Trellix ADVANCED RESEARCH CENTER

2023 脅威予測

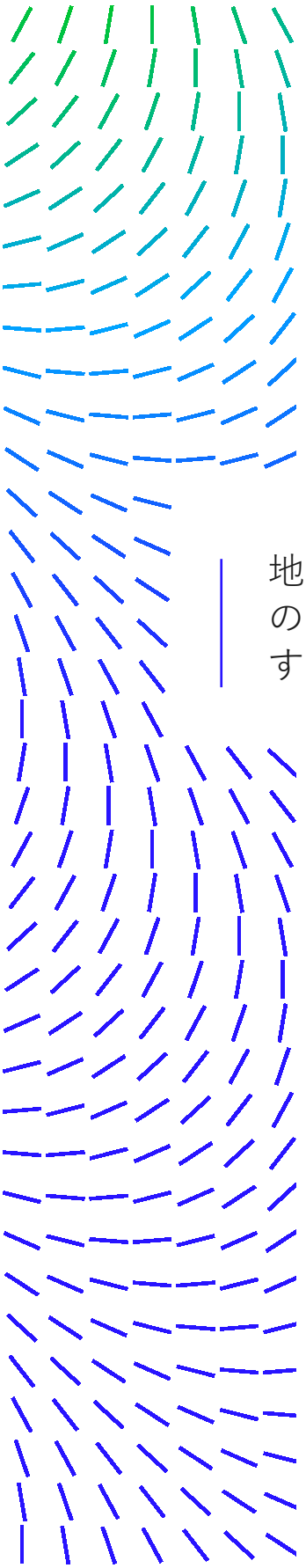
Threat Predictions

毎年、私たちは水晶玉を覗き込み、次の年のサイバー脅威がどのようなものになるかについての考えを共有しています。今回のTrellix Advanced Research Center (トレリックス アドバンストリサーチセンター)チームの脅威予測の内容は、ハクティビズムからサイバー戦争、ソフトウェアのサプライチェーンに至るまで、多岐に渡っています。

2022年は、2021年暮れから続く業界全体が騒然となったLog4Jの脆弱性から始まり、ウクライナを標的としたサイバー戦争と物理戦争がそれに続きました。2022年の終わりには、ハクティビストが自らの手で問題を解決し、新たな攻撃者が活動し、ランサムウェアの状況は変化しているものの、ますます活発になっていることが観察されています。世界経済にストレスがかかり続ける中、企業は、政治的または経済的な利益のためであれ、自らのアジェンダを推進しようとする脅威者の活動が活発化することを予期しておく必要があります。

悪意ある攻撃者を出し抜き、プロアクティブに防御を進めるには、セキュリティは常にオンで、常に学習していなければなりません。私たちのチームは、新しいサイバー活動を調査し、セキュリティ製品をより進化させるための脅威指標を開発し、お客様や業界全体が備えるべき調査を公開しています。

本レポートにて、Trellix Advanced Research Centerの研究者から、2023年のサイバーセキュリティの展望がどのようなものになるか、概要をご説明させていただきます。



地政学的な動機による サイバー攻撃の台頭

By Anne An

地政学は、サイバー脅威者が標的とする国や支援国の企業や個人を攻撃するための新たな道を開くものです。2022年を通じて、ハクティビストやその他のサイバー脅威者によって地政学的な緊張が高まっています。サイバー攻撃は、これらの事例において、侵略者に対する抵抗力と防衛力を弱め、外交政策に影響を与え、侵略者の戦略目標を支援するために、動的な軍事行動を伴い、補完してきました。ロシアのウクライナ侵攻、台湾海峡の政治的緊張、北朝鮮の日本・韓国へのミサイル発射実験はすべて、付随するサイバー脅威活動によって悪化しています。

地政学的な動機によるサイバー攻撃や誤報キャンペーンの台頭は、2023年も引き続きサイバー脅威の状況を形成する可能性があります

2022年2月のロシアのウクライナ侵攻をきっかけに、ウクライナ政府、軍、商業組織に対する破壊的なサイバー攻撃と誤報キャンペーンが新たに発生しました。米国やNATO諸国など、ウクライナを支援する国々も標的になっています。これらのサイバーによる脅威は、否認権を維持しながらターゲットに危害を加え、不安定化させるというロシアの協調策の一部です。戦争が2023年も継続された場合、ロシアの脅威者はおそらくウクライナの公共、エネルギー、金融、ビジネス、非営利セクターを標的とし、プロパガンダと偽情報キャンペーンを利用して攻撃を行う可能性があります。

台湾の場合、Trellixの遠隔測定データによると、台湾政府および商業組織を標的とした脅威活動は、台湾総統府やその他の政府機関に対するDDoS攻撃が公に報告される数日前、ペロシ氏のアジア訪問が決まった時点で始まっていた可能性が高いと考えられます。これらの活動は、ペロシ氏の台湾訪問の意思決定に影響を与えることを意図していた可能性があります。このように、ハクティビストなどのサイバー脅威行為によって成功したサイバー攻撃は、今後の中台危機において、軍事行動の支援や恐怖心を与えるためにさらに多くのサイバー攻撃につながることが考えられます。同様の戦術は、後に日本や韓国といった台湾の地域パートナーや米国などの支援国に対しても活用される可能性があります。また、中国は台湾の親北メディアのプラットフォームへの資金提供や仲介を通じて、台湾の民主主義制度を蝕む偽情報やプロパガンダへの関与を継続する可能性があります。

もう一つの例は、2022年9月と10月に北朝鮮政府が日本と韓国の上空に弾道ミサイルを発射した時期には、北朝鮮のLazarus Groupによる悪意のある活動の検出が急増していることが分かりました。これらの試みは、弾道ミサイル発射のプロセスを支援するための能動的または受動的な偵察活動の増加の一部であったと思われます。北朝鮮の攻撃的なサイバー作戦が政府のアジェンダ、特に核と弾道ミサイル計画に貢献し続けているため、2023年も韓国とその地域パートナー、そして同盟国の米国に対して同様の脅威パターンが見られる可能性があります。

ハクティビズムが表舞台に

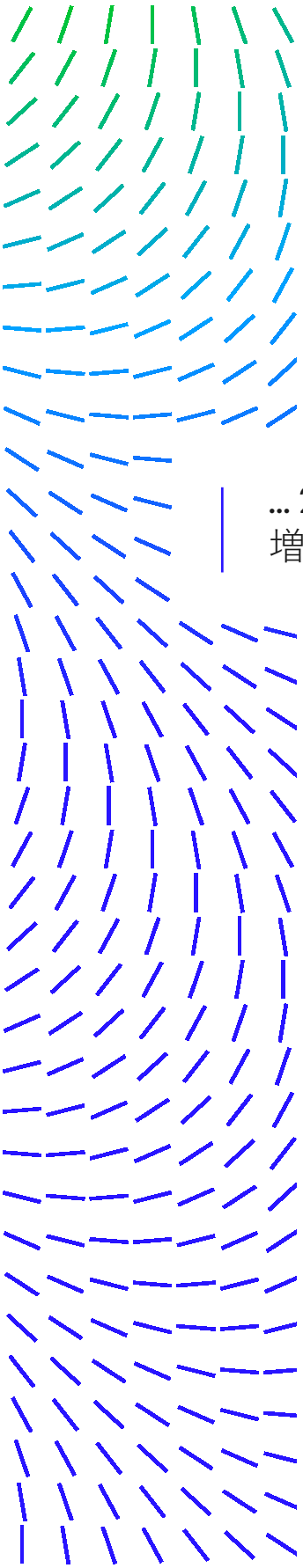
By Manoj Reddy

長年にわたり、世界のニュースは、国家がスポンサーとなり、金銭的な動機で行われるサイバー脅威によって占められてきました。ハクティビズム（活動家による政治的・社会的な動機によるハッキング）は、近年は影を潜めています。

現在の世界的な緊張を考えると、私たちはすでにハクティビズムの再興を目にしており、2023年にはより大きな役割を果たすと予想しています。プロパガンダによって緩やかに組織化された個人の集団が、共通の目的のために連携し、その怒りを表明して混乱を引き起こすために、サイバーツールの利用を拡大し続ける可能性があります。

愛国的なハクティビズムは、戦争やその他の紛争が続く 2022 年に増加し、DDoS 攻撃、改ざん、ドクシング、侵入、個人を特定できる情報 (PII) の漏えいなどの広範な行動に分解されます。ハクティビストは、電気通信、エネルギー、航空、テクノロジー、メディア、政府部門など、彼らのイデオロギー的および政治的見解と一致しない幅広い業界や部門を標的にしています。このような活動は、最近の歴史でも多くの例があります。ロシアとウクライナの戦争に関連して、ロシアのハッカー集団「Killnet」がウクライナを公的に支援している国のウェブサイトを攻撃したり、別のロシアの集団がウクライナ最大の民間エネルギー会社を標的にしたりするなどの事例があります。

2023年も緊張が高まることが予想される中、ハクティビズムは、対立する政党の政治的アジェンダに合わせて活動家が主導して行うため、行為に対する完璧な言い逃れができるため、今後も規模が拡大していくことが予想されます。



ソフトウェアの“知られたくない秘密”の増加

By Doug McKee

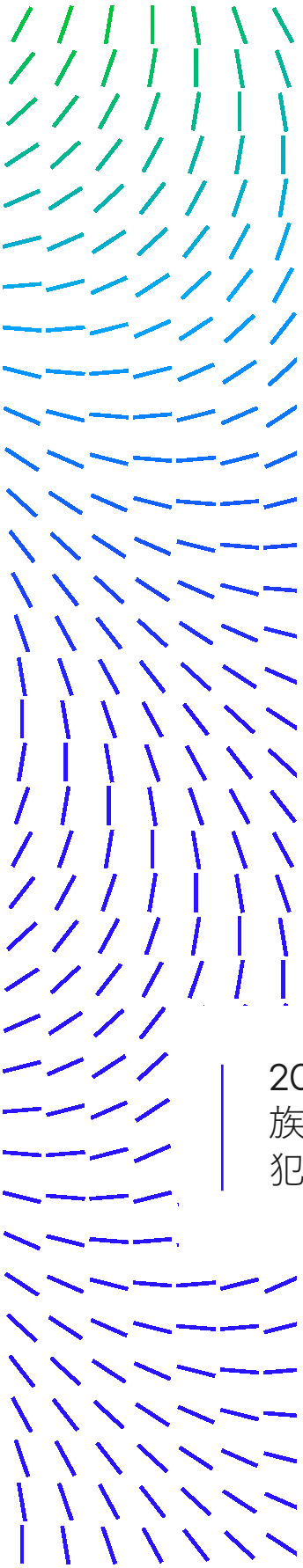
2022年、私たちはサプライチェーンへの攻撃と攻撃ベクトルが継続的に増加し、注目されていることを目の当たりにしました。IBMは、年次の情報漏洩レポートの中で、全侵害の19%がサプライチェーン問題の結果であることを強調しています。サプライチェーンに分類されるものを正確に定義することはまだできませんが、重要な基盤となるフレームワークの脆弱性は、紛れもなくサプライチェーンの一部です。2021年後半にLog4Jが行ったことを、この攻撃対象が脅威者にもたらす魅力のほんの始まりと考えるなら、

> … 2023年にはサプライチェーンの問題に関連する侵害が増加すると予想されます。

当然のことですが、ハッカーは怠け者です。 彼らは、最小限の労力で、最大の金銭的利益を得ること、あるいは特に国家の場合は、最大の損害を与えることを考えています。Microsoft や Apple などの大手企業は、自社製品で発見された脆弱性の数について否定的な報道をされていますが、実際のところ、過去数十年にわたって、これらのプラットフォームで脆弱性を発見し悪用することはますます難しくなっています。 これは、人的要因の悪用が依然として非常に重要であり、脅威グループによって実行される多くの理由の 1 つです。ただし、この難易度の増加により、ハッカーは他の分野でより簡単なターゲットを探すことにもなります. 特にオープンソース コミュニティでは、長い間使用されてきた一般的なフレームワーク、ライブラリ、および SDK のすべてが、セキュリティの回復力を確保するために必要な定期的なセキュリティ監査と変更に対応できているわけではありません。

攻撃者とセキュリティ研究者の両方が、サプライ チェーンの一部である基盤となるフレームワークの研究を強化する可能性があります。 その結果、より多くの脆弱性が発見 (または再発見*) され、悪用され、広範囲に影響を与えることが予想されます。これは、必ずしも Microsoft の重大なバグという形で現れるとは限りませんが、誰もが使用しているけれども、聞いたことのないフレームワークが登場する可能性があります。 そのため、組織内でどのようなコードが実行されているかを正確に把握し、深く理解する必要があります。

*https://blogs.trellix.jp/tarfile-exploiting-the-world



10代のサイバー犯罪者の活動があらゆる規模で活発化

By Rhonda Leopold

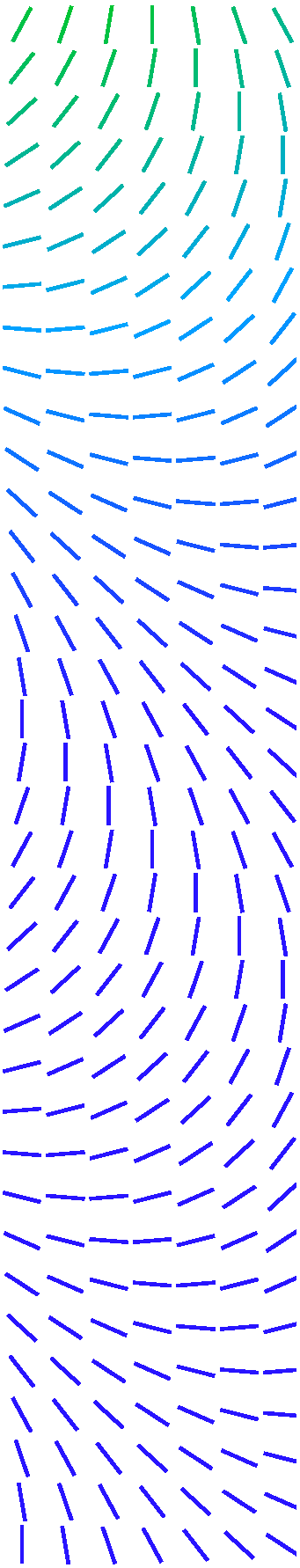
オンライン詐欺は、毎年何十億ドルもの経済的損失をもたらしています。学校、病院、企業のセキュリティ予算は今後も増え続けるでしょう。しかし、子どもたちが詐欺師にならないように、またオンラインで盗みをしないように教えることは、まだ社会に根付いていないのが現状です。ネット上での軽微な窃盗やハラスメントに関しては、子どもがサイバー犯罪者になる危険性を伝えるために、まだやるべきことがあります。ネット上で子供の安全を守ることは親の最大の関心事ですが、同時に、子供がネット上で倫理的な行動をとっているかどうかも心配しなければなりません。映画、大学の教科書、ソフトウェア、ゲームなどの違法ダウンロードは、子供にとって犯罪というより挑戦と捉えられることが多いようです。時には、親がこのような行為を奨励することさえあります。だからこそ、あらゆるレベルで教育が必要なのです。

技術的に優秀な若者が、悪徳業者や組織にリクルートされているのを私たちは目にしています。2021年後半から、16歳の若者がLapsus$ギャングを名乗り、マイクロソフト、NVIDIA、Okta、サムスンなどの国際組織のハッキングを成功させたと言われています。これらのサイバー犯罪組織は今日、フォーチュン500企業とセキュリティ企業の人材的な競争相手であり、いずれもオンラインで社会を保護するために取り組んでいます。

若者をサイバー犯罪の世界に引き込まないために、世界的な取り組みが行われています。サイバー犯罪の危険性を若い世代に伝えるために、ゲームを通じて危険性を教える「Hackshield」のような新しい取り組みもあります。しかし、世代間のギャップに対処し、親が子供たちをささいなサイバー犯罪やより悪質な犯罪から遠ざけるよう教育する必要があります。

> 2023年には、企業や政府に対する大規模な攻撃から、家族、友人、仲間、見知らぬ人をターゲットにした小規模の犯罪まで、

手っ取り早く金を稼ぐ、恥をかかせる、新しいスキルを試す、社会資本を得るなど、10代や若年層の活動が活発化すると予想されています。この問題は拡大し、予算の増加が続き、コストは私たち消費者に引き継がるかもしれません。キーボードでの犯罪とは何かを子供たちに教えることは不可欠です。



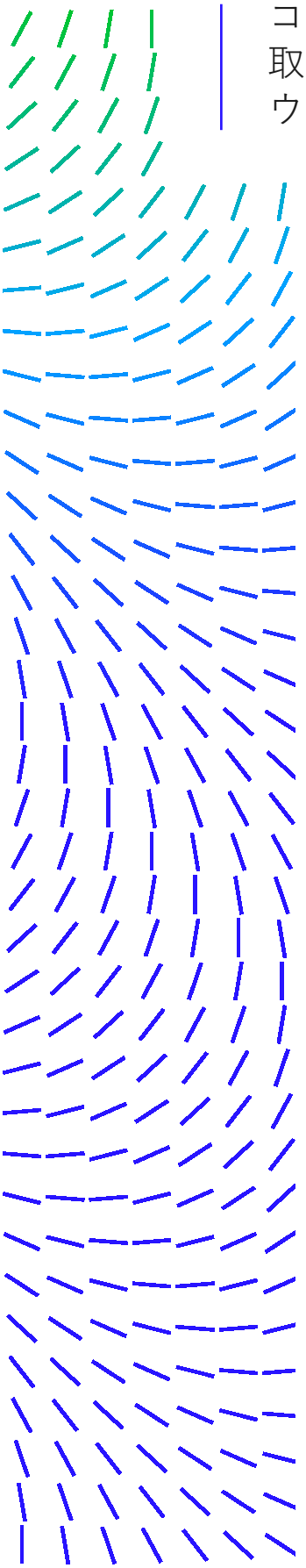
コード分析による攻撃者特定の精度低下

By Max Kersten

今日の世界では、デジタルの脅威が圧倒的です。インターネットは多くの人に前例のない匿名性を提供しますが、たびたびミスが発生します。このようなミス、あるいはパンくずによって、捜査当局や研究者は行為者を追跡することができます。サイバーセキュリティの分野では、マルウェアのサンプルを分析することが重要視されています。コーディングスタイルは、手書きの文字と同じように、攻撃者に関連付けることができることが何度も証明されています。時とともにマルウェアの開発は多様化し、行為者は、違法な金銭的利益を求める純粋な日和見主義的犯罪者ではなく、違法な金銭的利益を求める、高度に組織化され専門化されたプロフェッショナルになっています。このような主張は、真偽を問うものではありません。むしろ、多くのグループが時代とともに発展し、他のグループが日和見主義的であり続けることを示すものです。

しかし、純粋にコードだけを基にした帰属には問題があります。高度なスパイ活動を行うグループは、機密保持のためにキャンペーン用のツールを独自に作成することがよく知られていますが、他の種類のマルウェアの中には、そのような機密保持自体を必要としないものもあります。そのようなマルウェアの主な例はワイパーです。 ワイパーが使用されると、それは目新しいものではなくなり、マルウェアの検出と防止が実装されることになります。マルウェアの作成は、多くの場合、コーダーがマルウェアをサービスとして販売したり、アフィリエイトと協力したりすることによって行われると考えられています。作成は正当な請負業者に委託することもできます。その場合、契約した作成者はさまざまなコーディング スタイルを持っているため、コード ベースの帰属が非常にわかりにくくなります。 2022 年 6 月の私たちの遠隔測定では、意味のあるコードの重複がない複数のワイパーの使用が発見されました。その際、攻撃者は、 WhisperGate ワイパーの起動に失敗し、代わりに HermeticWiper に切り替えましたが、それら一連の作業は 3 時間以内に行われました。

WhisperGateワイパーのコードはHermeticWiperのコードとリンクしておらず、両者が同じ攻撃者によって使用されている（そして作成されている可能性がある）という仮定は、サンプルのコードベースのみに基づく根拠のない主張です。他のインテリジェンスによってこのような主張が（非）証明されるかもしれませんが、帰属が意味をなすためには、追加のコンテキストが必要であることに注意することが重要です。このことは、コードベースの属性に完全に依存することがいかに難しいかを示しています。特に、広くアクセス可能な悪意のあるファイル自体とは対照的に、すべてのアナリストが必要な追加コンテキストにアクセスできるわけではないためです。



コードベースの攻撃者特定の精度の低下は、それ自体は取るに足らないように見えますが、特に（流出した）マルウェアのソースコードの再利用や、

細分化されたアンダーグラウンドでの攻撃者間の連携を考慮すると、今後さらに問題になる可能性があります。したがって、私たちは、アナリストが事実によって（完全に）裏付けられていない主張を行う際には、信頼度を記載することを強くお勧めします。そうすることで、レポートがどのように受け取られるべきかを読者に明確に示すことができ、最初から適切な対応を取ることが可能になります。

サイバー戦争の進展に伴い、重要インフラに対し、世界的なサイバー脅威が差し迫る

By John Borrero Rodriguez

ロシアのウクライナ侵攻以来、サイバー攻撃は国家だけでなく、サイバー犯罪者、ハクティビスト、その他の低スキルのアクターから、劇的に進化しています。重要インフラを標的とした戦術は、サイバー戦争の状況を悩ませています。現在観察されている戦術のパターンは、多数の事業体に対する攻撃性とリスクの増大を示唆しています。同様に、サイバー戦争の巻き添えによる被害者の増加も観察されている。これらのリスクは、エネルギー、銀行、軍事の重要な部門に属する人々にとって、これまで以上に大きなものとなる可能性があります。

Turla、Metador、UNC3886のような脅威者は、その活動の増加により、自分たちが注目されていることに気づきました。さらに、UNC3886のVMware ESXi悪意のあるVIBファイルの永続化などの新しい手法や、不安定な国際紛争の増加により、APT（Advanced persistent threats）がより適応、拡大、およびキャンペーンを実施する絶好の機会が生み出されています。

2023年には、単純なセキュリティ計画だけでは、攻撃者を抑止あるいは防止することがより困難になります。世界中のシステム防衛者は、政府、軍、および複数のガバナンス環境で採用されている厳格な業界標準に基づき、より積極的な防衛アプローチを実施しなければならなくなるかもしれません。脆弱なターゲットの重要なインフラに混乱をもたらす高度なサイバー攻撃者が大幅に増加する可能性は十分にあります。新しい技術の発見が、他の悪意ある攻撃者がその技術を採用し、インターネットに接続されているユーザー、産業、重要な資産をさらに脅かすようにキャンペーンを変更する可能性があることは間違いありません。

サイバー戦争は、敵対勢力に同調したユーザーが行動を起こしたり、無防備なユーザーが架空のアプリケーションやキャンペーンに利用されたり、常に変化し続けています。今後は、重要インフラを標的とした攻撃の起点として、無防備なユーザーを利用するケースが増加することが予想されます。

重要インフラへの脅威がさらに増大するにつれて、戦争目的で指数関数的に大規模な分散型サービス拒否攻撃で乗っ取られるIoTデバイスが増える可能性があります。

コラボレーションが進むとフィッシングも増える

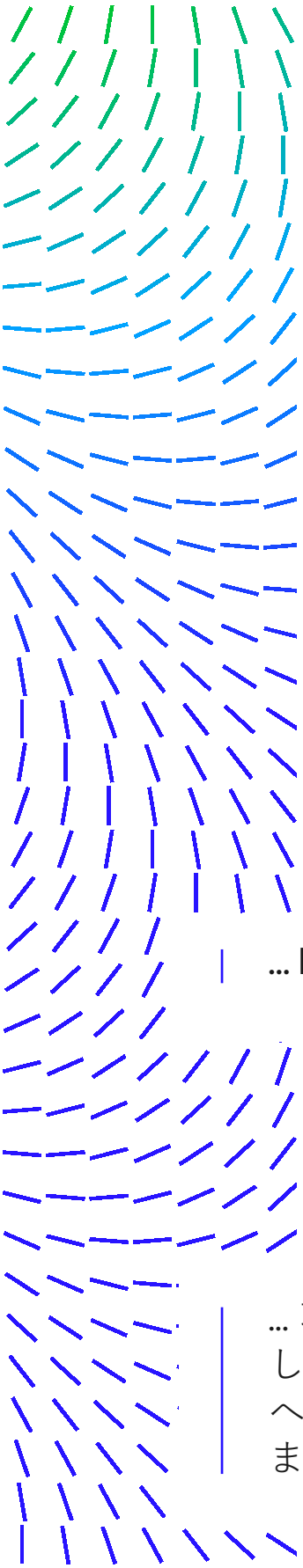
By Jaspreet Singh

2023 年には、武器化されたフィッシング攻撃が、一般的に使用されているビジネス コミュニケーション サービスやアプリ全体に広がると予想されます。

スミッシング、ビッシング、ソーシャルメディアフィッシング、およびビジネスメール侵害攻撃は、従来はフィッシング対策ツールバーとメールセキュリティ保護で管理されてきましたが、近い将来、フィッシングはメールやメッセージを超えて拡大し、よりステルス性の高い方法でコミュニケーションチャネル全体に広がる可能性があります。

Slack、Teams、ClickUp、ProofHub、Chantyなどのメッセージングチャネルやビジネスコラボレーションアプリは、組織にとってコミュニケーションを容易にし、コラボレーションを簡素化するために不可欠なものです。AIによる高度な手法を用いたフィッシングメールの開発が加わることで、フィッシングの状況はさらに複雑になっています。Zoombombingや類似の手法が観察されていますが、ビジネスコラボレーションアプリの利用が脅威のベクトルとして拡大することが予想されます。

世界各地の脅威者は、組織のネットワークに侵入し、掘削するために、既存の手法を強化および調整する可能性があります。ハイブリッドワークの浸透によって、個人の脆弱で管理の行き届かないホームネットワークやデバイスに攻撃対象領域を拡大する一方で、脅威者は、これを媒体として企業ネットワークを容易に攻撃できるようになり、利益を得ています。このため、企業を標的としたフィッシング攻撃の試みが増加し、企業は境界線と電子メール保護サービスの強化に力を入れるようになりました。新年も、他の通信チャネルを標的とした新しい戦術やテクニックに目を向けることは、決して見過ごせず、怠るべきではありません。



“Alexa、ビットコインのマイニングを始めて！”

By Ajeeth Srinivasan

私たちを取り巻く世界がよりデジタル時代に移行する中、IoT機器は私たちの日常生活の一部となっています。スマートデバイスは、車を運転したり、コーヒーを温めてくれたり、ドアを開けてくれたりします。興味深いことに、これらのデバイスや機能が不正を始めると、その裏側が見えてきます。

コインマイナーは、常に影に隠れ、システムリソースを利用して仮想通貨をマイニングする静かな性質で知られています。最近のデバイスの高精度化・高機能化に伴い、これらのデバイスの高性能なハードウェアがハッカーによって利用され、あなたの電気代で仮想通貨をマイニングする可能性があります。さらに悪いことに、これらのデバイスは、Pegasusで見られたように、国家やAPTグループによって、著名な標的を監視するために使用される可能性があります。このようなスマートデバイスには適切なマルウェア対策ソリューションが少ないため、セキュリティアナリストはマルウェアを手動でリバースエンジニアリングするのに苦労する可能性があります。

クリプトマイニングには膨大なリソースが必要ですが、最近の仮想通貨の価値の変動に伴い、仮想通貨を合法的にマイニングすることは最良の選択肢とは言えなくなっています。1台のIoT機器がマイニングに大きく貢献することはないかもしれませんが、Miraiのようなボットネットは、数千台のデバイスを1つの傘下に置くことができます。IoT機器から他のOSへコインマイナーが移動するケースもあり、IoT機器の製造においてセキュリティは最重要事項ではないことから、

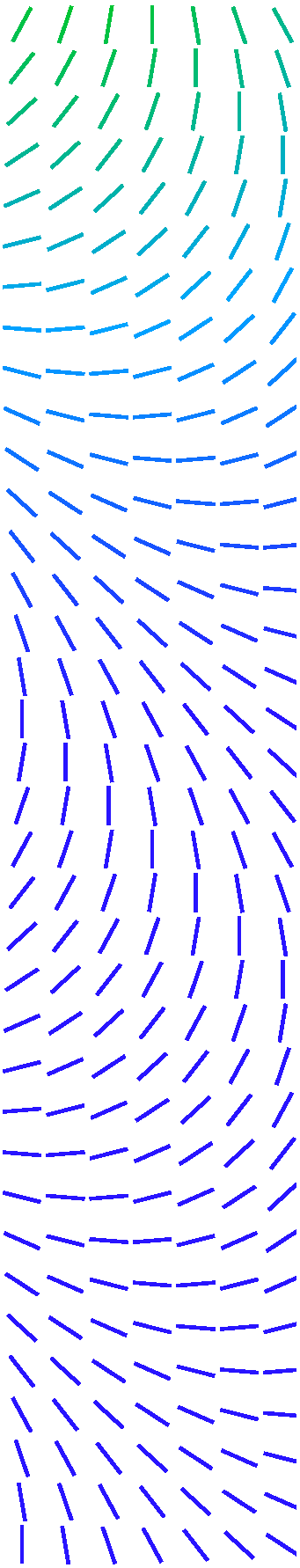
> … IoT機器経由のクリプトマイニングの急増が予測されます

宇宙のハッキング: ここからが本番!

By Ryan Fisher

より多くの衛星が打ち上げられ、社会が衛星データやインターネットアクセスに依存するようになると、

> … 攻撃対象領域が拡大し、通常は、攻撃が続くことを歴史が示しています。2023年には、人工衛星やその他の宇宙上の資産への侵害が増加し、より公になる可能性があると予想しています。

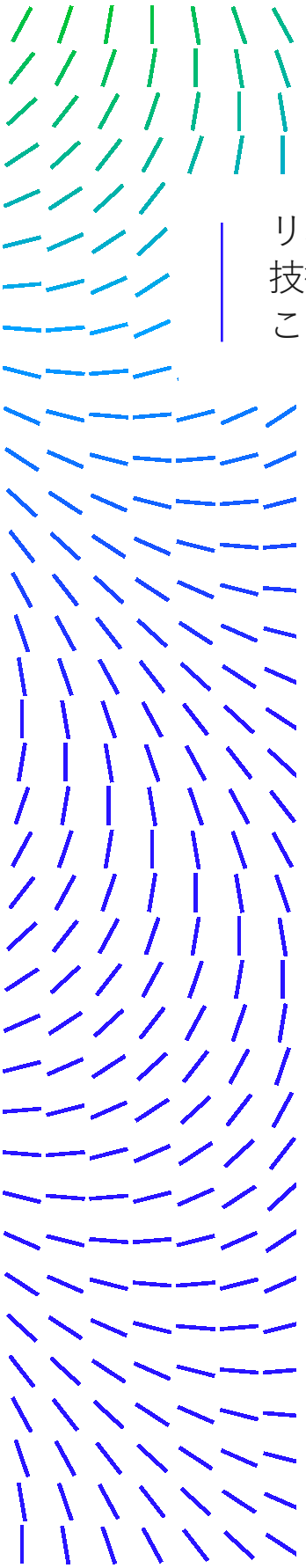


1957年に最初の人工衛星スプートニクが打ち上げられてから2019年までの間、年間600基弱の人工衛星が打ち上げられました。しかし、その数は2021年には1800基へと急増し、2022年にはさらに増えるでしょう。人工衛星は、専用のコンピューターであり、地上で発生しているのと同じようなサイバーセキュリティの脅威の多くに対して脆弱であるという事実から、衛星に対するリスクが強調されています。人工衛星の地上管制のリスクについては、1998年にハッカーがメリーランド州のゴダード宇宙飛行センターに侵入し、NASAのコンピュータネットワークを侵害した際に初めて実証されました。彼らはその後、ROSAT（X線衛星）に太陽電池パネルを直接太陽に向けるように指示しました。これによりバッテリーが焼け、衛星は使い物にならなくなりました。しかし、地上管制ステーションを突破することは必ずしも必要ではありません。特に、コストを抑えるために既製の部品を使用した小型で安価な「CubeSat」の普及が進んでいます。また、地上通信設備も比較的安価なため、衛星が上空を通過するのを待って、衛星のハードウェアやソフトウェアの脆弱性を突いた悪意のあるコマンドを送信するだけで、簡単にハッキングできる場合もあります。

地球低軌道（LEO）にペイロードを投入するコストが下がり続ければ、ますます多くの企業が衛星を打ち上げるようになるでしょう。そして、他の産業と同様に、設計の初期段階でサイバーセキュリティを十分に考慮しなければ、他のエンジニアリングの課題に後回しにされ、システムが危険にさらされる可能性があります。

ウクライナでSpaceX社のStarlink端末に対して行われたような標的型サービス拒否攻撃は、今後ますます増えていく問題かもしれません。Starlink社の場合は、すぐにサイバーセキュリティにリソースをシフトして妨害行為に対処することができましたが、すべての衛星会社が同じように機敏に対応できるわけではありません。この例として、Viasat社が経験したKA-SAT SATCOM攻撃は、2022年2月24日にロシアがウクライナに対して開始した物理的攻撃と同時期に発生しています。ウクライナを含む欧州の数カ国で数万台のSATCOM端末が突然動かなくなりました。詳細は明らかにされていませんが、現在のところ、管理ネットワークの設定ミスにより、攻撃者が地上局を侵害/偽装してコマンドを発行し、端末に悪意のあるファームウェア・アップデートを展開し、端末をオフラインにした、という説が有力視されています。

もう一つの懸念は、ランサムウェアです。宇宙開発は、純粋な科学研究から重要なインフラへと進化を続けていますが、それに伴い、重要なインフラが提供するサービスの価値を知っている悪意のある攻撃者が出現しています。重要インフラの衛星をロックし、プロバイダーやリンクを使用している企業に身代金を要求することは、これらのネットワークは長時間オフラインにしておくことができない特性上、ランサムウェアの作成者にとって有利な支払いとなる可能性が高くなります。



”これ、私の電話番号だから、よかったら電話してね！”

By Daksh Kapur

リバースビッシング（ボイスフィッシング）攻撃が急増し、技術的な知識の乏しいユーザーが格好のターゲットになることが予想されます。

リバースビッシングは、潜在的な被害者が攻撃者によってコールドコールされるビッシング（ボイスフィッシング）の変形のような詐欺行為で、攻撃者が用意した電話番号に対して被害者に電話をかけさせて、個人情報などを盗み出そうとする手口です。電話番号は、銀行取引や注文の取り消しなどの緊急通知を含む電子メールやSMSなどの一部として被害者に提供されるため、被害者はその番号に電話をかけざるを得なくなります。

最近まで、攻撃者は、マルウェアの配布や資格情報の取得のために、添付ファイルやURLといった従来の電子メール攻撃媒体を主に利用していました。このような攻撃では、セキュリティ製品は添付ファイルやURLをスキャンに重点を置き、その判定に基づいて検出結果を提供します。

リバースビッシングキャンペーンの厄介な点は、電子メールベースの攻撃で使用されてきたURLや添付ファイルのような従来の悪意のあるエンティティを含まず、ユーザーが電話をかける必要がある電話番号を含んでいることです。このようなケースでは、従来の攻撃ベクトルに基づくスキャン技術は適さないため、セキュリティ企業にとって大きな課題となります。

電子メールのコンテンツのパターンに基づいて検出ルールを作成し、スクリーンショット、アドレス、IPなどの他の電子メールパラメータと組み合わせることで、このような攻撃をある程度制御することは可能です。検知ルールやパラメータは、敵の戦術の進化のペースに合わせ、常に更新する必要があります。私たちは、このような攻撃に関する絶え間ない研究により、このような攻撃から進歩的な検出を提供することができます。

私たちは、リバースビッシングの事例が2021年以降500%以上増加し、それが減少しているようには見えないことを確認しています。

敵対者は、テキストやWhatsAppなどのサードパーティメッセージングアプリ、Googleレビューなどの情報媒体など、さまざまな媒体から被害者を攻撃するために爪を広げており、より厄介な状況になっています。上記のような媒体のコンテンツを規制するのは厄介なので、攻撃がすり抜けるトンネルになるため、さらに問題です。

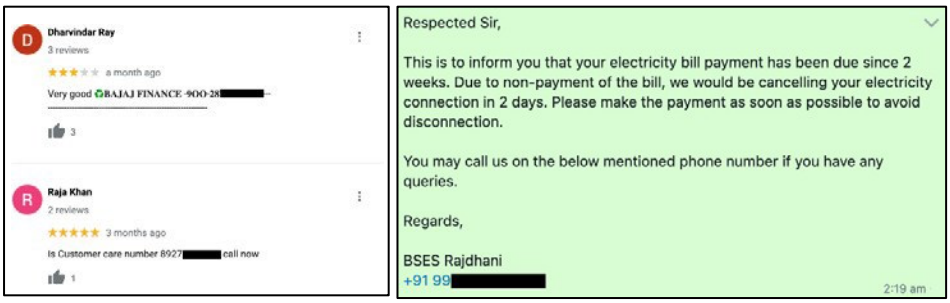


図1-電子メール以外の媒体で配信されるリバースピッシング攻撃の例

このような攻撃を効率的に検知するためには、さらなる研究が必要であり、それが実現するまでは、リバースピッシングは横行し、技術的な知識に乏しい人々が最も被害を受ける可能性があります。

Windowsドメインに対する攻撃が大規模化

By Bing Sun

Windowsドメイン/Active Directory全体、または組織のネットワーク全体を乗っ取ることは、Windowsエコシステムに対する多くの標的型攻撃の最終目標です。攻撃者が組織内部のネットワークに最初の足がかりを得ると、次に行うことは、Windowsドメインコントローラのような他の重要なシステムに移動し、ドメイン全体をさらに侵害することです。この目標を達成するために、攻撃者は特定の脆弱性を利用してユーザー特権を昇格させる必要があります。例えば、CVE-2021-42287/CVE-2021-42278 (Active Directory Domain Services Elevation of Privilege Vulnerability, aka noPac) を悪用して、ドメイン管理者を表すサービスチケットを攻撃者に付与することが可能です。

典型的な攻撃シナリオでは、攻撃者は通常、基本ユーザー（権限の低いユーザー）として内部ネットワークに侵入しますが、認証されたユーザー（すでにドメインのメンバーであることを意味します）として、ドメインの権限昇格の脆弱性を悪用して、ドメイン管理者に自分自身を昇格させることができます。その後、攻撃者はゴールデン チケット、シルバー チケット、DCSync などの従来のドメイン攻撃手法を使用して機密情報を取得し、重要なドメイン リソースへの永続的なアクセスを維持できます。

Windows Doman/Active Directoryは、複数のサービスやプロトコルを含む重要かつ複雑なシステムであり、これらのサービスやプロトコルに脆弱性があると、システム全体が侵害される可能性があります。これにより、攻撃者は組織の機密情報に完全にアクセスできるようになり、漏えいしたデータから利益を得ることができるようになります。Windows Doman/Active Directoryシステムの重要性と複雑性から、この「金鉱」領域はハッカーやセキュリティ研究者の注目を集め

バグの発見や新しい攻撃手法の開発に励んでいるのです。我々の観測によると、Microsoftは過去数年間にかなりの数のWindows Doman/Active DirectoryおよびNTLM/Kerberos関連の脆弱性を修正しており、毎年パッチが適用される脆弱性の総数は増加傾向にあるようです（2020年に8件、2021年に10件、2022年に22件）。さらに、NTLMのADCSへの中継やKerberosの中継攻撃など、新たな悪用ベクトルも発見されています。

2023年は、さらに多くのドメイン権限昇格の脆弱性が発見される可能性があり、同時に、ネットワークの完全な乗っ取りという明確な目標を持った、Windows に対する実際の攻撃が引き続き増加する可能性があります。

Trellix Advanced Research Centerについて

Trellix Advanced Research Centerでは、セキュリティの専門家と研究者のエリートチームが、洞察に満ちた実用的なリアルタイムインテリジェンスを作成し、お客様の業績や業界全体を推進するために活動しています。業界で最も包括的な行動憲章に基づき、熟練した研究者が市場に先駆けてトレンドを検知し、お客様やパートナーが新たな脅威に対処できるよう支援します。
詳しくは、https:// www.trellix.com/en-us/advanced-research-center.html.

https://twitter.com/TrellixARC

Trellix

Trellixについて

Trellixは、サイバーセキュリティの未来を再定義するグローバル企業です。オープンかつネイティブなTrellixのXDR（Extended Detection and Response）プラットフォームは、現在最も高度な脅威に直面するお客様が業務の保護や回復に確信を持って対応するための支えとなります。Trellixのセキュリティ専門家は、広範なパートナーエコシステムとともに、データサイエンスと自動化によりテクノロジーイノベーションを加速させ、4万を超える企業や政府機関のお客様の力となっています。

072022-05