2023 年版中間脅威レポート

脅威情勢の把握

www.deepinstinct.com/ja

目次

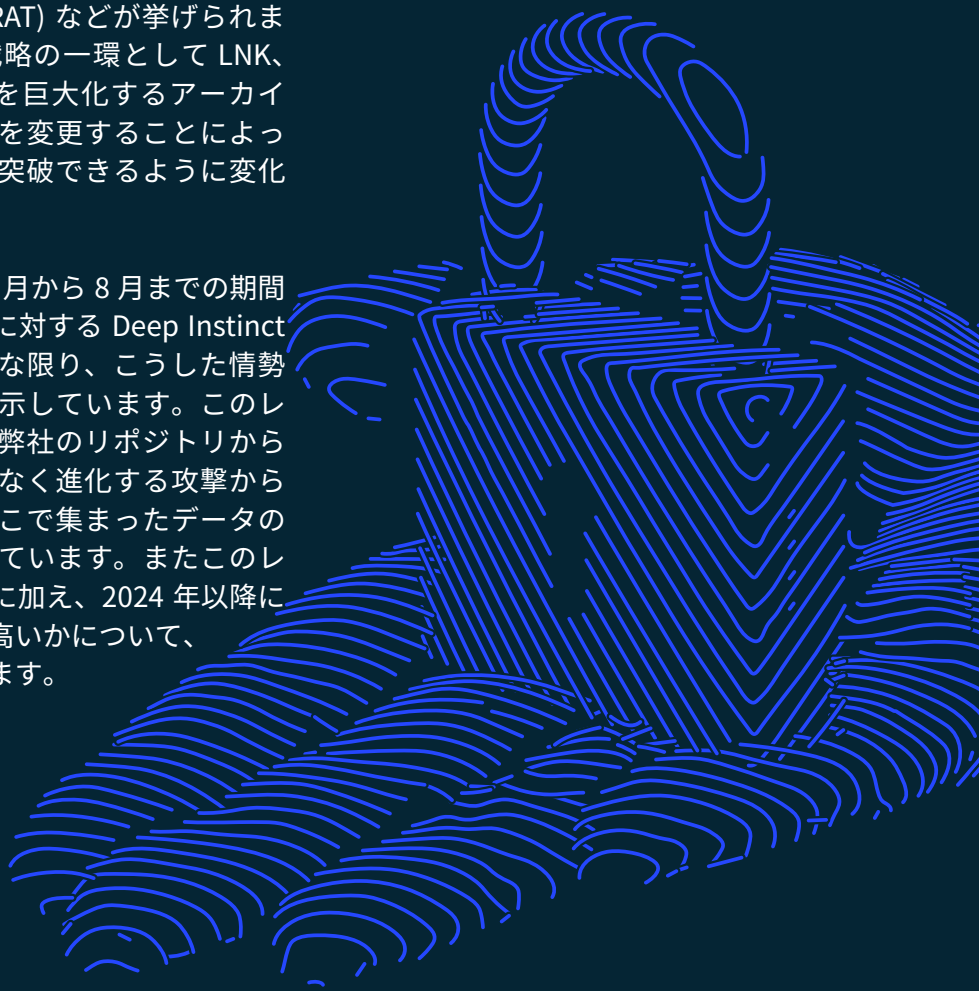
はじめに

Deep Instinct のサイバー脅威中間レポートをご覧いただきありがとうございます。このレポートでは、2024 年に向けて認識しておくべき、2023 年に起きた最も重大なサイバー脅威と全体的な動向についてご紹介します。年間を通していくつかの大きな進展が見られましたが、最も懸念すべき動向の 1 つが RaaS (Ransomware-as-a-Service) の急増です。LockBit のアフィリエイト プログラムの開始から BlackCat の最新のファミリーでの新たな言語の追加まで、RaaS が及ぼす影響およびその規模はランサムウェア ギャングにとって非常に魅力的なものとなっています。

ロシアとウクライナの戦争が続く中、国家の支援を受けているサイバー攻撃は進化しています。サイバー犯罪ギャングはさまざまな理由から分裂と再編成を繰り返しますが、Conti の各分派は活動開始当初から特に注目を集めてきました。犯罪ギャングによる適応は組織構造だけにとどまりません。ベンダーがマルウェアに対する抵抗力を強化するためにソフトウェア スイートに変更を加えてきたように、ギャングも主要なマルウェアを進化させてきました。

このような進化の例として、ほぼすべての情報窃盗マルウェアと遠隔ウイルス (RAT) などが挙げられます。これらは、マルウェア戦略の一環として LNK、HTML、JS、およびファイルを巨大化するアーカイブを採用して配布メカニズムを変更することによって、引き続き従来型の防御を突破できるように変化しました。

このレポートでは、2023 年 1 月から 8 月までの期間に確認された脅威情勢と動向に対する Deep Instinct の現在の見解と、さらに可能な限り、こうした情勢を裏付ける具体的なデータを示しています。このレポートに記載された情報は、弊社のリポジトリから得たものです。弊社は絶え間なく進化する攻撃からお客さまを保護しており、そこで集まったデータのリポジトリを定期的に解析しています。またこのレポートでは、現在の脅威情勢に加え、2024 年以降にどのように発展する可能性が高いかについて、タイムリーな見通しを提供します。



2023 年上半期の主なマルウェアの動向

ランサムウェアの動向

2023 年のランサムウェアの被害件数は、2022 年に比べて大幅に増加しています。実際、2023 年上半期の被害件数は、すでに 2022 年の年間の被害件数を上回っています。図 1 からわかるように、2023 年には、Zimbra や MOVEit の脆弱性など、一度に大量の被害者に影響を及ぼす大規模なキャンペーンでよく使用される脆弱性によって被害件数が急増する現象が複数回発生しています。

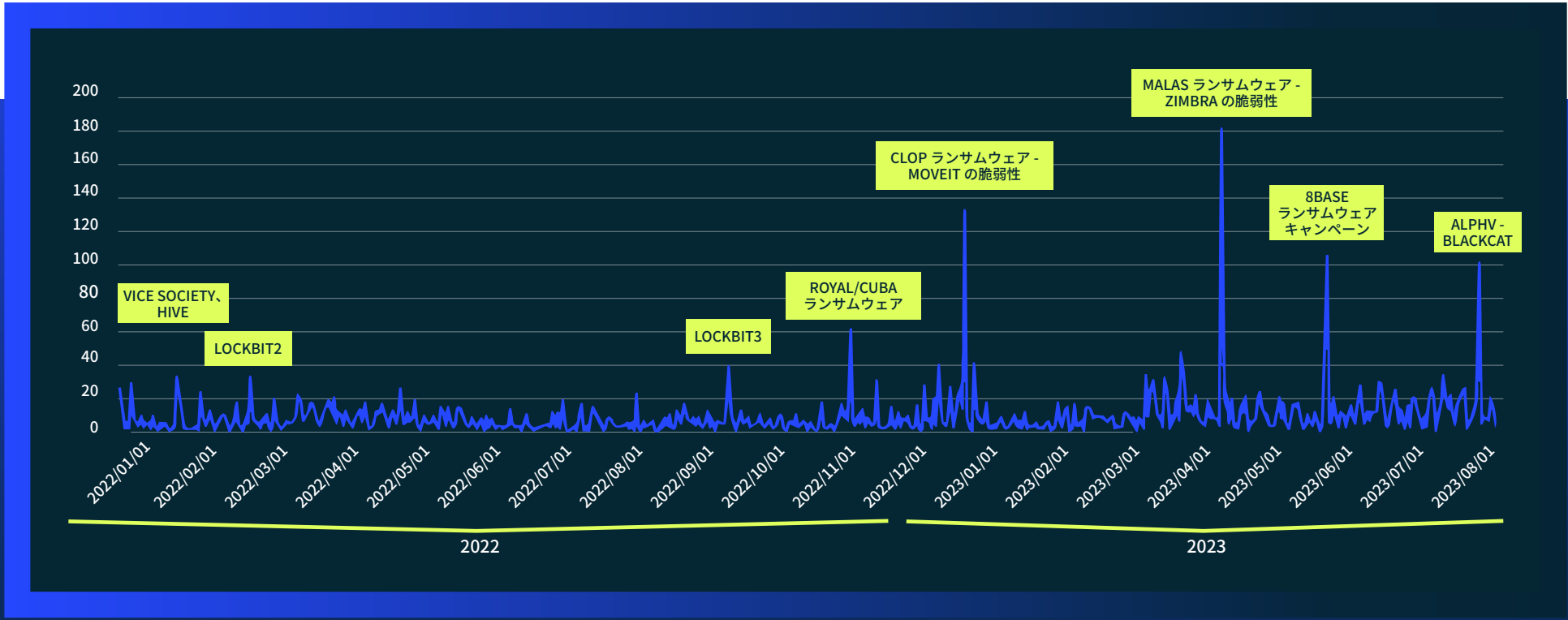


図 1：2022 年～ 2023 年のランサムウェアの被害者

2023 年上半期と 2022 年上 / 下半期の比較

前回の中間レポートでは、予測として大規模なランサムウェア キャンペーンに言及しました。図 1 と図 2 からわかるように、どの期間を比較しても、ランサムウェア運用者は工夫を重ねて被害件数の記録を更新しています。

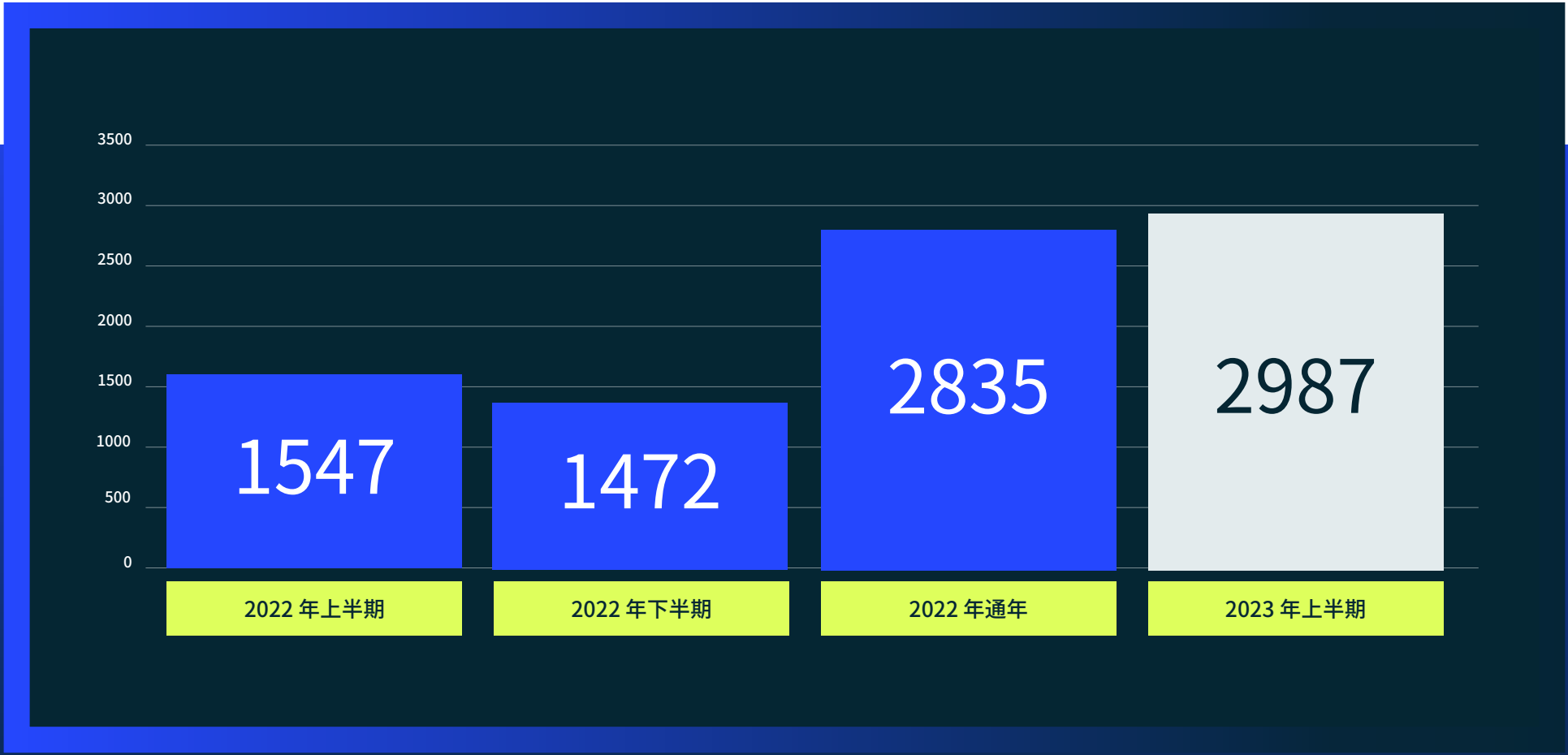


図 2 : 2022 年と 2023 年のランサムウェアの被害件数の比較

ランサムウェア攻撃者

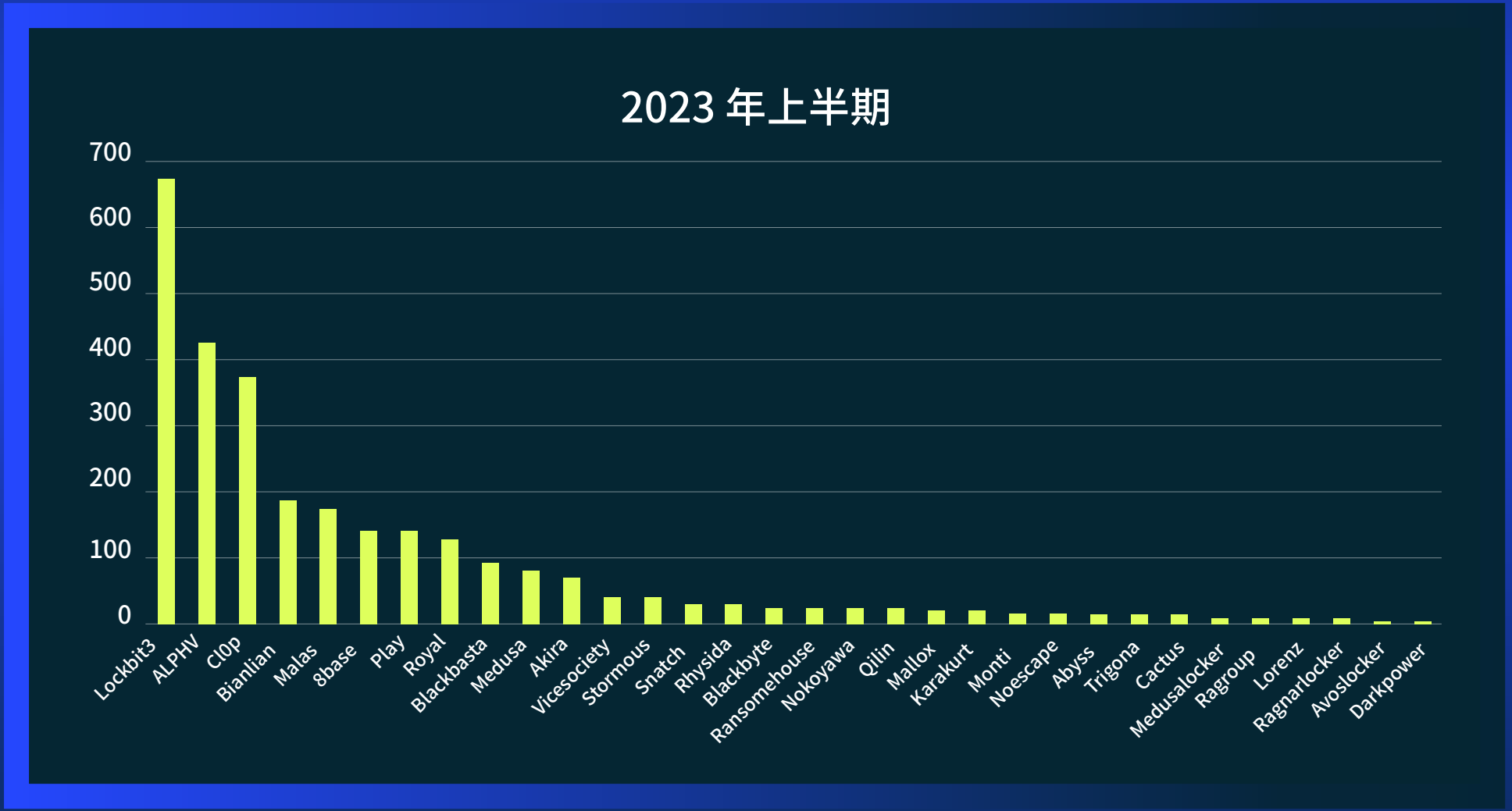


図 3 : 2023 年の脅威グループ別のランサムウェア被害件数

ファミリー別ランサムウェアと活動の概要

01 LOCKBIT

2020 年 1 月、Lockbit はアフィリエイト プログラムを開始し、RaaS として提供することを発表しました。また、ロッカーの開発には 2019 年 9 月から着手していたと言及しています。

サービス提供開始の約 1 年後、2021 年に LockBit はバージョン 2.0 にアップグレードしました。地下フォーラムでの広告によると、これは当時「世界最速の暗号化ソフトウェア」であったそうです。追加された新たな機能には、ネットワーク プリンターで身代金要求文を印刷するオプション、自動的にシャドウ コピーを削除し、ログを消去するオプションなどがありました。また、WoL (Wake-on-LAN) を使用して電源が切れているコンピュータの電源を投入するオプションも含まれていました。

さらに 1 年の運用後、LockBit は「LockBit Black」と呼ばれるバージョン 3.0 の開発を進めていることを発表しました。2022 年 7 月には LockBit 3.0 の最初の攻撃が報告されており、LockBit は最速のランサムウェアであるとのアピールを続け、そのソフトウェアを使用するアフィリエイトを引き付けています。

02 ALPHV

BlackCat (別名 AlphaVM または AlphaV) は、Rust プログラミング言語で作成され、RaaS モデルで運用されているランサムウェア ファミリーです。

BlackCat は主にサードパーティのフレームワークやツールセット (Cobalt Strike など) を介して配布され、侵入地点として無防備で脆弱なアプリケーション (Microsoft Exchange Server など) を悪用します。BlackCat には、Windows と Linux の両方のオペレーティング システムおよび VMware ESXi 環境で動作する亜種があります。

BlackCat は大半の攻撃で、BlackMatter 流出ツールを使用して被害者のデータを持ち出します。身代金が支払われないと、持ち出したデータを公開するか、独自のデータ漏洩サイトで販売します。

BlackCat は、成功したランサムウェア攻撃で稼いだ金の大半をアフィリエイトと内部関係者に還元するため、人気を集め続けています。

03 CLOP

主に Cl0p として知られるこのランサムウェアは、さまざまな業種や組織を標的としてデータを強奪し、多額の身代金を要求します。Cl0p は、新しいキャンペーンを取り入れて活発に進化しています。Cl0p ランサムウェアは、主に RaaS として展開されるロシアの脅威グループ TA505 に関連しています。この脅威グループは、MOVEit Transfer の最新のエクスプロイトなど、さまざまなゼロデイ エクスプロイトをキャンペーンに使用しています。

このランサムウェアは、元々は Cryptomix ランサムウェアであり、2019 年以降では初めての出現でした。FBI の最重要指名手配リストに載っているこのグループのリーダーは、連絡手段として主に自身の Twitter (X) アカウント "ransomboris" を使用しています。最近、Cl0p は、漏洩サイトのテイクダウンを回避するために、torrent を使用してデータを漏洩させるようになりました。

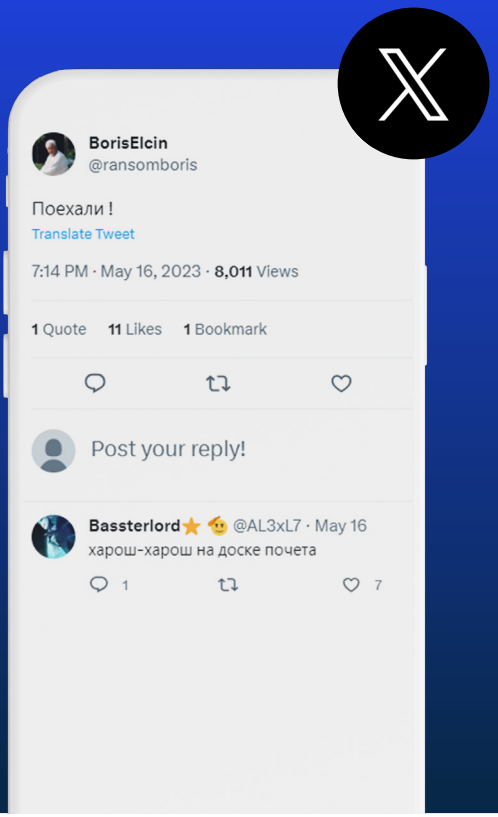


図 4 : Clop ランサムウェアのメンバーが米国での複数の大規模なキャンペーンを実行して FBI に指名手配された後に投稿した「さあ、行くぞ !」というツイート

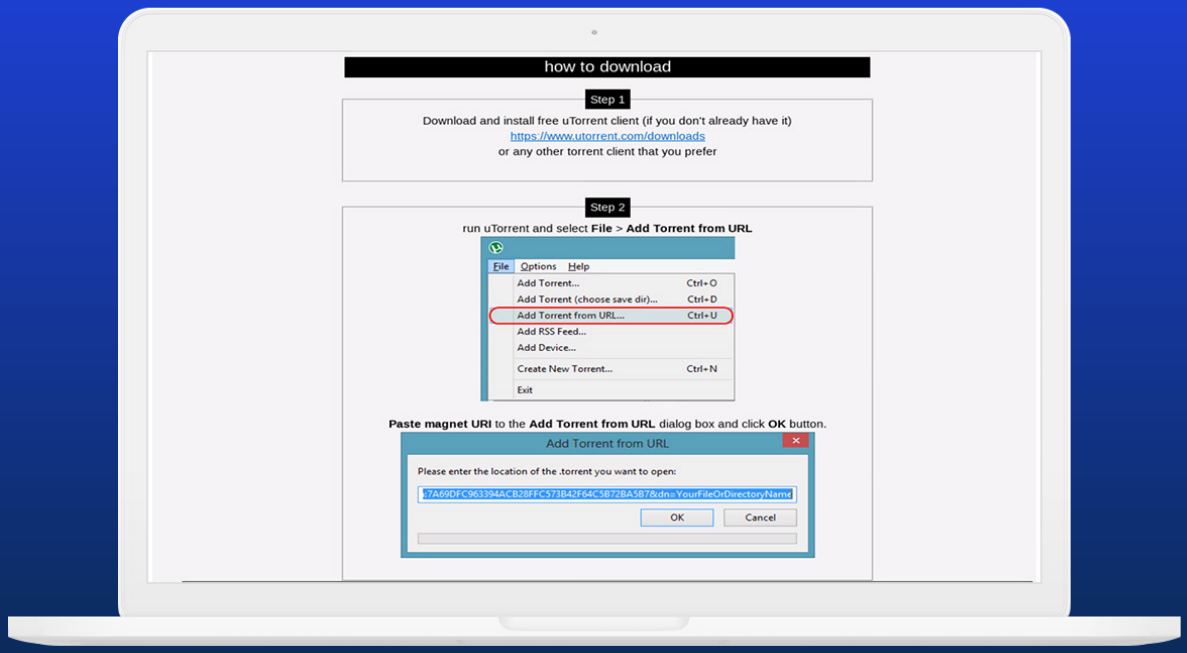


図 5 : Clop による torrent を使用したデータ漏洩

04 BIANLIAN

BianLian は、ランサムウェアの開発、展開、およびデータ強奪を行っているサイバー犯罪グループであり、2022 年 6 月以降、米国の複数の重要インフラの組織を標的として活動しています。また、プロフェッショナル サービスや不動産開発に加えて、オーストラリアの重要インフラも標的にしています。

その手口は、有効なリモート デスクトップ プロトコル (RDP) 資格情報を利用して被害者のシステムにアクセスし、オープン ソース ツールとコマンドライン スクリプトを使用して探索と資格情報収集を行い、ファイル転送プロトコル (FTP)、Rclone、または Mega を介して被害者のデータを持ち出します。その後、支払いに応じなければデータを公開すると脅迫して金を脅し取ります。BianLian グループは、当初はデータを持ち出した後に被害者のシステムを暗号化するという二重恐喝モデルを採用していましたが、2023 年 1 月頃に主にデータの持ち出しをメインとする手法に移行しました。ランサムウェア自体は、いくつかのアンチデバッグ機能を備えた Golang マルウェアです。

05 MALAS

これは 2023 年 3 月末に初めて確認された新しいランサムウェア グループであり、MalasLocker とも呼ばれます。典型的な身代金を要求する代わりに、復号ツールを提供して、被害者のデータ漏洩を止めてほしければグループが承認する慈善団体に寄付することを要求します。この要求戦略は、将来変更される可能性があります。

この脅威グループが暗号化に使用するのは、「age」と呼ばれるオープンソース ツールです。この脅威グループは、脆弱な Zimbra サーバーを悪用した大規模な攻撃キャンペーンを展開したことで、2023 年上半期のランサムウェア攻撃グループリストの上位にランクされました。

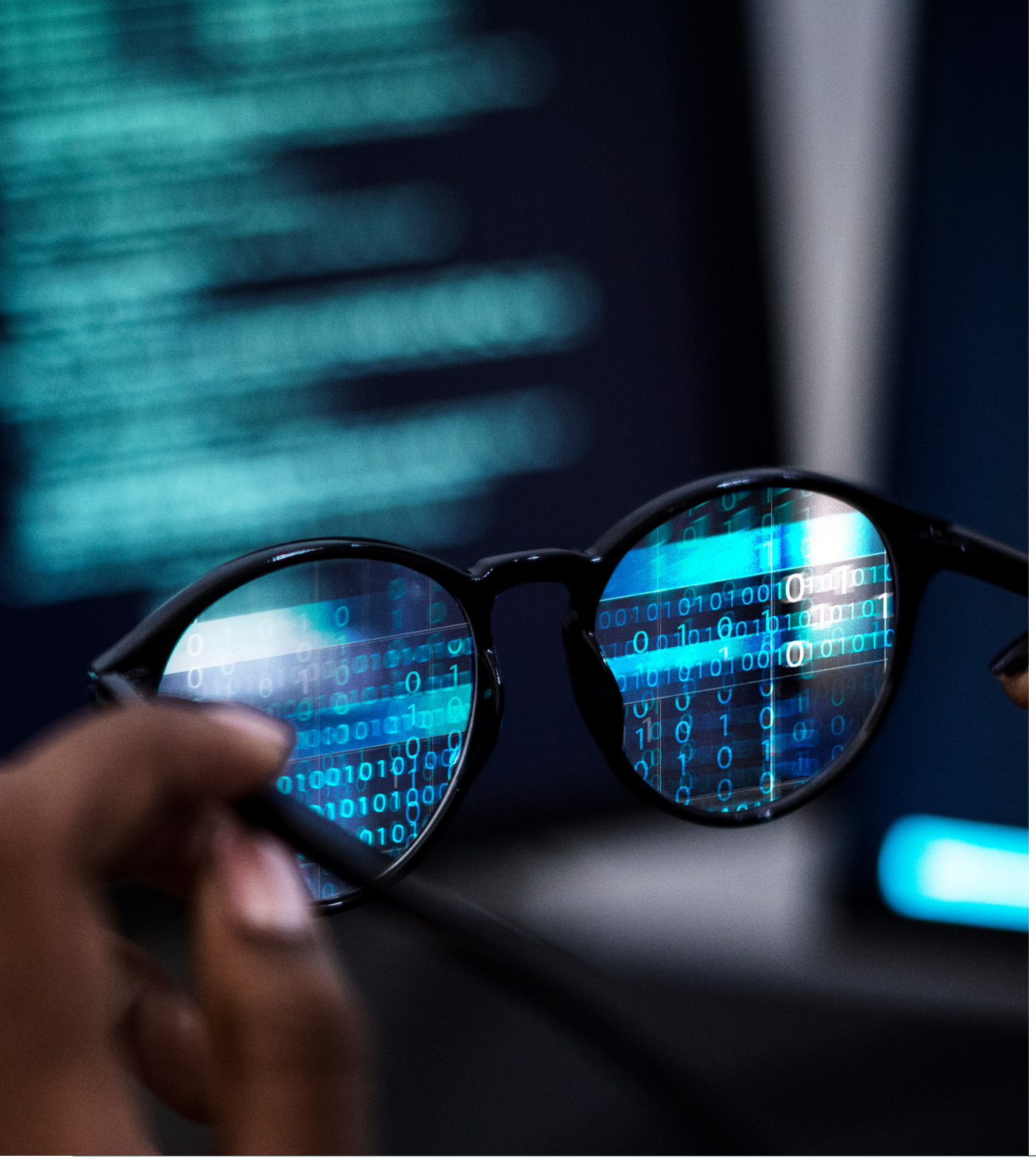
06 8BASE

8Base ランサムウェア グループは、2022 年 4 月に出現し、さまざまな業種の中小企業を中心に攻撃する攻撃的なアプローチですぐに悪名高い存在となりました。8Base のことはあまりわかっていませんが、そのやりとりの方法や漏洩サイトから得られる情報は、RansomHouse というグループとの類似性を示唆しています。RansomHouse は、侵害されたデータを購入し、データ漏洩サイトと提携して恐喝を行うことで知られています。そのため、8Base は RansomHouse と関連している可能性があるという噂が広がっています。また、8Base が漏洩した Babuk ビルダーに由来する可能性を示す手掛かりもあります。

07 PLAY

PlayCrypt とも呼ばれる Play ランサムウェアは、Process Hacker、GMER、IOBit、PowerTool などのツールを使用することで、ランサムウェアを実行する前にマルウェア対策システムと監視システムを無力化する手法をよく使用します。2023 年には、このグループが Microsoft Exchange の 2 つの特定の脆弱性を悪用していることが確認されました。興味深いのは、Play ランサムウェアおよび Hive と Nokoyawa という他の 2 つの系統の間に、明確な類似点が存在することです。

このことは、特に 2022 年に最もアクティブなランサムウェア グループのトップ 3 に入っていた Hive がその後の有名なランサムウェア脅威リストには入っていないことを考えた場合に、関連性があるという仮説につながりました。こうした内在するつながりから、これらのランサムウェア グループの変化する情勢に関する洞察が得られる可能性があります。



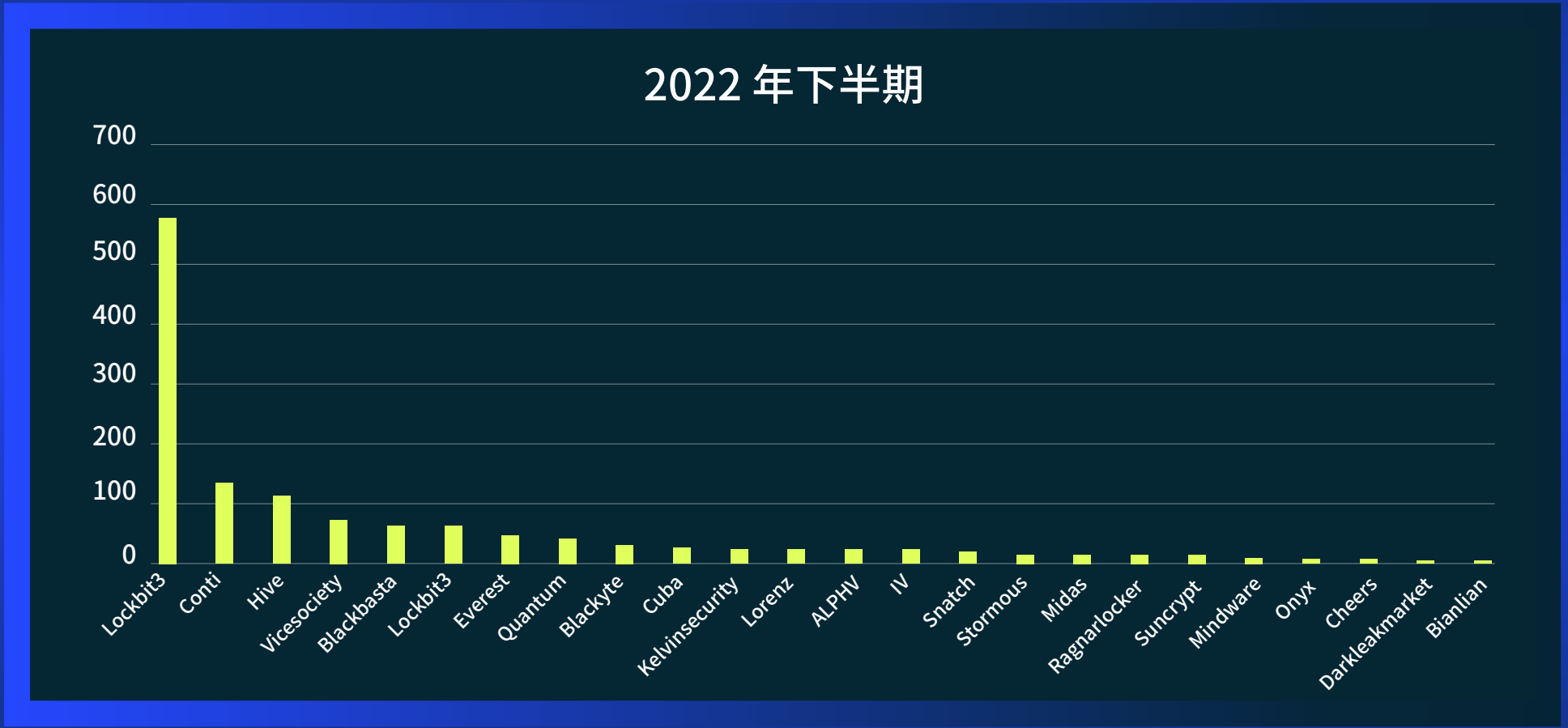
08 ROYAL

2022 年 9 月に初めて確認された Royal ランサムウェア グループは、その独特な暗号化手法で知られています。標準的な手法とは異なり、独自の部分暗号化戦術を採用することで、ファイル内の指定された割合のデータのみの暗号化を実現しています。これは特に大きなファイルに対して有効な方法であり、セキュリティ システムによる検知を回避するのに役立ちます。このグループの脅威は暗号化だけではありません。身代金が支払われなければ暗号化されたデータを公開すると被害者を脅迫する二重恐喝も行っています。

Royal は、最初の攻撃ベクトルとして主にフィッシングを使用しますが、有効なリモート デスクトップ プロトコル (RDP) の資格情報の悪用、Web アプリケーションとブローカーの侵害も確認されています。Royal の活動は特に重要なインフラストラクチャを標的としており、とりわけ医療分野はその攻撃に対して脆弱です。

Royal ランサムウェア グループは、その組織構造によって特徴付けられます。RaaS のアフィリエイトを採用するという広く使用されているモデルを避けて、悪名高い Conti ランサムウェア グループの元メンバーだけで密かに活動しています。

図 6：2022 年下半期に見られた主な脅威グループ



昨年下期には他にも複数のランサムウェアグループが活動していましたが、現在それほど大きなインパクトは確認されていません。

09 EVEREST

主に NASA のパートナーを標的としたことで知られる Everest ランサムウェア グループは、2020 年 12 月頃に出現し、南北アメリカ大陸で、特に金融、医療、および公共の組織を集中的に攻撃しました。その最も有名な標的の中には、通信業界最大手の AT&T や南米の複数の政府機関が含まれています。

他の多くのランサムウェア組織は標的を直接恐喝しますが、Everest はそれらとは異なり「初期アクセス ブローカー」として機能することが増えています。初期アクセス ブローカーは、自ら攻撃を実行するのではなく、組織への侵入ポイントを悪意のある他の攻撃者に販売します。一般に、ランサムウェア攻撃のほうが単なるアクセス情報の販売よりも多く稼げるため、これは比較的珍しい手口です。

10 LORENZ

これは ThunderCrypt と似ている脅威グループです。Lorenz は、被害者に身代金を支払うように圧力をかけるために、まずデータを他の攻撃者または考えられるライバル企業に販売できるようにします。最終的には、被害者のデータが含まれる、パスワードで保護された Roshal Archive (RAR) アーカイブの公開を開始します。

11 MIDAS

Midas Touch とも呼ばれる Midas は、Thanos ランサムウェアの亜種の 1 つです。Midas という名前は、神話に登場する触れたものすべてを金に変える能力で知られるフリギアの王に由来しているのかもしれません。このランサムウェアは、C# で記述され、SmartAssembly で難読化されています。

その他の既知の脅威

12 SNATCH ランサムウェア

このランサムウェア グループは、セキュリティ製品を回避するために PC をセーフ モードで再起動する、古いけれどもまだ機能する手法を利用しています。

13 LV ランサムウェア

LV ランサムウェアは、主に欧州、北米、およびアジアの製造、小売、およびテクノロジー企業を標的にします。REvil クリプターに似ているこのランサムウェアは、2020 年に初めて確認されました。

14 STORMOUS

この親ロシアの脅威グループは、Conti の元メンバーで構成されています。このグループは最近活動を再開し、新しい漏洩サイトを稼働させています。通常、そのパートナーシップとメッセージは、ウクライナに敵対する姿勢を示しています。

15 MINDWARE

Mindware は、おそらく SFile ランサムウェアのリブランドです。主に非営利の精神医療系の組織を攻撃するために使用されていました。

16 DARKLEAKMARKET

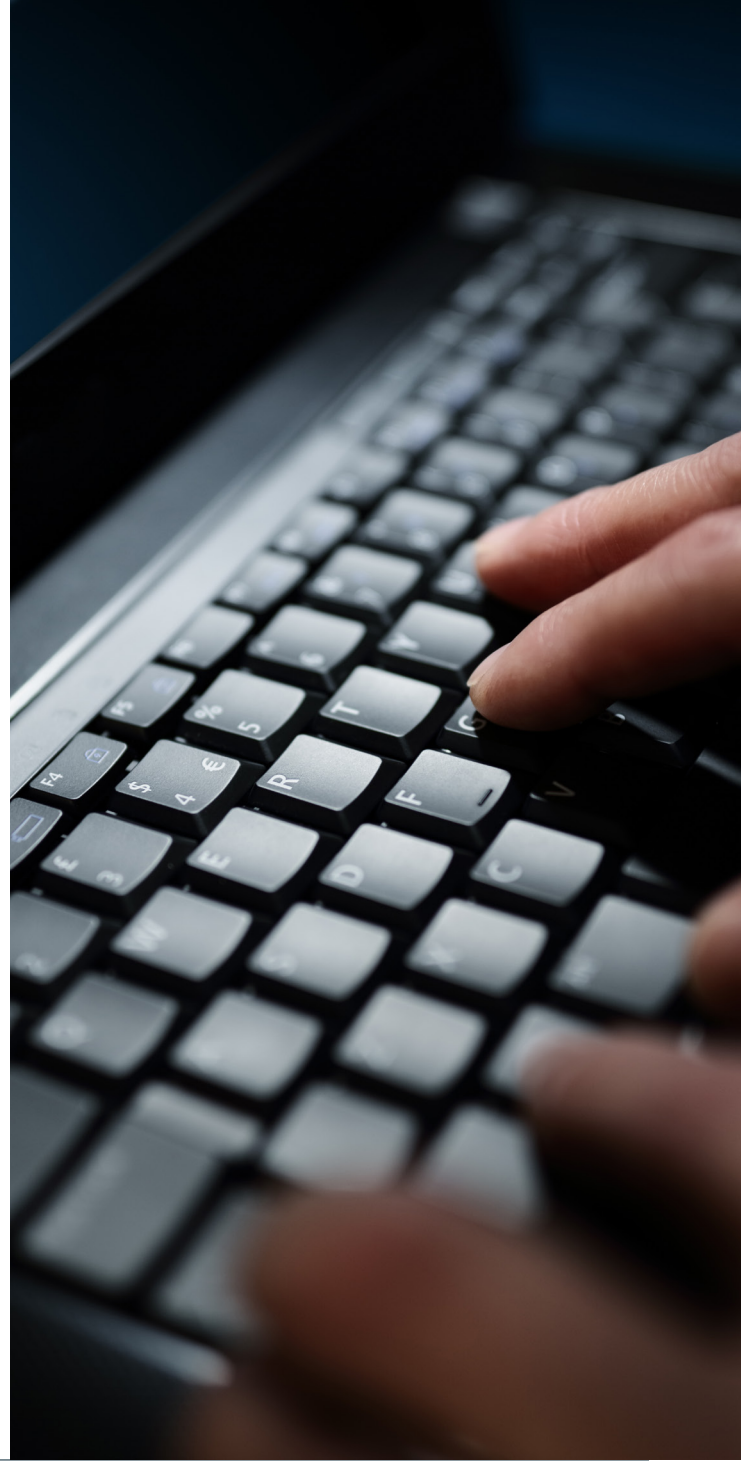
Darkleakmarket は、特にインド最大の民間銀行を攻撃したことでよく知られています。

17 CHEERS

Cheers は、主に Linux ESXi を標的とするランサムウェア グループです。

17 ONYX

Onyx は、ワイパー モードに移行した .NET ベースのランサムウェアです。



バンキング型トロイの木馬 / 情報窃盗マルウェア / スパイウェアのトップ 5

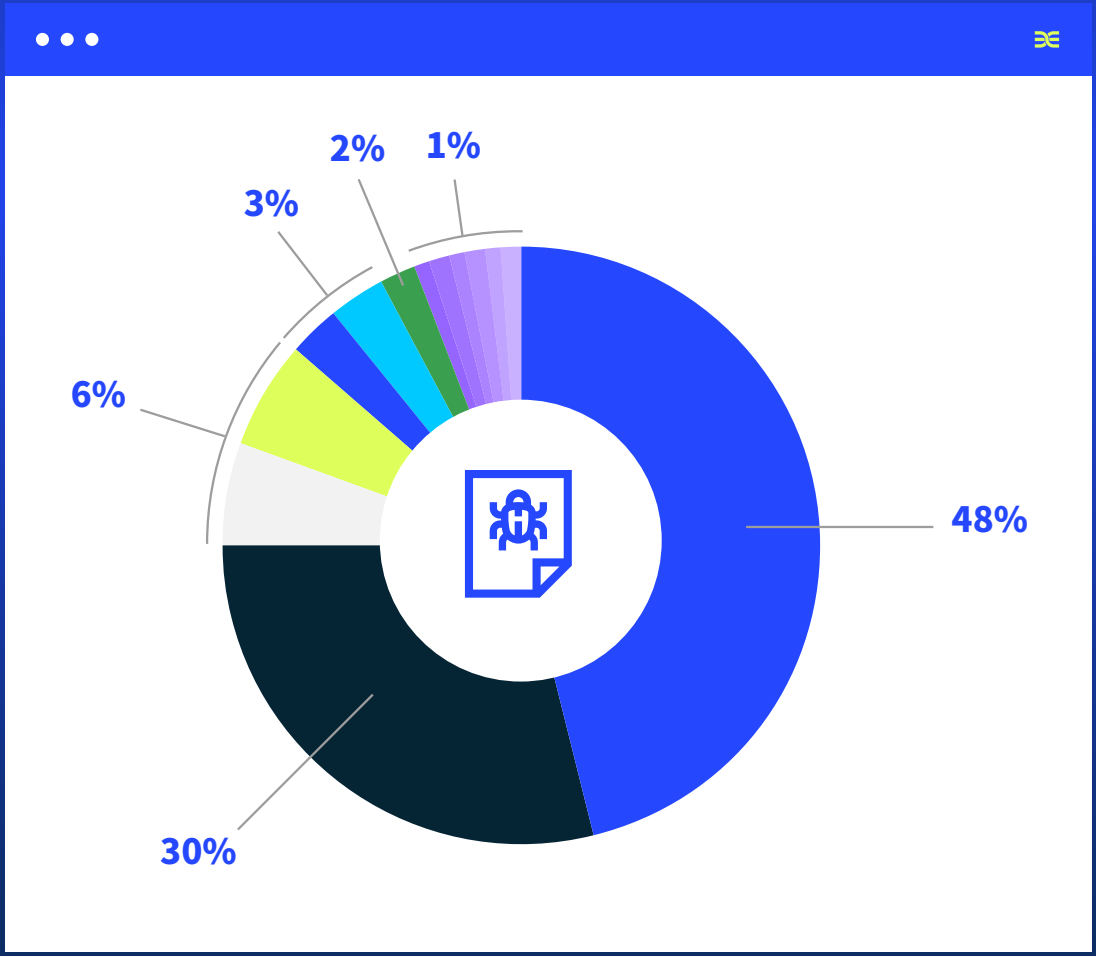


図 7 : バンキング型トロイの木馬 / 情報窃盗マルウェア / スパイウェア

主な情報窃盗マルウェアと RAT

01 EMOTET

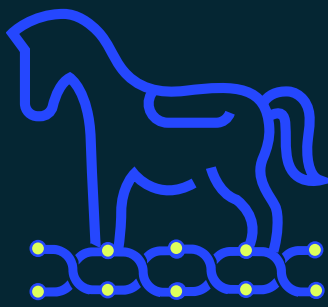
Emotet は、バンキング型トロイの木馬として 2014 年に登場しました。主に財務諸表や振り込み、支払請求書を模倣したスパム攻撃活動を介して拡散し、ほとんどは 電子 メールに添付されたマクロを含む Office ファイルを介して伝播します。マクロを有効にすると、悪意のある PE ファイル (Emotet) をダウンロードし、実行します。いったん実行されると、ネットワークトラフィックを傍受して記録し、ブラウザに不正なコードを挿入してバンキング サイトにアクセスすることで、金融データを持ち出し、保存することができます。

2017 年、Emotet の運用者は、他のマルウェアを被害者のコンピュータに送り込むことを目的とするマルウェアの一種であるドロッパーとして機能するように Emotet を設計し直しました。TrickBot バンキング型トロイの木馬や Ryuk ランサムウェアなどのマルウェアは、Emotet のドロッパー機能を利用して数多くのユーザーに感染します。

Emotet はセキュリティ対策を回避し、サーバー メッセージ ブロック (SMB) エクスプロイトまたは管理者資格情報の総当たりを利用して水平展開します。そのため、最も危険なマルウェアファミリーの 1 つとなっています。2021 年初め、欧州刑事警察機構と欧州司法機構を中心に組織された国際タスクフォースは、世界各地に点在する数百台のサーバーを侵害した Emotet のインフラストラクチャを押収し、その運用者数名を逮捕しました。また、2021 年 4 月、法執行機関は Emotet インフラストラクチャを使用して、感染したシステムからマルウェアを自動的にアンインストールしました。これらの措置により Emotet の活動はしばらく停止していましたが、2021 年 11 月に新たな亜種が再び確認されました。

2022 年初め、この悪名高い攻撃者は大規模なフィッシング攻撃活動を開始しました。この攻撃では、検知を回避するために高度に難読化された VBA マクロを実装していました。2022 年 5 月には、Emotet は Microsoft Office ドロッパーの代わりとして LNK ファイルの使用を試し始めました。このようなアプローチの変更は、マクロを無効にするという Microsoft の決定を受けたものであり、Emotet 以外のマルウェアでも行われています。

2023 年になると、Emotet に最初の攻撃ベクトルとして OneNote が追加されました。しかしこの手法は、Microsoft が OneNote 内でのスクリプトの使用を非推奨としたため、長続きしませんでした。その後、検知を回避するために、最近の動向であるバイナリ パディングおよび人為的なファイルサイズの巨大化が Emotet に採用されました。



Emotet は引き続き非常に活発で、バンキング型トロイの木馬のトップ 5 に入っています。

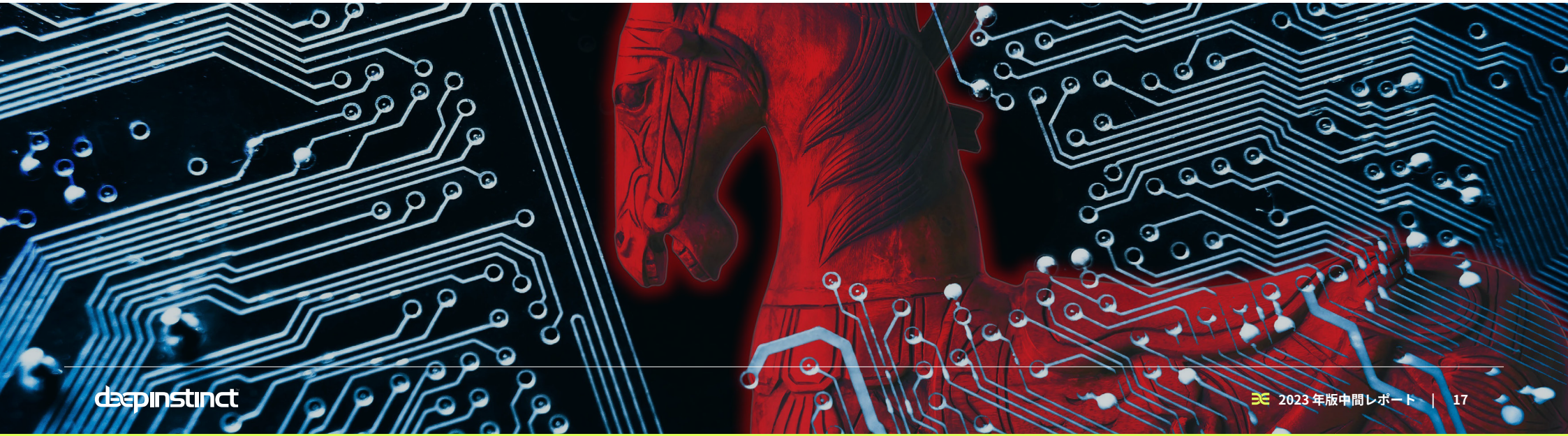
02 AGENT TESLA

2014 年にキーロガーとして出現し、後に最も高度で人気のある .NET ベースの RAT およびデータ窃盗マルウェアの 1 つになりました。サイバー犯罪者の初期アクセスを容易にするこのマルウェアは、通常は MaaS (Malware-as-a-Service) モデルで利用されます。この悪辣なビジネスの仕組みでは、初期アクセス ブローカー (IAB) と呼ばれる攻撃者が、その専門スキルを活かして企業ネットワークを悪用し、アフィリエイト犯罪組織と手を組みます。この 1st ステージのマルウェアは、侵入したシステムにリモート アクセスできるようにして、ランサムウェアなどの高度な二次ツールをダウンロードする下準備をします。

03 NANOCORE

APT33 脅威グループによって管理され、Nancrat または NanoCore とも呼ばれるこのマルウェアは、サイバー犯罪者だけでなく、国家の攻撃者によっても使用されています。NanoCore は、.NET フレームワークを使用して開発されたカスタマイズ可能な RAT です。プラグインを変更できるので、攻撃者は要件に合わせて機能を調整できます。2013 年に出現したこのマルウェアは、そのモジュール型の性質により、世界中で高く評価されています。プラグインを使用することで、NanoCore の機能を大幅に強化できるため、サイバーセキュリティに対する組織の脅威が高まります。

意外なことに、NanoCore は公式 Web サイトで、すべての公式プラグイン込みでわずか 25 ドルで販売されており、さらに 24 時間体制のテクニカル サポートが提供されています。さらに、ハッキング フォーラムで「クラックされた」バージョンも入手可能なので、そのアクセス性と使い勝手はさらに向上しています。合法的な商用ツールとして開発したのか、それとも悪意を持って開発したのか、当初の目的が不透明なまま、FBI は作成者の Taylor Huddleston を逮捕しました。このマルウェアの手頃な価格、シンプルさ、および広く拡散された情報が、その知名度の上昇に大きな役割を果たしています。



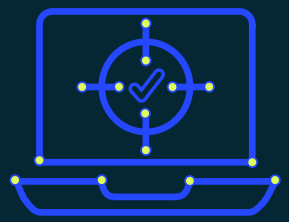
04 REDLINE STEALER

闇フォーラムで購入できるマルウェアの一種です。バージョンに応じて、100 ～ 150 ドルでスタンドアロン製品として使用するか、月額 100 ドルのサブスクリプション モデルで利用できます。このマルウェアは、保存されたパスワード、オートコンプリートの詳細、クレジット カード情報などのデータをブラウザから抽出するように設計されています。さらに、システムをスキャンして、ユーザーの名前、場所、ハードウェア設定、稼働しているセキュリティ ソフトウェアの詳細などの情報を収集します。RedLine の最新のバージョンでは、暗号通貨を盗み出す機能が組み込まれています。また、FTP と IM の各クライアントを標的として、ファイルのアップロード / ダウンロード、コマンドの実行、および侵害したシステムに関するデータの定期的な送信を行うことができます。

05 REMCOS

「Remote Control & Surveillance」を略した名前を持つこの RAT は、ユーザーに気づかれることなく被害者のマシンをリモートから操作および監視するための機能をサイバー犯罪者に提供します。これは、合法的なリモート管理ソフトウェアとして Remcos や他の攻撃的セキュリティ ツールを販売する欧州企業である BreakingSecurity によって 2016 年頃に初めてリリースされましたが、悪意を持つサイバー犯罪者によって頻繁に悪用され、さまざまな地下フォーラムで販売されています。

幅広い機能を備え、ダーク ウェブで購入できるので、スパイ、窃盗などの方法で被害者からデータを搾取しようとする攻撃者の間で人気があります。



2023 年の欧米企業に対する
いくつかの大規模なキャンペーンで
Remcos が検知されています。

06 QBOT

QakBot として知られた人気のある情報窃盗およびバンキング型トロイの木馬であり、2009 年から活動が確認されています。その主な特徴は、オンライン バンキングの資格情報をはじめとする金融関連情報を盗み取ることですが、ファイルやキー ストロークなどの個人情報を盗むこともできます。

ワームとしての機能も持っており、ネットワークやリムーバブル ドライブを介して拡散します。QakBot は感染したマシン上でブラウザを監視して、被害者がオンライン バンキングの Web サイトで行う操作を検知し、資格情報を盗みます。また、感染したマシンから、IP アドレス、国、Cookie などのシステム情報も収集します。QakBot の配布手法は多様です。たとえば、専用に作られたドキュメント添付ファイルから感染を広げるマルスパムという手口や、侵害した Web サイトにエクスプロイト キットを展開し、Web サイトの閲覧者に QakBot のペイロードを送る手口などが確認されています。

Qakbot は長年にわたってさまざまな配布手法を使用しており、検知を回避するために実装を改良しています。このプロセスによって、2022 年初めには VBA マクロの前のマクロである Excel 4 マクロ (XLM) を採用しました。これは、この古いマクロがアンチウイルス ベンダーから注目されておらず、検知される可能性が低くなるためです。しかし、その後すべてのマクロをブロックするという Microsoft の変更を受けて、XLM の使用は数か月のみで終わり、2022 年 5 月には LNK ファイルの使用に切り替えました。

07 ICEDID

BokBot とも呼ばれる、ユーザーの財務情報を盗むために設計された高度なバンキング型トロイの木馬です。他のマルウェアをシステムに侵入させることもできます。MITB (マンインザブラウザ) 攻撃を使用して、オンライン バンキングのログイン情報を盗み出します。この情報を取得した後、銀行口座を乗っ取り、不正な取引を行います。

IcedID は、独自の悪意のある電子メール キャンペーンを介して拡散することもありますが、他のマルウェア、特に Emotet によってフォローアップ ペイロードとして配信されることが頻繁に行われています。検知されないようにするため、システムのメモリや標準プロセスにそれ自体を埋め込むなどの戦略を採用しています。

さらに、このマルウェアの作成者は常に更新を行って、その耐久性を高め、最新の検知手法を巧妙に回避する能力を強化しています。IcedID は、バンキング型トロイの木馬として 2017 年に初めて発見されました。その後ドロッパーへと進化し、金銭的な動機を持つ多くのサイバー犯罪者によって 2nd ステージとして使用されました。

2023 年には、他の多くの攻撃者と同様に、最初のベクトルとして OneNote ファイルを採用しましたが、この手法は長続きしませんでした。また Nokoyawa ランサムウェアもドロップされていることが確認され、長年にわたって IcedID によってドロップされてきた他のランサムウェアのリストに加わることになりました。最近のバージョンは、BackConnect という名前のカスタム socks5 を使用しています。

08 LOKIBOT

Loki PWS と呼ばれることもあります。ユーザー名、パスワード、暗号通貨ウォレットの詳細など、重要なデータを盗み出します。2023 年には、Microsoft Office の脆弱性を悪用したキャンペーンで復活をしようとしていました。

注目すべきポイント

国家の支援を受けている攻撃

2023 年、国家の支援を受けている攻撃は増加の一途をたどり、あらゆる過去の記録を更新しています。ここではロシアは、世界有数の攻撃グループの 1 つになっています。Sandworm、Callisto、Gamaredon など、さまざまなロシアの APT グループは、2022 年に主にウクライナ政府の Web サイト、組織、および企業に対して多数のサイバー攻撃を仕掛けた後、東欧諸国に対してもキャンペーンを続行しました。

Mango Sandstorm (Mercury) とも呼ばれる MuddyWater は、イランの情報・治安省 (MOIS) の下部組織であるサイバー スパイ グループです。

Deep Instinct 脅威リサーチチームは、このグループが作成した新しい C2 (コマンド & コントロール) フレームワークを特定しました。

PhonyC2 と呼ばれるこのフレームワークは、カスタムメイドで常に開発が行われており、MuddyWater グループは遅くとも 2021 年には使い始めています。現在は、アクティブな PaperCut 悪用キャンペーンで使用しています。

国家の支援によって行われた攻撃のもう 1 つの例は、中国の攻撃者 Red Menshen (別名 Red Dev 18) によるもので、2021 年以降、中東とアジアの通信プロバイダーや、政府、教育、および物流関連の組織を標的としていることが確認されています。

Deep Instinct の脅威ラボは、Red Menshen APT による BPFdoor のこれまでどこにも報告されていない完全に未検知の新しい亜種を確認し、分析しました。

攻撃者はマクロを捨てて LNK、人為的なファイルの巨大化、および JavaScript に移行

Office ファイル内のマクロは、長年にわたって多くの攻撃者によって初期ステージとして使用されていました。しかし、Microsoft がマクロをデフォルトで自動的に無効にしたことにより、ユーザーが手動でコンテンツを有効にしないとこのベクトルを利用できなくなったため、この手法の魅力は薄れました。そのため攻撃者は、より目立たない、検知回避能力の高い一次ステップを探すようになりました。悪意のある LNK ファイルは、配信方法として長年使用されている手法です。

この手法が効率的なのは、Windows の基本的な機能を悪用するからです。具体的には、LNK ファイルに格納されたメタデータを使用して、PowerShell などの実行ファイルを自動的に起動します。最近話題になったもう 1 つの手法は JavaScript です。Deep Instinct のリサーチャーは、最近 Bumblebee と IcedID の新しいキャンペーンで JavaScript が使用されていることに気づきました。どちらも、難読化されてほぼ検知されない PindOS JS ドロッパーを共有していました。

この PowerShell から JavaScript への切り替えは、一般化が進んで確立されていた TTP が大きく変化したことを示しています。

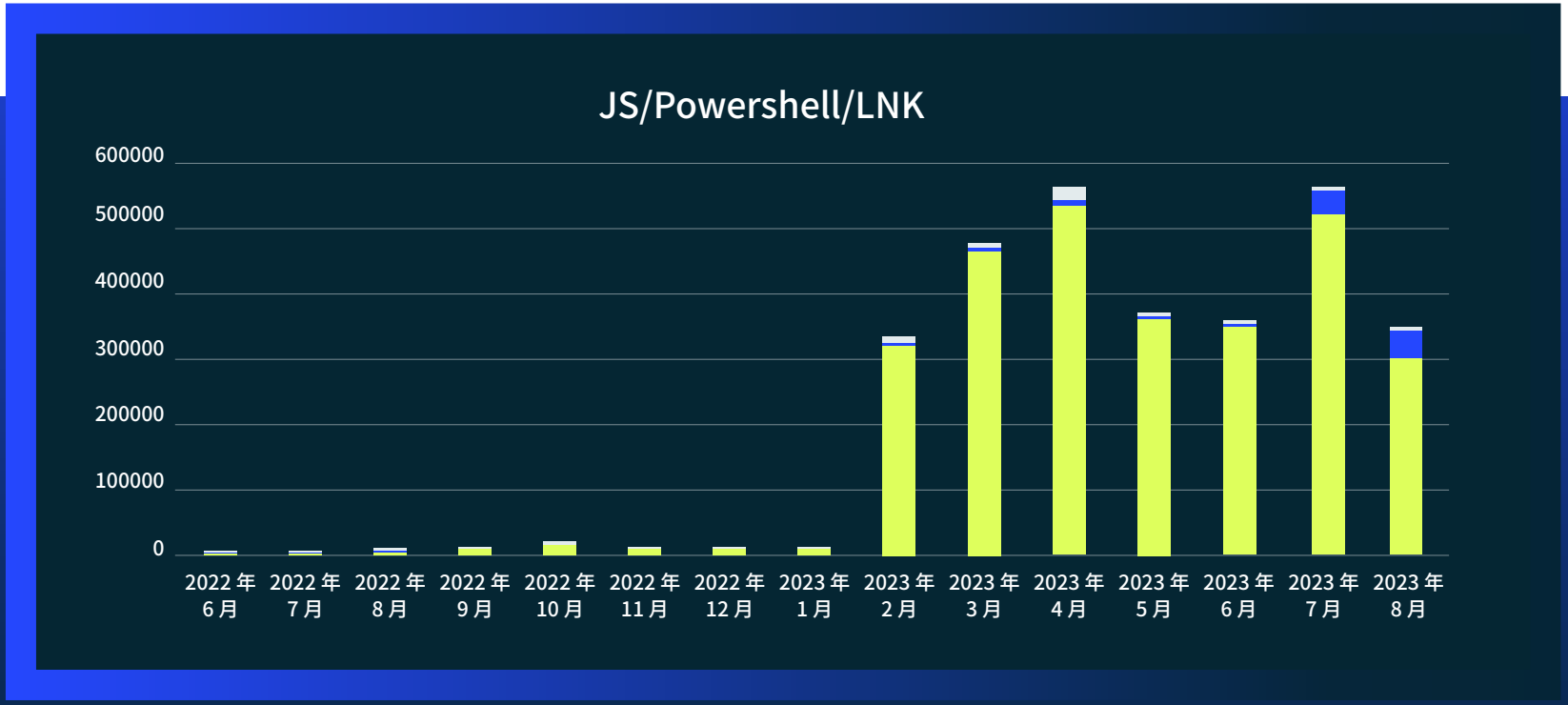


図 8：2022 年下半期 /2023 年上半期の攻撃者

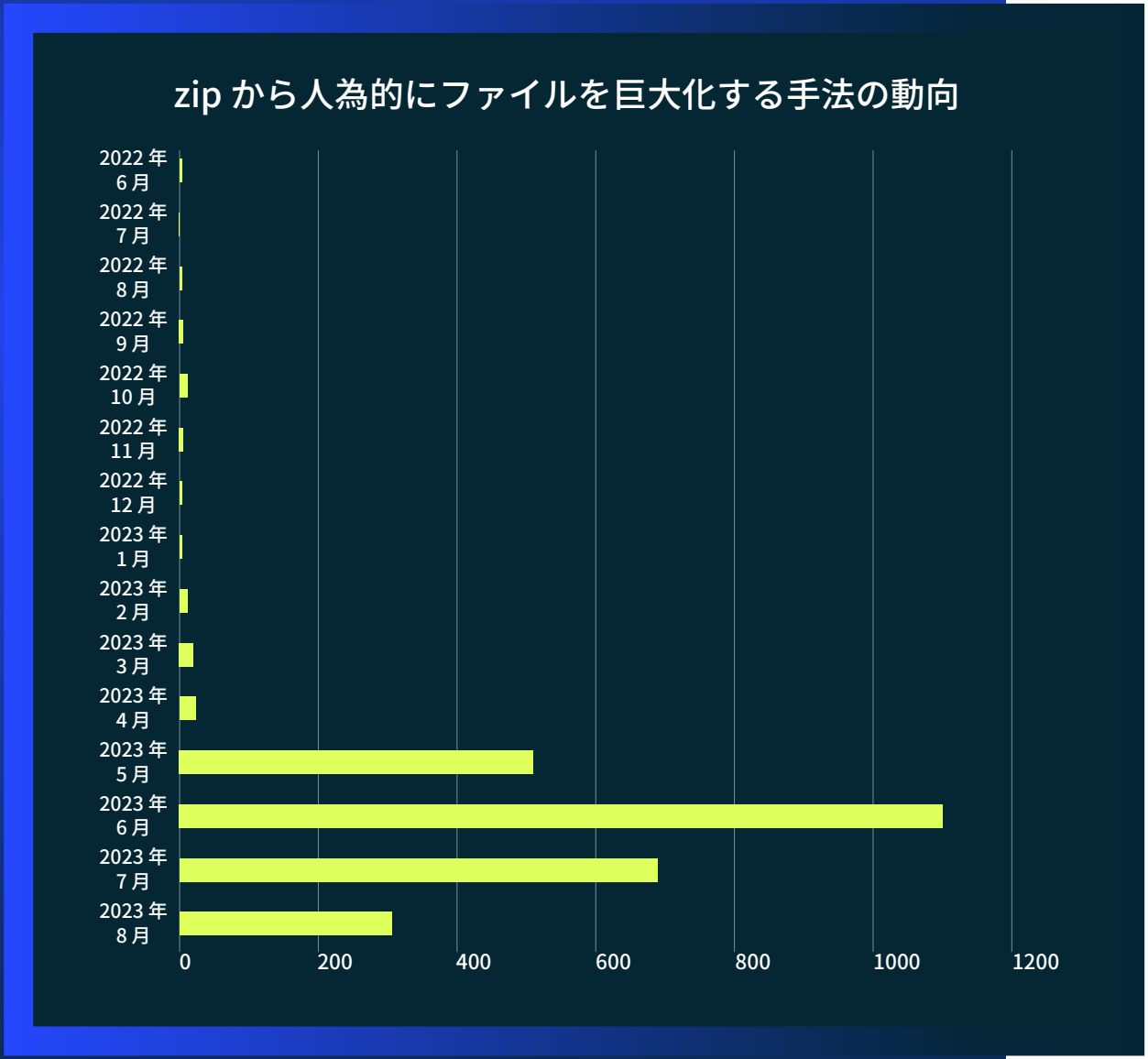


図 9 : 2022 年下半期 /2023 年上半期の zip から人為的にファイルを巨大化する手法の動向

さらに、悪意のあるファイル内のペイロードの前後に不必要なデータを詰めて人為的にファイルを巨大化し、セキュリティ製品 (EPP やサンドボックス) によるスキャンを回避するという手法も、増加が確認されています。

この手法はさらに、ファイルのハッシュを変更し、ハッシュベースの検知も回避できるようにしています。この手法では、配信される際のファイルサイズ自体は小さくしておくために、zip ファイルを使用します。zip ファイルを解凍すると、ファイルは指数関数的に巨大化し、アンチウイルス (AV) やエンドポイント検知・対応 (EDR) のスキャンを回避するために、数百 MB まで拡大します。

閉鎖された地下フォーラムに代わる新たな市場が出現

ダークネットや地下で活動していた多数の大規模なハッキングフォーラムが閉鎖されました。閉鎖された有名なフォーラムの一部がこちらです。

- **RAID Forums**
- **Genesis Market**
- **Breached Forums**
- **ASAP Market**

さらに、複数のランサムウェア漏洩サイトが FBI に押収され、サイバー攻撃者のギャング メンバーが逮捕されました。これらの逮捕にもかかわらず、増加は続いています。そこではミラーリング、代替プロトコルなど、押収を回避するためのさまざまな新しいアイデアが出現しています。また、閉鎖された市場やフォーラムの所有者が、それらに代わる市場を独自に開設しています。

漏洩サイトの被害件数は大幅に増加していますが、ほとんどの場合、被害者が身代金をなかなか支払わないか、あるいはまったく支払わないため、漏洩データがこれらのサイト上で公開されています。

悪用されることが多いシステム

脆弱性は、依然として大規模なサイバー攻撃の最も重要な要素です。攻撃に悪用されるまでの流れは以下のとおりです。

- **深刻な脆弱性が公表される**
- **攻撃者は脆弱なサーバーをスキャンにより探索し、発見する**
- **攻撃者はランサムウェアの配信とデータの持ち出しのために POC コードを開発するか、既存の POC コードを使用する**
- **攻撃者はすべての脆弱なサーバーで同様の脆弱性を悪用する**

年末に近づくと、上記のような動きが増加する傾向にあります。最近のわかりやすい例としては、MOVEit の脆弱性が挙げられます。MOVEit は幅広く利用されているプラットフォームですが、インターネット上のサーバーが完全に無防備となる脆弱性が公開されました。MOVEit の詳細については、弊社のブログをご覧ください。また、最近 MOVEit に新しい SQL インジェクションの脆弱性が見つかりましたが、これはまだ悪用されていません。今後も、Log4j と Log4Shell で見られたような、MOVEit の脆弱性を悪用した攻撃が増えることが予想されます。

図 10 : 悪用されている脆弱性

マルウェア作成に新時代をもたらす LLM

2023 年に強力な大規模言語モデル (Large Language Model: LLM) が台頭しましたが、攻撃者はすでにこれを利用しはじめています。攻撃者は、地下フォーラムやハッカー フォーラムのさまざまな「脱獄」ガイドを使用して ChatGPT やその代替プログラムを使用し、WormGPT など、攻撃用の独自の LLM を構築しています。

さらに、攻撃者は、ChatGPT がその回答の中で、「でっち上げられた」、存在しない、または非推奨のコード ライブラリを使用しているケースがあることに注目しました。攻撃者は、それらの存在しないライブラリを実装して悪意のあるコードを追加することにより、それらを悪用しようとしています。これによって、将来 ChatGPT がそれらのライブラリの使用をユーザーに提案した場合、ユーザーは知らずに悪意のあるコードを含むコード ライブラリをダウンロードしてしまう可能性があります。また弊社では、ChatGPT を使ってほぼ検知されない未知のマルウェアを作成できることを確認しています。

図 11 : WORMGPT

2024 年の予測

脅威は AI で さらにカスタマイズおよび高度化

LLM は人工知能 (AI) の同義語になりましたが、それは正確ではありません。我々も LLM には大きな可能性があると信じていますが、今はまだその最大限の潜在能力をほとんど発揮できていません。LLM がより正確で強力になると、攻撃者は LLM をさらに積極的に利用することになるでしょう。

弊社は、LLM は近いうちにスタンドアロンで脆弱性の調査やエクスプロイトの実装を行えるようになり、これまで見たことのないようなカスタム難読化やカスタム マルウェア ビルダーなどの攻撃を実行できるようになると予測しています。

より高度な AI、具体的にはディープ ラーニングを使用して攻撃者の AI と戦うことが重要なのは、そのためです。それらの増え続ける高度な脅威に対抗できるのは、ディープ ラーニングだけです。

大規模な侵害攻撃による被害は 今後も拡大

大規模な侵害は通常、広く使用されているシステム (SolarWinds、Log4j、MOVEit) におけるゼロデイ脆弱性が悪用された結果としてよく発生します。脆弱性管理は複雑であり、特に大規模組織ではシステムにパッチを適用するのに数か月を要する可能性があるので、ペイロードが実行可能になる前にブロックすることが被害を防ぐ最善の方法です。2023 年前半には、脆弱性が公表された後の特に最初の数週間のうちに、その脆弱性を突いた攻撃が急増することがすでに確認されています。

ステルス型マルウェアと AV サービスの中断が 攻撃者にとって重要な要素に

AV と EDR サービスの中断は、攻撃者にとってますます重要になっています。最近公開されたツールのほとんどは、脆弱なドライバー (BYOD) を使用する同一手法を使用しており、2 つの高度な特権アカウントを前提条件としていますが、攻撃者やセキュリティ研究者はこの開発経路に注目し続けると考えられます。

マクロの攻撃は衰退、他の脅威ベクトルが主役に

マクロは 10 年間、OneNote は非常に短い期間でしたが、攻撃に広く使用されてきました。しかし、今は LNK、JS、および人為的に巨大化する zip ファイルが広く使用されているようです。これらの初期攻撃ベクトルは、古典的な AV では検出するのが困難です。短期的には、広く使用される初期攻撃ベクトルが新たに出現する可能性は低いと予測しています。

国家によるサイバー攻撃で AI の利用が始まる

ロシアとウクライナの戦争が続く中、双方の国を起源とする攻撃者グループからこれまで確認されたものと同レベル、あるいはそれ以上のサイバー攻撃が行われることが予想されます。

1 年以上が経過し、旧ソビエト連邦の複数の強力な脅威グループが親ロシア グループと親ウクライナ グループに分かれて、全面的なサイバー戦場を構成しています。これらのサイバー攻撃は、主に機密データの漏洩またはサービスの停止を目的としています。漏洩サイトや地下フォーラムは双方の企業からの漏洩情報でいっぱいであり、親ウクライナの脅威グループによる漏洩情報も複数存在します。

さらに、米国や欧州などを主なターゲットにして世界各地で親ロシアの攻撃者による国家規模の攻撃が増えています。

大規模なサイバー戦争で AI や LLM が利用されると、サイバー戦場は非常に危険になります。ロシアが、オンライン上の「不愉快な」内容に対して、Oculus と呼ばれるいわゆるプロパガンダのような AI スキャナーを使用している兆候が、すでにいくつか確認されています。Oculus は、2023 年 2 月に提供を開始し、すでにソース コードが漏洩しています。この種のツールは、将来甚大な被害をもたらす可能性があります。

このレポートを作成したのは、Deep Instinct 脅威リサーチチームに所属する以下のメンバーです。

Shaul Vilkomir-Preisman

Bar Block

Simon Kenin

Mark Vaitzman

Deep Instinct は世界初で唯一のサイバーセキュリティに特化した独自ディープ ラーニング サイバーセキュリティ フレームワークを用いた予防ファースト アプローチで、ランサムウェアおよびその他のマルウェアを阻止しています。Deep Instinct は既知 / 未知 / ゼロデイ脅威を 20 ミリ秒未満で予測し、予防します。これは最も高速なランサムウェアの暗号化速度の 750 倍も高速です。

99% 超のゼロデイ脅威検知精度を誇り、誤検知率 0.1% 未満を約束します。脅威に対する完全な多層防御をハイブリッド環境全体にわたって提供する Deep Instinct Prevention Platform は、すべてのセキュリティ スタックに不可欠の追加機能です。

www.deepinstinct.com/ja