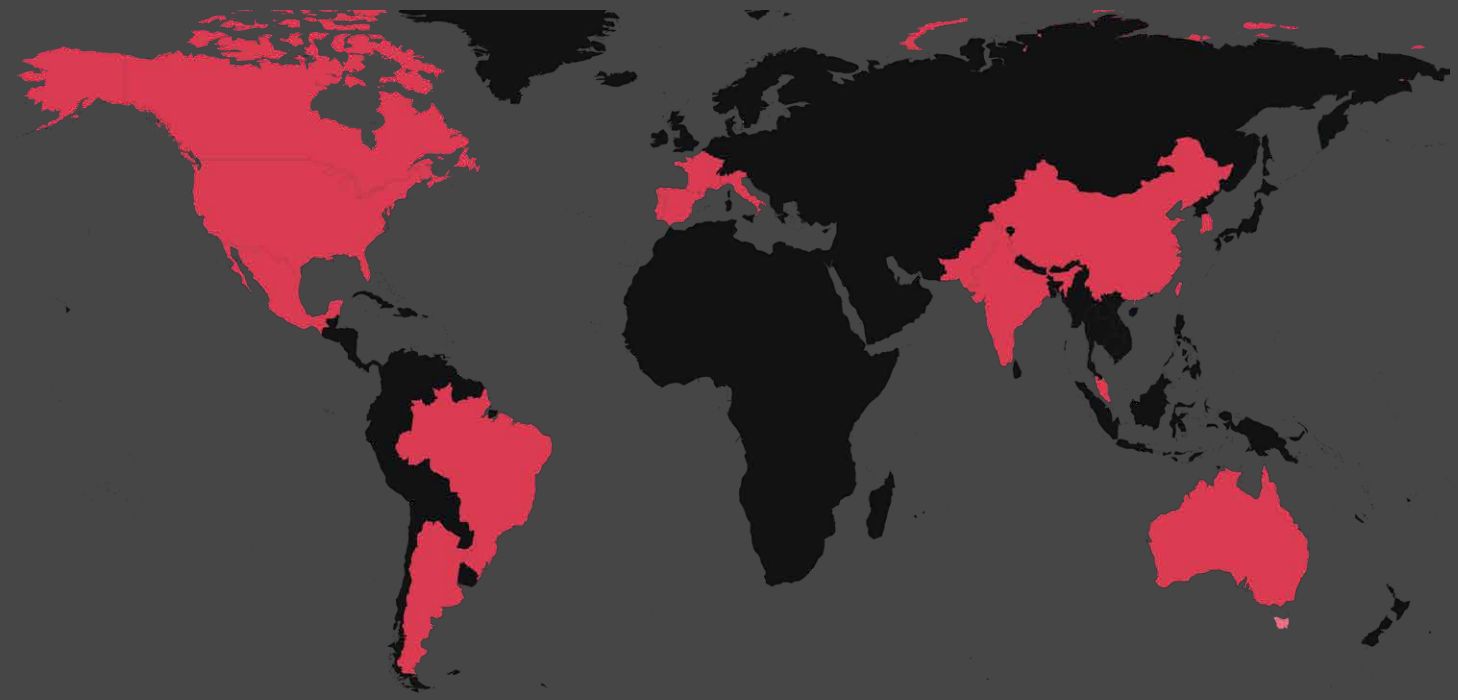
PwCがRed Kelpie（APT41やBARIUMと重複）と呼んでいる脅威アクターは、ShadowPadやCROSSWALK、Cobalt Strikeなどの汎用ツールなど、さまざまなマルウェアファミリーを利用している。その標的は多岐にわたり、複数の戦略的に重要な業界が含まれる。

ChaChaLoader

2021年、Red Kelpieは、この脅威アクターが使用する有名なローダーMotnugと、その進化版と思われるChaChaLoaderと呼ばれるローダーを用いた一連のキャンペーンを行った。MotnugとChaChaLoaderは、主にCobalt Strikeのロードに使用されたが、SIDEWALKと呼ばれるCROSSWALKを進化させたと思われる、新たに観察されたバックドアをロードするケースもわずかに存在した[118]。CobaltStrikeの代わりにSIDEWALKが導入された数少ないケースは、より高価値の標的であったと予想される。

これらのキャンペーンは、金融、小売、通信、製造、航空など、さまざまな業界を標的としている。

図表23：2021年のRed Kelpieの標的



金融サービス　小売　通信　製造業　航空

出所：PwC

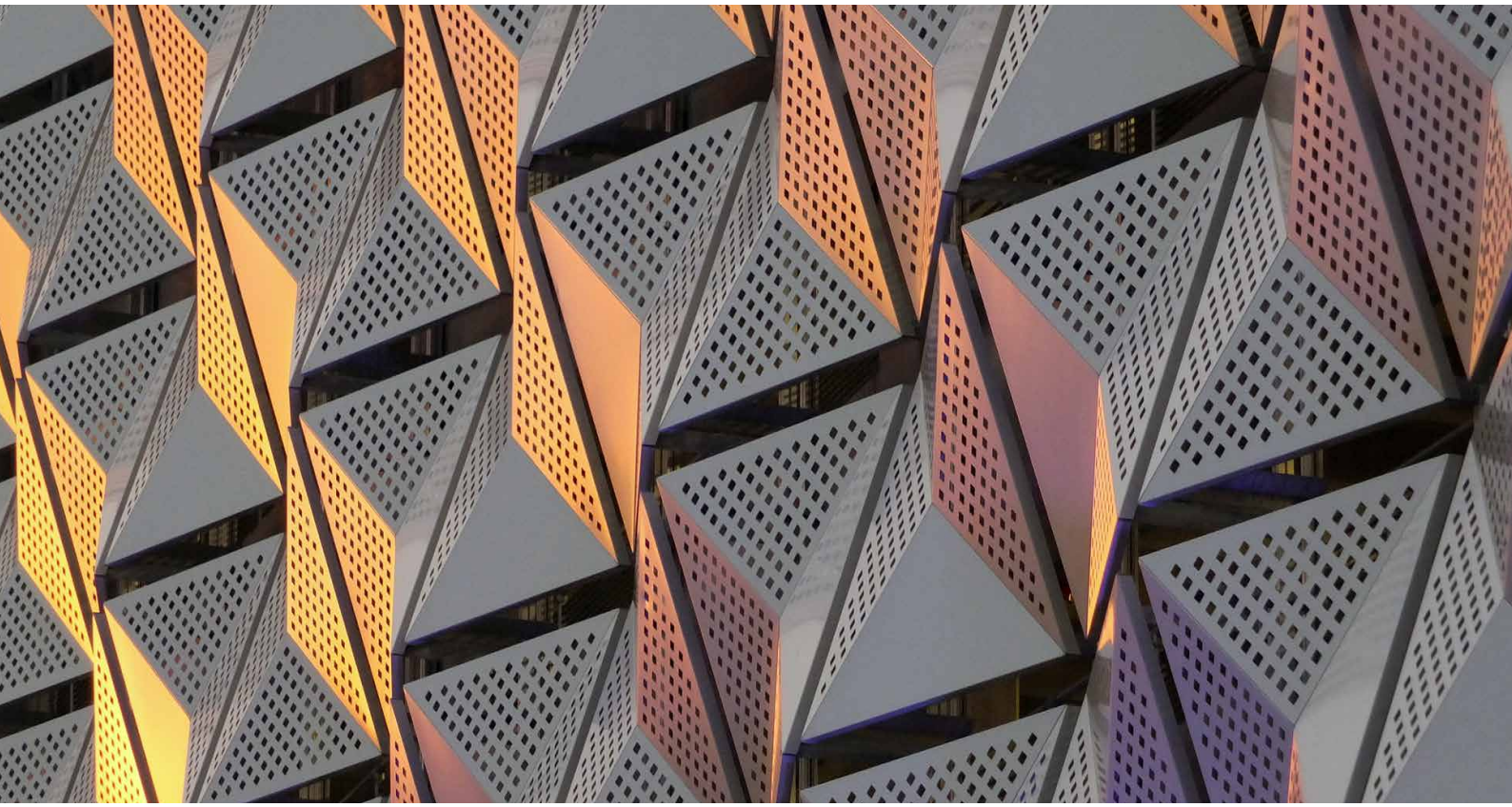
Confluenceの脆弱性

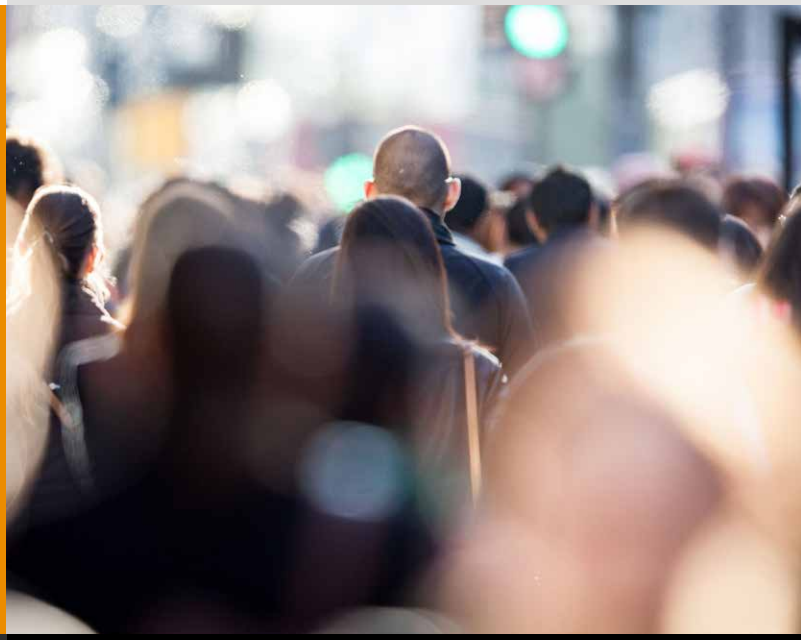
過去数年間、Red Kelpieはインターネットに面したインフラの脆弱性を大規模に攻撃して初期アクセスを獲得しているが、この戦術は2021年にも指摘されている。特に、Atlassian のサービスであるConfluenceのコード実行の脆弱性CVE-2021-26084を攻撃して、Cobalt Strikeをロードして実行するためのバッチスクリプトとDLLをドロップするRed Kelpieが観察された[119]。Red Kelpieは、以前にもCitrix／Cisco ソフトウェアの脆弱性に攻撃をかけて、非常によく似たバッチスクリプト（Cobalt Strike をロードして実行することも知られている）を展開していたことも観察されている[120]。

起訴されたにもかかわらず活動継続

2020年9月、米国司法省は、アジアを拠点とする7名の人物をコンピュータへの侵入行為を行ったとして起訴した。また、彼らが所属するグループは公開情報でAPT41、BARIUM、Winntiなどと称されているものである、としている[121]。

この起訴にもかかわらず、Red Kelpieの活動は2021年を通して継続した。おそらく、起訴によってRed Kelpieにとってより大きな代償となったのは、脅威アクターが利用していたアカウント、サーバー、ドメインの押収であり、それによって活動ペースの変更を余儀なくされたことであろう。PwCは、2020年後半から2021年にかけて、この脅威アクターが使用する新しいインフラを追跡調査したが、APT41／BARIUMのものとされる古い関連インフラとの重複が依然として観察されている。このキャンペーンの背後にいる複数のオペレーターが起訴されたことは、この脅威アクターの活動全体には、大きな影響を及ぼしていないものと思われる。





インシデント対応ケーススタディ：

Red Dev 14の「FUNRUN」

PwCは、中国を拠点とする脅威アクターによるシンクタンクへの侵入に対応し、これをRed Dev14.[122]によるものと特定した。ProxyLogonのエクスプロイトを利用して、脅威アクターはオンプレミスのExchangeサーバーにWebシェルをドロップした。当初、脅威アクターはWebシェルを通じて偵察（主にユーザー名や実行中のプロセスなどのシステム情報を収集）を試み、LSASSのメモリをダンプするコマンドを実行し、環境寄生型（living-off-the-land）のシステム上の正規の実行可能ファイル経由で認証情報を取得した。続いて脅威アクターはFUNRUNと呼ばれるバックドアの亜種を利用し、ProcDumpをドロップしてLSASSのメモリをダンプし、さらにMimikatzをディスクにドロップした。

こうして認証情報の取得に成功した脅威アクターは、SMBリモート共有を介してネットワーク内でラテラルムーブメントを行い、FUNRUNバックドアをネットワーク上の他のホストにインストールした。また、この脅威アクターは、Exchangeサーバー上の他のWebシェルを検索するコマンドを実行した。これは、Exchangeサーバーがすでに侵害されているかどうかをテストするために（おそらくProxyLogonによって）行ったものと思われる。これによって、別の脅威アクターがシステム上に存在する場合、Red Dev 14に通知される。存在した場合、目標を達成する方法に影響を与える可能性がある。

この「FUNRUN」バックドアは、PwCが「Red Pegasus」（別名：APT9）と呼んでいる、中国に拠点を置く脅威アクターによって使用されていることが確認されている[123]。しかし、Red Pegasusが最後にこのバックドアを使用しているのが観察された時期（2014年と2015年の間）から、PwCが観察した2021年のFUNRUNの活動までは、かなりの時間が経過している。こうした考察および、このバックドアはRed Pegasusとはロードの仕組みが異なること、Red Pegasusとインフラの重複がないことを踏まえ、PwCはこの活動をRed Dev 14という新しい名称の脅威アクターによるものとして追跡することを決定した。

Red Dev 14は、このキャンペーンの一環として、主に農業で複数地域の標的を攻撃した。

よろしければご連絡を……
電気通信業界を狙う中国拠点の脅威アクター

中国を拠点とする複数の脅威アクターが、引き続き電気通信業界を標的としている。同業界の組織は、顧客関連データ（プロバイダーによっては、Webサイトへの接続に関するメタデータや通話記録など）を含む、さまざまな価値の高い情報を保有している。このような情報は、脅威アクターがサーベイランス目的で利用するため、あるいは特定の標的の活動に関する既存の情報を収集するために利用することができる。

例えば、上述のとおり、Red Kelpieが引き続き電気通信業界を標的としていることが確認されている[124]ことに加えて、脅威アクターの間で共有されているツールShadowPadが通信プロバイダーを攻撃するために使用されていることも確認されている[125]。PwCが東南アジアの電気通信事業者のインシデント対応調査を支援した際、中国を拠点とする脅威アクターRed Salamander（別名：LotusBlossom）が使用するEvoraバックドアの亜種が確認された[126]。

インドを拠点とする脅威アクター：
変わらぬTTPと細部の変化

PwCがインドを拠点とする脅威アクターの活動を調査した結果、インドと戦略的に関係のある国、特に国境を接する中国とパキスタンに焦点が当てられていることがわかった。PwCが追跡調査している、インドを拠点として諜報活動を行う脅威アクターのほとんどが、標的とする国の政策や政治に関する文書、あるいは軍事や防衛に関するトピックのおとり文書を使用していることが確認されている。

Orange Kala（Donot）

Orange Kala（別名：Donot）は、2021年も前年同様の活動ペースと標的を維持し、TTPにはほとんど差異がなかった。少なくともひとつのケースでは、この脅威アクターはミサイル技術に関連するおとり文書を使用した[127]。このおとり文書のトピックは、少なくとも2020年11月以降において、他の複数のおとり文書の内容がミサイル防衛技術に大きく焦点を当てたニュース記事や雑誌記事から取られていたため、Orange Kalaにとって新しいものではなかった。しかし、このトピックに関するこれまでのおとり文書のほとんどが米国に関するものであったのに対し、今回のキャンペーンは、Orange Kalaがアジア太平洋地域のミサイル技術に焦点を当てていることをPwCが確認した最初の事例であった。このキャンペーンと年間を通じて、Orange Kala はマルウェア・アズ・ア・サービス（MaaS）ツール「WarzoneRAT」を多用していた。あるキャンペーンにおいて、この脅威アクターは悪意あるDLLを通じてWarzoneRATを展開し、最終的にバッチスクリプトのハードコードされた一連の長いコマンドラインコマンドをデコードして実行した[132]。このキャンペーンに関連してUAEのオンラインマルチウイルススキャナにアップロードされたおとり文書の中には、イラン海軍の新型艦船をテーマにしたものや、パキスタンが実施する多国籍海軍演習をテーマにしたものがあり、脅威アクターが軍事テーマに興味を持っている可能性が伺える。

ケーススタディ：
通信事業者を標的にしたRed Menshen

2021年を通じて、PwCはRed Menshen[128]と呼ぶ、中国を拠点とする脅威アクターによる複数の侵入を追跡調査し、対応した。この脅威アクターは、BPFDoorと呼ばれるカスタムバックドアを使用して、中東およびアジア地域の通信事業者、さらに政府組織、教育業界、ロジスティクス業界を標的としていることが確認されている。このバックドアは、TCP、UDP、ICMPなど、C2サーバーと通信するための複数のプロトコルをサポートしており、脅威アクターはバックドアとやり取りするためのさまざまなメカニズムを利用することができる。

PwCの調査によると、この脅威アクターは、侵入後の段階でさまざまなツールを使用している。これには、共有ツールMangzamelのカスタム亜種（Golang亜種を含む）、Gh0st のカスタム亜種、およびWindowsシステム全体へのラテラルムーブメントを支援するMimikatzやMetasploitなどのオープンソースツールが含まれる[129,130]。またPwCは、脅威アクターが有名なプロバイダーにホストされている仮想プライベートサーバー（VPS）を介して BPFDoorの被害者にコマンドを送信していること、またこれらのVPSが、脅威アクターがVPNトンネルとして使用している台湾にあるルーターを介して管理されていることを特定した。

PwCが観察したRed Menshenの活動のほとんどは、月曜日から金曜日の間に行われ（週末には観察されなかった）、大部分の通信はUTC01:00から10:00の間に行われた[131]。このパターンから、Red Menshenは常に8〜9時間の活動時間帯に活動していることが示唆され、これは現地の就業時間と一致していると考えられる。

共通するTTP

この一年間で、Orange Kalaと他のインドに拠点を置く脅威アクターの間で共通のTTPが複数確認された。この点について、PwCも調査を進めているが、こうした状況は、従来考えられていたよりもインドに拠点を置く脅威アクター間の相互関係が強いことを示している可能性がある。2021年2月、PwCは、2020年のOrange KalaとOrange Dev 1（別名：CONFUCIUS）の両方の活動へのリンクを持つ、悪意あるRTFファイルテンプレートを含むキャンペーン[133]を追跡調査した[134]。また、Operation Shaheen[135]として知られる、2017年のパキスタンを標的としたキャンペーンとのリンクも確認した。2021年のキャンペーンは、軍事および防衛をテーマとするものであった。おとり文書として防衛関連の提案に言及するものが確認されており、ひとつの事例はタイ王国海軍に対するものであった。Orange KalaとOrange Dev 1は、過去に防衛業界や政府を標的にしていたことが判明している。2021年の活動では、2020年[136]に報告された同様の活動とは異なる手法が用いられており、攻撃チェーンに新たなレイヤーが追加されていた。この新たなレイヤーは、最初のRTFファイルが被害者の端末に2つ目のRTFファイルをダウンロードし、悪意あるDLLのダウンローダーとして使用するというものであった。

2021年6月、Orange Athos（別名：Patchwork）によるキャンペーンにおいて、2019年の時点でOrange Kalaが使用していることが確認されたVBAスクリプトが用いられているケースが観察された[137]。このVBAマクロは、2019年と2021年の活動において、固有の変数名まで驚くほど類似していた。これは、マクロビルダーで作成されたものではなく、ある脅威アクターが作成した特注のマクロを再利用している可能性が高い。この悪意ある文書は、電子書籍・オーディオブック購読サービスScribd.comから取得したあるパキスタン人の経歴をモデルにしているが、脅威アクターは、当該人物の父親がかつて、パキスタンの国家宇宙機関である宇宙・高層大気研究委員会（SUPARCO）で働いていたと元のテキストを改変している。この文書は、Orange Athosの定番であるBADNEWSバックドアを被害者に配送するために使用された。また、今年前半に公開されたのレポート[138,139]は、SUPARCOをテーマとした悪意あるおとり文書についてさらに詳細な議論を行っている。これらのおとり文書は標的にWarzoneRATを配信するものであり、インドに拠点を置く脅威アクターOrange Dev 1にアトリビューションされる。

これらのキャンペーンでは、インドを拠点とする脅威アクターの間で、少なくとも複数のツールの共有や、単純なツールの相互利用が行われている。しかし、このような現象は、初期アクセスレベルでしか確認されておらず、インドに拠点を置く脅威アクターは、後段のバックドアの選択については依然として大きく異なる手法をとっている点に注意が必要である。

Orange Athos（別名：Patchwork）

Orange Athos（別名：Patchwork）は、2021年のさまざまなキャンペーンを通じて、BADNEWSバックドア（BozokRATとしても知られる）を多用し続けており、2016年時点で、公開情報で最初に報告されてからマルウェアのコードベースに加えられた変更はわずかである[140]。

脅威アクターは、中国とパキスタンの標的に引き続き焦点を合わせていた[141]。2021年4月に観察されたキャンペーンでは、脅威アクターは、中国とパキスタンの軍事協力に関連するおとり文書を使用した[142]。この文書は、Encapsulated Postscript（EPS）形式の画像に関連するUse-After-Free（UAF）脆弱性CVE-2017-0261を攻撃する悪意あるDOCXファイルであった。このテクニックは、この脅威アクターが中国を拠点とする複数の組織を標的にした2020年の複数のキャンペーンにおいて一貫して多用してきたTTPと非常に類似している。

侵入のひとつ[143]は、パキスタン連邦政府歳入庁の書式を装い、パキスタン連邦政府省庁の職員に対して、特別な税制優遇措置を受領する資格取得のために個人情報を入力させるというものであった。標的がRTFファイルを開くと、上記と同じ脆弱性（CVE-2017-0261）により、BADNEWSバックドアがインストールされる。特定の脆弱性を攻撃し続け、すでに公開情報として報告されているツールを使用していることから、Orange Athosもまた、有効性が実証されたTTPを用いて執拗な攻撃を続ける脅威アクターであると思われる。

Orange Yali（BITTER）

2021年を通じて、パキスタンの正規企業を装った複数のWebサイトを確認したが、これらは2020年以降、インドを拠点とする脅威アクターであるOrange Yali（別名：BITTER）によって開設・維持されていた可能性が高いと考えられる。これらのWebサイトは、通常、コンテンツやプレースホルダーテキストがほとんどなく、MSIインストーラとしてパッケージされたrkftlバックドアのペイロードや、SSHおよびTelnetクライアントPuTTYなどのユーティリティツールをステージングするために使用されている。また、Orange YaliはArtraDownloaderとして知られるマルウェアファミリーの使用を続けており、特に中国企業を標的としたキャンペーンにおいて[144,145] Compiled HTML（CHM）ファイルの使用を誘導していた。また、複数の報告によると、Orange Yaliは2021年を通じて少なくとも2種類のゼロデイエクスプロイト[146,147]を使用しており、これらはいずれも脅威アクターが自ら開発したものではなく、エクスプロイトブローカーから入手した可能性が極めて高いことがわかっている[148]。このことは、インドを拠点として諜報活動を行う少なくともひとつの脅威アクターが、非公開のゼロデイエクスプロイトを購入するためのリソースも有していることを示しており、この地域で活動する脅威アクターからはこれまで観察されなかった現象である。

主目的の諜報に加え金銭目的の活動も：パキスタンを拠点とする脅威アクターの活動

2021年を通じて、Green Havildar（別名：APT36、Transparent Tribe、Gorgon Group）は、この脅威アクターの主な目的と思われるインテリジェンス収集に沿って、特にインドの軍部、政府、公共部門を標的に含む活動を継続してきた。この脅威アクターは、初期アクセスに基本的なスピアフィッシングを利用し、個人の履歴書から会議プログラム、軍事・防衛関連のサンプルなど、さまざまなおとり文書を用いていた[149]。

Green Havildarは、CrimsonRATを使用したことで知られているが、このRATは攻撃ごとに設定を調整してビルドするモデルによって運用を続けていた。つまりこのRATは、幅広いサーベイランスおよびデータ窃取能力、一貫したコード難読化モデル、そしてC2活動が行われるポートを柔軟に変更する能力を備えている。2021年4月から7月にかけて、セキュリティ企業Team Cymruは、Green HavildarのC2インフラ設定を暴露するレポートを公開しており、これには、脅威アクターがRDP上でその設定をコントロール可能であることが記されている[150,151]。

2021年には、金銭的動機に基づくサイバー犯罪を主目的としてGreen Havildarを運用する活動が増加していることが観察された。この活動を実施した脅威アクターについて、公開情報ではGorgon Group（別名：Aggah、MasterMana）という名称で報告されている。2020年同様、Gorgon Groupのスパムキャンペーンの大半は、PowerPoint文書やOneDriveのリンクを使用し、AgentTesla、Remcos、QuasarなどのコモディティRATを配信するものであった。さらに、この脅威アクターが2つの異なるコモディティインジェクター、RunPEおよびHCryptを使用していることも確認された。

Gorgon Groupは、PastebinやBlogspotなどの公開ペーストサイト上で多段階の悪意あるスクリプトをホストすることも知られているが、PwCは、同様の目的でInternet Archiveのアカウントを使用する一連のキャンペーンも追跡調査している。2021年8月の報告[152]では、Gorgon Groupが、ペーストサイトの代わりに、侵害したWebサイトを使用して次段階の悪意あるペイロードをステージングしWarzone RATを配信していることが報告された。これは、多段階の攻撃能力を構成するインフラの検出とテイクダウンを回避するための取り組みである[153]。

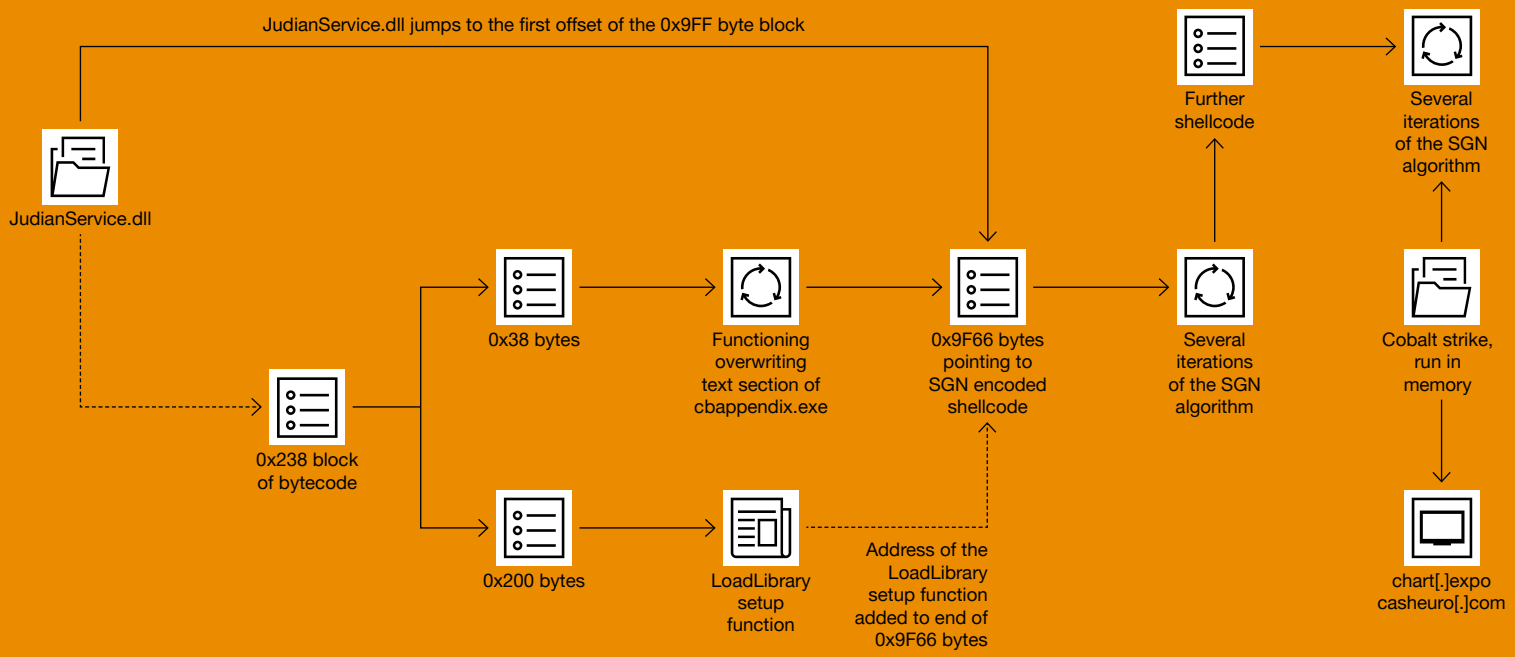
Green Havildarのインテリジェンス収集活動は、主にインドに加え、時にはアフガニスタンなどの近隣諸国[154]も含んでいるが、Gorgon Groupの活動は、必ずしも政治的領域に限定されない国際的な規模に及んでいる。例えば、2021年4月以降、PwCはオランダと韓国の組織を標的としたGorgon Groupのキャンペーンを追跡調査したが[155]、その中にはこの脅威アクターが頻繁に標的とする分野である製造業が含まれていた。Green Havildarとは対照的に、Gorgon Groupは無差別に標的を定める傾向があり、カスタムマルウェアの展開は確認されていない。

活動は低下：ベトナムを拠点とする脅威アクターの活動

2020年12月、FacebookがScarlet Ioke（別名：Ocean Lotus、APT32）をベトナムのIT企業CyberOne Groupにアトリビューションした後、少なくとも既知の進行中のキャンペーンに関しては、この脅威アクターの活動ペースが大幅に低下していることが確認された。一方、中国のサイバーセキュリティ企業は、過去1年間にわたり中国を標的としたScarlet Iokeの観察を続けており、これは当該脅威アクターが長年にわたって中国を標的としてきたことと合致する。例えば、セキュリティ企業Sangfor[156]は、別名：DgBase.dllと呼ばれるローダーを用いたScarlet Iokeの活動を報告している。また、ボットネット機能を備えたLinuxバックドアRotaJakiro[157]も、RotaJakiroとOceanLotusのバックドアとコードがかなり重複していることから、公開情報ではScarlet Iokeにアトリビューションされている。

2020年末から2021年9月にかけて、Cobalt StrikeおよびMetaSploit用のDLLローダーを使用するキャンペーン[158]が観察されたが、このローダーには、検出を回避するためにエンコーダーShikata Ga Naiを使用して多重のエンコーディングが施されていた。Cobalt Strikeのペイロードは、WebサービスGlitchを使用してC2活動を行うケースもあった。

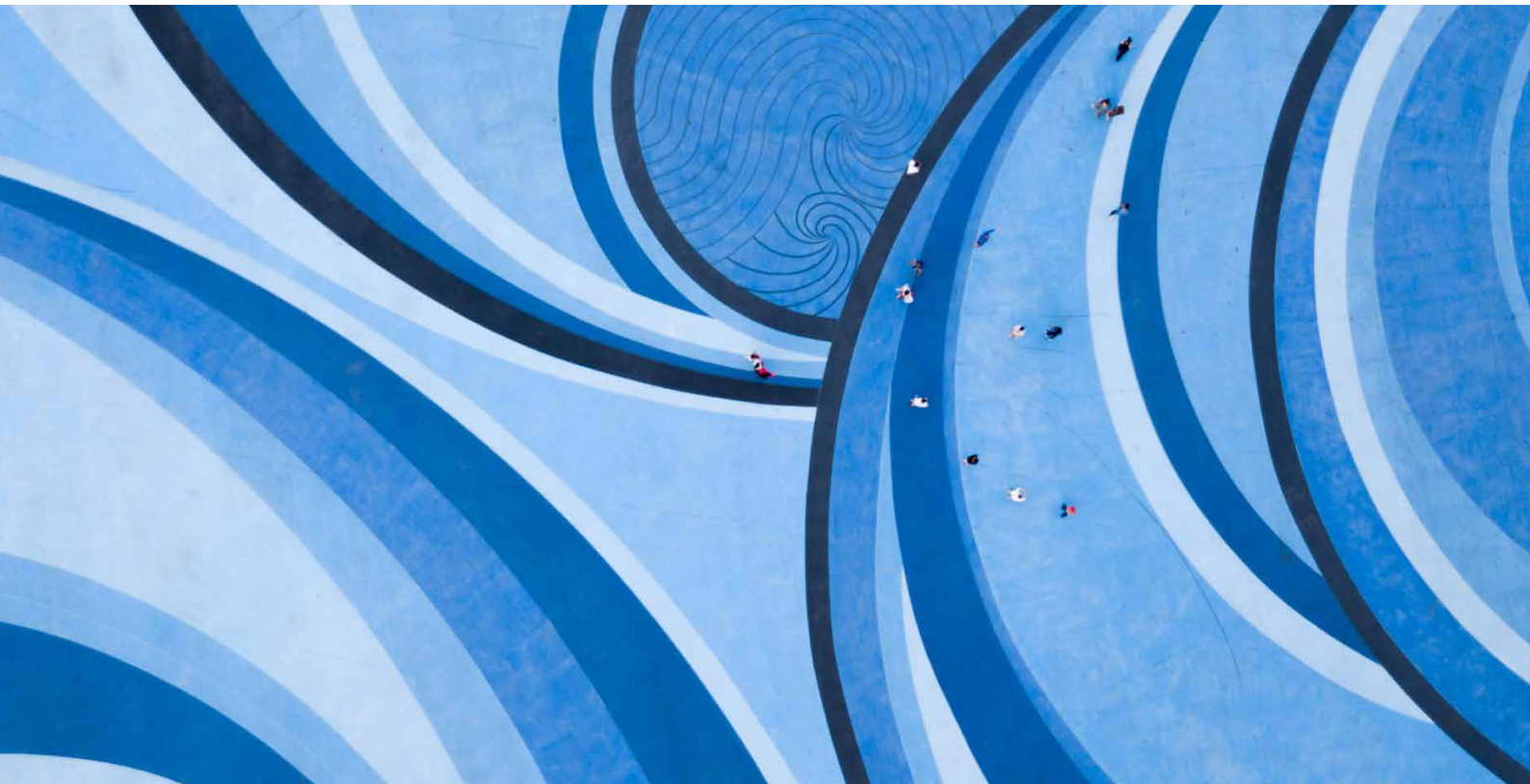
図表24：CobaltStrike Beaconをメモリ上にロードするScarlet Iokeによるものと見られる攻撃チェーン



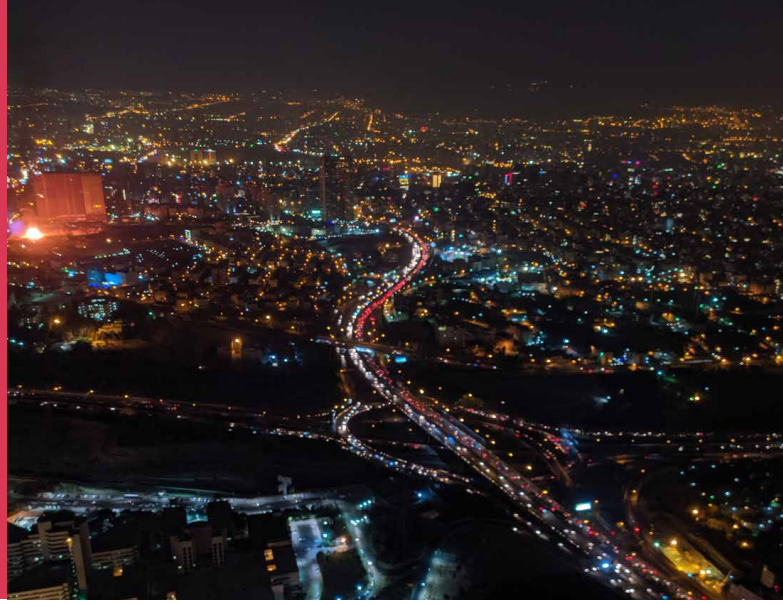
少なくともひとつのケースにおいて、当該DLLは、中国標準語圏で主に使用されているKingsoft製正規ソフトウェアのバイナリによってサイドロードされていた。さらに、PwCが確認したCobalt Strikeのサンプルの多くは、TencentのQQサービスや中国の検索エンジンSogouに偽装されており、これはScarlet Ioke によって一貫して用いられる手口であった。こうしたことから、このバイナリは、中国語を用いる被害者を標的にしたものである可能性が高いことが示唆される。またPwCは、観察されたTTPと標的に基づき、このキャンペーンがScarlet Ioke により行われたと考えるのが現実的であると評価している。この評価と矛盾する要因としては、以前のScarlet Iokeの活動との直接的なつながりがないこと、また、国内のレッドチーム演習でも見られるような典型的な侵入テストツールが使用されていることが挙げられる。

結局のところ、脅威アクターによって情報開示とアトリビューションへの対応方法は種々に異なる。Red KelpieやYellow Garudaのように、TTPに変更を加えずに活動を継続する場合もあれば、ツールやテクニックを変更したり根本から再構築を行ったりする場合もある。PwCの観察によれば、Scarlet Iokeが活動を停止した可能性は低いと判断している。むしろ、この脅威アクターは新たなキャンペーンを実行する計画を立てて、それに向けた再構築を進めている可能性が現実的であると評価している。

脅威アクターによって、自らの活動の情報開示とアトリビューションへの対応は種々に異なる。Red KelpieやYellow Garudaのように、TTPにほとんど変更を加えずに活動を継続する場合もあれば、ツールやテクニックを変更したり、根本から再構築を行ったりする場合もある。おそらくScarlet Iokeも後者と考えられる。



中東



イランを拠点とする脅威アクターの活動

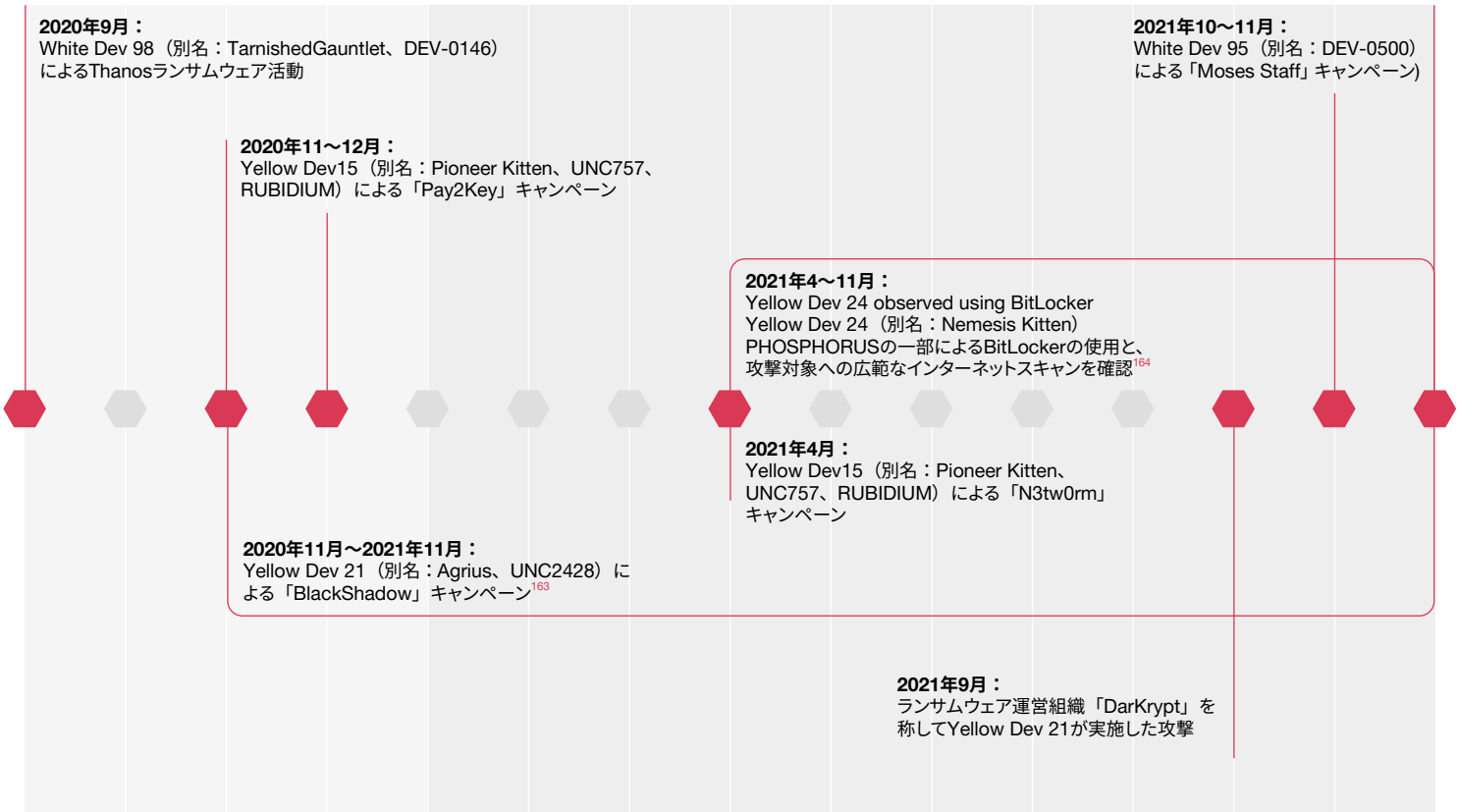
妨害工作の変遷

イランを拠点とする脅威アクターは、被害組織の破壊と混乱を目的とした妨害工作を長年にわたって行ってきた。このような攻撃は脅威アクターを衆目にさらすことになり、多くの場合、民間および公共部門によるアトリビューションと精査が行われる。こうした注目度を下げるべく、イランを拠点とする脅威アクターはしばしば、ハクティビスト集団を非難したり逆に装ったりする行動に出る。この戦術は、White Dev 95（別名：Moses Staff）のようなイランを拠点とする脅威アクターだと見られる組織によって、現在も採用されている[159]。

PwCは、イランを拠点とする脅威アクターが、動機を偽る戦術をとるケースが増加していることを観察した。これは、2020年後半に初めて出現し、2021年に顕著になった。例えば、Yellow Dev 15によるPay2KeyやN3tw0rmといったランサムウェアを使用した活動は、金銭的利益よりも破壊工作のためのものである[160]。ランサムウェアがハクティビスト的な行動と組み合わせて使用された場合、脅威アクターの本質と意図について混乱を招く可能性がある。

Yellow Dev 15やYellow Dev 21といったイランに拠点を置く脅威アクターは、破壊工作活動において、ハクティビストではなくサイバー犯罪者になりすまし、標的を恐喝するふりをする場合もあった[161]。Yellow Dev 21は、支払いがない場合、被害者のデータを第三者に売却すると脅したこともある[162]。

PwCは、イランに拠点を置くと思われる以下の脅威アクターが、そのキャンペーンにランサムウェアを活用していることを確度に差はあるが確認した。



ケーススタディ：N3tw0rm

2021年4月下旬、N3tw0rmというランサムウェア亜種が出現し、イスラエルの小売り、物流、NGO、建設業界を標的とした。その後、技術的分析によって、復号キーの提供が完遂されていないことが明らかになり、このN3tw0rmと、Yellow Dev 15がコントロールしている別のランサムウェア亜種であるPay2Keyとの類似点が明らかになった。2021年12月の時点で、N3tw0rmの身代金要求文書に記載されているビットコインウォレットは空のままであり、これは犠牲者が金銭を払っていないということを意味する。攻撃の動機は、金銭的なものというよりは破壊工作であると思われる[166]。

ケーススタディ：Moses Staff

2021年9月以降、「Moses Staff」と自称する脅威アクターが、イスラエルの組織に対して破壊的な「ロック&リーク」キャンペーンを開始した。PwCは、このキャンペーンの背後にいる脅威アクターをWhite Dev 95として追跡調査している。2021年後半に観察されたこのキャンペーンの犠牲者の大半は、イスラエル政府が犯したとされるさまざまな犯罪を暴露するという脅威アクターのミッションステートメントと事業地域が一致しないイスラエルの組織であった。また、その標的は、法務、物流、小売、公益事業、プロフェッショナルサービス、輸送、建設、製造、金融サービスなど多岐にわたっている。これを踏まえると、標的は不正行為の疑いの暴露というよりも、単に標的としてイスラエルに焦点を当てた結果選ばれた、つまり場当たり的に選ばれた可能性があることが示唆されている。

また、White Dev 95は、2021年以降に行われイランを拠点とする脅威アクターにアトリビューションされたイスラエルに焦点を当てた数々のキャンペーンと複数の類似点が見られ、特に、自らの活動に対する勢いをつけるために世間の注目を集めようとするものであった。そのため、White Dev 95は、複数のデジタルプラットフォームを運用して被害者のデータを流出させたり、Twitterで被害者と直接やり取りを行ったりしている。Moses Staffによるキャンペーンとイランを拠点とする脅威アクターによる類似活動との重要な相違点のひとつは、White Dev 95が攻撃の脅迫段階をスキップし、代わりに警告なしに盗んだデータを流出させることを選んだ点である。これは、被害者を混乱させ、キャンペーンの破壊的要素を最大化することに貢献していると思われる。

古参の脅威アクターに新しいTTPを教授することは不可能

PwCが追跡調査しているイランを拠点とする脅威アクターの大半は、昨年新しいタイプのツールを導入したが、従来の手慣れた手法も使い続けている。イランを拠点とする脅威アクターは、オープンソースツール、特に攻撃的なセキュリティツールの使用や、ソーシャルエンジニアリングキャンペーンでよく知られている。

オープンソースツール

Yellow Nix（別名：Static Kitten、MERCURY、MuddyWater）は、2021年を通じて、被害者への初期アクセスを獲得するためのツールとしてConnectWise Control（別名：ScreenConnect）やRemote Utilitiesといった商用リモート管理ツールを一貫して活用していた[167]。また、Yellow Nixは、ConnectWise Controlの配信メカニズムとして使用するなど、マクロ付きMicrosoft Officeドキュメントを断続的に使用していた[168]。

Yellow Dev 24[169]とYellow Dev 15[170]は、いずれもオープンソースのFRPツールを使用しており、これにより、被害組織のネットワークから脅威アクターが管理する外部のシステムにアクセスすることが可能になる。同様に、Yellow Orc（別名：APT 33、Refined Kitten、Stonedrill）は、事後攻撃とラテラルムーブメントに使用されるオープンソースのC2フレームワーク、PoshC2を使用することでよく知られている。2021年、PwCは、一般に公開されている同様のC2フレームワークを取り入れた、新しいYellow Orcの活動を観察した[171]。

ソーシャルエンジニアリング

イランを拠点とする脅威アクターの多くに共通しているのは、求人や人材募集をテーマにしたフィッシングの誘い文句を使い、ソーシャルメディアプラットフォームを利用して直接誘いかけ、標的との信頼関係を構築するという点である。フィッシングやソーシャルエンジニアリングのテクニックが多要素認証（MFA）をすり抜けるケースも一部見られたものの、PwCの観察によれば、MFAは依然として攻撃の大部分を阻止する上で非常に効果的である[172]。

Yellow Maero（別名：APT34、OilRig、COBALT GYPSY）は、ソーシャルエンジニアリングの長い歴史を誇る。PwCは2021年1月、Yellow Maeroが、米国に拠点を置く正規ITサービスプロバイダーを称し中東でのさまざまなIT、ビジネス、エンジニアリング人材を募集するパンフレットを使用していることを確認した[173]。こうしたおとり文書は、脅威アクターによって悪意を持って再利用されたものであるが、オリジナルは正規のものであった可能性が高い。

7月、PwCがYellow Orc（aka APT33, Elfin）として追跡調査している脅威アクターは、主に中東の石油・ガス、化学、エネルギー、ライフサイエンス、製造、鉱業、インフラ、政府関連などの業界に焦点を当てた求人案内と偽のキャリア検索Webサイトを使用するキャンペーンを実施した[174]。また、オープンディレクトリのコンテンツによると、この脅威アクターは、2021年初頭に米国を標的として悪意あるHTAファイルを使用すると同時に、世界保健機関（WHO）のCOVID-19感染者トラッカーを装ったマルウェアを利用した活動を実施した[175]。そのオープンディレクトリは、Yellow Orcが標的にソーシャルエンジニアリングを仕掛けるためにある女性の画像も使用していたとする証拠も示している[176]。この画像は、PwCがYellow Lidercとして追跡調査している脅威アクターが用いる「Marcella Flores」というペルソナに関する公開情報の報告と類似している[177]。Yellow Orcは、少なくとも2017年以降、求職をテーマにしたソーシャルエンジニアリングの手口を用いている。

Yellow Liderc（別名：Tortoiseshell、TA456）[178]と、これに密接に関係している組織としてPwCがYellow Dev 13と命名し追跡している脅威アクターは、2021年を通してLinkedInとFacebookをソーシャルエンジニアリング目的で使用し続け、偽の人材派遣会社・個人のネットワークを維持していた[179,180]。Microsoft、Metaの両社は、Yellow Lidercのソーシャルメディアを利用した執拗かつ忍耐強いプロセスを記録しており、それによれば、標的との最初の接触から悪意あるコンテンツの配信まで数カ月に及ぶケースもよくある[181,182]。

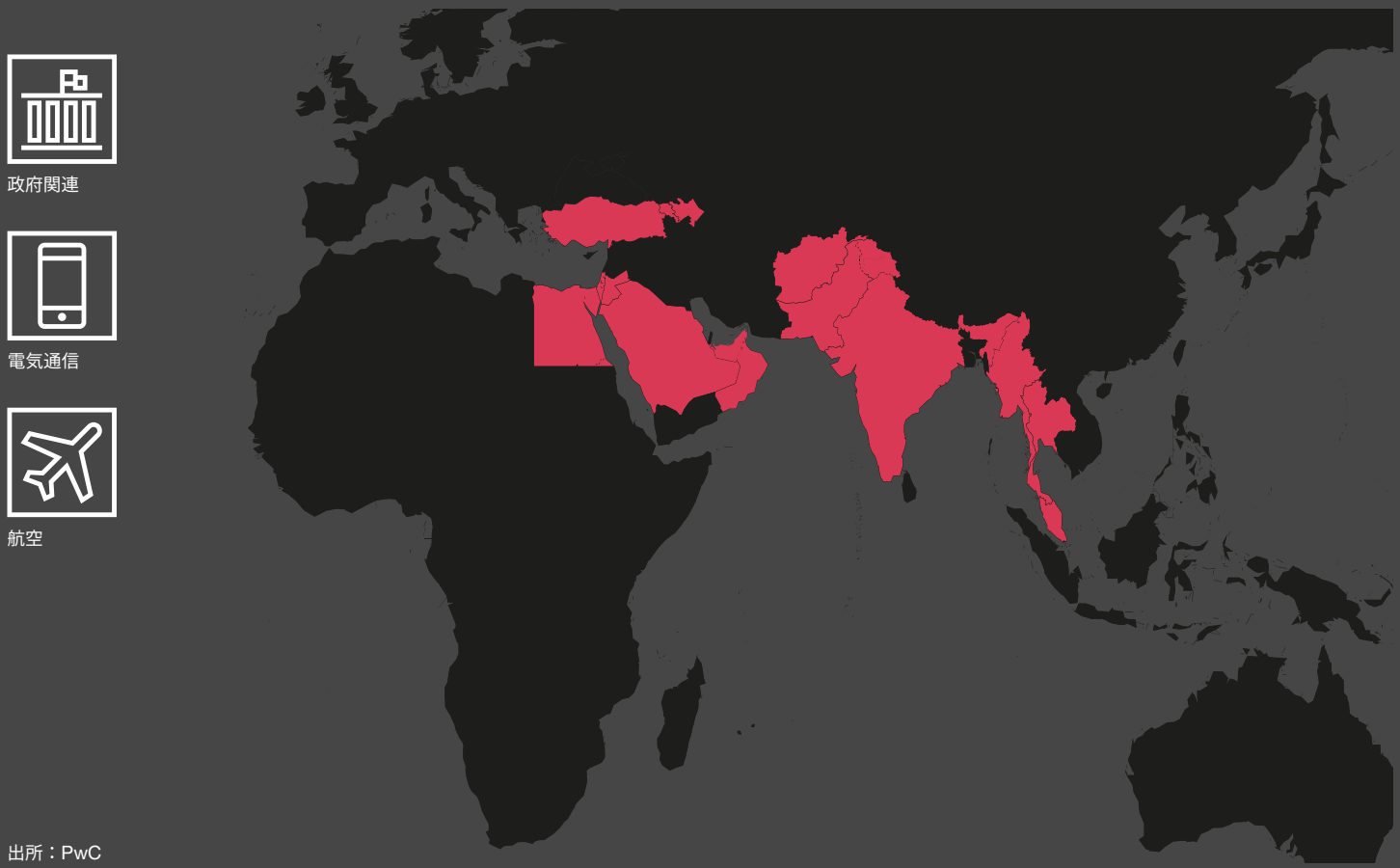
領域拡大

Yellow Nix

Yellow Nixは、イランに隣接する地域以外にもその活動領域を広げ続けた。2020年、欧州地域を標的とした複数の活発なキャンペーンに続き、2021年9月には、この脅威アクターが東南アジアに標的を移行したことがわかった。イランとマレーシアの当局の間で行われた経済協力協議後、特にマレーシアの政府、航空、通信業界を標的としている[183]。これはYellow Nixの典型的なケースであり、その活動はイランの政治・貿易投資の状況を忠実に反映したものであることが多い。また、Yellow Nixは航空業界への関心を高めているようである。

2020年9月、米国は、旅行者の動きを監視するために世界の航空・通信業界を標的とする脅威アクターとして悪名高いYellow Mimasに関わる個人に制裁措置を講じた。それ以来、PwCのアナリストはYellow Mimasの活動を観察しておらず、一般公開されている脅威レポートでもこの脅威アクターの存在は目立っていない。Yellow Mimasが活動停止期間に入ったのかどうかは不明であるが、Yellow Nixが航空会社を標的にした活動を活発化させていることから、Yellow Nixがどの程度の成果を上げているかは依然として不明ではあるものの、この業界からのインテリジェンス獲得を望むスポンサーの要求は満たされている可能性が高い。また、Yellow Nixの最近の標的はYellow Mimasと類似しており、Yellow Nixが関心を持つ個人に対するサーベイランスを行っている可能性があることを示している[184]。

図表25：Yellow Nixの標的地域・分野



出所：PwC

Yellow Dev 9

2019年に初めて公開情報として報告された、諜報活動を動機とするYellow Dev 9（別名：Lyceum、Siamese Kitten）は、その標的、インフラ、ツールの面で、PwCがYellow Maeroとして追跡調査するイランを拠点とする別の脅威アクターと類似している。Yellow Dev 9は、2021年にアフリカの通信・航空分野を標的とした活動を続け、LinkedInを介したソーシャルエンジニアリングや、情報技術企業を装ったドメイン上で人材募集をテーマにしたマルウェアをホストしている[185]。複数のセキュリティリサーチャーがYellow Dev 9に関する公開レポートを発表しているにもかかわらず、脅威アクターは、HTTPおよびDNSによってネットワークに接続するバックドアMilan、およびSharkと呼ばれる新種のマルウェアの開発を続けた。Yellow Dev 9のインフラには特定のパターンがあり、この脅威アクターは2021年の間に、「dns」、「update」「cdm」という文字列を含むコマンド&コントロール（C2）ドメインを一貫して登録している[186、187]。

Yellow Garuda

昨年、最も活発に活動し、広く報告された脅威アクターのひとつがYellow Garuda（別名：Charming Kitten、PHOSPHORUS, ITG18）である。この脅威アクターは高い能力と持続性を誇り、2021年に活動ペースを上げる一方で、フィッシング・インフラの広大なネットワークを維持している。Yellow Garudaのキャンペーンは、単純なクレデンシャルフィッシング[188]から、正規のWebサイトの侵害[189]、モバイルマルウェアの展開[190]、Telegramボットを使用した被害者端末のフィンガープリンティング[191]、ソーシャルエンジニアリングの倍増など、多岐にわたる。

これらの活動は、世界中のさまざまな業界の被害者を広範囲に標的にしている。2021年を通じて、イラン国内だけでなく、中東の近隣諸国、米国と欧州の典型的な標的が被害を受けている。

Yellow Dev 19

PwCがYellow Dev 19として追跡調査しているイランを拠点とする脅威アクターは、2020年の米国大統領選挙関連Webサイトを標的としており、米国政府の評価によれば、この攻撃は選挙に影響を与え妨害しようとするものであると評価されている[192]。PwCは2021年5月、Yellow Dev 19はイランの教育業界に学生または教員というかたちで密接に関係している可能性が高いという評価を行ったが、それを裏付けるかのように、2021年11月の米国起訴状には23歳、26歳の2名の名前が挙げられていた[193]。PwCはまた、Yellow Dev 19はサウジアラビア政府機関を標的にすることに関心がある可能性が高いことを特定している[194]。

米国政府の起訴状によると、このキャンペーンを主導したのは、Emennet Pasargadという会社で、イラン政府の支援を受けて活動しているとされている[195]。PwCのアナリストはまた、制裁を受けた役員と合わせて、この会社と Yellow Liderc との間に重複が見られることを確認している[196]。PwCは、Emennet Pasargadおよび／またはその職員が、破壊工作目的のランサムウェアなど他の攻撃活動にも関与している可能性が高く、イスラム革命防衛隊と密接に連携していると評価している。

Yellow Dev 24

PwCは、少なくとも2021年4月から11月にかけて、Yellow Dev 24（別名：Nemesis Kitten、PHOSPHORUSの一部）がFortinetデバイスやMicrosoft Exchangeサーバーなど、インターネット機器を大量スキャンしていることを確認した[197]。その後、オープンソースツールや環境寄生（living-off-the-land）技術を利用して、BitLocker経由でランサムウェアを展開するケースも見られた。Yellow Dev 24は、破壊工作を目的としてランサムウェアを導入し、同時に諜報活動を行う能力も備えたイランに拠点を置く複数の脅威アクターのひとつである。また、Yellow Dev 24は、標的の選択において場当たり的であるため、世界中の人々がこの脅威アクターの標的となり得る[198]。

このキャンペーンにおける被害者は、米国、オーストラリア、UAE、南アフリカなど、地理的に多様であった[199]。この脅威アクターは、わずか6カ月あまり[200]の間に、約1,000台のデバイスを危険にさらしたと報告されている。また、米国やイスラエルの防衛関連テクノロジー企業、アラビア湾の入港地、中東で事業を展開するグローバル海運企業など、それでも場当たり的ではあるが若干標的を絞った活動が、パスワードスプレー攻撃によって行われている[201]。

中東地域全体にわたる脅威アクターの活動

Teal Dev 2

トルコを拠点とする脅威アクターTeal Dev 2（別名：StrongPity）は、2021年を通じて、よく知られたバックドアStrongPityを展開し続けたが、PwCの観察では、この活動は同年後半に失速している。新たなTeal Dev 2のTTPが明るみになり、公開情報のレポートではStrongPityとAndroidマルウェアとのインフラ面のつながりが示されている。これまでこの脅威アクターのツールセットの一部として知られてはいなかったが、少なくとも2019年から使用されている可能性が高いとされている[202]。これらの観察に基づき、PwCは、Teal Dev 2が特定のツールやテクニックを惜しみなく投じることで数年間にわたり検出されずにいる可能性が高く、極めて標的を限定したキャンペーンであることを示している可能性が現実的であると評価している。

Grey Karkadann

Grey Karkadann（別名：Arid Viper、APT-C-23、Gaza Cybergangの一部）は、パレスチナの政治とパレスチナーイスラエル関係に焦点を当てており、中東地域の組織・団体を標的とするために従来の手慣れたテクニックを使い続けている。2021年において、Windows用マルウェアMicropsia[203]を使用し続けており、通常、主な標的に関連したトピックのおとり文書が添付されている。PwCはまた、そのモバイルマルウェア開発についても観察を継続している。このマルウェアは、サードパーティーのアプリストアや脅威アクターが管理するサイトを通じて配布されている。一般公開されているレポートによれば、Grey Karkadannは既知のAndroid端末向け不正プログラムに加え、iOS端末向け不正プログラムも有している[204]。この脅威アクターのモバイル端末向け不正プログラムには、広範なサーベイランス機能とステルス機能が含まれており、多くの場合、正規のアプリケーションを装ったものである[205]。

White Dev 21

2021年5月、PwCは中東情勢に関心を持つアラビア語圏の人々に焦点を当てた攻撃グループを観察した[206]。この活動は少なくとも2019年までさかのぼり、パレスチナ、レバノン、およびイラクに関連するニュースやテーマを幅広く網羅した内容のマクロ付きドキュメントを使用していた。これは、脅威アクターが複数の別々の被害者を標的にしている可能性が高いことを示している。一般公開されているレポートによれば、このキャンペーンはWIRTEと呼ばれる脅威アクターと関連しており、政府や外交機関、法律事務所、金融機関など、多くの業界の著名な組織が標的になっていることが強調されていることから、この脅威アクターは幅広い業界で懸念される存在となっている[207]。PwCの観察によれば、WIRTEとWhite Dev 21が過去に使用していたインフラには共通点が見られる。この脅威アクターについては、2019年にエジプトとパレスチナの政治に関連する選挙と外交関係をテーマにしたおとり文書を使用したことを観察しており、PwCは、Gaza Cybergang[208,209]の派生グループである可能性が現実的であると評価している。

欧州・旧ソ連

ロシアに拠点を置く脅威アクターは、2021年も秘密または機密情報へのアクセスを求め、サイバー作戦を継続した。これには、欧州全域の政府省庁、およびロシアの近海地域を標的としたものが含まれている。PwCは、脅威アクターであるBlue Athena（別名：Sofacy）が、中央アジア地域の鉱業・天然資源業界に特に関心を示していることを確認した。

また、ロシアを拠点とする脅威アクターBlue Otsoによるウクライナの組織を執拗に標的とする活動も引き続き確認されている。PwCは、2021年11月にウクライナ治安局（SBU）がBlue Otsoの運営組織とされる複数の人物の正体を暴くまで、ウクライナ東部の企業を対象としたBlue Otsoの活動を追跡調査してきた。

PwCは、ロシアを拠点とする脅威アクター以外にも、悪意ある活動を追跡調査している。例えば、White Turはまだアトリビューションが不明な脅威アクターのひとつで、特定の業界や地域に大きな関心を寄せている。また、グルジアを拠点とする脅威アクターRose Matsilは、2021年にロシアで発生した医療機関への攻撃に関連して観察されている。

Blue Dev 5 - 「高貴な」フィッシングアクター

ロシアを拠点とする脅威アクターBlue Dev 5（別名：NOBELIUM[210]、NobleBaron）は、2021年にPwCが追跡調査した中で最も活発かつ技術的にも洗練された脅威アクターのひとつであった。Blue Dev 5は、Microsoftのクラウド環境を侵害し、組織間の信頼関係を攻撃するなど、周到な策略と斬新なテクニックを披露した。

Blue Dev 5は、複数のクラウドサービス代理販売業者やMSPへの侵入に成功し、これらの組織が顧客と結ぶクラウドに関する信頼関係を利用して顧客のクラウド環境を侵害し、顧客のネットワークにピボットすべくMSPに提供されるアクセスを悪用した。Blue Dev 5は、被害者の組織にアクセスした後、特権アカウントや機密情報を含むAzure ADおよびMicrosoft 365インスタンスへの長期的かつステルス的な持続的アクセスを獲得することを目的としている。Blue Dev 5は、高いレベルの運用セキュリティを示しており、検出を回避して被害組織による疑わしい活動（例えば住宅IPアドレスから被害者組織の侵害アカウントへのログイン）の調査を困難にする対策をとっている。

今のところ、PwCがBlue Nova[211、212]として追跡調査しているSolarWindsサプライチェーン攻撃の背後にいる脅威アクターと、このBlue Dev 5を明確に関連付ける証拠は存在しない。しかし、Microsoftのクラウド環境に対して高度なIDベースの攻撃を行うテクニックを含め、この2つ脅威アクターのテクニックには大きな重複があることを指摘している。また、Blue Dev 5とBlue Nova[213]は、いずれも第三者の信頼関係を利用して、組織のIT環境にアクセスしていることも確認されている。

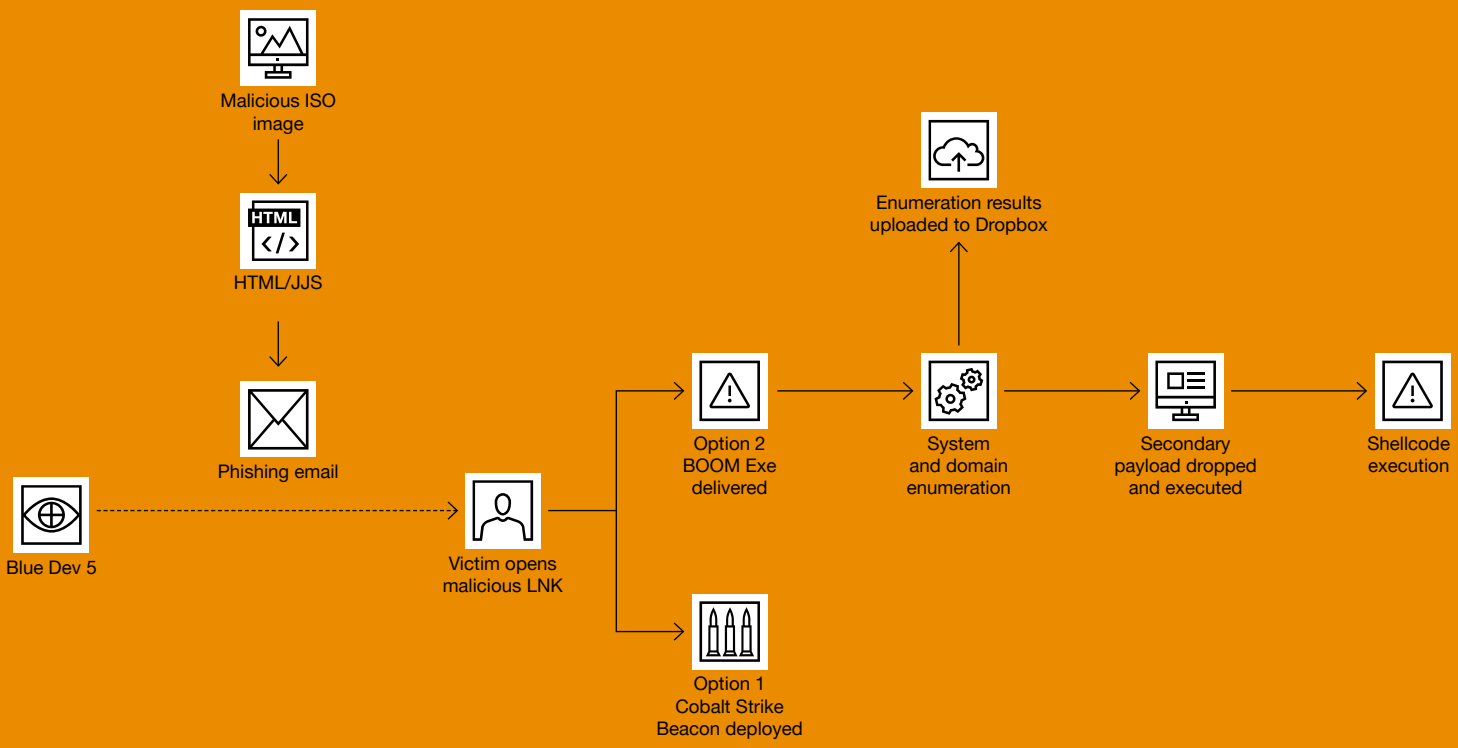
Blue Dev 5の脅威を懸念する組織は、次のような対策を講じる必要がある。

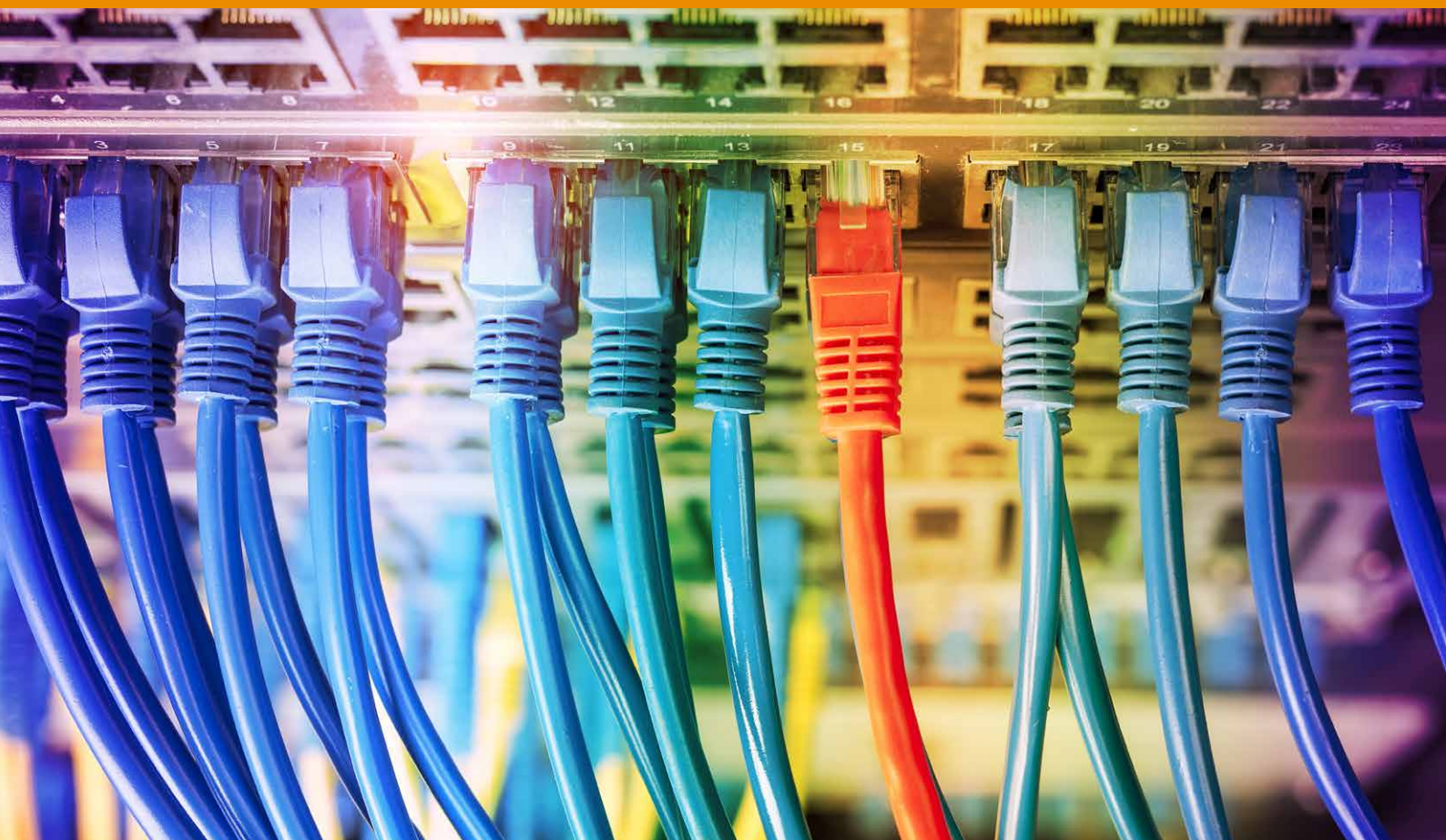
- 安全な管理プラクティスと特権アクセスの使用に関する厳格な制限を含む、堅牢な特権アクセス戦略の実装
- Azure ADとMicrosoft 365のログを監視し、特権アカウントの侵害と攻撃に使用されるテクニック、永続化テクニック、および珍しいグローバルイベントの確認を行う
- クラウド（Azure AD、Microsoft 365、Azure）構成と信頼関係を定期的に監査する

Blue Dev 5は、組織の環境にアクセスするために、パスワードスプレー攻撃や漏洩した認証情報の使用など、よく知られたテクニックも使用していることが確認されている。

Blue Dev 5は、2021年5月にカスタムローダーでパックされたCobalt Strike Beaconマルウェアを配布するために、USAID（米国開発庁）を装ったフィッシングキャンペーンを実施したことで大きな注目を集めた。PwCは、この事例は以下のような活動であったと見ている。

図表26：Blue Dev 5によるDropboxからのデータ送出を含む侵入チェーン



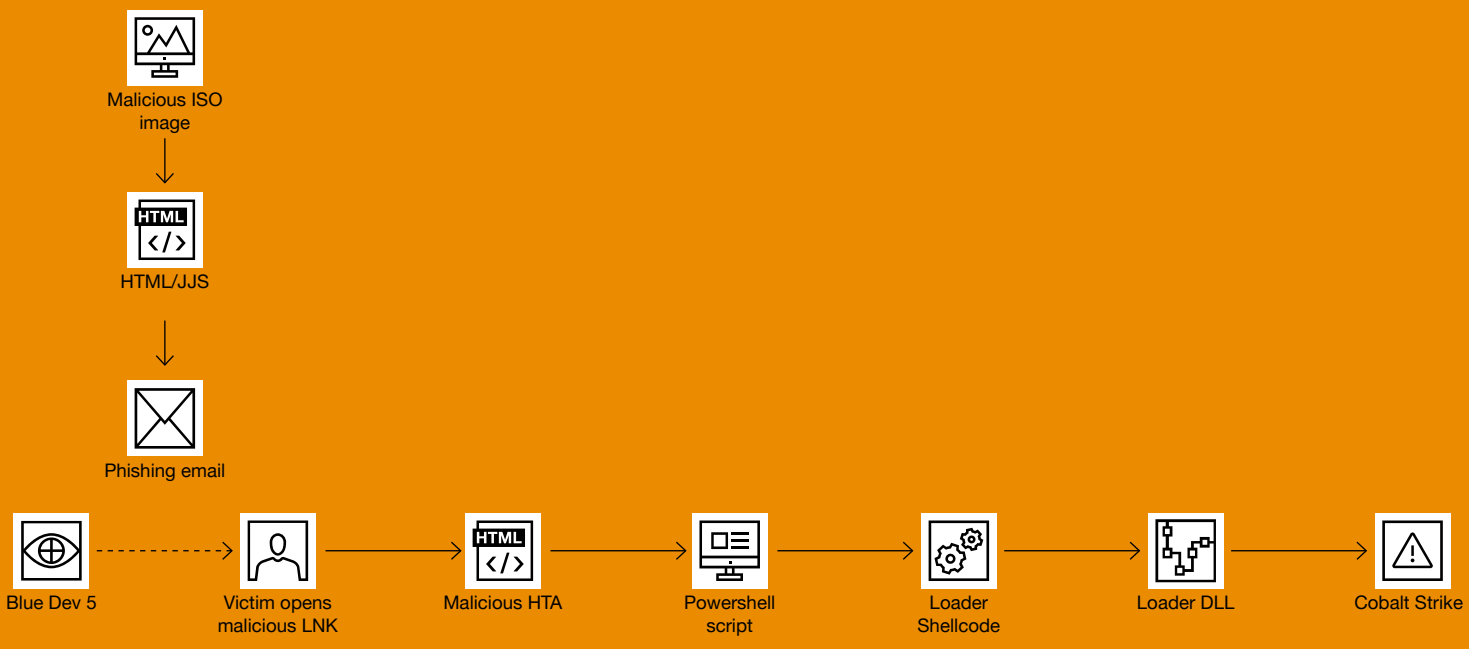


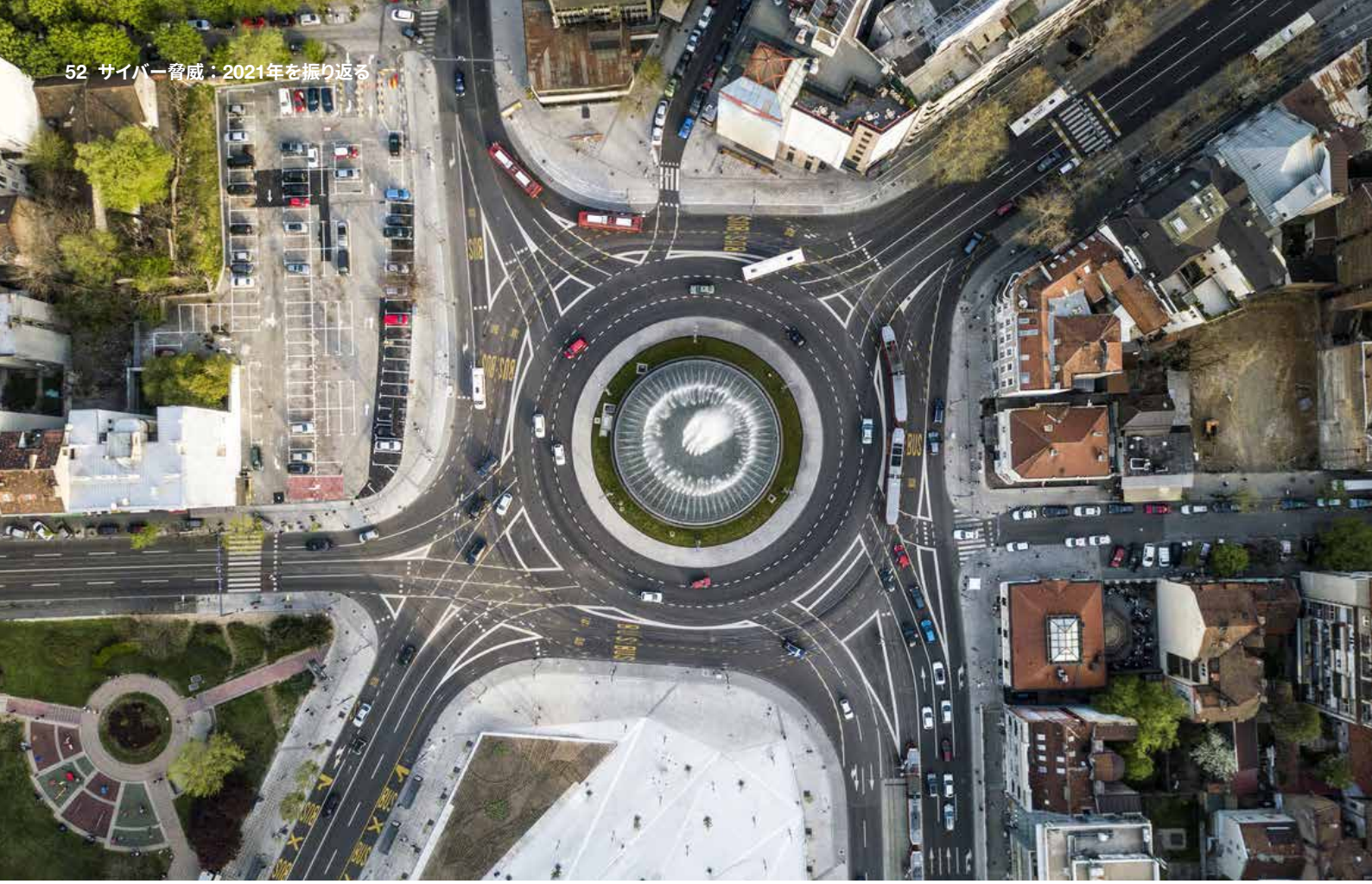
第一段階のHTML形式添付ファイルは、欧州各地の複数の大使館に勤務する職員によって開封されたという証拠があり[214]、この脅威アクターが行った広範な標的設定を窺い知ることができる。Blue Dev 5が使用したペイロードの中には、より標的を絞ったものもあったと思われる。2021年3月[215]に確認されたペイロードは、東欧諸国の外務省に関連する環境変数を確認するものであり、また、ウクライナ政府の文書管理システムの更新を偽装したものもあった[216]。

Blue Dev 5のインフラを時系列で追跡調査することで、PwCはそのTTPがより複雑になっていることも確認した。例えば、2021年11月に作成されたと思われるおとりHTMLの場合、脅威アクターは、最初のおとりHTMLと、最終的にCobalt Strike Beaconのペイロードを標的に送り込むまでに、複数の段階を加えていた。このケースでは、PwCが確認した他のもう一例と同様に、標的に対して、COVID-19のために大使館が閉鎖されるという内容のおとり文書を用いていた。

PwCは、Blue Dev 5が来年度も活動を継続し、そのTTPは時間とともに進化を続け、より検出が難しくなる可能性が現実的であると評価している。

図表27：Blue Dev 5 の初期アクセス侵入チェーンのバリエーションの1つ





バルカン半島にスポットライト：White Tur

2021年1月、PwCはセルビア軍を標的としたフィッシングドメインを観察した[217]。その直後、少なくとも2017年から継続しているセルビア、スルプスカ共和国両政府および防衛組織を標的とした追加の関連インフラの存在を確認し、現在、PwCがWhite Turと呼ぶ脅威アクターと関連して追跡調査中である。スルプスカ共和国は、ボスニア・ヘルツェゴビナの2つの構成体のひとつである。バルカン半島は、多様でありながら分裂した歴史の地域であり、複雑な戦略的背景が存在する。セルビアとスルプスカ共和国の両方が標的になっているのは、ここ数カ月、スルプスカ共和国のさらなる自治権獲得、あるいは完全な分離を唱える声が一部で強まっているためでもあり、特に注目される[218]。

この追加インフラにより、スルプスカ共和国内務省が2020年4月[219]に公表した以前の活動が明るみに出た。この活動は、同国首相になりすますスピアフィッシングキャンペーンであり、悪意あるHTAファイルを介してセルビア軍のフィッシングドメインに関連したC2ドメインからPowerShellをダウンロードして実行する。

この1年間、関連インフラを継続的に追跡した結果、軍事・防衛組織と密接に連携しているセルビアの研究開発組織が標的となっていることが確認された[220]。2021年9月、White Turは、スルプスカ共和国と防衛をテーマとする武器化した文書およびアーカイブファイルをホストするために、Webサイトに対して戦略的なWeb侵害を行った[221]。これ以前には、White Turの武器化ファイルは、脅威アクターが登録した専用インフラにホストされていた。

White Turの能力に関しては、JScriptバックドアにつながるマクロ武器化文書を使用していることが確認されている。また、オープンソースプロジェクトOpenHardwareMonitorを含む武器化したアーカイブファイルにパッケージされたWindowsバックドアを展開し、COMビット転送オブジェクトを使用してC2へ情報を送信していることも確認された。

全体として、White Turは諜報活動を目的とした脅威アクターであり、国家と連携している可能性が高いと評価される。地政学的緊張に基づき、この活動にかかわる潜在的候補者は、バルカン半島内のみならず、遠く離れた場所にも多数存在する。現時点において、PwCはWhite Turの潜在的支持者に対して高い確度で評価するための十分な技術的証拠を有していない。しかし、PwCは、バルカン半島は今後も、さまざまなきっかけと動機を持つ脅威アクター（White Turを含む）にとって関心の高い地域である可能性が高いと判断している。White Turについては、**ブログ**でさらに詳しく解説している。

クラウドサービスの悪用：Blue Odin

Blue Odin（別名：CloudAtlas）は、悪意ある文書を用いてロシアおよびロシアに隣接するウクライナのさまざまな組織を標的としており、ペイロードを綿密に制御することで知られている脅威アクターである。そのため、リサーチャーによる追跡調査も困難となっている。

2021年、Blue Odinの活動には、運用セキュリティ（OPSEC）のエラーから新しいTTPに至るまで、複数の新しい側面が観察された。ある事例では、中欧の某国国防省を標的にした悪意ある文書内にオンライン翻訳サービスへのリンクが埋め込まれており、このリンクを使って、おとりコンテンツのソースが元の英語からウクライナ語に翻訳されるという仕組みになっている。このことから、この文書を作成した運用者は、ウクライナ語を母国語としている可能性がある。

もうひとつ観察されたのは、2021年初頭のBlue OdinによるResponderの使用である。Responderはオープンソースツールであり、SMB強制認証攻撃に用いられる。このタイプの攻撃では、被害者のシステムが脅威アクターの管理するサーバーに対してNTLMによる認証を試み、脅威アクターがチャレンジハッシュを取得する。このハッシュに対して、後に被害者のパスワードを復元するためにオフラインで総当たり攻撃を行うことが可能である。この悪意ある文書は、外務・外交関係の個人を標的にしている可能性が高く、脅威アクターが管理するサーバー上の画像へのUNCパスが含まれており、上述の強制認証攻撃につながる。奇妙なことに、文書に埋め込まれたIPアドレスのひとつはタイプミスと思われ、指定されたIPはResponderサーバーをホストしているようには思えず、1文字違いのIPアドレスが指定されている。これは、この脅威アクターの悪意ある文書に使用されていた以前の手法（主にリモートテンプレートのリンクを使用）とは異なることを意味する。例えば、2021年12月[222]に観察された悪意ある文書では、Equation Editor攻撃を含むリモートテンプレートを取得し、HTAをダウンロードして実行、その結果VBShowerの亜種が展開されるというものであった。このチェーンは、2019年にKasperskyが最初に報告した攻撃チェーンに非常に類似している[223]。

PwCが観察した活動から、Blue Odinの標的はロシアの戦略的優先事項ではなく、ウクライナの戦略的優先事項に沿っている可能性が現実的であると評価している。例えば、ウクライナ国内でのBlue Odinの活動は、主に東ウクライナの自称分離主義地域とクリミア地域に焦点を合わせていると思われる。また、エネルギーや政府を含むロシアの組織を標的としたBlue Odinの活動も確認されている[224]。

Blue Otsoのジェットコースター

Blue Otso（別名：Gamaredon、Armageddon）は、2021年に、機密システムの広範囲にわたる侵害からウクライナ保安局による正体暴露まで、大成功と大失敗の両方を経験している。

2021年2月、ウクライナ国立サイバーセキュリティ調整センター（NCCC）は、Blue OtsoがSEI EB[225]およびASKOD[226]として知られるウクライナ政府文書管理システムに侵入したことを報告した。最初の侵害の兆候は散発的であったが、PwCは、ASKODサーバー1台に関連するインシデント対応に関与した1名ないし複数の個人が、オンラインのマルチウイルススキャナにアップロードしたと思われるファイル群を特定した[227]。これらのファイルには、ダウンローダースクリプト、流出ツール、VNCクライアント、Microsoft Word文書にリモートテンプレート参照を追加するためのスクリプトなど、Blue Otsoマルウェアのさまざまなツールが含まれており、NCCCによる評価と一致している。また、これらのアーカイブには、ファイル変更タイムスタンプも含まれており、PwCは、被害者端末に展開または変更した時刻と合致している可能性が現実的であると評価している。これらのタイムスタンプは、脅威アクターが、この事案が公表される数週間前の少なくとも2021年2月5日から被害者にアクセスしていた可能性が高いことを示唆している。

Blue Otsoの活動も、2021年に大きな混乱に見舞われた。最初に注目が集まったのは、4月にウクライナ治安局が、SBU職員の個人番号宛にメッセージを送信した人物に関連して逮捕者が出たことを公表した時であった[228]。これらのメッセージには、後にPwCがmurders-dkr[.]ruと特定したWebサイトへのリンクが含まれており、そこには、分離主義組織のひとつによって懸賞金をかけられたSBU職員のリストを含むとされるアーカイブファイルへのリンクが貼られていた。これは、これまでロシアを拠点とする脅威アクターと考えられていたBlue Otsoが、ウクライナ国境内の非占領地域からの活動によって支えられている可能性が非常に高いことを示す最初の公開情報となった。

その後、2021年11月にSBUが多数のBlue Otsoオペレーターの身元を開示し、この脅威アクターの活動がクリミアに拠点を置くFSBの一部門と関連していると主張したことで、騒動は拡大した[229,230]。この部門はFSBの第18センター（別称、情報セキュリティセンター）の下部組織であると伝えられており、以前に米国司法省によるデータ侵害とも関連付けられたことがある。伝えられるところによると[231]、SBUは2015年に初めてセンター18の関与を示唆し、その際、Blue Python（別名：Turla,Snake）との関連で知られるFSBセンター16の関与も示唆した。PwCの分析[232]では、この発表は、ウクライナで戦争が勃発する以前、大規模な軍事訓練の後、ウクライナとロシアの国境付近でロシア軍が兵力を増強しているタイミングで行われたと指摘している。

最近の分析によると、Blue Otsoはこの開示にも動じている様子はない。PwCは、2022年以降もこの脅威アクターが活動を継続する可能性が現実的であると評価している。

スポットライト：

新たな脅威アクター

このセクションでは、2021年にPwCが発見した特定のサイバー脅威アクターに着目する。これは、当該脅威アクターがこれまで活動していなかったことを意味するものではない。しかし、PwCが追跡調査を継続的に拡大し、可視化と収集に基づいて新たな脅威アクターを特定していく中で、あまり知られていなかった脅威アクターや、PwCがまだ完全な把握に至っていない脅威アクターを本レポートで取り上げることは価値があると考えている。以下に紹介する脅威アクターは、その能力、標的、他の脅威アクターとのつながり、あるいは実行する活動の種類など、興味深い内容を示しているため、取り上げたものである。

Red Dev 17

2021年、PwCは、Red Dev 17と名付けた一連の侵入に対する追跡調査を開始し、これが中国を拠点とする脅威アクターによって行われた可能性が現実的であると評価している。PwCの分析によると、Red Dev 17は少なくとも2017年から活動していたと思われる。

Red Dev 17の対象は主にインドで、インド軍やインドに拠点を置く多国籍テクノロジー企業、国営エネルギー企業などが含まれている。PwCは、Red Dev 17に関連する侵入の背後にいる脅威アクターが、公開情報でOperation NightScoutとして知られているキャンペーンにも関与している可能性が非常に高いと評価している。

Red Dev 17は、文書武器化フレームワーク8.t（別名：RoyalRoad）を用いており、LogitechやWindows Defenderバイナリなど無害のユーティリティを攻撃して、被害者のシステムにChinoxyまたはPoisonIvyの亜種をサイドロードして実行する。

PwCは、Red Dev 17と、Red Hariasa（別名：FunnyDream APT）と呼ばれる脅威アクターの間で、能力およびインフラ面でつながりがあること、さらにRed Wendigo（別名：Icefog、RedFoxtrot）とShadowPad C2サーバーのインフラに重複が見られることを確認した。現時点では、Red Dev 17 をこれらの脅威のいずれかと直接関連していると断言できる証拠はないが、Red Dev 17は、ツールやインフラを共有し、特に東南アジアや中央アジアを標的とする脅威アクター群の中で活動している可能性が現実的であると評価している。

Blue Dev 6

2021年10月、サーバーレス実行環境であるCloudflare WorkersをC2チャンネルとして使用する複数の武器化文書が観察された。PwCは、この活動が2020年8月にQuoIntelligenceが初めて報告した[233]脅威アクターであるBlue Dev 6（別名：ReconHellCat）によって行われた可能性が高いと評価している。武器化文書は、リモートテンプレートとマクロを使用して、Cloudflare Workersで実行されたC2からダウンロードしたペイロードを実行した。このペイロードは入念に難読化されており、ブラウザのフォルダーを繰り返し表示するコードやC2通信時の認証など、BlackSoulマルウェア（別名：BlackWater）との類似点がいくつか見られた。PwCが分析したキャンペーンの対象は、エネルギー、防衛、政府、国際人道支援団体など、多岐に及ぶものであった。

Yellow Dev 23

PwCは、Yellow Dev 23（別名：MalKamak、DEV-0270）として、通信とITの両業界に焦点を当てた新たな攻撃グループを追跡調査した。公開情報によれば、2021年後半にこの脅威アクターについて報告がなされており、イスラエル、特にそのIT・電気通信業界に大きく焦点を当てたキャンペーンが記されている[234,235]。こうした情報に加え、PwCは、2月から7月にかけて、この脅威アクターがFacebookやOffice365のログイン画面に偽装したタイポスクワッティングドメインを確認している。公開情報によれば、この脅威アクターにアトリビューションされているマルウェアサンプルの一部は、中東のIT業界を標的とすることで知られ、Yellow LidercとしてPwCが追跡調査しているイランを拠点とする脅威アクターのものと重複が見られる[236]。

インシデント対応ケーススタディ

White Dev 89

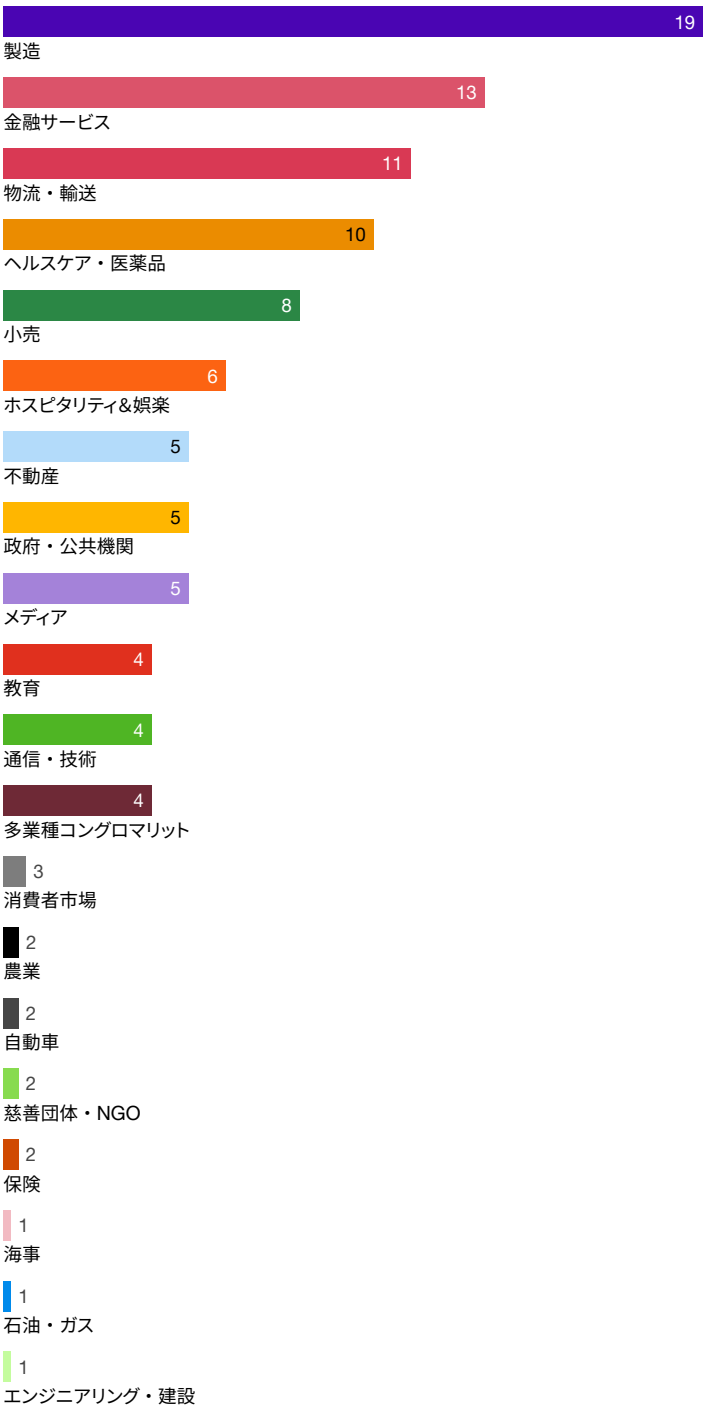
2021年、PwCは、White Dev 89と名付けた脅威アクターが関与する医療機関のインシデント対応調査を支援した。この脅威アクターは、場当たり的に標的を定め、おそらくマルバタイジング（不正広告による感染）キャンペーンを使用して、トロイの木馬を仕組んだZoom、AnyDesk、Windscribeなどのアプリケーションを被害者に提供しようとしたことが観察された。これらは、それぞれの正規のアプリケーションをインストールすると同時に、悪意あるPowerShellスクリプト（おそらくPowerShellEmpireエージェントの修正版）をドロップして実行される。このようにして取得したアクセスにより、脅威アクターは、感染したシステム上で基本的な偵察活動を行うことが可能となった[237]。

White Dev 89が標的とする端末のプロファイリングを完了すると、Cobalt Strike Beaconを展開するための追加のPowerShellスクリプトをドロップしていることが確認された。これにより、SMBを経由したネットワーク上の他のシステムへのラテラルムーブメントなど、さらなる活動が開始される。White Dev 89が使用したその他のラテラルムーブメントのテクニックには、特権アカウントの侵害、標的ネットワークをマッピングするためのADFindやBloodHoundなどのツールの実行、侵入後の7-ZIPとSubInAclの使用などが挙げられる。

この脅威アクターの最終的な目的は明らかではないが、既知の他のキャンペーンとの関連性が見られた。特に、以前QakBotキャンペーンで使用されたインフラとの重複が確認されたため、White Dev 89はQakBotの背後にいる脅威アクターと同一組織であるか、以前QakBotを使用して初期アクセスを行ったことがある組織である、という仮説を立てるに至った。

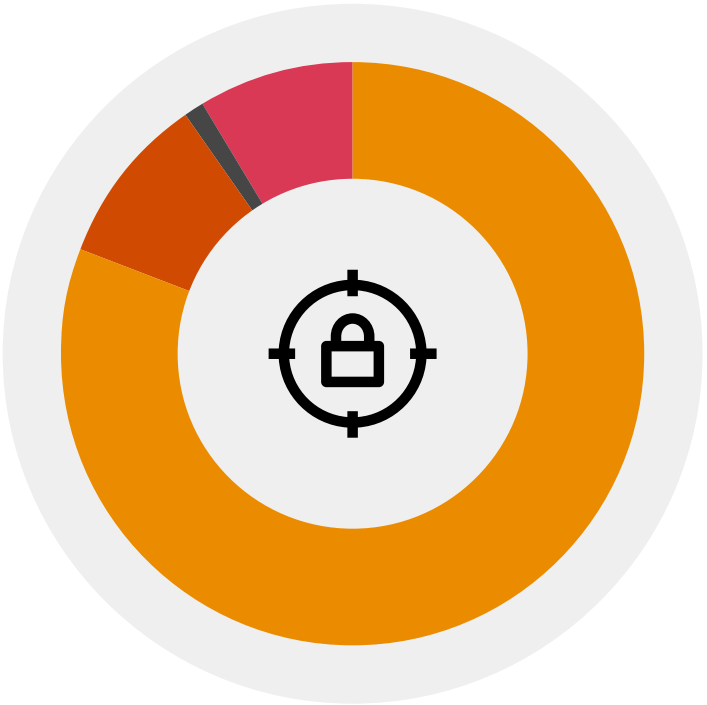
PwCインシデント対応統計

図表28：2021年ランサムウェアインシデント対応事案件数（分野別）



出所：PwC

図表29：2021年インシデント割合（種類別）

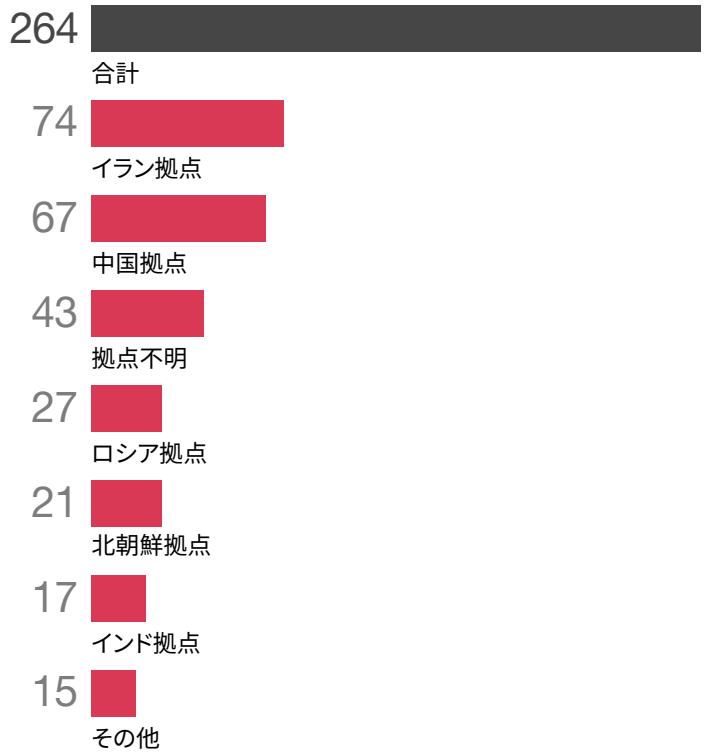


- APT 6, **5.2%**
- 犯罪 92, **77.3%**
- インサイダー 11, **9.2%**
- ハクティビスト 1, **0.8%**
- 不明 9, **7.5%**

出所：PwC

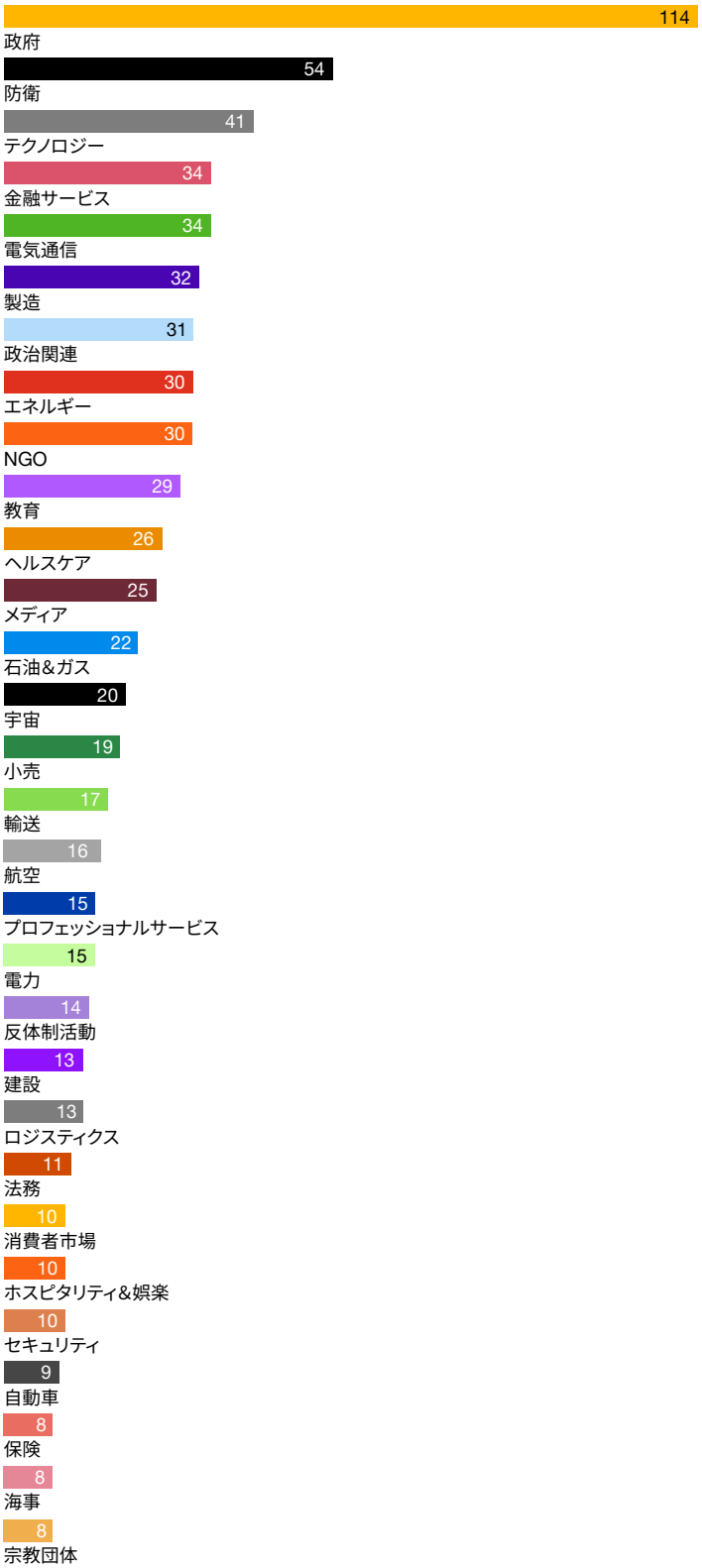
PwC脅威インテリジェンスのレポート統計

図表30：2021年脅威アクター報告数（拠点別）



出所：PwC

図表31：2021年脅威アクター報告数（分野別）



出所：PwC

スポットライト：

産業分野

本セクションでは、2021年に特定業界で観察された主なサイバー脅威を紹介する。

電気通信

2021年、諜報活動を目的とした脅威アクターが電気通信業界に関心を寄せ続けた。例年通り、機密情報収集が目的であったと思われる[238]。PwCは、2カ国を拠点とする脅威アクターによって80社以上の通信事業者が侵害されたと推定している。

本レポートの冒頭で言及したように、Red Menshen（旧Red Dev 18）は、数カ国に拠点を置く通信事業者を含むアジア太平洋地域の複数の組織に対して、カスタマイズしたマルウェアBPFDoorを展開した[239]。

PwCは、電気通信業界を標的とする、Red Kelpie（別名：APT41）を含む中国を拠点とする脅威アクターが、パキスタンを拠点とするプロバイダーに対してローダーマルウェアMotnugを使用したことを観察している[240]。この被害組織は、イランを拠点とする脅威アクターYellow Mora[241]にも狙われたと思われる。2021年初頭、PwCは、南アジア地域の電気通信業界を標的としたYellow Mora（別名：Greenbug）によるキャンペーンを分析した[242]。PwCの分析では、Yellow Moraが被害者の環境に長期間にわたり潜んでいた可能性が高く、この脅威アクターの活動方法に関する公開報告とも一致している[243]。Yellow Nix（別名：Static Kitten、MERCURY、MuddyWater）による同様の活動は、2021年1月に始まり、年間を通じて、中東、南アジア、東南アジア、中央アジアの多数の電気通信組織を標的にしていた[244]。PwCは、これらの標的の選定について、少なくとも部分的には個人をサーベイランスし追跡することを目的としたものと捉えており、これはYellow Mimasのような密接に連携したグループによる同業界への過去の標的の選定とも一致していると評価している[245]。

また、この業界はランサムウェアにも狙われた。例えば、Blue Lelantos社の新しいランサムウェアMacawが米国を拠点とする企業に対して展開された。また、2021年に最も活発なランサムウェア運営組織であるWhite JanusとWhite Apepも、それぞれLockbit 2.0とDarkside／BlackMatterランサムウェアでこの業界の複数の企業を標的にしている。全体として、複数の国営通信会社、およびエクアドルのCorporacion Nacional de Telecomunicacione、Schepisi Communications、スペインのMasMovilなど、有名な民間通信事業者がこの一年間にランサムウェアの被害を受けている。

テクノロジー

革新的テクノロジーは、製品やサービスをコピーしようと企てる組織にとって価値があり、知的財産は常に脅威アクターから狙われる可能性がある。テクノロジー企業自体、特に顧客にサービス（ITやサイバーセキュリティを含む）を提供している場合、サプライチェーン攻撃や「アイランドホッピング」攻撃の標的になる可能性がある。2021年、複数の航空会社（One Star Alliance加盟航空会社やアジア太平洋地域の航空会社を含む）がIT情報サービスの提供を受ける通信技術サプライヤーSITA社への初期侵入によって危険にさらされた[246]。この一連の侵入に関する公開情報の分析[247]では、Red Kelpieが犯人である可能性が高いと指摘されている。また、PwCは、Red Djinnも同様の種類の侵入を試みたことも観察した。この脅威アクターは、おそらくラテラルムーブメントによって標的のメインネットワークに侵入するために日本企業の海外子会社を狙った。

脅威アクターが、悪意あるインフラに関連するSSL証明書にテクノロジー企業の名称を使用していることが確認されている。例えば、中国を拠点とする脅威アクターは、ShadowPadのC2インフラでNVIDIA Corporation[248]の名称を騙った。また、モバイルアプリ企業の証明書で署名されたHyperBroマルウェアのサンプルも確認されている。HyperBroは、中国に拠点を置く複数の脅威アクターの間で共有されている可能性を示唆する証拠があるものの、もとの使用者はRed Phoenix（別名：APT27、Emissary Panda、Lucky Mouse）であることがわかっている。PwCは、このRed Phoenixが特にテクノロジー業界を標的にし続けていること、また少なくとも米国のテクノロジー企業一社に侵害したことを確認した。

サイバー犯罪者によるテクノロジー業界への攻撃も始まっており、AcerはREvilによる2回の攻撃を受けた。このうち、2回目のランサムウェア攻撃では、これまでに公表された中で最高額となる5,000万USドルの身代金要求があったとのことである[249]。

最後に、イスラエルのテクノロジー企業も、White Dev 95に目をつけられていることがわかった（「ハクティビスト」キャンペーンと称している）。PwCはWhite Dev 95について、イスラエルに対して情報工作（IO）を行う、破壊工作を動機とする脅威アクターである可能性が非常に高いと評価している。この脅威アクターは、恐喝目的ではなく、被害者のネットワークを暗号化し、盗んだデータをすぐに流出させるという、「ロック・アンド・リーク」を行うという特徴がある。

金融サービス

金融サービス（FS）業界の組織は、依然としてサイバー犯罪を目的とする脅威アクターにとって価値の高い標的となっている。サイバー犯罪者向けマーケットプレイスである「RaidForums」「XSS」「Exploit」に掲載された情報を3カ月以上分析した結果、金融サービス業界は最も影響を受けた分野のトップ3に常にランクインしている。これは、潜在的な金銭的利益の規模という点で、FSがバイヤーにとってより関心の高い業界であったためと思われる。

以前から存在する組織犯罪グループは、多額の身代金の支払いが見込まれるため、特にFS事業者を標的にする場合がある。例えば、2021年初頭、米国の保険会社CNAは、従業員が偽のブラウザアップデートを実行したことがきっかけで危険にさらされた。この企業は、最終的に身代金4,000万USドルを支払ったと報告されている。2021年5月、ランサムウェアAvaddonの運用組織は、AXAグループのアジア部門に属するデータ（クライアントの個人情報を含む）および機密医療データを流出させ、身代金が支払われない場合はDDoS（分散型DoS）攻撃でAXAのWebサイトを攻撃すると脅した。さらに最近では、2021年11月下旬に、White Austarasが行ったと思われるMirrorBlastキャンペーンが確認され、カナダやフランスを拠点とする保険会社および、米国や香港を拠点とする多くの資産・財産管理会社を標的とすることを示唆するスパムメールが含まれていた[250]。

北朝鮮を拠点とする脅威アクターは、投資やベンチャーキャピタル、暗号通貨取引所（またはその他の暗号通貨取り扱い組織）など、あらゆるFS組織に深刻な脅威を与え続けている。2021年2月の米国司法省による北朝鮮国籍の人物（Black Artemisの一部と思われる）の起訴状には、脅威アクターがトロイの木馬を仕込んだ暗号通貨取引アプリケーションを使って、ニューヨークの金融機関から1,180万USドルを窃取したと記載されている[251]。Black AlicantoとBlack Dev 2は、一貫してFS事業体を標的としており、しばしば標的にスピアフィッシングメールを送信するほか、暗号通貨に関連する、または正規ジョイントベンチャーを装ったおとり文書を使用する場合がある。

小売

2021年、ランサムウェア運用組織は引き続き小売業を標的としている。同業界の業務の性質上、稼働時間を中断することが難しいことを悪用し、被害者に迅速に身代金を支払うよう効果的に圧力をかけている。小売業界の急速なデジタル化によって、ランサムウェア運用組織はエンドポイントの決済システムを麻痺させることが可能になった。これは収入減をもたらすものであり、組織は、標的に対して身代金の要求に応じるようさらに圧力をかけるようになっている。

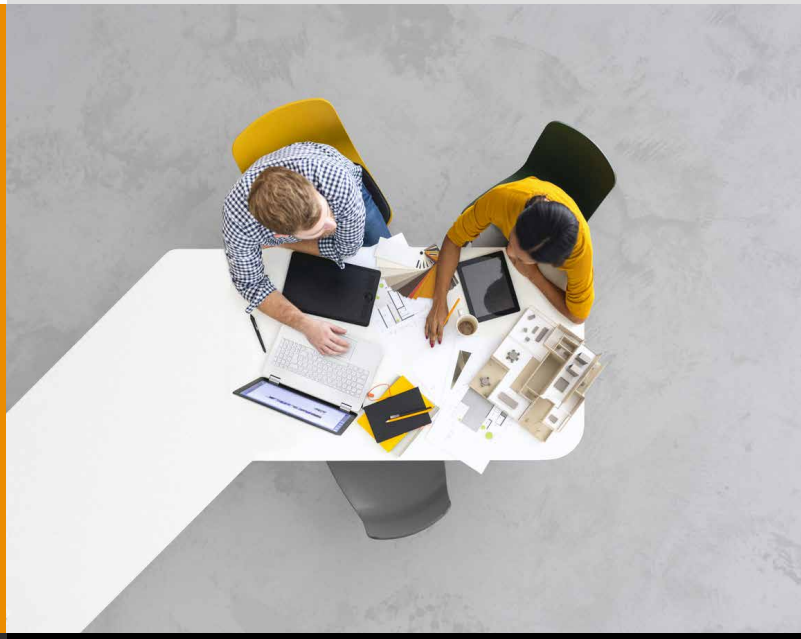
小売業を標的としたランサムウェアの亜種が観察された中で、脅威アクターであるWhite Onibiが運営するContiが最も活発であった。このランサムウェアは、衣料品店から宝石店まで、さまざまな小売業者を標的として、多額の身代金の要求や、固有の機密情報[252,253,254]（White Onibiは2021年にこの情報をオークションにかけた）を窃取することに成功している[255]。

他のランサムウェア運営組織も小売業を標的にしていた。Kaseyaに対するサプライチェーン攻撃の一環として、ITサプライヤーであるVisma EsscomのネットワークにSodinokibiランサムウェアによる攻撃が行われた。Visma Esscomが感染した結果、スウェーデン全土の500店舗以上のCoopストアが、決済システムのオフライン化により閉店を余儀なくされた[256]。別の例では、2021年12月に小売業のSPARがランサムウェアに感染し、英国内の330店舗が場合によっては数日間にわたりオフラインになったことが報告されている。これらのインシデントは2021年の小売業を苦しめ、正常な事業運営を脅かした無数の事例のごく一部にすぎない[257,258,259,260]。

犯罪者向けマーケットプレイスの出品内容を分析したところ、小売企業関連の出品の大半は顧客データを含むものであったが、中には、Eコマースサイト上でのカード決済の支払い先を購入者にリダイレクトする機能を謳うものもあることがわかった（特に「Exploit」フォーラム上の出品）。オンライン販売を展開するブランドにとっては、Magecartと呼ばれるクレジットカードのスキミング行為がいまだに行われていることも忘れてはならない261。ブラックフライデーの販売期間の直前に、英国国家サイバーセキュリティセンター（NCSC）は、4,000以上の中小小売事業者に対して、Magento Eコマースプラットフォームで侵害された決済ポータルを使用していることに注意喚起を行った。

インシデント対応ケーススタディ：

DarkSide - 初期アクセスから身代金要求まで4時間



2021年4月、DarkSide（PwCではWhite Apepとして追跡調査）により実行されたランサムウェア攻撃の被害に遭ったグローバル小売業のクライアントを、複数の国のPwCインシデント対応チームが支援した。

このインシデントを分析した結果、脅威アクターは当初、LogMeInとして知られるリモートアクセスツールを利用して、クライアントのIT資産にアクセスしたことが判明した。このツールは、同組織のITサービスプロバイダーのうち一社が、小売店のワークステーションとサポートシステムのメンテナンス用としてリモートアクセスできるようにするために、合法的な目的で使用されていたものである。初期侵入は、LogMeInソフトウェアの機能を利用したもので、有効な認証情報を持つユーザーは、クライアントの従業員が操作することなくシステムにリモートアクセスすることができるというものであった。

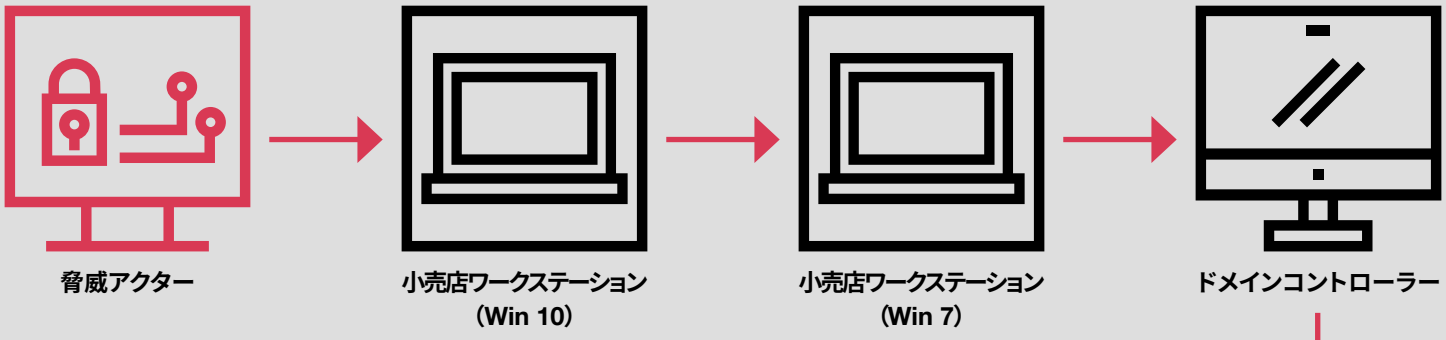
A国の小売店クライアントを侵害した後、脅威アクターは管理ツールをダウンロードし、それを使ってクライアントのネットワーク上で内部偵察を行った。同時に、LSASSのメモリダンプにより、ドメイン全体で使用されているデフォルトの管理者アカウントに特権を昇格させた。この特権を使用して、脅威アクターは、サポート期間が終了し、アップデートされていないB国のシステムに軸足を移した。

脅威アクターは続いてこれらのシステムから収集した認証情報を使用して、ドメイン管理者ユーザーを作成し、そのアカウントのパスワードを脅威アクターのLastPassアカウントで生成して保存した。

脅威アクターは、ドメインコントローラーを侵害すると、スケジュールタスクを作成し、クライアントのITインフラ内の全てのコンピュータに展開し、ランサムウェアをダウンロードして実行するよう命じた。初期侵害からランサムウェアが展開されるまでの時間は、およそ4時間であった。ランサムウェア運用組織は1,200万USドルの身代金を要求したが、クライアントは3週間にわたるインシデント対応と復旧作業を通じて、組織を稼働させるためのマニュアルの業務プロセスを確立することに成功した。

ダークサイド

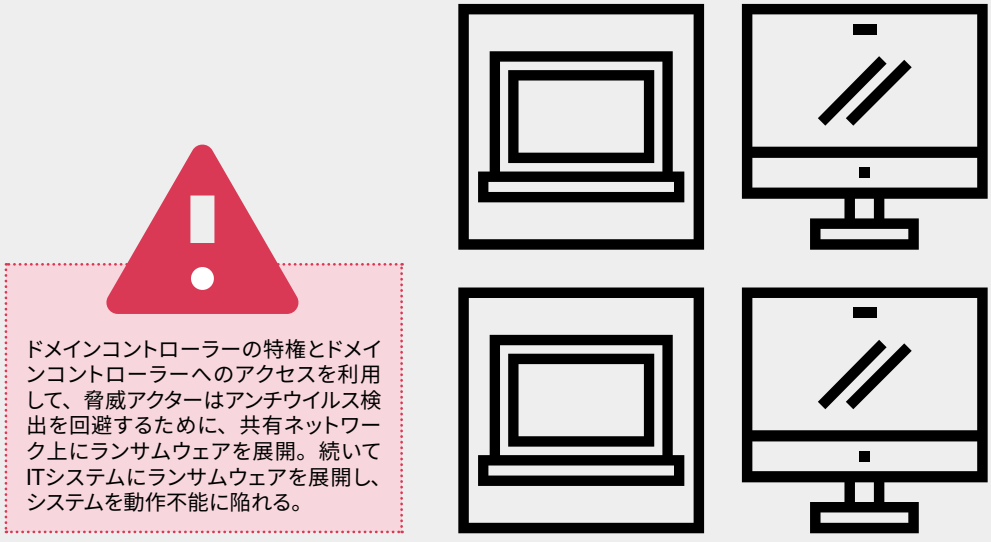
DarkSideー初期アクセスから身代金要求まで4時間



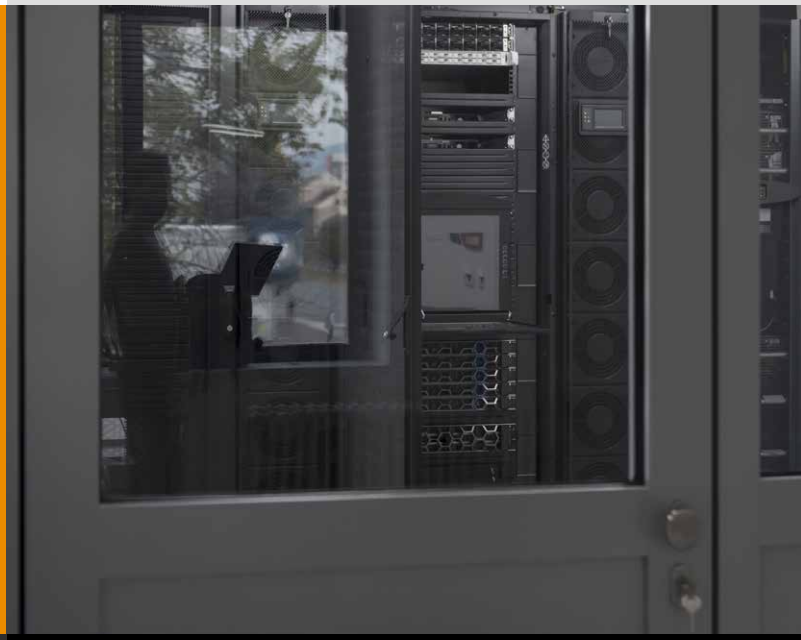
脅威アクターが、クライアントのサービスプロバイダーの正規のRDP認証情報を使用してA国の小売店WSに侵入。

リモート接続に成功した後、脅威アクターはLOLbinsを使用してB国の小売店のワークステーションにラテラルムーブメントを行った。

脅威アクターはパスワードを窃取し、ドメイン管理者権限を取得し、C国のドメインコントローラーへの侵入に成功



ドメインコントローラーの特権とドメインコントローラーへのアクセスを利用して、脅威アクターはアンチウイルス検出を回避するために、共有ネットワーク上にランサムウェアを展開。続いてITシステムにランサムウェアを展開し、システムを動作不能に陥れる。



インシデント対応ケーススタディ：

身代金を要求するShinyHunters

2021年12月、PwCはインドを拠点とする小売業界クライアントのインシデントに対応した。当初、クライアントのクラウドインフラ全体のシステムリソース使用量が急増し、その後、PwCが追跡調査するサイバー犯罪脅威アクターWhite Dev 100（別名：ShinyHunters）から身代金請求メールが届いた。

分析の結果、脅威アクターはまず、この組織の元経営幹部が所有し、その後漏洩したクラウドアクセスキーを使用してネットワークにアクセスしたことが判明。続いて、漏洩した認証情報を使用して、クライアントのインフラへのWebコンソールアクセス権を取得した。しかし、どのインスタンスにもアクセスできず、ネットワークをマッピングするための偵察コマンドを実行した。

この脅威アクターは、新しいインスタンスとSSH鍵を作成し、最終的にそれらをSSH認証鍵ストアに注入することができた。これらの行為とセキュリティグループの変更により、脅威アクターはクライアント環境に自由にSSH接続することが可能になった。さらに、多くの.sshディレクトリにアクセスし、利用可能なプライベートSSHキーを複製して、ラテラルムーブメントをサポートした。この脅威アクターは、ネットワーク内を移動しながら、テストや自動化インスタンスなど、関心あるシステムを特定し、さらなるアクセスのために攻撃をかけた。この間、脅威アクターは、侵害された環境にある複数の端末ウィンドウへのアクセスを維持した。この活動の分析から、複数の運用者が作業を行ったのか、一名による作業だったのか、まだ判断は下せていない。

製造

製造業界にとって、感染したシステムの可用性や完全性に影響をもたらす攻撃は、どのようなものであれ組織にとって重大なリスクとなる。このような攻撃は、操業の一時停止、生産・配送の遅延を引き起こし、収益面の損失を招くだけでなく、修復に多額の費用がかかることから再稼働のハードルも上がる。また、納期の遅れ、サプライヤーとの契約不履行、評判の悪化など、さまざまな問題が発生する。この業界では、不満を持った従業員による機密データの競合他社への販売、巧妙な組織犯罪グループが行うランサムウェア攻撃など、重大かつ標的型の攻撃がますます増加している。

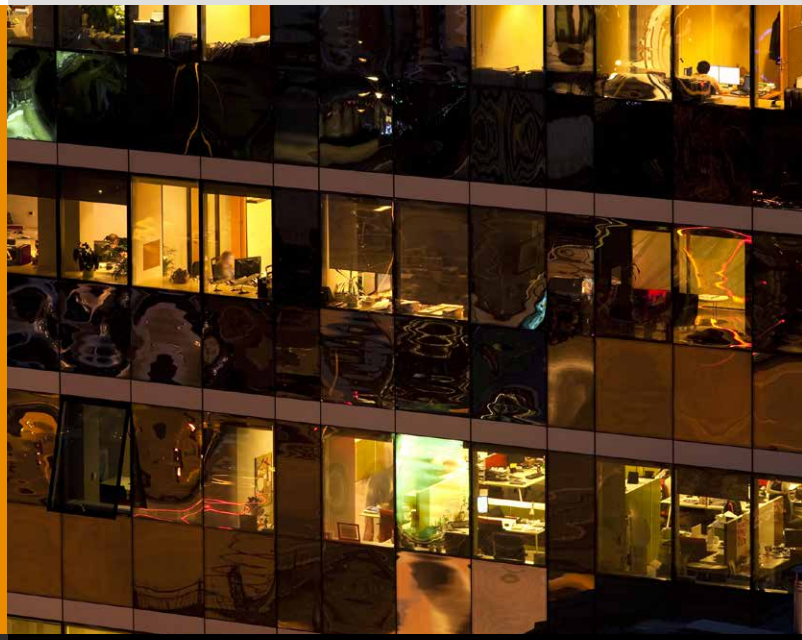
BlackMatterランサムウェアキャンペーンの運営組織は、2021年1月から5月にかけて、製造業界を最大の標的として、一連の高度な攻撃により1,750万ポンド以上に相当するビットコインの支払いを得た[262]。Lockbit 2.0もまた、製造業に大きな焦点を当てており、2021年1月から9月の間に流出したサイトデータの21%は、製造業の被害者が所有していたものである。

ビジネスEメール詐欺（BEC攻撃）は、製造業を含む全ての業界にとって、依然として相当な脅威となっている。2021年、PwCは、ナイジェリアを拠点とするBronze Dev 2（別名：SilverTerrier）が関与する可能性が高いキャンペーンを観察した。この脅威アクターは、製造業界の組織を対象に、緊急予算文書を装った悪意あるファイルを添付したスピアフィッシングメールを送り、リモートアクセス型トロイの木馬（RAT）AgentTeslaを配信したのである。

製造業では、諜報活動が依然として盛んであり、防衛や航空宇宙産業のクライアントと関係があることから、インテリジェンス収集を目的とした脅威アクターが高い関心を寄せている。さらに、この業界全体にわたり行われている技術投資は、新たな関心の高まりをもたらすと思われる。2021年4月、Black Artemisは、求人募集を装った、武器化したおとり文書をあるメーカーに配信し、被害者ネットワークに悪意あるペイロードを展開させた263。諜報攻撃を受けてしまった場合、すでに競争が激しい国際市場において優位性を失うだけでなく、保有する個人情報にアクセスされた場合には、規制上の罰則を受ける恐れもある。

インシデント対応ケーススタディ：

LockBitに直面する製造系多国籍企業



2021年3月、PwCは工業製造業界のある多国籍企業に影響を与えたランサムウェアインシデントに対応した。これは、LockBit運営組織が10カ国のサーバーとワークステーションでランサムウェアを実行したというケースである。

インシデントの分析と調査により、2020年第4四半期から、脅威アクターがクライアントに関する情報を収集し、攻撃の準備を開始していたことが明らかとなった。初期アクセス後、脅威アクターは、ファイルホストサービスのMEGAを使用してマルウェアをダウンロードし、Web検索を行い、感染したシステムの位置と性質を把握した。その後、脅威アクターはネットワークスキャンツール（Softperfect Network Scanner）をダウンロードして実行し、侵害されたアカウントを使用して、一般的なツール（Mimikatzなど）によりラテラルムーブメントを実行した。

その後、米国内のドメインコントローラーに侵入し、さらに米国内の別のサーバーに移動し、2021年3月には日本のドメインコントローラーを利用してランサムウェアを配布している。

攻撃の最後の瞬間、脅威アクターはクライアントのアンチマルウェアソリューションを操作し、ランサムウェアを停止させないようにした上で、最終的にランサムウェアを配布し実行した。この攻撃は、被害組織に大きな混乱をもたらしたが、データの流出を示す明確な証拠はなかった。

結論

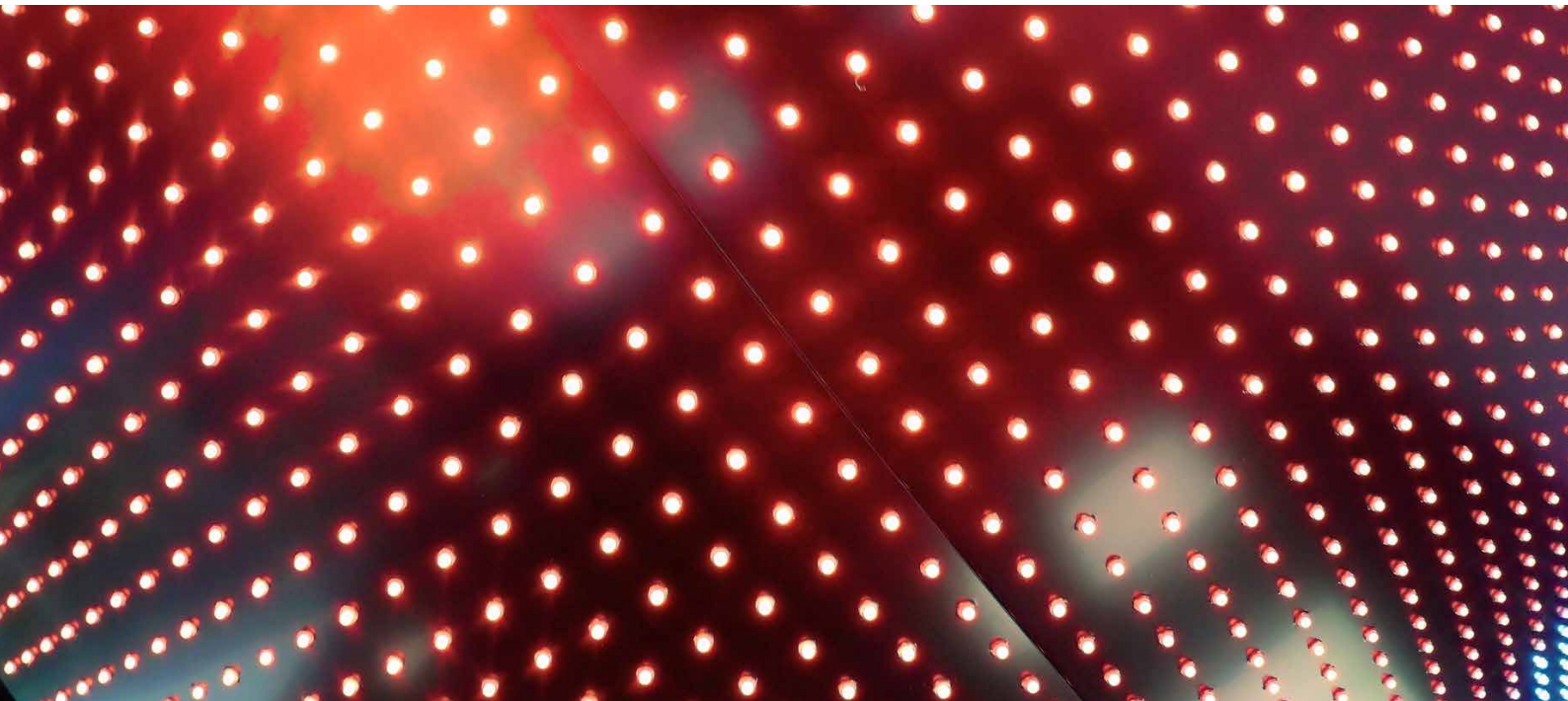
2021年のサイバー脅威状況は、さまざまな動機とスキルレベルを有する脅威アクターが増加し続けた1年であった。

近年同様、ランサムウェアは、世界中のあらゆる規模・業界の組織に最も広く浸透し、短期間で影響を与える脅威であった。そして、ランサムウェア開発者はアフィリエイトスキームの規模、収益、能力を拡大し続けている。サプライチェーンへの攻撃は、今やサイバー脅威の「ニューノーマル」の一部と化しており、サイバー犯罪を目的とする脅威アクターは、最大の効果を得るために、サプライチェーンをその戦略に組み込んでいる。

同時に、デジタルクォーターマスター（これまで国家主導の活動に加担してきた組織と、高性能の攻撃ツールや能力をさまざまなクライアントに提供する民間のブローカーの両方）の隆盛とその影響力により、安全なデジタル社会に対する別のタイプの脅威が浮き彫りとなっている。

これら全ての脅威は、ゼロデイ脆弱性に改めて焦点が当てられることによって頂点に達した。いくつかの事例ではゼロデイ脆弱性によって標的型攻撃と大規模無差別攻撃の両方が可能になった。また、金銭的・戦略的動機の高まりにより、エクスプロイトの研究開発活動が促進されている。

PwCは、2021年に浮上した、あるいは継続したテーマ―ランサムウェアとそれを取り巻く犯罪エコシステム、脆弱性とツールのブローカーの重要性、新たに発見された脆弱性が備えの足りない被害者にもたらす影響などは、2022年も継続すると評価している。脆弱性やインシデントが紙面を賑わすようになり、サイバーセキュリティに対する世間の注目はこれまでになく高まっている。そして、防御者が組織や社会との協力、共有、支援を継続していくこと―予防・検出対策や、脅威アクターを効果的に阻止することが可能なインシデントの軽減・対応計画や予防・検出対策に注力することがより一層重要となっている。



PwC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、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企業として、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）、レッドチーム編成、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支えています。

PwCは、戦略的思考、強力な技術力、そして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筋道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、検出および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、世界各地の公共・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。

巻末脚注

1. ‘2021 has broken the record for zero-day hacking attacks’, MIT Technology Review: Patrick Howell O’Neill, https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/ (23rd September 2021)
2. ‘New German government coalition promises not to buy exploits’, Recorded Future, https://therecord.media/new-german-government-coalition-promises-not-to-buy-exploits/ (8th December 2021)
3. Full (vulnerability) disclosure’, PwC Threat Intelligence, CTO-SIB-20210810-01A
4. ‘Play evil games, win evil prizes’, PwC Threat Intelligence, CTO-SIB-20210625-01A
5. Google, ‘Project Zero’, https://googleprojectzero.blogspot.com/
6. ‘Shining a light on ShadowPad usage throughout 2019’, PwC Threat Intelligence, CTO-TIB-20200213-01A
7. ‘Chasing Shadows’, PwC Threat Intelligence, CTO-TIB-20211021-01A
8. ‘My, My, MySSL tracking C2 infrastructure through certificate reuse’, PwC Threat Intelligence, CTO-TIB-20210226-01B
9. ‘HAFNIUM exploiting Exchange vulnerabilities’, PwC Threat Intelligence, CTO-QRT-20210303-01A
10. ‘HAFNIUM targeting Exchange Servers with 0-day exploits’, Microsoft, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ (2nd March 2021)
11. ‘Operation Exchange Marauder: Active Exploitation of Multiple 0-day Microsoft Exchange Vulnerabilities’, Volexity: Josh Grunzweig, Matthew Meltzer, Sean Koessel, Steven Adair, Thomas Lancaster, https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-0-day-vulnerabilities/ (2nd March 2021)
12. ‘Eat, Sleep, Liderc, Repeat’, PwC Threat Intelligence, CTO-TIB-20210730-01A
13. ‘Caught in a .NET’, PwC Threat Intelligence, CTO-TIB-20210211-02A
14. ‘Cyber Threats 2020: A Year in Retrospect’, PwC Threat Intelligence
15. ‘A closer look at commercial quartermasters’, PwC Threat Intelligence, CTO-SIB-20210906-01A
16. ‘Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus’, Citizen Lab, https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/ (15th July 2021)
17. ‘Protecting customers from a private-sector offensive actor using 0-day exploits and DevilsTongue malware’, Microsoft, https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/ (15th July 2021)
18. ‘How we protect users from 0-day attacks’, Google, https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/ (14th July 2021)
19. ‘Another commercial quartermaster’, PwC Threat Intelligence, CTO-TIB-20210806-02A
20. ‘Another commercial quartermaster’, PwC Threat Intelligence, CTO-TIB-20210806-02A
21. ‘A closer look at commercial quartermasters’, PwC Threat Intelligence, CTO-SIB-20210906-01A
22. ‘FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild’, CitizenLab: Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, Ron Deibert, https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/ (13th September 2021)
23. ‘A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution’, Google Project Zerolan Beer & Samuel Groß, https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html (15th December 2021)
24. ‘Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities’, United States Commerce Department, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list (3rd November 2021)
25. ‘You Only Click Twice: FinFisher’s Global Proliferation’, CitizenLab: Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ (13th March 2013)
26. ‘FinSpy: Unseen Findings’, Kaspersky, https://securelist.com/finspy-unseen-findings/104322/ (28th September 2021)
27. ‘Exclusive: An American Company Fears Its Windows Hacks Helped India Spy On China And Pakistan’, Forbes: Thomas Bewster, https://www.forbes.com/sites/thomasbrewster/2021/09/17/exodus-american-tech-helped-india-spy-on-china/?sh=13286ba07009 (17th September 2021)
28. ‘Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community’, CitizenLab: Masashi Crete-Nishihata, Jakub Dalek, Etienne Maynier, John Scott-Railton, https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/ (30th January 2018)
29. ‘Red Dev Redemption’, PwC Threat Intelligence, CTO-TIB-20210202-01A
30. ‘Red Dev Redemption 2’, PwC Threat Intelligence, CTO-TIB-20210223-01A
31. ‘Red Dev Redemption 3’, PwC Threat Intelligence, CTO-TIB-20210401-01A
32. ‘“LuoYu”: The eavesdropper sneaking in multiple platforms’, Team T5: Leon & Shui, https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf (28th January 2021)
33. ‘Red Dev 7 gets a Nue name’, PwC Threat Intelligence, CTO-TIB-20201016-01A
34. ‘APT trends report Q2 2017’, Kaspersky, https://securelist.com/apt-trends-report-q2-2017/79332/ (8th August 2017)
35. ‘LootRAT deals four of a kind’, PwC Threat Intelligence, CTO-TIB-20200130-02A
36. ‘Threats under the Spotlight: February 2021’, PwC Threat Intelligence, CTO-TUS-20210317-01A
37. ‘Malware WinDealer used by LuoYu Attack Group’, JPCERT: Yuma Masubuchi, https://blogs.jpcert.or.jp/en/2021/10/windealer.html#1 (26th October 2021)
38. ‘Threats under the Spotlight: April 2021’, PwC Threat Intelligence, CTO-TUS-20210511-01A
39. ‘White Dev 75, like shooting phish in a barrel’, PwC Threat Intelligence, CTO-TIB-20210303-01A
40. ‘New White Dev 75 infrastructure’, PwC Threat Intelligence, CTO-TIB-20211015-01A
41. ‘’When Best Practice Isn’t Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users’, Amnesty, https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/ (19th December 2018)
42. ‘Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa’, Amnesty International, https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/ (16th August 2019)
43. ‘Yellow Garuda’s VIP Telegram tool’, PwC Threat Intelligence, CTO-TIB-20220110-01A

44. UNC788: IRAN'S DECADE OF CREDENTIAL HARVESTING AND SURVEILLANCE OPERATIONS, VB2021 localhost, https://vblocalhost.com/uploads/VB2021-Haeghebaert.pdf (October 2021)
45. 'A fresh bouquet of malware', PwC Threat Intelligence, CTO-TIB-20210511-02A
46. 'Lockbit 2.0', PwC Threat Intelligence, CTO-TIB-20211027-02A
47. CTO-TIB-20211209-01A - Nothing else BlackMatters, CTO-TIB-20210827-01A - How to be a ransomware operator
48. 'Economy of the United States by sector', Wikipedia, https://en.wikipedia.org/wiki/Economy_of_the_United_States_by_sector
49. https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html
50. 'Department of Justice Launches Global Action Against NetWalker Ransomware', US Department of Justice, https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware, 27th January 2021
51. 'Babuk - A new kid on the block', PwC Threat Intelligence, CTO-TIB-20210201-02A
52. 'Ransomware gang leaks data from Metropolitan Police Department', BleepingComputer: Sergiu Glatan, https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-from-metropolitan-police-department/ (11th May 2021)
53. 'DarkSide', PwC Threat Intelligence, CTO-QRT-20210512-01A
54. 'Hackers Breached Colonial Pipeline Using Compromised Password', Bloomberg: William Turton, Kartikay Mehrotra, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password (4th June 2021)
55. 'Ransomware Attack on Health Sector - UPDATE 2021-05-16', Ireland National Cybersecurity Centre, https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf (16th May 2021)
56. 'JBS: Cyber-attack hits world's largest meat supplier', BBC, https://www.bbc.co.uk/news/world-us-canada-57318965 (2nd June 2021)
57. 'Kaseya supply chain compromise', PwC Threat Intelligence, CTO-QRT-20210703-01A
58. 'Important Notice August 4th, 2021', Kaseya, https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-August-4th-2021 (4th August 2021)
59. 'Treasury Takes Robust Actions to Counter Ransomware', US Department of Treasury, https://home.treasury.gov/news/press-releases/jy0364, 21st September 2021
60. 'Ukrainian Arrested and Charged with Ransomware Attack on Kaseya', US Department of Justice, https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya, 8th November 2021
61. 'Ransomware gets more ban for its buck', PwC Threat Intelligence, CTO-SIB-20210525-01A
62. 'DarkSide', PwC Threat Intelligence, CTO-QRT-20210512-01A
63. 'Understanding REvil: The Ransomware Gang Behind the Kaseya VSA Attack', Palo Alto Unit 42: John Martineau, https://unit42.paloaltonetworks.com/revil-threat-actors/ (6th July 2021)
64. 'QakBot – a dip into the pond', PwC Threat Intelligence, CTO-TIB-20200515-02A
65. 'Egregor Meet the new boss', PwC Threat Intelligence, CTO-TIB-20201203-01A
66. 'Rezident evil: Dridex indictments', PwC Threat Intelligence, CTO-SIB-20200102-01A
67. 'WastedLocker - EvilCorp's new smoking gun', PwC Threat Intelligence, CTO-TIB-20200730-01A
68. 'New World, New Macaw', PwC Threat Intelligence, CTO-QRT-20211117-01A
69. 'A new DoppelPaymer', PwC Threat Intelligence, CTO-TIB-20200710-01A
70. 'Causing more Grief', PwC Threat Intelligence, CTO-TIB-20211028-01A
71. 'Darkside Ransomware Decryption Tool', Bitdefender, https://www.bitdefender.com/blog/labs/darkside-ransomware-decryption-tool/ (11th January 2021)
72. 'Darkside', PwC Threat Intelligence, CTO-QRT-20210512-01A
73. 'DarkSide, Blamed for Gas Pipeline Attack, Says It is Shutting Down' New York Times, https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html (14th May 2021)
74. 'Nothing else BlackMatters', PwC Threat Intelligence, CTO-TIB-20211209-01A
75. 'Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice', US Department of State, https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/ (4th November 2021)
76. 'Moscow court arrests all REvil ransomware hackers detained after FBI request to Russia', TASS, https://tass.com/russia/1388649 (15th January 2022)
77. 'Exploitation of Accellion File Transfer Appliance', Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/uscert/ncas/alerts/aa21-055a, 24th February 2021
78. 'Accellion Provides Update to FTA Security Incident Following Mandiant's Preliminary Findings', Accellion, https://www.globenewswire.com/news-release/2021/02/22/2179666/0/en/Accellion-Provides-Update-to-FTA-Security-Incident-Following-Mandiant-s-Preliminary-Findings.html (22nd February 2021)
79. 'Kaseya supply chain compromise', PwC Threat Intelligence, CTO-QRT-20210703-01A
80. 'Emotet is back', PwC Threat Intelligence, CTO-QRT-20211116-01A
81. 'World's most dangerous malware Emotet disrupted through global action', Europol, https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action (18th November 2021)
82. 'How the new Emotet differs from previous versions', Intel 471, "https://intel471.com/blog/emotet-returns-december-2021", 9th December, 2021
83. 'Colder than IcedID', PwC Threat Intelligence, CTO-TIB-20210511-01A
84. 'AaaS you like it', PwC Threat Intelligence, CTO-SIB-202108802-01A
85. 'Report of the Panel of Experts established pursuant to resolution 1874 (2009)', United Nations Security Council, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf (30th August 2019)
86. 'All LNKs lead back to Black Dev 1 Part 1', PwC Threat Intelligence, CTO-TIB-20210408-01A
87. 'All LNKs lead back to Black Dev 1 Part 2', PwC Threat Intelligence, CTO-TIB-20210525-01A
88. 'Who is Black Alicanto hiring', PwC Threat Intelligence, CTO-TIB-20210913-01A
89. 'All LNKs lead back to Black Dev 1 Part 1', PwC Threat Intelligence, CTO-TIB-20210408-01A
90. 'Unveiling the Cryptomimic', NTT Security: Hajime Takai, Shogo Hayashi, Rintaro Koike https://vb2020.vblocalhost.com/uploads/VB2020-Takai-etal.pdf (2020)
91. 'Lazarus Group Campaign Targets Cryptocurrency Vertical', F-Secure, https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf (18th August 2020)
92. 'Attributing Attacks Against Crypto Exchanges to LAZARUS – North Korea', ClearSky, https://www.clearskysec.com/wp-content/uploads/2021/05/CryptoCore-Lazarus-Clearsky.pdf (May 2021)
93. 'Capital injection', PwC Threat Intelligence, CTO-TIB-20210630-03A
94. 'Bitcoin is silver, compromise is gold: Emerging North Korea-based threat actors on the hunt for cryptocurrency', PwC: Sveva Vittoria Scenarelli, https://www.youtube.com/watch?v=BOZecjABjSk

95. ‘The Banshee, The Flower, The Dragon and Prince’, PwC Threat Intelligence, CTO-TIB-20210508-01A
96. ‘North Korean attackers use malicious blogs to deliver malware to high-profile South Korean targets’, Cisco Talos: Jung soo An, Asheer Malhotra, Kendall McKay, https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html (10th November 2021)
97. ‘Nuclear Policy For BabySharks’, PwC Threat Intelligence, CTO-TIB-20211014-01A
98. ‘Cyber Threats 2020: A Year in Retrospect’, PwC Threat Intelligence (2020)
99. ‘Your dream job awaits - just please enable editing’, PwC Threat Intelligence, CTO-TIB-20210916-01A
100. ‘Paint me like one of your BMP files’, PwC Threat Intelligence, CTO-TIB-20210428-01A
101. ‘New campaign targeting security researchers’, Google, https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/ (25th January 2021)
102. ‘ZINC attacks against security researchers’, Microsoft, https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/ (28th January 2021)
103. ‘North Korean Hackers Caught Snooping on China’s Cyber Squad’, The Daily Beast: Shannon Vavra, https://www.thedailybeast.com/north-korean-hackers-caught-snooping-on-chinas-cyber-squad (22nd November 2021)
104. @ESETresearch, Twitter, https://twitter.com/ESETresearch/status/1458438155149922312?s=20 (10th November 2021)
105. ‘China’s 5-year plan has 7 technology targets’ watch for responses’, S&P Global, https://www.spglobal.com/marketintelligence/en/newsinsights/latest-news-headlines/china-s-5-year-plan-has-7-technology-targets-watch-for-responses-63161384 (15th March 2021)
106. ‘BlackTechs ELF-esteem’, PwC Threat Intelligence, CTO-TIB-20210329-01A
107. ‘BlackTech’s Gh0st’, PwC Threat Intelligence, CTO-TIB-20201113-01A
108. ‘Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors’, Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt (29th September 2020)
109. ‘Red Djinn’s red flags’, PwC Threat Intelligence, CTO-TIB-20210903-02B
110. ‘Back to Black(Tech): an analysis of recent BlackTech and an open directory full of exploits’, PwC: Sveva Vittoria Scenarelli, Adam Prescott, https://vblocalhost.com/conference/presentations/back-to-blacktech-an-analysis-of-recent-blacktech-operations-and-an-open-directory-full-of-exploits/ (7th October 2021)
111. ‘Red Djinns spider web’, PwC Threat Intelligence, CTO-TIB-20211202-01A
112. ‘NICKEL targeting government organizations across Latin America and Europe’, Microsoft, https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/ (6th
113. ‘Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity’, US CISA, https://us-cert.cisa.gov/ncas/alerts/aa20-258a (24th October 2020)
114. ‘A committee of vultures’, PwC Threat Intelligence, CTO-SIB-20210722-01A
115. ‘Okrum and Ketrican: An Overview of Recent Ke3chang Group Activity’, ESET, July 2019, https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf
116. ‘BfV Cyber-Brief Nr. 01/2021 - Bedrohung deutscher Stellen durch Cyberangriffe der Gruppierung APT31’, Bundesamt für Verfassungsschutz, https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-cyberabwehr/broschuere-2021-01-bfv-cyber-brief-2021-01 (18th January 2021)
117. ‘Red Keres flows into South East Asia’, PwC Threat Intelligence, CTO-TIB-20210211-01A
118. ‘Learning to ChaCha with Red Kelpie’, PwC Threat Intelligence, CTO-TIB-20210624-02A
119. ‘Active exploitation of CVE-2021-26084’, PwC Threat Intelligence, CTO-QRT-20210906-01A
120. ‘This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits’, Mandiant, https://www.mandiant.com/resources/apt41-initiates-globalintrusion-campaign-using-multiple-exploits (25th March 2020)
121. ‘Seven International Cyber Defendants, Including “Apt41” Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally’, US Department of Justice, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer (16th September 2020)
122. ‘Introducing Red Dev 14’, PwC Threat Intelligence, CTO-TIB-20210412-01A
123. Mandiant, ‘Advanced Persistent Threat Groups’, https://www.mandiant.com/resources/apt-groups
124. ‘Learning to ChaCha with Red Kelpie’, PwC Threat Intelligence, CTO-TIB-20210624-02A
125. ‘ShadowPad not a dead cert’, PwC Threat Intelligence, CTO-TIB-20211116-02A
126. ‘Inside a Red toolbox’, PwC Threat Intelligence, CTO-TIB-20210518-01A
127. ‘Orange Kala enters the Warzone’, PwC Threat Intelligence, CTO-TIB-20210112-01A
128. ‘Compromising Eurasian Telecoms justforfun’, PwC Threat Intelligence, CTO-TIB-20210709-01A
129. ‘A Window into Red Dev 18’, PwC Threat Intelligence, CTO-TIB-20210831-02A
130. ‘Of Gh0sts and Golang’, PwC Threat Intelligence, CTO-TIB-20211011-01A
131. ‘Red Dev 18 Further Developments’, PwC Threat Intelligence, CTO-QRT-20210727-01A
132. ‘Batch scripts back alright’, PwC Threat Intelligence, CTO-TIB-20210223-02A
133. ‘Orange Kala or Orange Dev 1 - you decide’, PwC Threat Intelligence, CTO-TIB-20210520-01A
134. ‘BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps’, Blackberry Cylance, https://www.blackberry.com/us/en/forms/enterprise/bahamut-report (October 2020)
135.135. ‘The White Company: Inside the Operation Shaheen Espionage Campaign’, Cylance, https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/ knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf (18th March 2021)
136. ‘BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps’, Blackberry Cylance, https://www.blackberry.com/us/en/forms/enterprise/bahamut-report (October 2020)
137. ‘Sharing is Caring’, PwC Threat Intelligence, CTO-TIB-20210818-01A
138. ‘Confucius APT deploys Warzone RAT’, Uptycs: Abhijit Mohanta, Ashwin Vamshi, https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat (12th January 2021)
139. ‘Warzone RAT – Beware of the Trojan malware stealing data triggering from various Office documents’, Quickheal: Ayush Puri, https://blogs.quickheal.com/warzonerat-beware-of-the-trojan-malware-stealing-data-triggering-from-various-office-documents/ (1st July 2021)
140. ‘Monsoon – Analysis of an APT campaign’, Forcepoint https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysisreport.pdf
141. ‘Cyber Threats 2020: A Year in Retrospect’, PwC Threat Intelligence
142. ‘Orange Athos has BADNEWS for its adversaries’, PwC Threat Intelligence, CTO-TIB-20210204-02A
143. ‘Threats under the Spotlight October 2021’, PwC Threat Intelligence, CTO-TUS-20211118-01A

144. ‘Orange Yali continues to set up shop in Pakistan’, PwC Threat Intelligence, CTO-TIB-20210527-02A
145. ‘Operation “Magichm”: CHM file release and subsequent operation of BITTER-organization’, QiAnXin, https://ti.qianxin.com/blog/articles/%22operationmagichm%22:CHM-file-release-and-subsequent-operation-of-BITTER-organization/ (15th March 2021)
146. ‘Windows kernel 0-day exploit (CVE-2021-1732) is used by BITTER APT in targeted attack’, DBAPPSecurity, https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/windows-kernel-0-day-exploit-is-used-by-bitter-apt-in-targeted-attack/ (10th February 2021)
147. ‘0-day vulnerability in Desktop Window Manager (CVE-2021-28310) used in the wild’, Kaspersky: Boris Larin, Costin Raiu, Brian Bartholomew, https://securelist.com/0-day-vulnerability-in-desktop-window-manager-cve-2021-28310-used-in-the-wild/101898/ (13th April 2021)
148. ‘APT trends report Q2 2021’, Kaspersky, https://securelist.com/apt-trends-report-q2-2021/103517/ (29th July 2021)
149. ‘CrimsonRAT - Green Havildars premium export’, PwC Threat Intelligence, CTO-TIB-20210310-02A
150. ‘Transparent Tribe APT Infrastructure Mapping Part 1: A High-Level Study of CrimsonRAT Infrastructure October 2020 – March 2021’, Team Cymru: Joshua Picolet, https://team-cymru.com/blog/2021/04/16/transparent-tribe-apt-infrastructure-mapping/ (16th April 2021)
151. ‘Transparent Tribe APT Infrastructure Mapping Part 2: A Deeper Dive into the Identification of CrimsonRAT Infrastructure October 2020 – June 2021’, Team Cymru: Joshua Picolet, https://team-cymru.com/blog/2021/07/02/transparent-tribe-apt-infrastructure-mapping-2/ (2nd July 2021)
152. ‘Aggah Using Compromised Websites to Target Businesses Across Asia, Including Taiwan Manufacturing Industry’, Anomali, https://www.anomali.com/blog/aggahusing-compromised-websites-to-target-businesses-across-asia-including-taiwan-manufacturing-industry (12th August 2021)
153. ‘Cyber Threats 2020: A Year in Retrospect’, PwC Threat Intelligence
154. ‘Threats under the Spotlight - December 2020’, PwC Cyber Threat Intelligence, CTO-TUS-20210111-01A
155. ‘Not Enough Mana to Conduct that Operation’, PwC Threat Intelligence, CTO-TIB-20210630-02A
156. ‘针对性伪装攻击，终端信息安全的间谍--海莲花 APT’, Sangfor, https://mp.weixin.qq.com/s/WnKc0JbjA5_lsjPFSzFoYA (31st March 2021)
157. ‘RotaJakiro: A long live secret backdoor with 0 VT detection’, 360 Netlab, https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/ (28th April 2021)
158. ‘Youre not Shikata Ga Nai believe this’, PwC Threat Intelligence, CTO-TIB-20211102-02A
159. ‘Whose campaign is it anyway’, PwC Threat Intelligence, CTO-TIB-20211121-01A
160. ‘Ransomware or sabotage, that is the question’, PwC Threat Intelligence, CTO-SIB-20210927-01A
161. ‘Ransomware or sabotage, that is the question’, PwC Threat Intelligence, CTO-SIB-20210927-01A
162. ‘Whose campaign is it anyway’, PwC Threat Intelligence, CTO-TIB-20211121-01A
163. ‘New Version Of Apostle Ransomware Reemerges In Targeted Attack On Higher Education’, SentinelOne, https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/#:~:text=New%20Version%20Of%20Apostle%20Ransomware%20Reemerges%20In%20Targeted%20Attack%20On%20Higher%20Education,-Amitai%20Ben%20Shushan&text=SentinelLabs%20has%20been%20tracking%20the,destructive%20attacks%20starting%20December%202020. (30th September 2021)
164. ‘Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021’, Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/ (16th November 2021)
165. ‘Sharp dressed threat actor’, PwC Threat Intelligence, CTO-TIB-20211222-02A
166. ‘Pay2Key to N3tw0rm’, PwC Threat Intelligence, CTO-TIB-20210513-01A
167. ‘Missed connections’, PwC Threat Intelligence, CTO-TIB-20210216-01A
168. ‘A blast from the past’, PwC Threat Intelligence, CTO-TIB-20210622-01A
169. ‘Scanning the internet for vulnerabilities’, PwC Threat Intelligence, CTO-TIB-20211118-01A
170. ‘The mysteries of Pay2Key’, PwC Threat Intelligence CTO-SIB-20210113-01A
171. ‘The [redacted] sheds light on a campaign’, PwC Threat Intelligence, CTO-TIB-20210712-01A
172. ‘White Dev 75, like shooting phish in a barrel’, PwC Threat Intelligence, CTO-TIB-20210303-01A
173. ‘Yellow Maeros Art Attack’, PwC Threat Intelligence, CTO-TIB-20210226-02A
174. ‘New job, same malware’, PwC Threat Intelligence, CTO-TIB-20210806-01A
175. ‘The [redacted] sheds light on a campaign, PwC Threat Intelligence, CTO-TIB-20210712-01A
176. ‘The [redacted] sheds light on a campaign, PwC Threat Intelligence, CTO-TIB-20210712-01A
177. ‘I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona’, Proofpoint, https://www.proofpoint.com/us/blog/threat-insight/iknew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media (28th July 2021)
178. ‘Of course Im real....’, PwC Threat Intelligence, CTO-SIB-20210818-01A
179. ‘Eat, Sleep, Liderc, Repeat’, PwC Threat Intelligence, CTO-TIB-20210730-01A
180. ‘Iran-based threat actor responses to rising geopolitical tensions’, PwC Threat Intelligence, CTO-SIB-20200108-01A
181. ‘Taking Action Against Hackers in Iran’, Meta, https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/ (15th July 2021)
182. ‘Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021’, Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021 (16th November 2021)
183. ‘Yellow Nix shifts south east’, PwC Threat Intelligence, CTO-TIB-20211015-03A
184. ‘Yellow Nix has a complaint’ ,PwC Threat Intelligence, CTO-TIB-20211216-02A
185. ‘New Iranian Espionage Campaign By “Siamesekitten” – Lyceum’, ClearSky, https://www.clearskysec.com/siamesekitten (17th August 2021)
186. ‘Finding Yellow Dev 9, PwC Threat Intelligence, CTO-TIB-20211028-02A
187. ‘Lyceum calling’, PwC Threat Intelligence, CTO-TIB-20200605-01A
188. ‘Get your shine on Yellow Garuda’, PwC Threat Intelligence, CTO-TIB-20210514-01A
189. ‘Only if your invited’, PwC Threat Intelligence, CTO-QRT-20210907-01A
190. ‘A fresh bouquet of malware’, PwC Threat Intelligence, CTO-TIB-20210511-02A
191. ‘Charming Kittens Telegram bot’, PwC Threat Intelligence, CTO-TIB-20210909-01A
192. ‘Alert (AA20-304A) Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data’, US CISA, https://us-cert.cisa.gov/ncas/alerts/aa20-304a
193. ‘Learning on the job with Yellow Dev 19’, PwC Threat Intelligence, CTO-TIB-20201118-02A
194. ‘Learning on the job with Yellow Dev 19’, PwC Threat Intelligence, CTO-TIB-20201118-02A
195. ‘Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election’, United States Department of the Treasury, https://home.treasury.gov/news/press-releases/jy0494 (18th November 2021)
196. ‘New leaks and possible IRGC links’, PwC Threat Intelligence, CTO-SIB-20210809-01A

197. ‘Scanning the internet for vulnerabilities’, PwC Threat Intelligence, CTO-TIB-20211118-01A
198. ‘Scanning the internet for vulnerabilities’, PwC Threat Intelligence, CTO-TIB-20211118-01A
199. ‘Scanning the internet for vulnerabilities’, PwC Threat Intelligence, CTO-TIB-20211118-01A
200. ‘Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021’, Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021 (16th November 2021)
201. ‘Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021’, Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021 (16th November 2021)
202. ‘StrongPity APT Group Deploys Android Malware for the First Time’, Trend Micro, https://www.trendmicro.com/en_us/research/21/g/strongpity-apt-group-deploysandroid-malware-for-the-first-time.html (21st July 2021)
203. ‘Threats under the Spotlight November 2021’, PwC Threat Intelligence, CTO-TUS-20211203-01A
204. ‘Taking Action Against Arid Viper’, Facebook, https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf (April 2021)
205. ‘Hiding in plain sight’, PwC Threat Intelligence, CTO-TIB-20211126-01A
206. ‘Phishing in the Middle East’, PwC Threat Intelligence, CTO-TIB-20210629-02A
207. ‘WIRTE’s campaign in the Middle East ‘living off the land’ since at least 2019’, Kaspersky, https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-theland-since-at-least-2019/105044/ (29th November 2021)
208. ‘Elections in Palestine – on the campaign trail’ , PwC Threat Intelligence, CTO-TIB-20191216-02A
209. ‘There’s a (Houdini)RAT in the Embassy’, PwC Threat Intelligence, CTO-TIB-20191112-01A
210. Note: we do not currently cluster Blue Dev 5 activity with the same threat actor that conducted the SolarWinds activity, which we track as Blue Nova, due to differences in observed TTPs.
211. The UK NCSC assessed it is highly likely this actor was Russia’s Foreign Intelligence Service (SVR).
212. ‘UK and US call out Russia for SolarWinds compromise’, NCSC, https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise (15th April 2021)
213. Blue Nova targeted Mimecast to gain access to the keys used to authenticate service accounts to victim mail servers, as well as targeting the software developed by SolarWinds.
214. ‘Blue Dev 5 - The Roots of Targeting’, PwC Threat Intelligence, CTO-TIB-20210608-01A
215. ‘ Blue Dev 5 - Mysteries of Foreign Affairs’, PwC Threat Intelligence, CTO-TIB-20210527-01A
216. “NobleBaron | New Poisoned Installers Could Be Used In Supply Chain Attacks”, Volexity, https://www.sentinelone.com/labs/noblebaron-new-poisoned-installerscould-be-used-in-supply-chain-attacks/ (1st June 2021)
217. ‘(Darth) Vladars under attack Part 1’, PwC Threat Intelligence, CTO-TIB-20210310-01A
218. ‘Bosnia is in danger of breaking up, warns top international official’, The Guardian, https://www.theguardian.com/world/2021/nov/02/bosnia-is-in-danger-of-breakingup-warns-eus-top-official-in-the-state (2nd November 2021)
219. ‘MINISTARSTVO UNUTRAŠNJIH POSLOVA REPUBLIKE SRPSKE’, Republika Srpska Ministry of Interior, https://mup.vladars.net/lat/index.php?vijest=vtk&id=23325&vrsta=aktuelnosti (24th April 2020)
220. ‘(Darth) Vladars under attack Part 2’, PwC Threat Intelligence, CTO-TIB-20210423-01A
221. ‘(Darth) Vladars under attack Part 3’, PwC Threat Intelligence, CTO-TIB-20210903-01A
222. ‘Hunting Blue Odin Servers’, PwC Threat Intelligence, CTO-TIB-20211215-01A
223. ‘Recent Cloud Atlas activity’ Kaspersky, https://securelist.com/recent-cloud-atlas-activity/92016/ (12th August 2019)
224. ‘Exploring Blue Odin’, PwC Threat Intelligence, CTO-TIB-20210308-01A
225. ‘The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies’, NCCC, https://www.rnbo.gov.ua/en/Diialnist/4823.html (24th February 2021)
226. ‘The NCCC at the NSDC of Ukraine has updated information on cyberattacks on the document management system of state bodies’, NCCC, https://www.rnbo.gov.ua/en/Diialnist/4824.html (25th February 2021)
227. ‘Inside the ASKOD Compromise’, PwC Threat Intelligence, CTO-TIB-20210319-01A
228. ‘SBU finds hacker hunting for personal information of employees’, Security Service of Ukraine, https://ssu.gov.ua/en/novyny/sbu-vyiavyla-khakera-yakyi-poliuvav-napersonalni-dani-spivrobitnykiv-sluzhby (23rd April 2021)
229. ‘ SSU identifies FSB hackers responsible for over 5,000 cyber attacks against Ukraine’, Security Service of Ukraine, https://ssu.gov.ua/en/novyny/sbu-vstanovylakhakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy (4th November 2021)
230. ‘Ukraine discloses identity of Gamaredon members, links it to Russia’s FSB’, The Record: Catalin Cimpanu, https://therecord.media/ukraine-discloses-identity-ofgamaredon-members-links-it-to-russias-fsb/ (4th November 2021)
231. ‘Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare’, Looking Glass Cyber, https://web.archive.org/web/20190921173500/https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf (28th April 2015)
232. ‘Blue Otsos Armageddon’, PwC Threat Intelligence, CTO-SIB-20211210-01A
233. ‘ReconHellcat Uses NIST Theme as Lure To Deliver New BlackSoul Malware’, QuoIntelligence, https://quointelligence.eu/2021/01/reconhellcat-uses-nist-theme-aslure-to-deliver-new-blacksoul-malware/ (6th January 2021)
234. ‘Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms’, Cybereason, https://www.cybereason.com/blog/operation-ghostshell-novel-rattargets-global-aerospace-and-telecoms-firms (6th October 2021)
235. ‘Iran-linked DEV-0343 targeting defense, GIS, and maritime sectors’, Microsoft, https://www.microsoft.com/security/blog/2021/10/11/iran-linked-dev-0343-targetingdefense-gis-and-maritime-sectors/ (11th October 2021)
236. ‘Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks’, Symantec, https://symantec-enterprise-blogs.security.com/blogs/threatintelligence/tortoiseshell-apt-supply-chain (18th September 2019)
237. ‘A Zoom call with White Dev 89’, PwC Threat Intelligence
238. ‘Cyber Threats 2020: A Year in Retrospect’, PwC Threat Intelligence
239. ‘Compromising Eurasian Telecoms, justforfun’, PwC Threat Intelligence, CTO-TIB-20210709-01A
240. ‘Learning to ChaCha with Red Kelpie’, PwC Threat Intelligence, CTO-TIB-20210624-02A
241. ‘Yellow Mora is listening’, PwC Threat Intelligence, CTO-TIB-20210426-01A
242. ‘Yellow Mora is listening’, PwC Threat Intelligence, CTO-TIB-20210426-01A
243. ‘Sophisticated Espionage Group Turns Attention to Telecom Providers in South Asia’, Symantec, https://symantec-enterprise-blogs.security.com/blogs/threatintelligence/greenbug-espionage-telco-south-asia (19th May 2020)

244. ‘Yellow Nix working overtime remotely’, PwC Threat Intelligence, CTO-TIB-20210309-01A
245. ‘Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry’, US Department of the Treasury, https://home.treasury.gov/news/press-releases/sm1127 (17th September 2020)
246. ‘Global Cyber Bulletin - June 2021’, PwC Threat Intelligence, CTO-GCB-20210706-01A
247. ‘Big airline heist: APT41 likely behind a third-party attack on Air India’, Group-IB: Nikita Rostovcev, https://blog.group-ib.com/colunmtk_apt41 (10th June 2021)
248. ‘ShadowPad not a dead cert’, PwC Threat Intelligence, CTO-TIB-20211116-02A
249. ‘Acer confirms second cyber attack in 2021’, ZDNet: Jonathan Greig, https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/ (14th October 2021)
250. ‘Well its been a MirrorBlast’, PwC Threat Intelligence, CTO-TIB-20211025-01A
251. ‘Billion Dollar Baby’, PwC Threat Intelligence, CTO-SIB-20210322-01A
252. ‘Conti ransomware rakes in over $25 million in just four months’, Acronis, https://www.acronis.com/en-us/cyber-protection-center/posts/conti-ransomware-rakes-inover-25-million-in-just-four-months/ (23rd November 2021)
253. ‘Retailer Fat Face Pays $2 Million Ransom to Conti Gang’, Bank Info Security, https://www.bankinfosecurity.com/retailer-fat-face-pays-2-million-ransom-to-contigang-a-16277 (26th March 2021)
254. ‘Graff multinational jeweller hit by Conti gang. Data of its rich clients are at risk, including Trump and Beckham’, Security Affairs, https://securityaffairs.co/wordpress/123980/cyber-crime/conti-ransomware-graff-jeweller.html (31st October 2021)
255. ‘Conti Ransom Gang Starts Selling Access to Victims’, Krebs on Security, https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/ (25th October 2021)
256. ‘Coop supermarket closes 500 stores after Kaseya ransomware attack’, Bleeping Computer, https://www.bleepingcomputer.com/news/security/coop-supermarketcloses-500-stores-after-kaseya-ransomware-attack/ (3rd July 2021)
257. ‘Hundreds of SPAR stores forced to shut following a major cyber incident’, Teiss, https://www.teiss.co.uk/spar-supermarket-cyber-incident/ (13th December 2021)
258. ‘NCSC statement on cyber incident affecting Spar stores’, NCSC, https://www.ncsc.gov.uk/news/spar-stores-incident (10th December 2021)
259. ‘ Canadian retailer Home Hardware hit by ransomware’, ITWorld Canada, https://www.itworldcanada.com/article/canadian-retailer-home-hardware-hit-byransomware/445416 (2nd April 2021)
260. ‘Office Depot parent expects over $20M loss due to malware attack’, Retail Dive, https://www.retaildive.com/news/office-depot-parent-expects-over-20m-loss-dueto-malware-attack/597544/ (30th March 2021)
261. ‘The many tentacles of Magecart Group 8’, Malwarebytes: Jérôme Segura, https://blog.malwarebytes.com/threat-intelligence/2021/09/the-many-tentacles-ofmagecart-group-8/ (13th September 2021)
262. ‘Nothing else BlackMatters’, PwC Threat Intelligence, CTO-TIB-20211209-01A
263. ‘Your dream job awaits, just please enable editing’, PwC Threat Intelligence, CTO-TIB-20210916-01A

日本による支援

関連サービス
サイバーインテリジェンス

www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting/cyber-intelligence.html

昨今のサイバー攻撃は、愉快犯・経済犯に留まらず国家が関与する諜報活動などにおいても、攻撃背景の複雑化や攻撃手法の高度化といった傾向が強まっています。

企業は、地政学リスクを起因とした高度なサイバー攻撃に対応するため、「攻撃者の意図・能力を分析・把握する」「自組織に起こり得る脅威を予測する」「予測の蓋然性を評価し、対策を講じる」といったサイバーインテリジェンスに基づいた取り組みが求められています。

PwCは、日本に特化した技術分析情報、セキュリティ有識者による非公開の人的情報、ソーシャルメディア、ダークウェブ、ディープウェブなどの公開情報を活用し、サイバーインテリジェンスを提供します。

サイバーインテリジェンスでは、対象となる企業組織、同業界、日本地域に向けられたサイバー攻撃の傾向を分析して脅威シナリオを提供することに加え、企業特性に応じた対策の提言や実施の実現を支援します。PwCが提供するサイバーインテリジェンスは、以下の3つを特長としています。

1. **日本ならびに日本企業に特化したインテリジェンスの提供**
   PwCグローバルネットワークによる海外のサイバー脅威情報の共有に加え、PwC独自の情報網により、日本国内のサイバー攻撃動向に関する情報を収集します。グローバルの縮図としての脅威ではなく、日本という地域・日本企業に特化したインテリジェンスを提供します。

2. **クライアント組織の内部特性に合わせたインテリジェンスの提供**
   脅威と自組織の関係性を把握して対応の必要性を判断し、有効なアクションにつなげるためには、脅威情報の収集段階において、組織外部からの情報だけでなく、組織内部の情報を含めて十分に分析する必要があります。PwCは、入念な調査によって対象企業の組織内部の情報を収集・理解した上で分析を行い、実際のアクションに結び付く意思決定に役立つインテリジェンスを提供します。

3. **インテリジェンスをアクションにつなげ、対策実現を支援**
   クライアントの組織構成や事業内容、海外子会社を含むサプライチェーンといったビジネス環境を理解した上で分析を実施します。攻撃リスクに対する事業へのインパクト、組織のガバナンス状況などに応じた具体的な対策を提案し、実現を支援します。

日本のお問い合わせ先

PwC Japanグループ
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 リーダー
上席執行役員パートナー
林 和洋

ディレクター
村上 純一

www.pwc.com/jp

本報告書は、PwCメンバーファームが2022年5月に発行した『Cyber Threats 2021: 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。 www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html
日本語版発刊年月：2022年8月　　管理番号：I202205-10