SOPHOS
Cybersecurity evolved.

2021 年版
ソフォス脅威レポート

この不透明な世界でサイバーセキュリティを
どう舵取りするのか

著者：**SophosLabs、Sophos Managed Threat Response、
Sophos Rapid Response、Sophos AI、Cloud Security**

目次

助け合うことが大きな力に 2

エグゼクティブサマリー 3

ランサムウェアの今後 5
- 盗み出されたデータが作り出す「第 2 の恐喝」市場 5
- 攻撃の増加に伴い身代金の金額も増加 7
- ランサムウェア緊急対応チームの活動 9

企業を日々狙う脅威 ―「炭鉱のカナリア」 10
- Windows サーバーや Linux サーバーを標的とする攻撃 10
- 「コモディティ」マルウェアの過小評価は危険である 12
- 配信の仕組み 14
- 情報セキュリティの 20 年を振り返る 18

COVID-19 に便乗した攻撃 20
- 家庭が新しい境界に 20
- サービスとしてのクライムウェア (CaaS) 21
- スパム、詐欺、反故にされた約束 22
- リモートワークによりクラウドコンピューティングのセキュリティ保護の重要性が高まる 25
- 大規模な脅威への迅速な対応における CCTC の意義 27

油断禁物：新しいプラットフォームを介する脅威 28
- Android Joker マルウェアの増加 28
- 広告 /PUA とマルウェアの境界が曖昧に 29
- 自分を保護するツールが悪用される：サイバー犯罪者によるセキュリティツールの悪用 31
- デジタル疫学 33

助け合うことが大きな力に

Joe Levy (ソフォス、CTO)

「早く行きたければ一人で行きなさい。遠くへ行きたければみんなで行きなさい」

これは、アフリカのことわざですが、サイバーセキュリティ業界にとってこれほど胸に響く言葉はないでしょう。強いチーム意識を持って集団で取り組むことで、個々のベンダーがサイバー犯罪に立ち向かうよりもはるかに大きな成果を上げることができます。

しかし、アプローチを改善し、脅威インテリジェンスを包括的に共有し、この共有とコラボレーションに貢献する (さらに、そこから利益を得る) 参加者を増やすことによってのみ、サイバーセキュリティベンダーはより強固な防御策を講じることができ、持続的で効果的な変化をもたらし続けることができます。

2017 年、ソフォスはこの助け合いの精神の下、*Cyber Threat Alliance (CTA)* に参加しました。これは、情報セキュリティ業界の競合他社が協力し合う機会を長年妨げてきた障壁を取り除くことを目的として結成された組織です。CTA は、脅威インテリジェンスを共有し、互いの立場を越えて解決策を追求するという当初の使命をさらに超えて成功を収め、サイバーセキュリティ業界の国連のような存在となっています。

ソフォスは、CTA との提携によって可能になった早期警告やベンダー間のデータ交換を通じて、お客様をより確実に保護できるようになりました。また、ソフォス独自の脅威情報を提供することで、他のベンダーの顧客を保護する役割も共に担っています。

2020 年 3 月、新型コロナウイルス感染症 (COVID-19) の拡散を封じ込めるため、世界中でロックダウンが実施される中、ソフォスのチーフサイエンティストの Joshua Saxe が Twitter で声を上げました。犯罪集団がさまざまな攻撃で COVID-19 に便乗し始めていることに衝撃を受けた 4,000 人以上の情報セキュリティアナリストは、断固として対抗するために結集し、その日のうちに立ち上げられた Slack チャネルで COVID-19 Cyber Threat Coalition (CCTC) を結成しました。このチャネルは、この危機に対してコミュニティが活用できる「共有スペース」を構築するものであり、CTA の支援を受けて非営利団体として活動を進めようとしています。

最終的に、このような脅威インテリジェンス共有の試みから、組織の枠組を超えた教訓を得ることができます。盲人が象を語るたとえ話に示されるように、個別の主観的経験だけでは、どのベンダーも包括的または絶対的な真実を提示することは不可能です。複雑なものの真の姿は、個々の経験を集結させることから浮かび上がってきます。このように協力して取り組むことによって、何百万人もの人々がサイバー犯罪の被害から保護されました。しかし、この取り組みが成功した*理由*は、それだけでは説明できません。危険な状況にある人々を守ることが、参加者や結成者の主な動機となっていたため、取り組みが成功したのです。そこに利益追及の動機はなく、差し迫った危険から弱者を守りたいという思いだけでした。

それが、このモデルの正しさを証明し、個人では成し得ない規模で重要な溝を埋めるものとなっています。しかし、私たちにできることはそれだけではありません。業界として、現在ブロックリストや Yara ルールを共有しているように、将来的には機械学習モデルやトレーニングデータセットの共有を検討するようになる可能性があります。また、STIX や ATT&CK フレームワークのような新たな標準の策定や強化に対して貢献することも可能です。さらに、業界に特化した ISAC や ISAO に参加することもできるでしょう。

つながりが深まる未来は、私たち全員にとって利益の拡大 (そして保護の強化) をもたらします。

エグゼクティブサマリー

2021 年版ソフォス脅威レポートでは、SophosLabs によるマルウェアとスパムの分析、および Sophos Rapid Response、Cloud Security、Data Science の各チームの活動によって、過去 12 か月間に知見が得られたトピック領域を取り上げます。ソフォスがお客様を保護するために行っているこれらの日常的な活動は、脅威に関する知見を提供し、インシデント対応の担当者や IT セキュリティ専門家が、今後 1 年間にネットワークやエンドポイントを防御するために何に注力すべきかを示します。

本レポートは、次の 4 部構成になっています。第 1 部は、ランサムウェアの変遷と今度の方向性について説明します。第 2 部は、大規模組織が直面する最も一般的な攻撃の分析と、「炭鉱のカナリア」に例えられる脅威の重要性について説明します。第 3 部は、世界的なパンデミックが 2020 年の情報セキュリティに与えた影響について説明します。第 4 部、従来は企業の攻撃対象の一部とは考えられていなかったプラットフォームを標的とする攻撃範囲の調査について説明します。

本レポートの主なポイントを以下にまとめます。

ランサムウェア

- ランサムウェアを使用する攻撃者は、テクノロジーと手法の両面でイノベーションを加速させています。
- データを窃取し、機密データの公開を告知してターゲットを恐喝するランサムウェアグループが増えています。
- ランサムウェアグループが大規模組織に対する積極的な攻撃に一層力を入れるようになり、要求される身代金額が急増しています。
- さらに、ランサムウェア攻撃を行う攻撃者集団は、地下組織の犯罪者同士で密接に連携しているとみられ、それぞれ独立したグループというよりも、むしろサイバー犯罪カルテルのように振る舞っています。
- 以前は数日 / 数週間かかっていたランサムウェア攻撃が、今では数時間で実行される場合があります。

「日常」の脅威

- Windows と Linux の両方を実行しているサーバープラットフォームは、集中的に攻撃の標的にされ、内部から組織を攻撃するために利用されています。
- RDP や VPN コンセントレーターのような一般的なサービスは、ネットワーク境界で攻撃の焦点となっています。また、RDP は侵害されたネットワーク内のラテラルムーブメントにも使用されています。
- 他のマルウェアの「コンテンツ配信ネットワーク」として機能するマルウェアファミリーが増えています。このため、ローエンドの「コモディティ」マルウェアであっても大規模な侵害を引き起こす恐れがあります。
- これまでにソフォスが調査した最も被害の大きな攻撃の多くは、セキュリティの基本的対策に見落としがあることが根本的な原因であることが判明しています。

COVID-19

- リモートワークの推進によって新たな課題が生まれ、保護レベルが一様でない何千ものホームネットワークにまで組織のセキュリティ境界が拡大しています。
- クラウドコンピューティングは、コンピューティング環境の保護に対する多くの企業のニーズに応えることに成功している一方で、従来の企業ネットワークとはまったく異なる独自の課題も抱えています。
- 攻撃者は、救命活動に関わる医療機関を標的にしないと約束して活動を正当化しようとしましたが、その後に約束を反故にしました。
- さまざまな形態や規模の犯罪者集団がサービス経済圏を形成しており、新たな犯罪者が参入しやすくなっています。
- 2020 年に世界中のサイバーセキュリティの専門家が結集して形成した組織は、新型コロナウイルスに便乗したソーシャルエンジニアリングを悪用する脅威に対抗する緊急対応チームとなりました。

攻撃に使用される新しいプラットフォーム

- 攻撃者は、手動による攻撃で、侵入テスト向けに開発された多様な「レッドチーム」用のツール / ユーティリティを日常的に活用しています。
- モバイルプラットフォームの運営者は、悪意のあるコードがアプリに含まれていないかを監視しています。その一方で、攻撃者は巧妙なやり方でコードスキャンを迂回する手法を開発し続けています。
- 従来は、大量の広告配信を目的としていたため、悪意はないにせよ「潜在的に迷惑なソフトウェア」に分類されていたソフトウェアが、明らかなマルウェアと見分けにくい戦術をとるようになっています。
- データサイエンティストは、脅威検知のギャップを埋める手法として、生物の疫学分野から着想を得たアプローチをスパム攻撃やマルウェアのペイロードに応用しています。

ランサムウェアの今後

2020 年のランサムウェア攻撃は、新型コロナウイルスへの警戒で疲弊している多くの人にさらなる痛みをもたらしました。パンデミックが人命と生活に甚大な影響を及ぼし、医療機関は COVID-19 の戦場となり、学校は 3 月以降も新たな学習方法を編み出すために奮闘しました。このような状況下で、多くのランサムウェアファミリーは医療機関や教育機関を標的として攻めの手を緩めませんでした。

パンデミック下で厳しい経営環境に置かれている組織がランサムウェア攻撃を受けると、その身代金は非常に重くのしかかります。しかし、安全なバックアップを維持することにより、新学期の初日を狙ったとみられる攻撃から回復に成功した学校もあります。

ランサムウェアの運用者は、エンドポイントセキュリティ製品を回避する方法や、ランサムウェアを急速にばら撒く方法を新たに開拓しています。また、標的となった個人や企業が、ランサムウェアの被害が及ばない場所に安全に保存された十分なバックアップを持っているという、(攻撃者から見た問題についても、解決策を考案しています。

しかし、多種多様に存在すると見られるランサムウェアは、実はそれほど多彩ではないのかもしれません。ソフォスのアナリストが増え続ける攻撃を調査してきた中で、異なるファミリーの間で一部のランサムウェアコードが共通しているとみられ、一部のランサムウェアグループは競合ではなく協業していると考えられることが明らかになりました。

これらを踏まえると、ランサムウェアを使用する犯罪者が次にどのような行動をとるのかについて、確かな予測を立てるのは困難です。ランサムウェアの作成者や運用者は、エンドポイントセキュリティ製品に対する防御に多くの時間を費やしてきました。そのような対策に対して、私たちはさらなる対策を講じています。犯罪者が創造力と多芸さを発揮して、新しい戦術を編み出しているのに対して、私たちは犯罪者の活動を研究し、攻撃を阻止するための妙案を見つけるため、粘り強く取り組んでいます。

盗み出されたデータが作り出す「第 2 の恐喝」市場

今年まで、ランサムウェアについて経験があるセキュリティ企業の間で一般的な慣行となっていたのは、「インターネットに接続する RDP ポートなどの明白な侵入方法を遮断する」「オフラインでのバックアップをしっかりと取る」「Dridex や Emotet のような小規模で被害が軽微なマルウェアの感染にも迅速に対処して、致命的な影響もたらすペイロードの配信を防ぐ」ことでした。

米国全土の学区が標的となったことで大きく報道されたランサムウェア攻撃が失敗したのも、IT 管理者が重要なデータのバックアップを維持して影響を回避できたことが要因でした。

被害者の備えを考慮した対抗策として、一部のランサムウェアファミリーは「第二のビジネス」に手を延ばしています。これにより、被害者が重要データを含むすべてのバックアップを安全に維持している場合であっても、身代金を支払うように圧力をかけます。つまり、マシンを人質にとるだけでなく、マシン上のデータを窃取し、ターゲットが身代金を支払わなければ情報を公開すると脅します。

ソフォスのアナリストの研究によると、過去半年の間に、ランサムウェアの攻撃者は被害者のネットワークからデータを窃取するために、共通 (しかも徐々に拡大中) のツールセットを利用するようになっています。よく知られた合法的なユーティリティを含むこのツールセットは、誰もが使用でき、エンドポイントセキュリティ製品によって検知されません。この攻撃方法をとるランサムウェアファミリーは増加し続けており、現在では Doppelpaymer、REvil、Clop、DarkSide、Netwalker、Ragnar Locker、Conti なども含まれています。攻撃者は、どのようなデータを盗んだかを公表する「リーク」サイトを運営しています。REvil の Web サイトでは誰でもデータを購入できます。

犯罪者はツールセットを使って、組織の機密情報をコピーしてアーカイブに圧縮し、ネットワークの外部に転送して被害者の手の届かないところに移動させます。これまでに、以下のようなツールが使用されたことが確認されています。

- Total Commander (FTP クライアント組み込み型ファイルマネージャー)
- 7zip (アーカイブ作成ソフト)
- WinRAR (アーカイブ作成ソフト)
- psftp (PuTTY の SFTP クライアント)
- Windows cURL

データ窃取に関しては、攻撃者は取捨選択せず、含まれるファイルの種類に関係なくフォルダ全体を盗み出します (一般的にランサムウェアは、攻撃で主要なファイルタイプに対する暗号化を優先させ、他の多くのファイルタイプを除外します)。

データ窃取の対象とするデータの量は気にかけていないようです。ディレクトリ構造はビジネス固有であり、圧縮のしやすさはファイルタイプによって異なります。少ないものでは 5GB、大きいものでは 400GB の圧縮データが、ランサムウェアが展開される前に窃取されたことが確認されています。

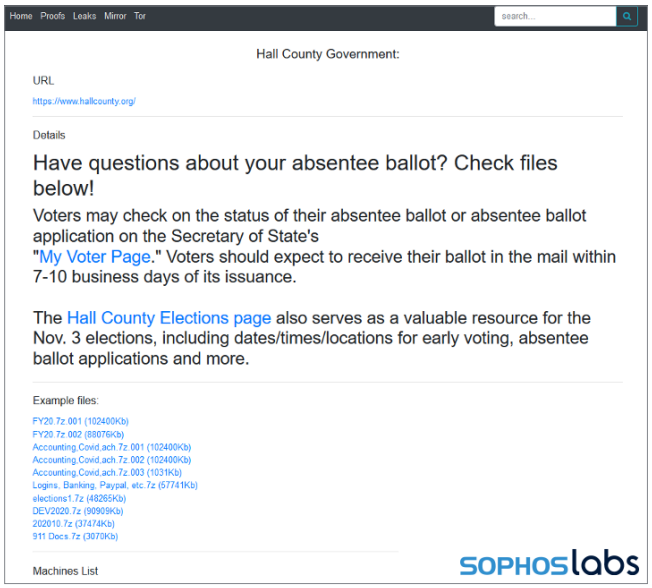


図 1: 2020 年 10 月、ランサムウェア Doppelpaymer のリークページで、攻撃者が米国ジョージア州ホール郡のネットワークを攻撃していたことが明らかになりました。リークサイトで言及されている「elections」というファイルには、2020 年に行われたジョージア州予備選挙の投票証明サンプルや、2018 年の選挙での開票作業員の名前や電話番号のリストなど、機密性の高いファイルが含まれていました。AP 通信は、同郡が投票用紙の検証に使用していた署名検証データベースが、このランサムウェアによって暗号化されたことを報じました。出典：SophosLabs

犯罪者は、通常、窃取したデータを合法的なクラウドストレージサービスに送信します。これらのサービスは、一般的な通常のネットワークトラフィックの送信先であるため、このような活動を検出するのは困難です。以下の 3 つのクラウドストレージサービスは、窃取したデータの保存先として最も広く攻撃者に使用されています。

- Google Drive
- Amazon S3 (Simple Storage Service)
- Mega.nz
- プライベート FTP サーバー

破壊行為の最終段階として、ランサムウェアの攻撃者は、重要データのバックアップを含むローカルサーバーを探します。見つけた場合には、ネットワーク全体の暗号化攻撃を実行する直前に、これらのバックアップを削除または個別に暗号化します。

したがって、キーデータのバックアップをオフラインで保存することが、これまで以上に重要となっています。ランサムウェアの犯罪者に見つかれば、破壊されてしまいます。

攻撃の増加に伴い身代金の金額も増加

SamSam と呼ばれるランサムウェアの運用者が 600 万ドルもの大金を獲得したことにソフォスのアナリストが驚嘆したのは、わずか 2 年前のことでした。ソフォスが 2020 年に対応した攻撃では、ランサムウェアの運用者は、SamSam の犯罪者集団が 32 か月間に稼いだ金額の 2 倍以上の金額で交渉を開始しました。

今日のランサムウェアは「階級別」に活動し、ヘビー級は大規模な企業ネットワークを攻撃し、ウェルター級は市民社会 (公安や地方自治体) や中小企業をターゲットとします。さらに、フェザー級は個人のコンピューターやホームユーザーをターゲットとします。最重量のヘビー級というと、強く立派そうに聞こえますが、高額の身代金を要求するからといって、下層のフェザー級ランサムウェアよりも高機能であるとみなすのは正しいとは言えません。

ソフォスの専任チームは、ランサムウェア攻撃の標的となった組織を調査し、またこれらの組織と連携して活動することも多くあります。フォレンジックのために攻撃を後で再構築したり、実行中の攻撃を中断させたりすることもあります。Sophos Rapid Response は、被害を阻止または抑制できる可能性がある場合に関与しますが、攻撃が非常に素早く進行して手の打ちようがないことがあります。そのような場合、ターゲットは身代金を支払うべきかどうかの判断を迫られ、この段階ではソフォスの役割は終わっています。

そこで登場するのが Coveware のような企業です。同社は、ランサムウェアのターゲットの代理人として、攻撃者との交渉を引き受けます。ソフォスは、「ベビー級」ランサムウェアが身代金の要求金額が増大する主たる要因になっているのではないかと考えていましたが、Coveware の CTO を務める Alex Holdtman 氏によって、この点が確認されました。

身代金の平均支払い額（四半期ごと）

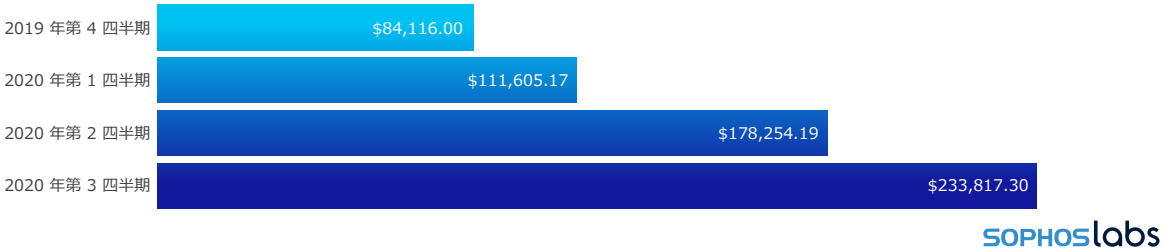


図 2: 身代金の平均支払い額はこの四半期で 21%上昇し、過去 1 年間で 3 倍近くになっています。出典：Coveware

この四半期だけで、身代金の平均支払い額は 21% 上昇しました。しかし、Coveware は、非常に大規模なランサムウェア攻撃が 1 回か 2 回あれば、それに引きずられて平均値が高くなると考えています。直近の四半期の身代金の平均支払い額は、暗号通貨 233,817.30 ドル分に相当します。1 年前の平均支払い額は 84,116 ドルでした。

ランサムウェアの攻撃者は、ダウンタイムのコストが如何に高いかを理解しており、ランサムウェア攻撃でどこまでの身代金を獲得できるかを試行錯誤してきました。

複数のランサムウェアファミリーは、取引を成立させるための「第二のビジネス」として恐喝を取り入れています。すでに述べたように、Netwalker などのグループがこの戦術を使っています。これにより、攻撃のターゲットがデータを完全に回復可能なバックアップを持っていたとしても、ランサムウェアの犯罪者によって内部情報が公開されることがないようにと、支払いに応じざるを得なくなる可能性があります。

下級のランサムウェアでも要求額は上昇していますが、「重量級」の金額には遠く及ばないと Holdtman 氏は述べています。多くの中小企業や個人が被害を受けていますが、身代金の要求額は比較的横ばいで推移しています。

ランサムウェア緊急対応チームの活動

ランサムウェア Maze がまだ活動していたころ、その標的になった組織が Sophos Rapid Response チームに支援を要請しました。ソフォスは調査を行い、攻撃が進行している間に積極的に対策を講じました。この攻撃の経過について、以下に概要をまとめます。

攻撃発生前

攻撃が活発化する前の何らかの時点で、攻撃者はターゲットのネットワーク上にあるコンピューターを侵害しました。

続いて、このコンピューターがネットワーク内の「足掛かり」として使用されました。 ここから攻撃者はリモートデスクトッププロトコル (RDP) を使用し、複数回にわたって他のコンピューターに接続しました。

1 日目

悪意のある活動の最初の証拠は、保護されていないドメインコントローラー (DC) に Cobalt Strike SMB ビーコンがサービスとしてインストールされたときに現れました。攻撃者は、脆弱なパスワードを使用するドメイン管理者アカウントを利用して、すでに感染させたコンピューターから DC を制御できるようにしました。

2 日目

攻撃者は、スケジュールされた一連のタスクやバッチスクリプトを作成して実行した上で、これらを削除しました。調査で確認された証拠によると、このタスクは、後にランサムウェア攻撃を展開するために使用された手法に類似するものでした。攻撃者が使用予定の手法をテストしている可能性がありました。

攻撃者は、侵害されたドメイン管理者アカウントと RDP アクセスを使用し、ネットワーク内のラテラルムーブメントを通じて他の重要なサーバーにアクセスしました。

攻撃者は、合法的なネットワークスキャンツールである Advanced IP Scanner を使用してネットワークのマッピングを開始し、後にランサムウェアを展開させる IP アドレスのリストを作成しました。攻撃者は、ターゲットの IT 管理者が使用するコンピューターに属する IP アドレスについて、別のリストを作成しました。

次に、攻撃者は Microsoft の ntdsutil というツールを使用して、Active Directory のハッシュ化された認証情報データベースのダンプを実行しました。

さまざまな WMI コマンドを実行して感染したマシンの情報を収集した攻撃者は、次にデータの窃取に注力しました。ファイルサーバーを特定し、侵害したドメイン管理者アカウントにより RDP を介してリモートからアクセスし、そこに含まれるフォルダを圧縮しました。

攻撃者は、アーカイブをドメインコントローラーに移動させ、Mega というクラウドストレージアプリケーションを DC にインストールしようと試みました。これはセキュリティでブロックされたため、代わりに Web ベースのバージョンを使用して、圧縮ファイルをアップロードしました。

3 日目

Mega へのデータのアップロードが終日続きました。

4 日目、5 日目

この間、悪質な活動は確認されません。過去のインシデントでは、IT セキュリティチームが作業しておらずネットワークの監視が手薄になる週末や休日を待って、ランサムウェアの攻撃者が攻撃を仕掛けるのが観察されています。

6 日目

この日は日曜日です。侵害されたドメイン管理者アカウントと特定された IP アドレスのリストを利用して、最初の Maze ランサムウェアの攻撃が開始されます。700 台以上のコンピューターが攻撃対象となりますが、セキュリティ機能により速やかに検知されブロックされました。攻撃が阻止されたことに攻撃者が気付いていないのか、または盗んだデータを使って被害者を恐喝することを狙っているのか、いずれにしても、この段階で攻撃者は 1,500 万ドルの身代金を要求しました。

7 日目

セキュリティチームは、追加のセキュリティを導入し、24 時間 365 日体制で脅威の監視を続けました。インシデント対応の調査が開始されました。侵害された管理者アカウントがすぐに特定され、悪意のあるファイルが複数発見され、攻撃者と感染マシンの間の通信がブロックされました。

8 日目

攻撃者が使用したツールや手口がさらに発見され、データ窃取に関連する証拠が見つかりました。さらに多くのファイルやアカウントがブロックされました。

9 日目

防御されているにもかかわらず、攻撃者はネットワークと別の侵害されたアカウントにアクセスし続け、2 回目の攻撃を開始しました。この攻撃は、最初の攻撃と同様に、DC 上でコマンドを実行し、txt ファイルに含まれる IP アドレスのリストを利用しました。

攻撃はすぐに特定されました。ランサムウェアが自動的に検知され、侵害されたアカウントとマルウェアのペイロードの両方が無効化され削除されました。暗号化されたファイルはありません。

しかし、攻撃者は諦める気配を見せず、再び攻撃を試みました。2 回目の攻撃からわずか数時間後に、3 回目の試みが開始されました。

この段階で、攻撃側はすでに余裕を失っているように見られ、データの抽出元となったメインのファイルサーバー 1 台だけを標的にしていました。

Maze の攻撃者はアプローチを変え、仮想マシン (VM) のフルコピーと VirtualBox ハイパーバイザーのインストーラーを展開しました (この攻撃については、2020 年 9 月に SophosLabs Uncut で詳細に説明しています)。

3 回目の攻撃も同様の結果に終わりました。Sophos Rapid Response チームは攻撃を検知して阻止し、ファイルが暗号化されることはありませんでした。ソフォスのチームは、顧客が犯罪者グループを遮断するのを支援し、攻撃者はそれ以上の攻撃を実行できなくなりました。

企業を日々狙う脅威 —「炭鉱のカナリア」

サイバー攻撃についてニュースの報道でしか把握していないのであれば、世の終わりが近いと感じても不思議ではありません。大規模な組織を標的とした攻撃が毎日のように行われています。しかし、大規模なデータ侵害のように、企業の富を奪い、株価を暴落させて悪評を生むような壊滅的な攻撃だけではありません。SophosLabs チームは、これらの「札付き」マルウェアを「最重要指名手配」リストで追跡していますが、多くの攻撃は、はるかに平凡です。

これらの通常の攻撃、そして配信されるマルウェアの一部は、すでに十分に理解されており、簡単に封じ込めることができます。しかし、それぞれの攻撃は、迅速かつ効果的に対処しなければ、はるかに深刻な事態をもたす危険性を秘めています。これらの日常的でありきたりの攻撃は、言わば「炭鉱のカナリア」のようなものであり、またたく間に制御不能に陥る可能性のある危険の初期の兆候となります。

Windows サーバーや Linux サーバーを標的とする攻撃

ソフォスが 2020 年に対応したセキュリティインシデントの大部分は、さまざまなバージョンの Windows が実行されているデスクトップ やノート PC でした。その一方で、Windows サーバーと Windows 以外のサーバーに対する攻撃も着実に増加しています。一般的に、サーバーはさまざまな理由から長らく格好の攻撃対象とされてきました。サーバーは、しばしば無人または監視されていない状態で、長期間にわたって実行されます。多くの場合、個々のノート PC に比べて、サーバーは多くの CPU とメモリを搭載しています。さらに、ネットワークで特権が付与されており、機密性や価値が最も高い組織のデータにアクセスできることがあります。執拗に活動する攻撃者にとって、サーバーは魅力的な足掛かりになります。これらの特徴は 2021 年も変わらず、ソフォスはサーバーを標的とした攻撃が今後も増加すると予測しています。

サーバーを標的とする攻撃の大部分は、ランサムウェア、クリプトマイナー、データ窃取という 3 つのプロファイルのいずれかに該当します。サーバー管理者の感染対策として、メールクライアントや Web ブラウザなどの従来型デスクトップアプリケーションをサーバーから実行しないようにすることがベストプラクティスとなります。したがって、サーバーを標的とした攻撃には、必然的に戦術の転換が必要となります。

インターネットに接続し、Windows を実行しているサーバーは、RDP のブルートフォース攻撃による絶え間ない攻撃を受けています。少なくとも直近の 3 年間、この攻撃手法はランサムウェア攻撃に伴って最も使用されています (したがって、この手法が使用されていればランサムウェア攻撃の実行を予測できます)。Sophos Rapid Response チームの調査から明らかになっているランサムウェア攻撃の重要な根本原因は、RDP を使用してターゲットのネットワークに最初にアクセスすることです。これによって、それらのマシンを使用してネットワーク内に足場を築き、DC サーバーを制御し、そこから次の攻撃を実行できるようになります。

対照的に、クリプトジャッキング攻撃は、Windows の脆弱性や、データベースソフトウェアなどのサーバーハードウェアで一般的に実行されるアプリケーションの脆弱性といった、範囲のより広い脆弱性を標的にする傾向があります。

たとえば、Lemon_Duck というクリプトマイナーは、インターネットに接続して Microsoft SQL Server を実行しているサーバーに対して、ブルートフォース攻撃を方法の 1 つとして使用しています。攻撃者がデータベースのパスワードを正しく推測すると、データベース自体を使用してクリプトジャッカーのペイロードを再構築し、サーバーのファイルシステムに書き出して実行します。感染したマシンは、クリプトジャッカーを拡散するために、EternalBlue や SMBGhost の脆弱性を利用しようとします。

Lemon_Duck の攻撃は、あらゆる OS を対象としているため、Linux サーバーにも感染する可能性があります。このマルウェアは、比較的小さなリストの SSH パスワードを使用してブルートフォース攻撃を試みます。これに成功すると、攻撃者は悪意のあるシェルコードを読み込み、Redis と呼ばれるサービスの抜け穴を利用して常駐化します。クリプトジャッカーは、Hadoop クラスター内から自身を起動するコマンドを実行することにより、自身を隠すこともできます。

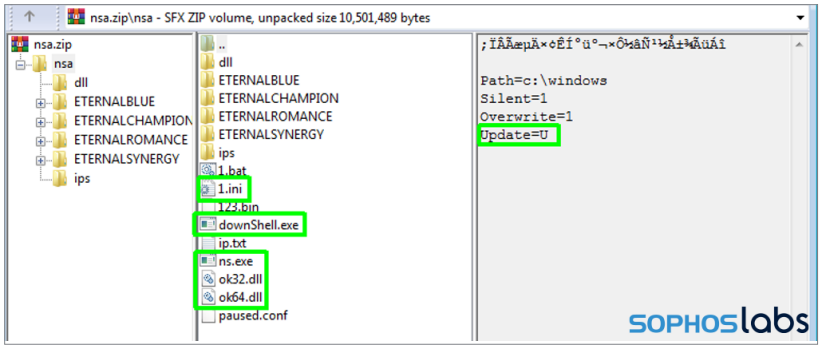


図 3: 広く拡散している MyKings というクリプトジャッカーは、ボットネットをインストールするためのコンポーネント (緑色で強調表示) を Zip アーカイブに含めて配布しました。これは、Shadow Brokers によって NSA から流出したいくつかのエクスプロイトも含みます。出典 : SophosLabs。

攻撃者は、簡単に小金を稼いだり暗号通貨を地道に獲得したりするためではなく、サーバーに保存されている価値の高いデータを盗むためにサーバーを標的にすることがあります。2020 年にソフォスは、Cloud Snooper というマルウェアを使って Linux サーバーを標的にする攻撃者を検出しました。問題となったサーバーは、クラウドのコンピューティングクラスターでホストされていました。検知を回避するために、巧妙なメッセージリレーシステムを考案し、通常の HTTP 接続を介して C&C メッセージをピギーバック方式で運んでいました。

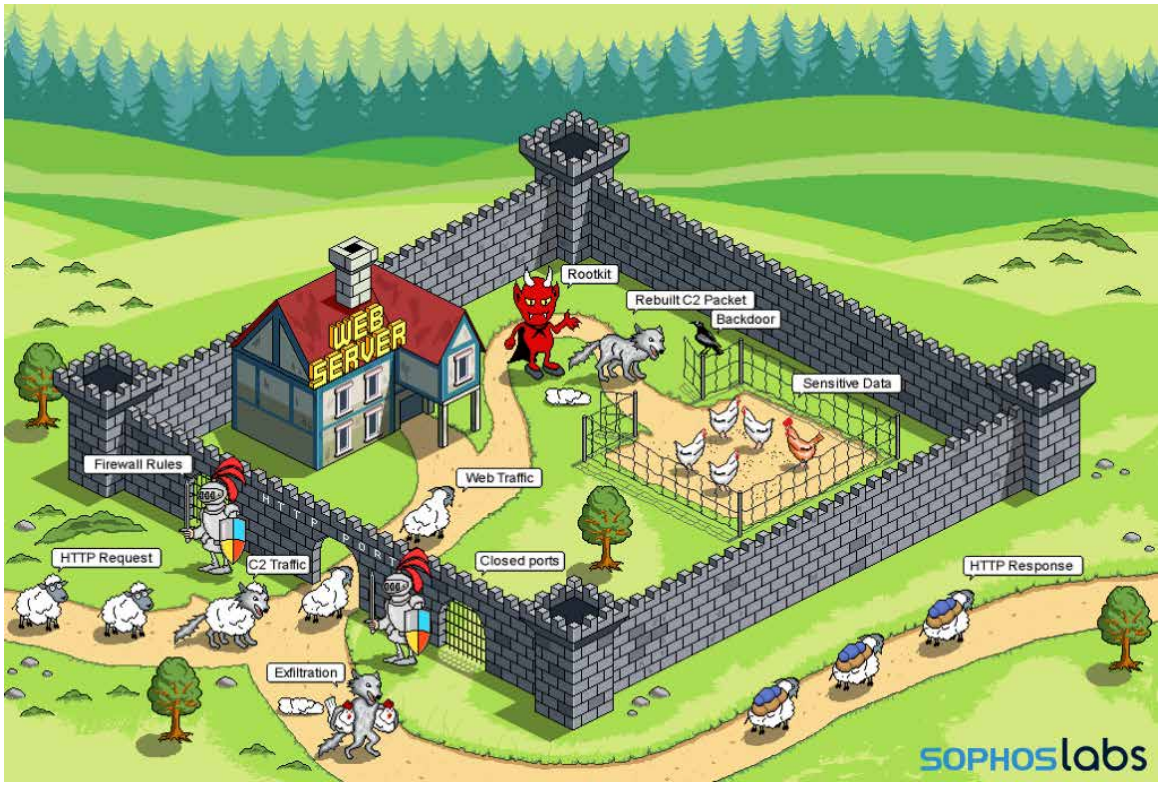


図 4: APT マルウェアの Cloud Snooper を「羊の皮をかぶったオオカミ」にたとえて説明しています。平凡な HTTP リクエストとレスポンスを装い、ネットワークトラフィックを監視してリアルタイムで TCP/IP パケットを書き換えるツールも利用して、自身のコマンドを隠し、データを抽出します。出典 : SophosLabs

サーバー管理者は、これまではサーバーにエンドポイント保護の製品をインストールしていませんでした。しかし、このような攻撃の出現によって、これまでの常識は通用しなくなりました。

「コモディティ」マルウェアの過小評価は危険である

国家が支援する持続的な標的型攻撃 (APT) によってゼロデイ脆弱性の影響を受ける人は、それほど多くいません。ほとんどの攻撃は、従来の手法で配信されるありふれたマルウェアを使用し、通常はスパムメールや害のなさそうな添付ファイル / リンク、そして添付ファイルを開くようにターゲットを誘導する手口を活用します。このような一般的なマルウェアについて、ソフォスのテレメトリでは毎月数千件に上る検出結果を受け取っています。これは通常、ソフォス製品のいずれかで保護されたコンピューターが攻撃をブロックしたことを示しています。

保護されておらず、マルウェアが完全に実行可能なコンピューターでは、マルウェアがターゲットのコンピューターをプロファイリングし、Web サイトのログイン認証情報や保存されたパスワードといった、何らかの価値 (銀行口座、金融サービス口座など) のある情報を抽出して攻撃者に送り返し、数秒後あるいは数日後に届く次の指示を待機します。

しかし、これらが平凡なマルウェアファミリーに過ぎないという事実に惑わされて、慢心や安心することは危険です。これらの悪意のある平凡なマルウェアを適切かつ迅速に処理しないと、以下に説明するような甚大な問題を引き起こすマルウェアが配信される恐れがあります。前述のとおり、SophosLabs チームはマルウェアの「最重要指名手配」リストを維持しており、これらの執拗なマルウェアファミリーについては専任アナリストが対応しています。これらのマルウェアの一部について、以下に簡単にまとめます。

Dridex と Zloader

最も一般的なマルウェアのタイプの 1 つとして、ローダーがあります。ローダーの主な役割は、運用者または運用者と契約している攻撃者に代わって別のマルウェアペイロードを配信することです。マルウェアファミリーの Dridex と Zloader は、いずれも成熟しており攻撃者から定評のあるローダープラットフォームです。Dridex と Zloader のどちらも、ターゲットシステムに関する情報を収集して犯罪者に送り返します。攻撃者は、ボットから送られた情報を基に、どのようなコンポーネント / ペイロードを配信するかを決定できます。

Dridex ローダーの主な機能は、C&C サーバーと通信し、暗号化されたペイロードを取得して展開することです。攻撃者は、VNC (リモート制御アプリケーション) や SOCKS プロキシなどを秘密裏に使用して、必要に応じてペイロードを配布しているだけなので、アナリストがこれらのペイロードを突き止めるのは非常に困難です。攻撃者はこれらのペイロードによって、ユーザーのデバイスの状況に合わせてアクションを実行できます。また、犯罪者自身のシステムからは直接的にアクセスできないターゲットシステムのリソースにアクセスできるようになります。

感染時の動作を決定するサーバーサイドのロジックを理解できないとしても、マルウェアのアナリストが使用するコンピューターにはボットが感染しようとしないことから、何らかのルールがあることが推論できます。ボットはインストールされているプログラムのリストを運用者に送信します。その中に解析ツールや仮想マシンのコンポーネントが含まれていれば、ボットはそのマシンにペイロードを配布しません。Zloader の場合、ボットの運用者はスパムメッセージを介してマルウェアを拡散します。コンピューターへの感染が一定期間内 (スパム配信後 8 ～ 12 時間) に完了しなければ、ペイロードの送信を停止します。

さらに、ペイロードを配布する対象は「クリーン」なマシンでなければなりませんが、あまりに「クリーン」なマシンも避けられます。基本の Windows だけがインストールされたマシンにはペイロードは配信されず、多くのセキュリティツールを搭載しているマシンにもペイロードは配信されません。

Agent Tesla (情報窃取マルウェア) と RATicate (RAT)

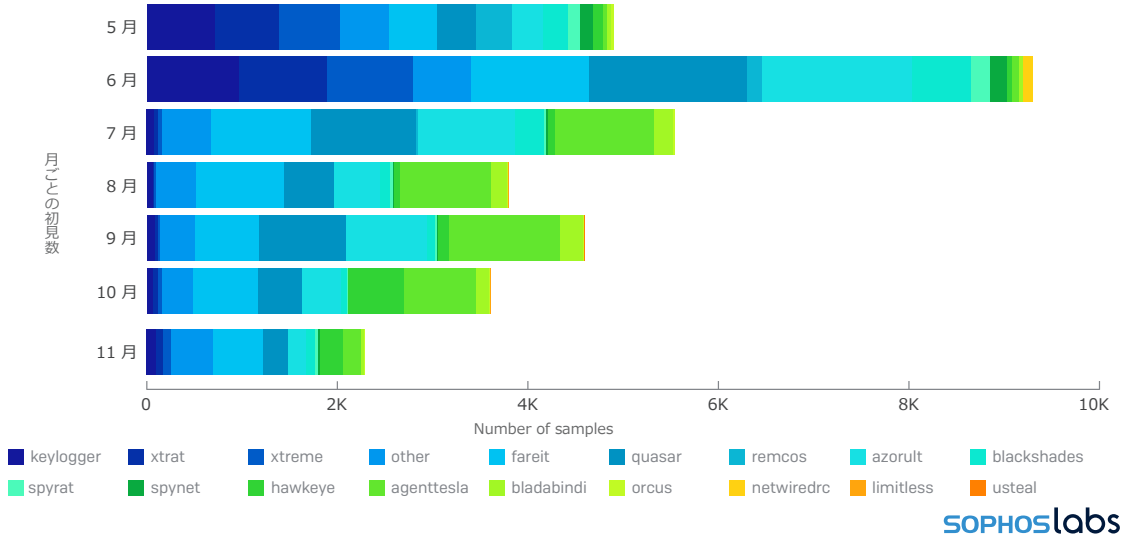


図 5: 新たに発見されたリモートアクセス型トロイの木馬 (RAT) マルウェアのサンプルは、ソフォスの社内サンドボックスシステムですべて実行されます。この表は、7 か月間に新たに発見された一意のサンプル (最も一般的な RAT ファミリー 18 種類に分類) の数を表しています。* 月の途中までのデータ。出典：SophosLabs

リモートアクセス型トロイの木馬（RAT）と情報窃取マルウェアは、どちらも最も古い形態のマルウェアです。名前が示すとおり、RAT は、感染したコンピューターをリモートから操作します。情報窃取マルウェアも、名前のとおり、認証情報、証明書などの機密情報の窃取と抽出を実行します。ソフォスが過去 1 年間に対処した「最重要指名手配」ファミリーは、Agent Tesla (情報窃取マルウェア) と RATicate (RAT) の 2 つです。

RAT は通常ローダーと同様に、自身の更新バージョンを含む追加のペイロードを配信するメカニズムを実装しています。RATicate は、Agent Tesla を含む他のマルウェアを配布していることが確認されています。また、これらの RAT ファミリーの配信や通信に同じ IP アドレス、またはサーバーが使用されていることも確認されています。これは、一見して無関係なグループの間で何かの情報共有が行われていることを示唆しています。

Trickbot の解体

Trickbot は、少なくとも 4 年前から長期間活動しているマルウェアです。これは、TLS を利用して C&C インフラストラクチャと通信するといった、現在では一般的な挙動 / 特徴の多くを開拓した悪名高いボットネットです。このボットは、いくつかの名の知れたランサムウェア攻撃に関与しており、それ自体が認証情報の窃取に高い威力を発揮します。

図 6: Trickbot のテイクダウンに使用されたのは、たった 1 行のコードです。出典：SophosLabs

本レポートを作成している 2020 年 10 月、Microsoft と米国司法省は、制御した複数のサーバーからボットネットの C&C システムを介してコマンドを送信して、ボットネットの約 90% と C&C インフラストラクチャとの通信を停止させたことを発表しました。

各ボットがダウンロードした Trickbot のインフラストラクチャに、捜査担当者によって「毒入り」の構成がアップロードされたのです。ボットネットはこの構成によって、自身が実行されている感染マシンが主要 C&C サーバーであると認識するようになりました。これにより、ボットネットは実際の C&C サーバーと通信しなくなり、ペイロードや指示を受け取ることができなくなりました。

Trickbot の運用者は、この取り組みによって大きな影響を受けましたが、今後次第に回復して最終的には元の運用に戻ると予想されます。

配信の仕組み

マルウェアや攻撃者が標的とするマシンにアクセスしたり、ネットワークに侵入したりする方法は限られています。ほとんどのマルウェア攻撃の手法は、悪意のあるファイルへのリンクや添付ファイルを含むメールを使用するなど、よく知られた経路をたどります。または、攻撃者がより積極的に関与し、RDP を標的にしたり、インターネットに接続してネットワーク境界でホストされる他の脆弱なサービスを標的にしたりする場合もあります。

RDP - ランサムウェアで最も使用される攻撃手法

Windows リモートデスクトッププロトコル (RDP) は、Windows のすべての現行バージョンで利用可能な標準サービスです。RDP を使用すると、IT 管理者やコンピューターユーザーは、物理的にコンピューターを使用せずにログインできます。したがって、パンデミックにより誰もがリモートワークを突然強いられるような状況下では非常に便利です。残念ながら、この 3 年間にランサムウェアの攻撃者は、このリモートアクセスプラットフォームを加速的な勢いで悪用し、足場を築いて企業に大規模な被害をもたらし、標的とする組織から多額の利益を得ています。

各ハニーポットでの RDP ログイン試行

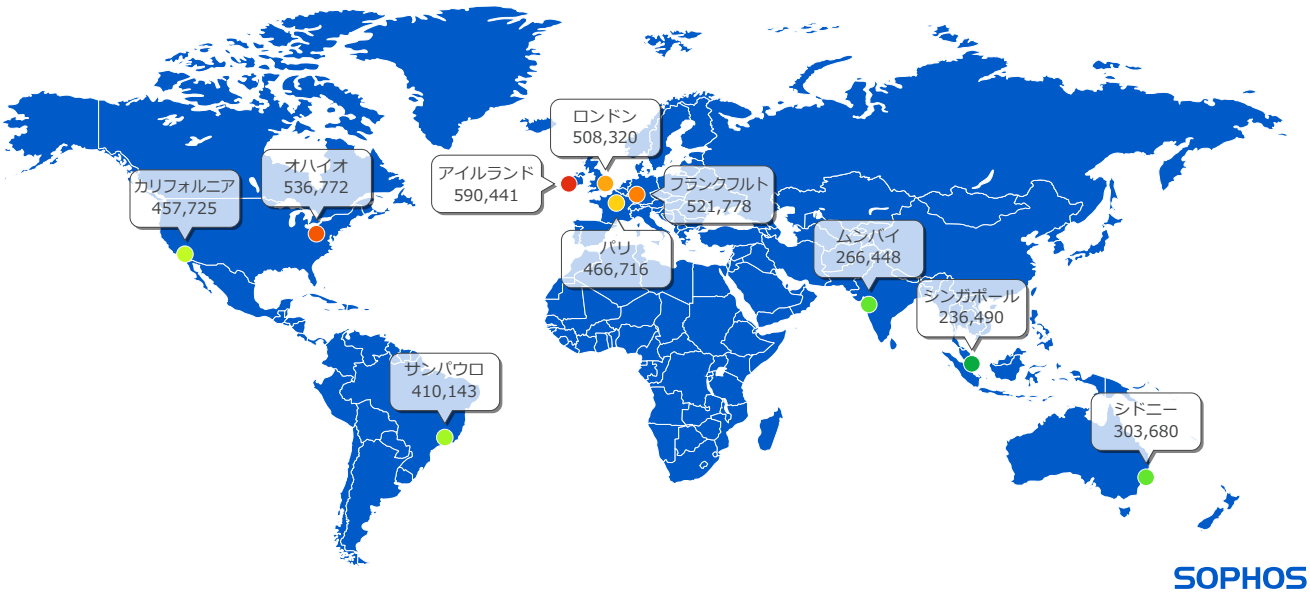


図 7: ソフォスは、攻撃者がブルートフォース攻撃を仕掛けるように、全世界のデータセンターにハニーポットを配布しました。ハニーポットマシンは、自然な形で展開されましたこの地図は、各地のハニーポットが 1 か月のテスト期間にどれだけの攻撃を受けたかを示しています。

COVID-19 によってロックダウンが実施され、多くの組織や従業員が業務を継続するために RDP に頼らざるを得ない事態が起きたため、問題が悪化しました。ここでの最大のリスクは、RDP がインターネットからの激しい攻撃に耐えるようには設計されていないという点です。RDP のパスワード強度が低く、簡単に推測できると、攻撃者は自動ログイン試行のブルートフォース攻撃によりネットワークで足場を獲得し、これを自由に利用できるようになります。

主要インシデントへの対応を担当するソフォスのチームは、RDP が依然としてランサムウェアイベントの主要な「根本原因」の 1 つであると報告しています。したがって、IT 管理者は、これまでと変わらず次のことに留意すべきです。RDP は、インターネットから直接アクセスできるように配置してはなりません。ファイアウォールの内部に配置し、最初に VPN またはその他のゼロトラストのファシリティを介して接続するようにユーザーに要求すべきです。また、管理者は Windows のパスワードポリシーを強化して、より長いパスワードと多要素認証トークンまたはアプリの使用を必須にすべきです。

ロックダウンの前に、ソフォスは問題がどれほど深刻化しているかを調べるため、世界中の 10 か所のデータセンターにハニーポットを設置して調査しました。30 日間にハニーポットが受けた RDP へのログイン試行は、中央値で 467,000 回 (1 時間あたり 600 回) に上りました。この調査では、最終的にハニーポットを切断するまでの間に、各地でログイン試行の頻度と激しさが着実に増加していったことが明らかになりました。

失敗したログイン試行で使用された上位 5 つのユーザー名

ユーザー名	ログイン失敗数
administrator	2,647,428
admin	376,206
user	79,384
ssm-user	53,447
test	42,117

図 8: リモートデスクトップのブルートフォース攻撃では、デフォルトの「administrator」アカウントを含む最も一般的な Windows ユーザー名が使用されます。出典：SophosLabs

ビジネスメール詐欺とビジネスメールなりすまし

ビジネスメール詐欺 (BEC) とは、主にユーザーを騙して金銭を請求するスパムの正式名称です。BEC 攻撃では、スパムの攻撃者は企業の経営幹部から発信されたように見せかけたメッセージを送信し、送金や高額の購入を代わりに実行するように従業員に指示します。そのために、社内メールの外観を偽装 (ビジネスメールなりすましとも呼ばれます) する場合や、組織のメールサーバ上のアカウントを制御して偽のリクエストを送信しようとする場合があります。

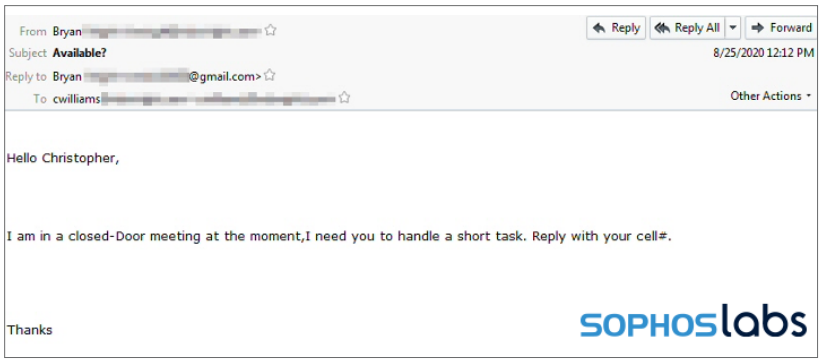


図 9: これは、ビジネスメール詐欺の実例です。詐欺師が経営幹部を装い、従業員に緊急に対応するよう求めています。メールの返信先アドレス (Gmail アカウント) が送信元ヘッダーと異なるので、ターゲットがメールヘッダーに注意を払っていれば明らかに不審であるとわかります。出典：SophosLabs

BEC の攻撃者は幹部を装って、標的となる従業員に高額なギフトカードの購入や緊急の金融取引などを依頼します。攻撃は通常、標的となる個人や組織に応じて高度にカスタマイズされます。BEC のメールメッセージは、スパムのようなパターンをとらず、悪意のあるスパムとは外観もまったく異なります。(多くの場合) 添付ファイルや悪意のあるリンクを含まず、ターゲットの組織内から発信されたように見せかけます。さらに、従来の悪意のあるスパムよりも説得力を持たせるため、ターゲット組織の典型的なメールの「署名」や従業員に馴染みのあるその他の要素を取り入れることもあります。

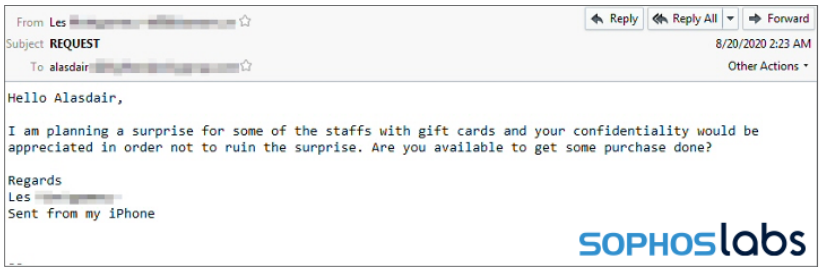


図 10: ターゲットが最初のリクエストを確認すると、詐欺師はもっともらしい口実で「頼み事」をします。出典：SophosLabs。

BEC 詐欺は、詐欺のターゲット (従業員) と詐欺の主体 (幹部) が物理的に離れていることを前提とし、また、誰かが状況を把握してギフトカードの購入や送金を阻む前にターゲットが迅速に行動することを頼みとします。BEC の詐欺師は、幹部がビジネスで外出していることを把握しているときにメッセージを作成することがあります。

このような詐欺のリクエストは、多くの場合に攻撃者とターゲットの間でのやり取りを伴います。詐欺師は、まずターゲットに応答するように簡単な要求を送り、一連のメッセージへと進み、最終的にはもっともらしい口実に基づいて購入を「お願い」します。

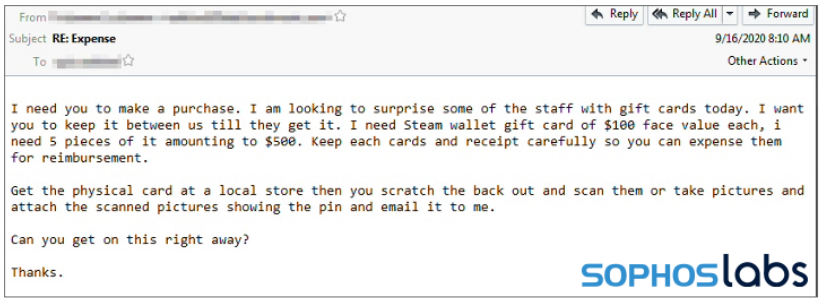


図 11: 攻撃中のある時点で、BEC の詐欺師は、ターゲットに馴染みのない口座に対して突然の多額の電信送金を行うといった、非常識な要求します。注意深い従業員であれば、「ギフトカードを贈り物にするはずなのに、裏面のスクラッチ部分を削った PIN の写真を要求するのは妙だ」と、依頼の内容に疑問を抱くチャンスとなります。出典：SophosLabs

従業員のほとんどがオフィスで働いていたころであれば、ターゲットと主体の物理的な距離が近ければ詐欺であることがすぐに判明していたでしょう。しかし、現在の分散した職場環境では、幹部と従業員が近距離にいる可能性が低いため、相手のデスクまで直接歩いて行ってリクエストを確認してもらう機会が減ります。

BEC 詐欺は COVID-19 の感染拡大以前から存在していましたが、リモートワークが拡大する中で猛威を振るうようになりました。人の役に立ちたいという善意に付け込んだ攻撃であり、詐欺行為としては特に侮辱的なものです。このようなメールを受け取った場合は、自分の直感を信じ、可能であればその人物に直接話しかけてみましょう。それが無理な場合は、他の人に相談することをお勧めします。このような依頼に対して従業員が実際に関与する度合いが高まるほど、被害が発生する前に詐欺が発覚する可能性が高くなります。

驚きの復活劇：遥か昔の Office の不具合が再び蘇る

悪意のある Office ドキュメント (Maldoc) と、そのドキュメントが展開しようとするエクスプロイトについては、古いものが何度も再利用されています。Microsoft がアップデートを公開すると姿をくらまし、その後、復活することがあります。SophosLabs は何年にもわたって、さまざまなエクスプロイトを Maldoc に埋め込んで使用する攻撃を追跡してきました。新たに脆弱性が公開されても、誰もが即座にパッチを適用するわけではありません。また、セキュリティ企業が新しい攻撃の挙動などの特徴に基づいて効果的な「セーフティネット」を構築するまでに、少し時間がかかることがあります。このため、マルウェアのペイロードを展開するための足がかりとして、Maldoc はサイバー犯罪者に好まれて利用されることがよくあります。

この 1 年間でソフォスが確認した Maldoc のほとんどは、ビルダーと呼ばれるツールを使って構築されています。ビルダーは、文字どおり簡単に操作できるメニューシステムを提供し、攻撃者は Maldoc に組み込むエクスプロイトを決定できます。エンドポイント保護製品は、通常はドキュメントに埋め込まれたスクリプトなど、新しいエクスプロイトも検出できるようにその機能を向上させています。一方で、Maldoc の作成者は、非常に古いバグを掘り起こして、マクロやその他の悪意のあるコンテンツをドキュメントに隠すために利用しています。

このようなバグは、俗に **VelvetSweatshop** エクスプロイトと呼ばれますが、エクスプロイトとはまったく異なるものです。実際のところ、VelvetSweatshop は Microsoft Office 2003 に存在した欠陥ですが、これが初めて悪用されたのは 2013 年です。このときは、CVE-2012-0158 の脆弱性を攻撃する Excel ワークブックが、この不具合を使用していました。「読み取り専用」とマーク付けされた Excel のスプレッドシートや Word の .doc ファイルは、よくあるパスワードで保護されたドキュメントに過ぎません。ご明察のとおり、そのパスワードの 1 つが VelvetSweatshop です。

脅威を検知する高度な機能を回避するために、この手法を用いた悪意のある Excel スプレッドシートが、今年に入って多数配信されています。暗号化されていることから、実際の悪意のあるコンテンツは強力な暗号の背後に隠されており、セキュリティ製品では解読できません。また、攻撃者が使用する最新のアルゴリズムに対応していない限りスキャンできません。デフォルトのパスワードが使用されているため、Excel はパスワードを要求せずに復号化された内容を開きます。したがって、実行の観点からは暗号化が透過的になっています。エンドポイント保護製品には、暗号化とデフォルトパスワードへの対応が追加されていますが、犯罪者は、エンドポイント保護製品の AV スキャナーにまだ実装されていない暗号アルゴリズムを発掘し続けています。

今の高校生が生まれる前からあるような古いバグを発見するというのは、驚くべきことです。しかし、攻撃用のドキュメントビルダーの作成者がこのようなバグを利用しようとすることは、驚くことではありません。

情報セキュリティの 20 年を振り返る

年次レポートでは、過去 1 年間に起こった重要な出来事を振り返ることができますが、さらに長期的な視点で過去 20 年を振り返ることによって、現在の脅威の状況に至った経緯を理解するための一助となるのではないでしょうか。21 世紀を迎え、情報セキュリティは独立した専門分野となり、紛れもない一つの業界として成り立つようになりました。この間に、脅威が進化し、大きな意味を持つ象徴的な脅威や事象が起こりました。

企業と個人の両方がビジネスや娯楽でインターネットを取り入れるのに伴って、大規模ネットワークは、新たに出現した広く拡散する自己増殖型マルウェアであるワームにとって最適なターゲットとなりました。ワームは、これまでに全世界で数千万のシステムに感染し、1,000 億ドル以上の損害と修復費用が発生しています。

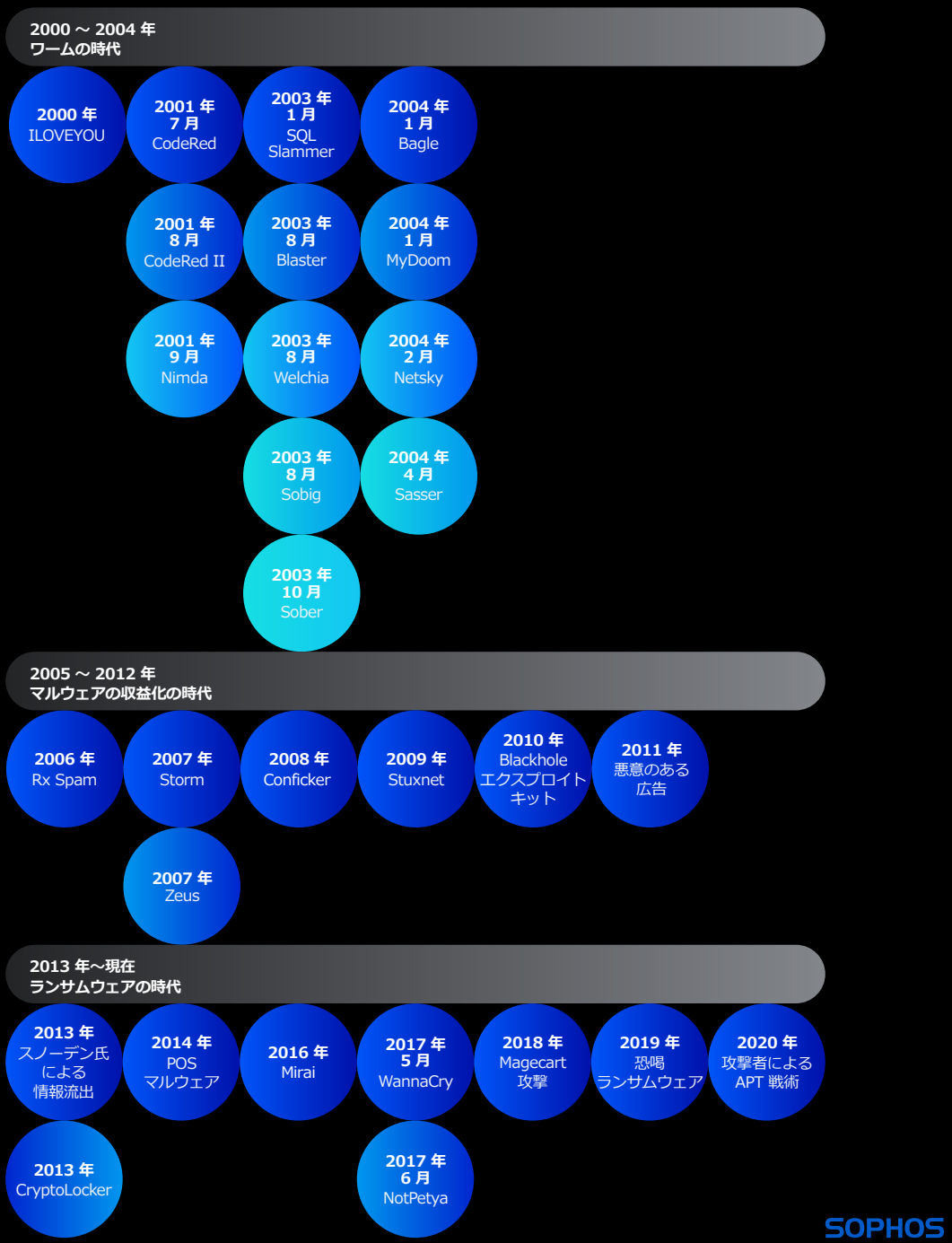


図 12: 出典：ソフォス

2000 ～ 2004 年 - ワームの時代

2000 年 - ILOVEYOU

ILOVEYOU は、現在もなお続くソーシャルエンジニアリングの手口を使用するワームです。スパムメールの添付ファイルとして配信され、結果的にインターネットに接続された Windows コンピューター全体の約 10% に感染しました。

2001 年 7 月 - CodeRed

発見者が当時飲んでいた「マウンテンデュー」のフレーバーにちなんで名付けられた CodeRed は、IIS のバッファオーバーフローの脆弱性を利用して自身を拡散させ、Web サイトを改ざんします。1 か月後には、ネットワーク接続されたコンピューターにバックドアをインストールするアップグレード版が登場しました。

2001 年 8 月 - CodeRed II

2001 年 9 月 - Nimda

2003 年 1 月 - SQL Slammer

サイズがわずか 376 バイトの Slammer は、Microsoft データベースアプリケーションのバッファオーバーフローを悪用しました。8.5 秒ごとに感染を倍増させ、わずか 15 分でインターネットを広範囲に破壊しました。

2003 年 8 月 - Blaster

Blaster は、「Patch Tuesday」が開始される数か月前に、Microsoft のパッチをリバースエンジニアリングして作成されました。Windows XP と Windows 2000 の RPC サービスに含まれていたバッファオーバーフローの脆弱性を悪用して、日付が 15 よりも大きい場合、または月が 9 月以降の場合に、windowsupdate.com に対して DDoS 攻撃を実行しました。

2003 年 8 月 - Welchia

2003 年 8 月 - Sobig

2003 年 10 月 - Sober

2004 年 1 月 - Bagle

2004 年 1 月 - MyDoom

2004 年に送信されたメールの 25% は MyDoom ワームに起因する推定されています。このワームは、新たな被害者に広範にメールを送信し、サービス拒否 (DDoS) 攻撃を実行しました。

2004 年 2 月 - Netsky

2004 年 4 月 - Sasser

2005 ～ 2012 年 - マルウェアの収益化の時代

2005 年頃まで、マルウェアは好奇心や業務を中断させるために実行されていると考えられていました。潜伏し金銭を獲得するために設計されたボットネットマルウェアが支配的な勢力となりました。いわゆる医薬品のスパムが始まったのも、この頃です。ソフトウェアの脆弱性に対するエクスプロイトは、マルウェアの重要な構成要素となり、悪意の広告を可能にしました。サイバー犯罪者は、場所を問わず金銭的な利益を得る方法を利用し始めたのです。

2006 年 – Rx Spam

単なる迷惑行為 (またはワームを増殖させる手段) だったものが、スパムで宣伝された偽の薬を主に販売する旨味のあるビジネスになりました。医薬品スパムは、通常は診察を受けるだけで入手できる薬を販売して数十億ドルの利益を得たと推定されています。

2007 年 - Storm

2007 年 - Zeus

2008 年 - Conficker

Conficker は世界中の数百万台のコンピューターに急速に感染したものの、大きな被害は引き起こしませんでした。今でもワームの真の目的は明らかになっていませんが、依然として何千ものホストが感染した状態にあります。インターネットの「環境放射線」の一部として、Conficker のスキャントラフィックは日常的に検知されています。

2009 年 - Stuxnet

Stuxnet は、産業システムを狙った最初のデジタル兵器の 1 つであり、イランでウラン濃縮に使用される核濃縮遠心分離機を標的としました。Stuxnet は、国家が戦争の手段としてマルウェアを使用するという、永続的な影響を残しました。

2010 年 - Blackhole エクスプロイトキット

エクスプロイトキット (ソフトウェアの脆弱性を攻撃するツールキット) は、サイバー犯罪のエコシステムのさまざまな構成要素を組み合わせています。CaaS (サービスとしてのクライムウェア) は、Blackhole エクスプロイトキットの作成者がサービスを提供し始めたことで登場しました。

2011 年 - 悪意のある広告

2013 年 ～ 現在 - ランサムウェアの時代

この時代に最も大きな影響を及ぼしたのがランサムウェアです。ワーム、銀行関連の情報を標的とするトロイの木馬、悪意のある広告、スパムの脅威が継続する一方で、ランサムウェアほどの破壊力を持つものはありません。過去 7 年間にランサムウェア攻撃によって発生した被害額は、推定で数兆ドル規模に上ります。ランサムウェアは、人命を脅かす最初のマルウェアとなる可能性が高いとも考えられています。さらに、今日の脅威の多くは最終的にランサムウェアを配信しています。サイバー犯罪のエコシステムはすでに活況を呈していますが、エクスプロイトキットと同様にランサムウェアによって爆発的な勢いが生み出されています。

2013 年 - スノーデン氏による情報流出

2013 年 - CryptoLocker

CryptoLocker は、短期間しか活動が続きませんでしたが、暗号化と暗号通貨という 2 つの既存のテクノロジーを組み合わせることで、その後の犯罪者に勝利の方程式を提供しました。CryptoLocker は、脅威のあり方を完全に塗り替え、現在も影響を及ぼしています。登場後 3 か月で CryptoLocker が獲得したビットコインの金額は 3,000 万ドル近くに達しました。

2014 年 - POS マルウェア

2016 年 - Mirai

2017 年 5 月 - WannaCry

WannaCry は、これまでに見られた中で最も広く広範に拡散しているランサムウェア / ワームのハイブリッドであり、パッチ適用の遅れが如何に悲惨な結果をもたらすかを実証しました。NSA から窃取されたエクスプロイトを利用したものであり、Shadow Brokers によって公開されました。WannaCry の攻撃のために、Microsoft はサポート対象外の製品向けに臨時アップデートをリリースせざるを得なりました。

2017 年 - NotPetya

NotPetya は、世界最大の海運 / 物流企業数社を機能不全に陥れ、100 億ドルを超える損害をもたらしたと報告されています。影響を受けた企業の一部は、今も完全に回復できていません。

2018 年 - Magecart 攻撃

2019 年 - 恐喝マルウェア

南アフリカのヨハネスブルグ市を攻撃した Maze ランサムウェアでは、恐喝が初めて使用されました。犯罪者は、暗号化とデータ窃取を実行しただけでなく、身代金を支払わなければデータを公開すると企業を脅したのです。この戦術は、ランサムウェアを使用する多くの攻撃者によって模倣されています。

2020 年 - 攻撃者による APT 戦術

国家が使用するツールや戦術の採用は、数年前に始まり、2020 年には主流になりました。プロのサイバー犯罪組織は、Cobalt Strike のような高度なツールを使って壊滅的な影響を与えていますが、Dharma などの一部のグループは初心者向けに「全自動」のツールキットを作成して販売しています。

COVID-19 に便乗した攻撃

新型コロナウイルス感染症 (COVID-19) は、サイバーセキュリティのあらゆる面に劇的な影響を与えました。この状況に便乗した攻撃者は、新たにリモートワークを始めたホワイトカラー労働者を標的にして攻撃を仕掛けています。大量のスパムキャンペーン、COVID-19 の影響を受けて厳しい経営を強いられている組織 / 市民社会を狙って財務的ひっ迫に追い打ちをかけるランサムウェア、さまざまな詐欺、マスクやトイレットペーパーなどのさまざまな物資不足に付け込む利益獲得行為など、サイバー攻撃は社会不安に拍車をかけ、社会に蔓延する不安と恐怖をさらに悪化させています。

家庭が新しい境界に

2020 年 3 月、COVID-19 の感染拡大を抑制し、医療体制のひっ迫を軽減するため、リモートワークが可能な人々とほぼすべての学年の生徒が急きょ自宅での勤務や学習を強いられることになり、それまでのあらゆる「ノーマル」が終わりました。突如として、人々は自宅で仕事をしているというよりは、職場で生活しているような状態に陥ったのです。

多くの人が、通勤せずに働くという「ニューノーマル」に適用するために苦労しています。VPN アクセスや多要素認証サービスに対する需要が急激に高まり、ノート PC は入手困難になり、Zoom はわずか 2 か月間で過去 10 年間にも相当するユーザー数を獲得しました。その間、Microsoft、Adobe、Apple、Google は、さまざまなプラットフォーム向けにアップデートやメンテナンスパッチをリリースしました。

COVID-19 とコロナウイルスを語るメール詐欺の増加

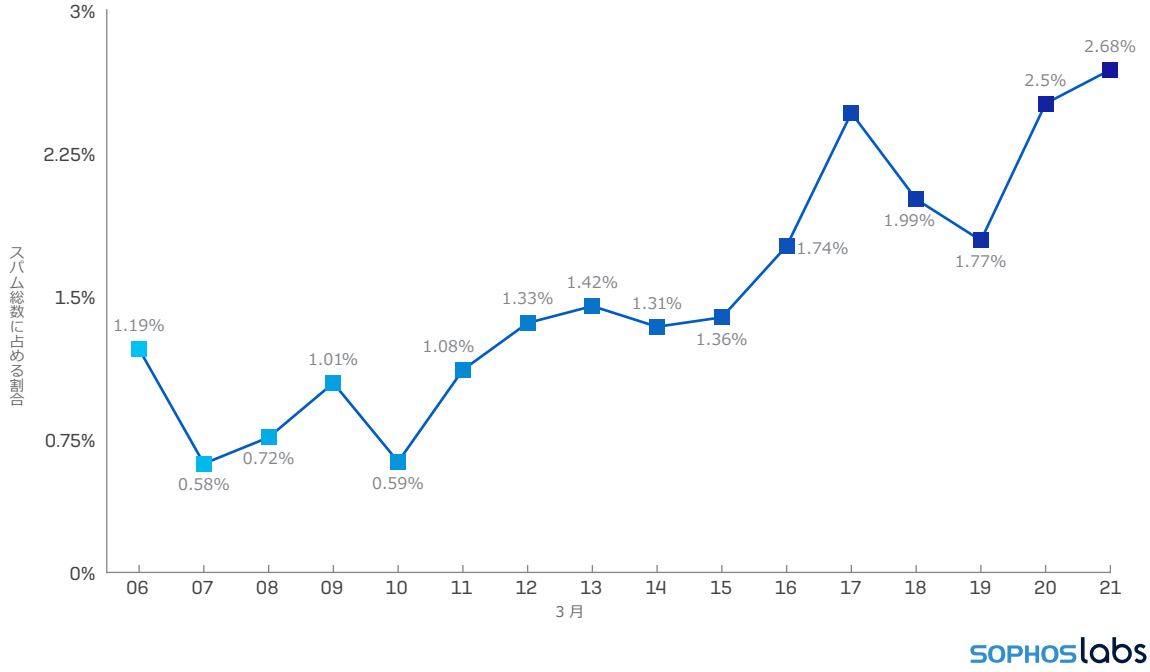


図 13: ロックダウン後の数週間に、世界的にかなりの割合のスパムメールで「COVID-19」や「Coronavirus」が言及されていました。出典：SophosLabs

COVID-19 によって、従業員は IT 部門に頼らずに、パッチ適用やセキュリティアップデート、オンライン会議や子どものオンライン学習のための接続の問題などに、自分自身で対処せざるを得なくなりました。

ヘッドセット、マイク、適切な照明、そしてネットワークとエンドポイントの両方のセキュリティに対する需要が高まっています。家庭内の子供でさえも、フィッシング、スパム、ネット荒らし、ネットいじめ、人気ゲームの無料コピーを装って誘うマルウェアなどについて、急場しのぎのトレーニングが必要になったのです。

それは簡単なことではなく、2020 年 2 月時点の状態にまで回復するには至っていません。しかし、ある意味においては「ニューノーマル」によって生活の質が改善されていると感じている人も多いのではないでしょうか。多くの組織は、ロックダウンが終了して職場に復帰できるようになった後もリモートワークを継続することを決定しました。これは、環境にも従業員の生活の質にも大きな利益をもたらします。

職場の境界が拡大し、多くの従業員がリモートで働くようになったことで、ホームネットワークが最後の防衛線となる状況が生まれています。各家庭の玄関に設置されたモデムが、企業ネットワークの境界になったのです。このようなネットワーク構造の中で多層防御を如何に実現するかについて、組織は対策を抜本的に見直す必要があります。

サービスとしてのクライムウェア (CaaS)

マルウェア作成者は、ソフトウェアのスタートアップ企業に例えることができます。最初は粗削りですが、成功した作成者は忠実な支持者を獲得します。また、正規ソフトウェアのビジネスモデルと同じように、悪意のあるソフトウェアにもビジネスモデルが多数存在します。

マルウェアの作成者や、マルウェアの簡単な配信や新機能による強化を可能にするツールの作成者の一部は、製品をそのまま販売するのではなく、Adobe Creative Suite の年間ライセンスのように、製品のライセンスを販売しています。このクラスのビジネスモデルは「サービスとしてのクライムウェア」(CaaS) と呼ばれ、これが「ニューノーマル」になりつつあるようです。

Emotet は、CaaS マルウェアの悪名高い一例です。これは、スパムにより配信されるトロイの木馬であり、何年も前から存在していますが、犯罪者が簡単に新規参入できるようにするサービスを中心に据えていると見られます。Emotet はマルウェアの 一種であり、セキュリティ研究者からは「ローダー」という総称で呼ばれています。Emotet の主たる役割は、他のマルウェアをターゲットのコンピューターに配信することです。そのために、兵器化されたスパムメールを大量のターゲットに配信する高度なネットワークを使用します。

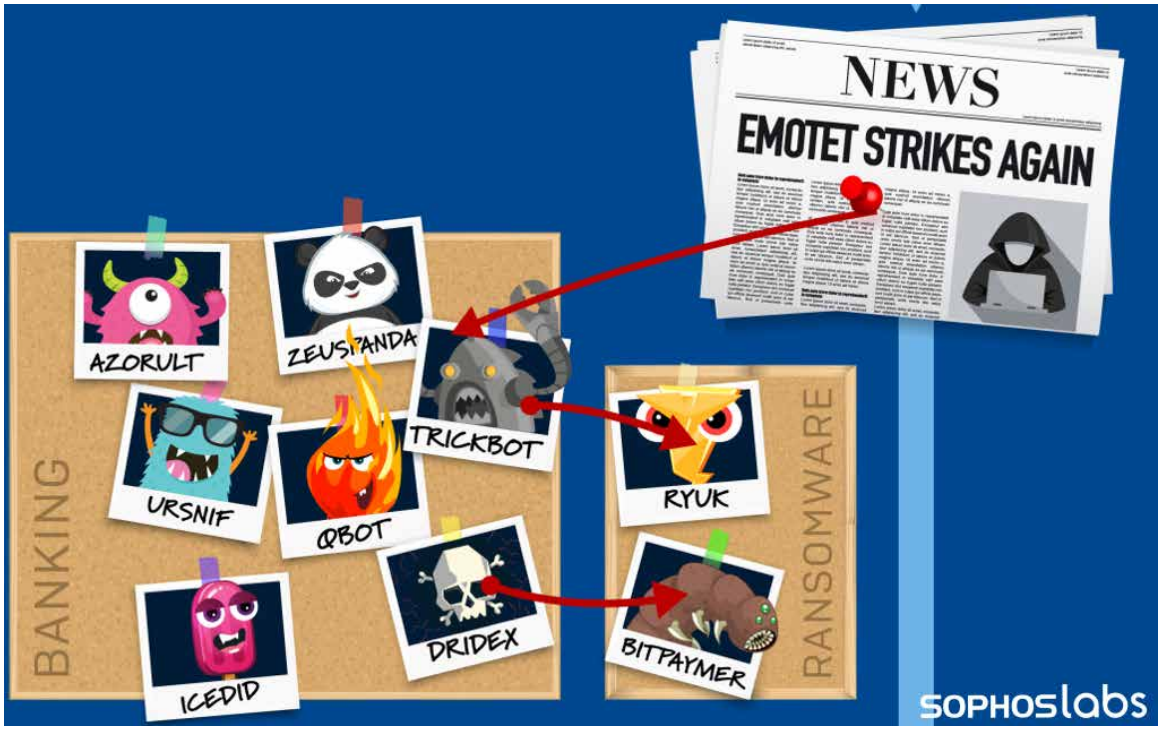


図 14: 出典：SophosLabs

しかし、今年に入ってから Emotet の活動には 2 つの不可解な期間がありました。このマルウェアは 5 か月近くにわたって C&C サーバーとの通信を維持していましたが、攻撃を配信するスパムメールは完全に鳴りを潜めました。しかし、7 月には Emotet を配信するスパムメールが再び 配信され始めました。

Dharma ランサムウェアも、注目に値する CaaS マルウェアです。他のランサムウェアが高額な身代金を要求するのに対して、Dharma はこれまで一定の少額な身代金を要求し続けています。その理由は、Dharma のビジネスモデルにあります。これは「ガイド付き」のランサムウェアであり、将来の犯罪者にコツを伝授します。これらの犯罪者は基本的にサブスクリプション料金を支払って Dharma の作成者からペイロードを入手し、攻撃の収益を作成者と分け合います。

攻撃者がそれぞれの専門領域へと分岐していくのに伴い、犯罪者は請負業者、フリーランサー、関連組織として連携していくビジネスモデルは当面継続すると考えられます。

スパム、詐欺、反故にされた約束

世界中でロックダウンが行われる中、スパムメールを媒介とする詐欺行為が大量に行われました。新型コロナウイルスの厄災のない順調な状況であっても、効果的なスパムキャンペーンは受信者がメッセージに対して行動するように切迫感をあおります。これはよく知られている心理トリックであり、少しの間をとってスパムメッセージの内容を考えれば、偽物であることに気づくはずです。しかし、恐怖の反応が引き起こされると、考える前に行動してしまい、罠に陥ることになります。

COVID-19 によって、すでに誰もが張り詰めた心理状態にあることから、スパムを悪用するサイバー犯罪者は易々と利益を得ています。

Fig.15. Source: SophosLabs.

ロックダウンが始まって数週間後、ソフォスは、「登録されるドメイン」が急増していることに注目しました。わずか数週間で、「*COVID-19*」「*Corona*」「*virus*」といった文字列の組み合わせを含む新しいドメイン名が、1 日あたり何千も登録されるようになりました。

Domain	First Seen	Nameserver	Ns Ip
coronavirusshaquilleoneal.com	2020-03-14 07:00:38	ns-cloud-b1.googledomains.com	216.239.32.107

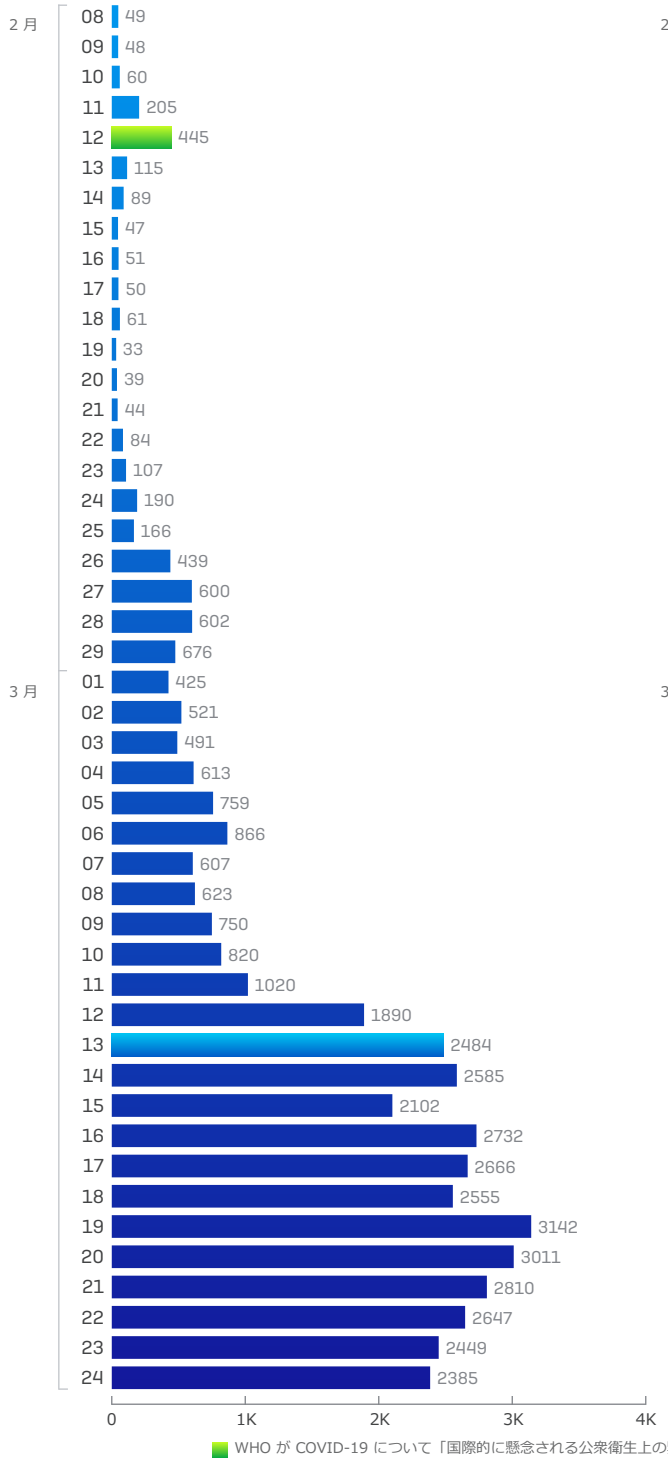
SOPHOSlabs

図 16: 出典：SophosLabs

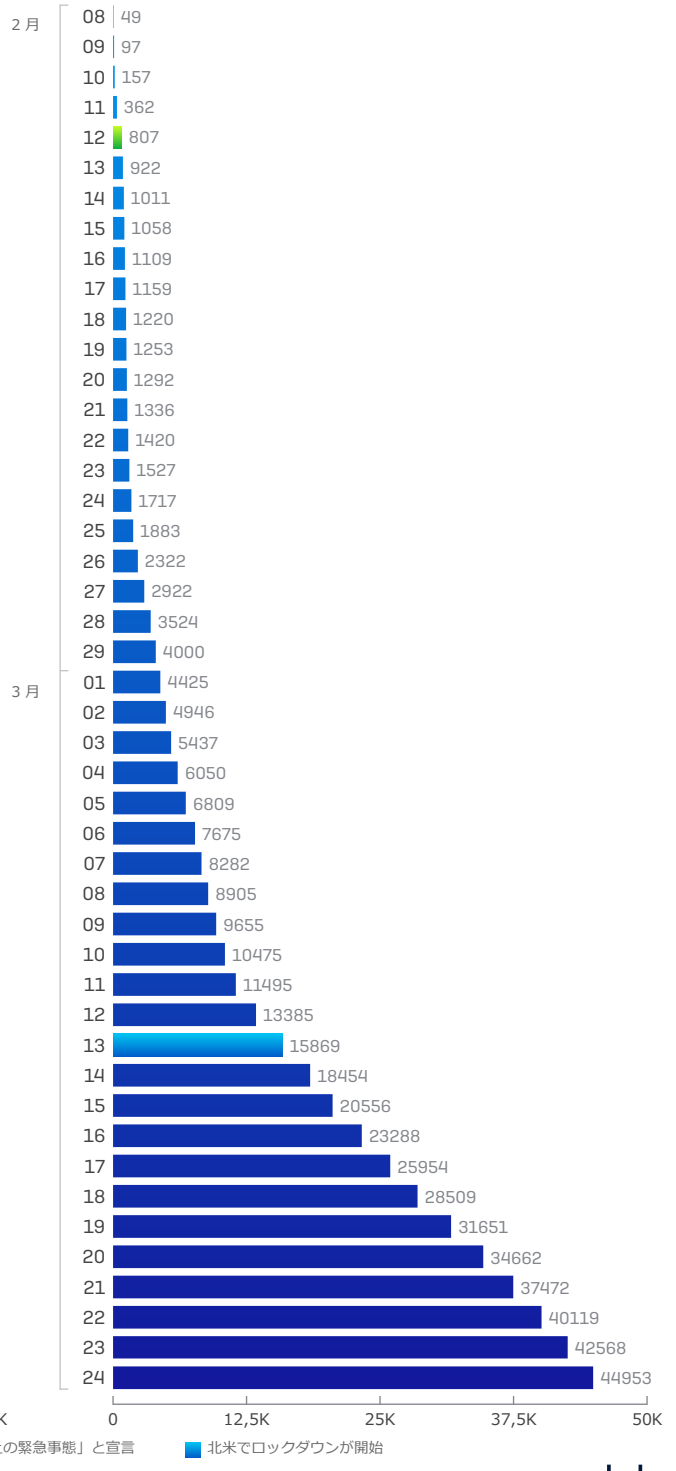
明らかに悪ふざけと思われるサイトがある一方で、地域または国家の合法的な保健当局によって使用されているドメインと紛らわしいほど似たサイトもあります。

ソフォスはさらに、TLS 証明書の透明性ログ (CT ログ) で COVID-19 関連のドメインやサブドメインを探しました。証明書の CT ログは、独自の TLS 証明書を持つサブドメイン (この情報は、ドメイン登録データ自体には示されません) やドメイン名を追跡するのに便利です。

COVID ドメインの新規登録数 (1 日あたり)



COVID ドメインの新規登録数合計 (現在までの累計)



SOPHOSlabs

図 17: COVID-19 の危機が始まってからの数か月間、「COVID-19」または「corona」といった文字列を含む何千ものドメインが毎日のように登録され、多数の TLS 証明書のライセンスが提供されました。出典：SophosLabs

「COVID-19」または「corona」の文字列を含むホスト名を持つ新しい TLS 証明書の登録数（月別）

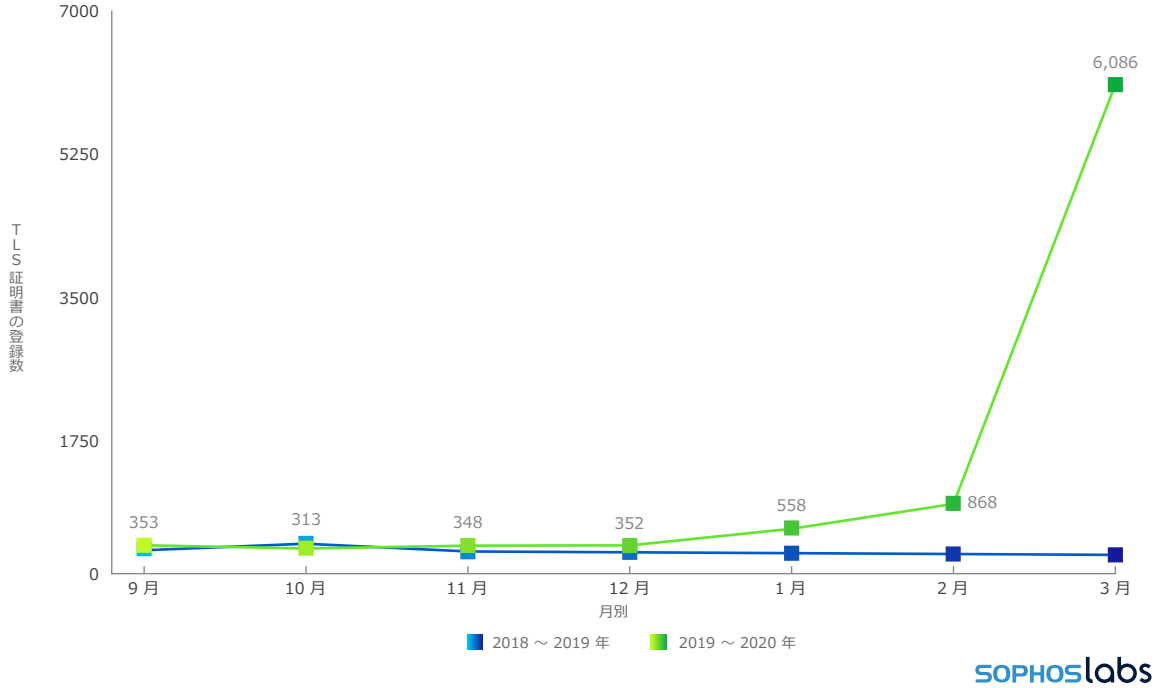


図 18: パンデミックに言及した TLS 証明書の登録数は、ドメイン登録とほぼ同じ時期に急増しました。出典：SophosLabs

3 月には COVID-19 ドメインに対して 1 日平均 200 件以上の証明書請求がありました。この数はその後も増え続け、6 月までに 1 日平均 625 件に達しました。10 月には、新しい TLS 証明書の請求数は 1 日あたり 951 件となりピークに達しました。

これらのドメインの大部分は、合法的または無害なドメインですが、多くは登録されたもののコンテンツが提供されていません。これは、将来のレピュテーションチェックのために、登録者によってドメインが取り置かれている可能性を示唆しています。

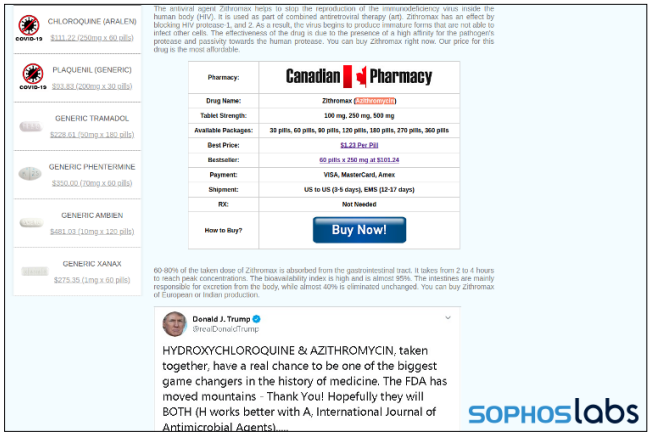


図 19: 悪名高い「ピルミル」の詐欺師ですら、Twitter に現れた「奇跡的」治療法に便乗せずにはいられないらしく、広告にもツイートを掲載しています。出典：SophosLabs

フィッシングやマルウェアとの関連が確認されているのは、ごく一部（1% 未満）です。多くは一時的なものであり、1 日ほどでホスト名が解決されなくなります。

リモートワークによりクラウドコンピューティングのセキュリティ保護の重要性が高まる

2020 年 3 月に COVID-19 のロックダウンが始まると、前例のない働き方改革が急速に開始され、これは今日まで続いています。働き方、教育、イベントや会議への参加方法、そして娯楽のあり方が恒久的に変化するのに伴い、クラウドコンピューティングはその急速な進化のために欠かせない要素となっている一方で、多くの課題に直面しています。

アクセス権限の過剰なプロビジョニング、クラウド内の資産やリソースに対する不十分な可視性、監査の欠如といった問題のために、クラウド環境はサイバー脅威に対して脆弱になっています。また、他のあらゆる場所と同様に、マルウェアはクラウドでも深刻な影響を及ぼします。たとえば、クラウドではクリプトジャッキングが問題になっています。処理負荷の高いクリプトマイナーのプロセスは、物理マシン上で実行される場合でも問題であり、高額な電気代が発生します。しかし、クラウドインスタンスで実行されると、さらに深刻な影響を与えます。クリプトマイナーの標的となった組織は、少額な暗号通貨を採掘して提供するために仮想ワークステーションが、負荷の高い計算を実行することになり、そのために消費した CPU サイクルの料金をクラウドプロバイダーから課金されます。

さらに、ランサムウェア攻撃により、物理マシンがターゲットになった場合と同様にクラウドインフラストラクチャが利用できなくなり、リモートワークで分散している従業員の多くに深刻な影響が及びます。ランサムウェアは、仮想ハードドライブやオブジェクトストレージも、物理ストレージと同じように、簡単に暗号化できます。クラウドインフラストラクチャがランサムウェアによって攻撃されると、データの暗号化に費やした CPU サイクルに対して請求されるだけでなく、身代金までも請求されることになります。

過去 1 年間にセキュリティインシデントに見舞われた組織

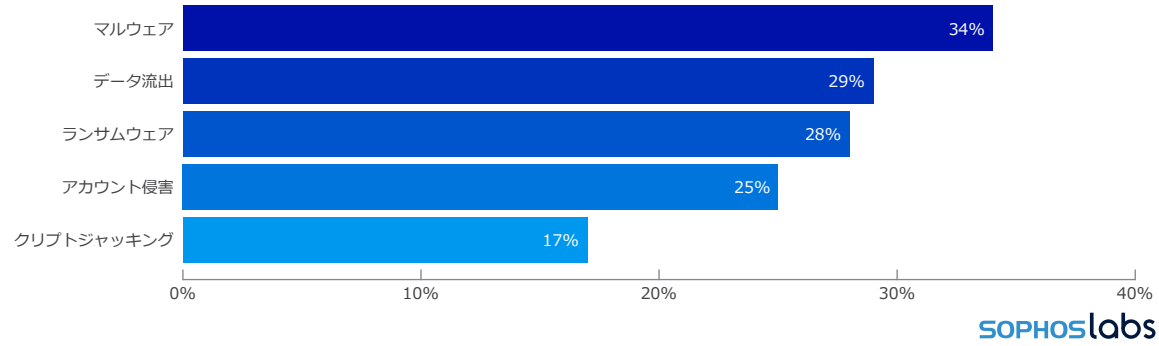


図 20: 2020 年のクラウドセキュリティレポートで、ソフォスは 3,500 人以上の IT 管理者を対象にクラウドの利用経験について調査しました。その結果、物理ネットワークに影響していたセキュリティの問題の多くが、仮想ネットワークでも起こっていることが明らかになりました。出典：SophosLabs

ロックダウン時には、多くのオフィスが閉鎖される前に IT 部門は実際のヘルプデスクに人員を配置するように、仮想ヘルプデスクとしてサービスをリモートの従業員に提供する方法を確立しなければなりませんでした。COVID-19 への対応で求められた大きな変化は、3 つの波となって現れました。

ロックダウンが始まって最初の数週間で、第一波となる「アクセスの波」が起こり始めました。突然出勤できなくなった何百万人もの人々が、組織の環境にあるリソースにアクセスする必要が生じたために、仮想プライベートネットワーク (VPN) やその他のゼロトラスト機能へのアクセスに対する需要が急増し、既存のリソースでは対処できなくなりました。VPN とともに、企業は新しいファイアウォールなどのセキュリティアプライアンスを追加する必要があることを認識し、最新の UTM システムを導入して、クラウドサービスが提供する基本的なレイヤー 3 のファイアウォールを強化しました。

COVID-19 以前は、出張者やリモートワーカーに比べてオフィスで働く従業員がはるかに多かったため、VPN は大規模に利用されていたわけではありませんでした。しかし、3 月が終わり、5 月、そして 6 月へと時間が経過するにつれ、これらの従業員にとって VPN は、「唯一」ではないとしても組織運営の維持に欠かせない生命線の 1 つとなりました。

しかし、これらの組織は、従業員が自宅から VPN にアクセスするために個人所有のデバイスを使用すべきではないこともすぐに認識しました。また、ノート PC の新規の供給量が減少したことで、分散したワークフォースの IT 関連のサポートするすでに厳しい状況になっている組織にとって新たな課題が生まれました。物理的なマシンが不足したため、組織は当面の間、セキュアコンピューティング環境のニーズを満たすために、一見無限に見える仮想マシンというリソースに注目したのです。これが第二の波、つまり「仮想デスクトップの波」の始まりでした。

多くの従業員が仮想の企業デスクトップを使用するようになりました。クラウドでこれらのデスクトップをホスティングすることは、実用的でコスト面でも合理的でしたが、依然として保護が必要でした。

IT 部門は、突如として数百台、または数千台もの従業員用の仮想マシンをサポートしなければならなくなりました。仮想サーバー、仮想デスクトップ、その他のクラウドサービといった、クラウドで増大する資産のインベントリを管理し、安全に構成するための可視化ツールが急きょ必要になりました。

攻撃のタイムライン

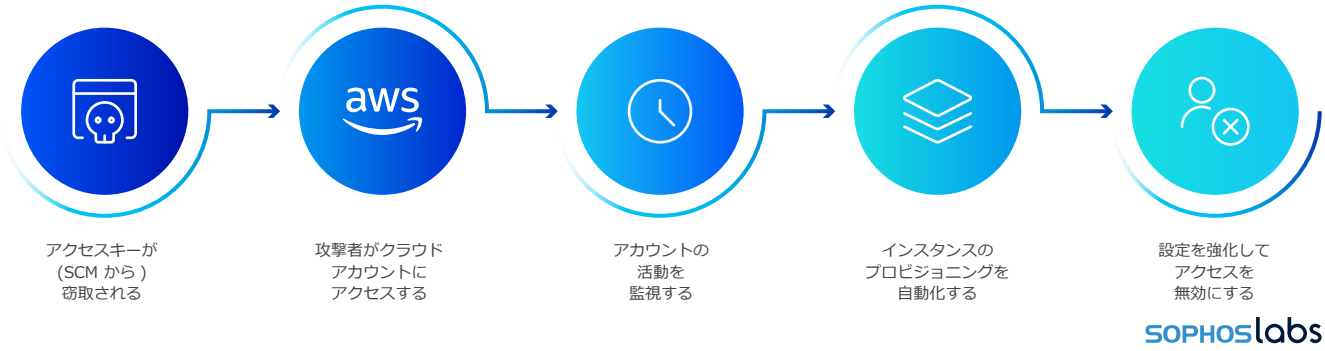


図 21: ソフォスが調査したクリプトジャッキング攻撃は、開発者が誤ってパブリックリポジトリのコードにクラウドの認証情報を埋め込んでしまったことから始まりました。これを発見した攻撃者は、その認証情報を利用して、ネイティブクラウドプロバイダーの API を使用して攻撃し、ビットコインのマイニングのために数百の仮想マシンインスタンスを立ち上げました。同時に、それらのインスタンスの機能を自動化して終了を困難にしました。その後、他の合法的なユーザーへのアクセスを無効にしました。
出典：SophosLabs

COVID-19 の時代になって、多くの人々の働き方を含め、生活のあらゆる面が大きく変わりました。ロイター社の最近の調査では、ロックダウンによって新しいテクノロジーへの移行が加速したと答えた CEO と CTO の割合が 97% に上りました。しかし、予算がひっ迫し、不確実性が高まっている状況において、これらの CTO の 3 分の 1 近くは、可能な限り費用対効果の高い方法で変革を実現することを責務として認識していました。

ソフォスの最新のクラウドセキュリティレポートでは、クラウドコンピューティングに関連するセキュリティインシデントの大部分は、認証情報の窃取（フィッシング）と構成ミスによる侵害という 2 つの主要な根本原因によって起こっていることが明らかになっています。調査対象となった 3,700 人以上の IT 管理者の 10 人中 7 人は、調査前 12 か月間にサポートするクラウドインフラストラクチャの侵害が発生したと回答しています。

大規模な脅威への迅速な対応における CCTC の意義

図 22: 出典：ソフォス

COVID-19 のロックダウンが始まって 1 週間後から、ソフォスのチーフサイエンティストである Joshua Saxe は全世界に向けて有志を募りました。この「仮想のバケツリレー」によって、瞬く間に結成された COVID-19 Cyber Threat Coalition (CCTC) は、「COVID-19 に関する恐怖や不安を煽り、便乗するあらゆる種類の脅威やソーシャルエンジニアリングに断固として対抗する」という共通の目標を掲げた組織であり、4,000 人以上のメンバーが存在します。

CCTC のメンバーであり、米国シカゴを拠点に活動しているセキュリティアナリスト / ポッドキャスターの Nick Espinosa 氏は、次のように語ります。「私は消防士ではないので、建物の火災への対処については素人です。しかし、病院のような重要インフラストラクチャの防御を強化する取り組みを支援することはできます」

喫緊の取り組みが求められていました。攻撃者は、ロックダウンが始まった当初から、新たなこのパンデミックに関連する用語を悪用しながらスパムやマルウェアなどの脅威を拡散させました。本レポートで述べているように、「COVID-19」、「corona」、「CoV」といった文字列を含む何千ものドメインが、一時期は毎日のように新規に登録されました。ソフォスは、証明書データにこれらの文字列を含む TLS 証明書に結び付けられたドメインを追跡し、さらに数千のドメインを発見しました。

COVID-19 Cyber Threat Coalition (CCTC) の参加メンバー数

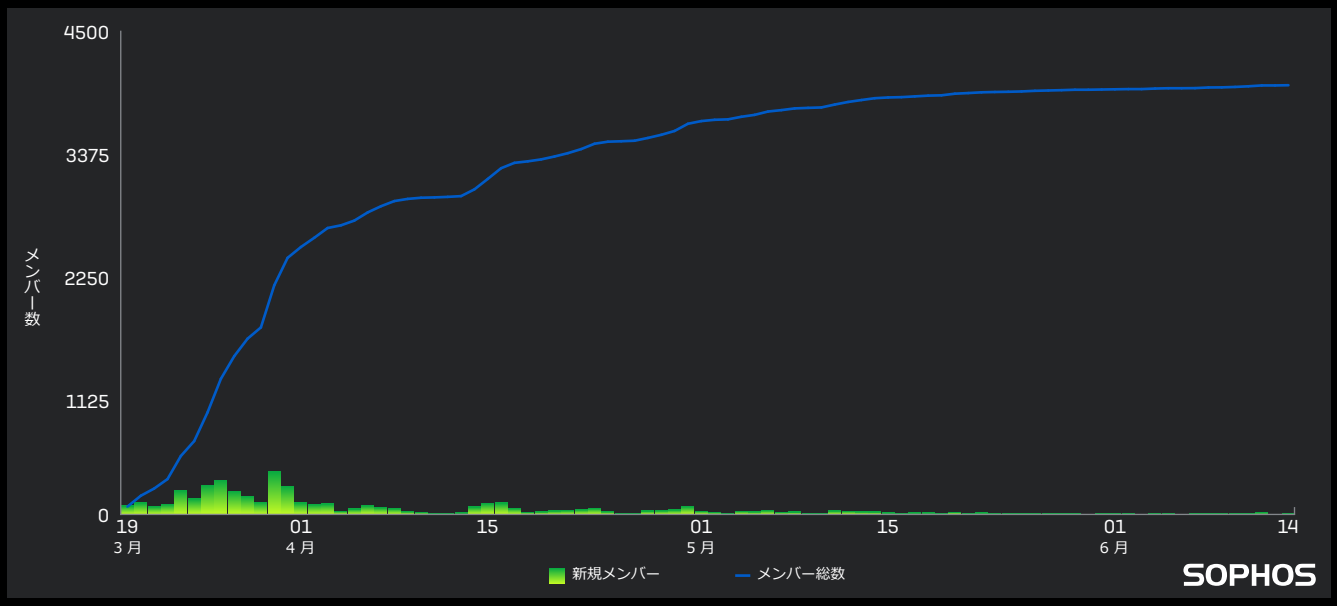


図 23: 出典：ソフォス

COVID-19 が世界にもたらした脅威が特異であることから、この世界的な危機に便乗する悪意のあるスパムは、とりわけ悪辣で攻撃的です。「COVID-19 に便乗するハッキングが爆発的に発生していることを確認しました」と、Espinosa 氏は述べています。WHO (世界保健機関)、米国 CDC (疾病予防管理センター)、英国 NHS (国民保健サービス)、製薬会社、米国や英国以外の保健当局などからの公式メッセージを装ったスパム攻撃が大規模に展開されました。

アナリストは、バイナリの文字列にも COVID-19 への参照が含まれ、LoL (環境寄生型 Living off the Land) スクリプトで変数として使用されていることを確認しました。

CCTC の参加者は、緊急に立ち上げた Slack チャネルを通じて、あらゆる種類のインシデントに関する検体や情報を共有しました。組織は当初は混乱も見られましたが、すぐに活動を実行するための基本的な構造が形成されました。「多くのメンバーが結集し、『消火活動』のために大量の情報が共有されました」と、Espinosa 氏は語ります。

CCTC の成果物となる、新たに収集された IoC (攻撃の痕跡情報) を一覧する情報フィードは、誰でも自由に使用できます。これらの IoC は、ベンダーを問わず導入されている既存の防御テクノロジーを補完します。CCTC が Cyber Threat Alliance (CTA) とパートナーシップを結び、CTA に参加するセキュリティベンダーが CCTC の脅威インテリジェンスを取り込み、それらの脅威から防御するようになったことで、CCTC の脅威インテリジェンスの防御効果が増幅されました。

目標を同じくするセキュリティ専門家の速やかな連携には気持ちが救われたと、Espinosa 氏は述べています。同氏によると「出だしから混乱した」状態でしたが、すぐに自律的な組織化を遂げました。CCTC の共有プラットフォームが完成したことで、今後 COVID-19 のようなパンデミックが起こってもゼロから始める必要がなくなり、脅威に迅速に対処できます。免疫系の健全な作用と同じことが、脅威からの防御にも当てはまります。

油断禁物：新しいプラットフォームを介する脅威

ルーター、携帯電話、ファイアウォール、スマートテレビ、ストリーミングボックス、VoIP ボックス、カメラ付きインターホン、ネットワークに接続されたストレージ、一部のスマート家電など、コンピューターやサーバーのように見えないコンピューティングデバイスが私たちの生活に浸透しています。

しかし、コンピューターに見えないからといって、同じように誤用または悪用されないわけではありません。

Android Joker マルウェアの増加

Android プラットフォームと Google Play ストアを所有する Google と、Google Play ストアを介してマルウェアをダウンロードさせようと画策するマルウェア作成者が競争を繰り広げる中、Android ユーザーはその狭間に置かれています。Google は、悪意のある目的や Android ユーザーにとって望ましくない結果となるコードを探すため、Google Play ストアへの掲載のために提出された Android アプリのソースコードを検査するシステムに何年もの歳月を費やしてきました。一方、マルウェアアプリの開発者は、Google Play ストアのコードチェックを回避しようと躍起になっています。

Joker (別名 Bread) は、SMS を盗み出したり、勝手に課金したりする詐欺アプリであり、コードチェックを回避するために進化を続け成功しているマルウェアファミリーの 1 つです。研究者が昨年最初に発見して以来、Google は、Joker を改造した何千もの悪質なアプリを Google Play ストアから削除しています。マルウェアを取り除くために多大な労力を投入しているにもかかわらず、Joker は執拗に戻ってきます。

Joker は、ユーティリティ / ツール、壁紙、翻訳ツール、メッセージングサービスなど、さまざまな人気アプリのクローンを装って登場します。注意しなければならないのは、一般的に使用されているアプリの本物のバージョンに外観も動作もそっくりなアプリに、Joker が埋め込まれている可能性がある点です。Joker アプリでは、アプリ作成者がさまざまな正当な理由で日常的にコンパイルしているサードパーティ製ライブラリの 1 つに、小さなマルウェアコードが追加されてその奥深くに埋め込まれています。

Joker は、Google Play ストアのセキュリティコードチェックを回避することに繰り返し成功していますが、その理由はいくつかあります。

1. 悪意のあるアプリは、単純な文字列の置換から複雑な商用パッカーまで、さまざまな難読化の手法を利用して分析を遅らせ、Google Play ストアを騙します。
2. Joker の「開発者」がアプリを最初に提出するときには、悪意のあるコードは一切含まれていません。このため、Google Play ストアに提出されたアプリが悪質でないという履歴が確立されます。しかし、その後のアップデートによって、悪意のあるコードがアプリに現れます。
3. アプリは後で、実行時のペイロードの復号化や動的なダウンロードを実行します。

Joker マルウェアは、一般的な DEX の代わりにネイティブコード (JNI) を使用します。ネイティブコードは、プログラミングに C 言語を使用しているため、悪意のあるコードの解析が遅れます。これに比べて、Java コードの変種である DEX は、人間が解読可能なものにデコンパイルするのがはるかに簡単です。このマルウェアは、SMS メッセージを送信するため、収益を得るため、そして C&C ネットワークとの通信方法として、この JNI コードを使用します。インターネットの代わりに電話網を介して JNI と帯域外シグナリングを使用することで、Joker は JNI を解釈しない自動 DEX スキャナーを回避できる可能性があります。

新しいアプリを対象とする Google の自動コードレビューに対して、Joker は明らかに優位に立っています。2021 年に Joker が減速する兆候は見られず、近い将来にはさらに競合が加わる可能性もあります。

広告 /PUA とマルウェアの境界が曖昧に

悪意のある広告 (マルバタイジング) は、依然としてさまざまなデバイスに対する脅威の主な発生源となっています。ソフォスは最近、マルウェア攻撃には分類されていない悪意のある広告の脅威について、現在の 2 つのトレンドを掘り下げて調査しました。それは、「ブラウザをロックする」Web ページを使用するテクニカルサポート詐欺と、モバイルデバイスを狙って詐欺 (「フリースウェア」) アプリにリンクする広告です。ソフォスでは、これらを「偽アラート」攻撃、つまりターゲットを脅して詐欺師に利益をもたらすように誘導する不正広告に分類しています。

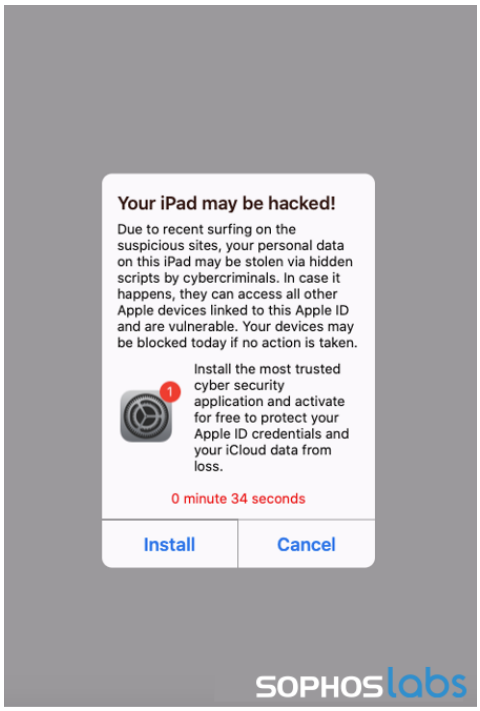


図 24: 出典：SophosLabs

テクニカルサポート詐欺は一般的に、ターゲットをだましてコンピューターへのリモートアクセス権限を提供させ、法外な価格のテクニカルサポートソフトウェアやサービスを購入させたり、詐欺目的でターゲットのクレジットカードデータを窃取したりすることを目的としています。このような詐欺の多くは、これまでは電話を直接かけるテレマーケティングを利用していました。しかし、多くの詐欺師は、セキュリティ上の理由からコンピューターがロックされているとユーザーを信じ込ませようとする悪質な Web 広告を使用し、詐欺師にユーザーが電話をかけるように仕向けるモデルに移行しています。

ユーザーに電話させるために、Microsoft や Apple のアラートを装いつつ、カーソルを改変したり (マウスポインタが指す場所を偽ったり隠したりする機能)、ブラウザの処理能力をひっ迫させる「無限ダウンロード」攻撃など、そのページからの移動を困難にするように設計されたスクリプトを実行する Web サイトキットを展開します。ソフォスが発見したキットの中には、バグを悪用するもの (攻撃の視点から研究を進める SophosLabs のセキュリティチームが今年 Firefox で発見) や、他のブラウザで同様の攻撃を実行するものがあり、いずれも悪意のあるポップアンダー 広告によって拡散されます。

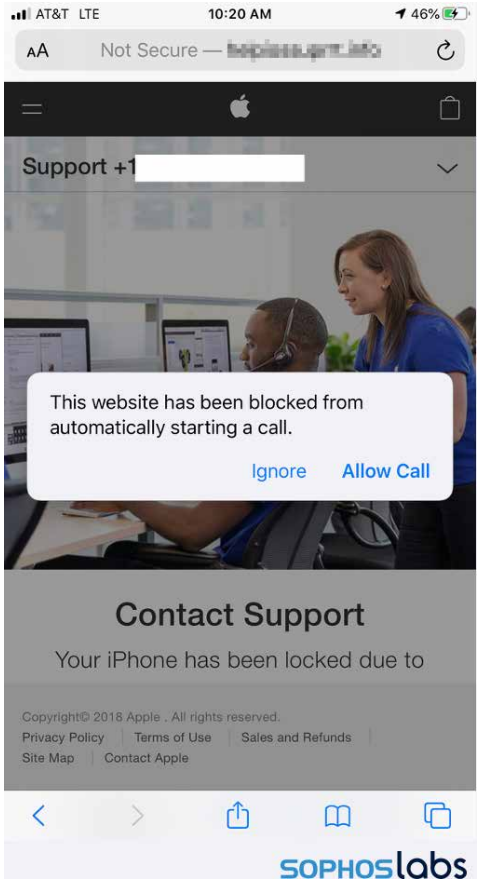


図 25: 出典 : SophosLabs

PC や Mac のブラウザでこれらの攻撃を行う同じ広告ネットワークインフラは、テクニカルサポート詐欺や、潜在的に迷惑なモバイルアプリケーションにリンクする偽のアラートも提供します。たとえば、仮想プライベートネットワークサービスや「クリーン」なツールを名乗り、マルウェアを除去すると宣伝し、定額料金を請求するアプリなどがあります (実際には Android マルウェアである場合もあります)。ソフォスは、このような攻撃を実行するために特別に構築された商用ソフトウェアをロシアの開発者から入手して調査し、これらの広告を配信する一連の広告用サーバーを発見しました。

自分を保護するツールが悪用される：サイバー犯罪者によるセキュリティツールの悪用

攻撃の中には、マルウェアを全く使用しないものもあれば、攻撃の最終段階までマルウェアが配信されるのを待機するものもあります。その代わりに、ネットワーク上のコンピューター上で実行されているオペレーティングシステムのツールだけを使用します。また、インシデント対応と侵入テストという、情報セキュリティ業界の 2 つの主要な領域で使用されているさまざまなツールの機能を悪用する犯罪者も存在します。

情報セキュリティ業界では、マルウェアをほとんど使用せず、オペレーティングシステムの既存のコンポーネントや一般に使用されているソフトウェアパッケージを使用する攻撃を、環境寄生型 (LoL: Living off the Land) と定義しています。これらの攻撃は通常、PowerShell、バッチファイル、VBScript スクリプトなどのネイティブスクリプト (総称して LOL スクリプト) によって自動化されます。攻撃者はこれらの LOL スクリプト を使用し、LOLbin と呼ばれる LoL バイナリ (アプリケーション) を使用し、一連のコマンドを実行します。

元来、セキュリティ業界の「レッドチーム」向けに設計されたソフトウェアは、「攻撃者によって持ち込まれた攻撃手法」を検出して対策するようになっています。この環境寄生型の攻撃では、ネットワーク管理者や侵入テスト担当者が一般的に使用しているセキュリティツールを展開して使用します。これには、セキュリティ評価や技術テスト向けに設計された、Cobalt Strike、Metasploit フレームワークの要素などのツールが含まれます。

Netwalker 攻撃ツールセットの ATT&CK マトリクス

初期アクセス	実行	権限昇格	防御の回避	認証情報アクセス	探索	ラテラルムーブメント	影響
Tomcat の脆弱性を利用	PowerShell スクリプト	CVE-2020-0796	ファイルレスローディング	mimikatz	SoftPerfect Network Scanner	psexec	Netwalker ランサムウェア
Weblogic の脆弱性を利用	psexec	CVE-2019-1458	Eset AV remover	Mimidogz	NLBrute	Teamviewer	Zeppelin ランサムウェア
フィッシングメール		CVE-2017-0213	Gordon の ESET パスワード回復ツール	Mimikittenz		Anydesk	Smaug ランサムウェア
		CVE-2015-1701	Trend Micro セキュリティエージェントのアンインストールツール	Windows Credentials Editor			データ窃取
			Microsoft Security Client のアンインストール	pwdump			
				NLBrute			
				LaZagne			
				WinPwn			

SOPHOSlabs

図 26: Netwalker ランサムウェア攻撃で使用されたツールセットでは、攻撃のさまざまな段階で、オープンソース、フリーウェア、商用ユーティリティが幅広く使用されました。出典：SophosLabs

攻撃者にとって、これらのツールにはいくつかの理由で価値があります。これらのツールは正当な目的 (監査やシステムセキュリティの向上) で使用されることが多く、そのようなツールや活動をアンチウイルスやセキュリティソリューションが検知することは困難になっています。したがって、悪意のある活動を特定するには、LOL スクリプトを使用する場合の挙動の研究に注力する必要があります。そしてもちろん、独自のツールをゼロから作成するよりも、既存のツールを使う方が簡単です。

LOL スクリプトとリバースシェルの使用は、この 1 年間で見られた新しい傾向ではありませんが、2020 年には手動による複雑なランサムウェア侵入攻撃で広く使用される要素となりました。実際に、攻撃時に観測された攻撃ツールは、数も種類も増加しています。

RaaS 攻撃ツール「Dharma」のキルチェーン

初期アクセス	実行	権限昇格	防御の回避	認証情報アクセス	探索	ラテラルムーブメント	窃取	影響
RDP パスワードスプレー	PowerShell	CVE-2019-1388	マルウェアからの保護の無効化	mimikatz	PCHunter	グループポリシーオブジェクト	PowerShell スクリーンショットメーラー	Dharma ランサムウェア
盗まれた RDP 認証情報	WMI	CVE-2018-8120	Revo アンインストーラー	Remote Desktop Passview	Process Hacker	リモートデスクトップ	TOR	
	AutoIT	CVE-2017-0213	IOBit アンインストーラー	LaZagne	GMER	WinRM リモート管理	dropmefiles[.]com	
	コマンドライン/RDP			NLBrute	高度な IP スキャナー			
				Hash Suite Tools	NS2.EXE			

SOPHOSlabs

図 27: 出典：SophosLabs

攻撃ツールは、市販のアプリケーションからオープンソースの GitHub リポジトリまで幅広く、以下のような機能的を持ちます。

- ボットネットに似た C&C のフレームワーク
- シェルコードの生成と難読化
- アンチウイルスの回避とサンドボックスの検知
- パスワードまたは認証情報の抽出
- Kerberoasting (ドメイン管理者権限の永続性の維持)
- さまざまなサービスで使用されるパスワードに対するブルートフォース攻撃の能力
- システムデータの窃取

これらのタイプのツールのほとんどは、「使い始め」の状態では、無害なペイロードしか含まれないか、ペイロードをまったく含まないかのどちらかです。しかし、ソフォスの挙動検知テクノロジーによって取得したコンテキスト情報から、これらのツールの多くがこれまでに悪意のある活動に関与しているが明らかになっています。

ソフォスのテレメトリによると、最もよく使用されている攻撃ツールは、(使用頻度の高い順に) Metasploit、BloodHound、mimikatz、PowerShell Empire、Cobalt Strike、Veil Evasion、Hydra THC、Enigma、Nishang、Shellter の 10 種類です。Metasploit は検出される頻度が非常に高いツールであり、次に多く検出される BloodHound の約 2 倍の頻度で出現しています。

ソフォスは現在、99 種類の攻撃ツールの使用状況を追跡していますが、攻撃者は 2021 年を通してこれらの効果的なツールを繰り返し利用し続けることになることが予測されます。

デジタル疫学

「検知されていないマルウェアに感染しているコンピューティングデバイスの割合は？」「検知されていない敵によってコマンドラインが実行される割合は？」「標的型フィッシングメールが検知されない割合は？」「これらの割合は、業界、地理的位置、ネットワークのセキュリティ機能といった要素に応じてどのように変化するのか？」

このような質問は、多くの人がウイルス検査を受けない可能性があり、実施されている検査の偽陽性率と偽陰性率が非常に高い可能性がある状況における、「COVID-19 に感染している人の割合は？」という質問に似ています。

つまり、答えることが難しい質問です。

これらの課題にもかかわらず、COVID-19 に関して、疫学者は毎日のように重要な質問に回答し続けています。残念ながら、サイバー攻撃について、サイバーセキュリティの研究者は十分な回答を提供できていません。不確実な状況下でも、論理的な対策を講じるために構築されたツール、手法、手順において、サイバーセキュリティは疫学に後れをとっています。しかし、それを言い訳にすることは許されません。直面する脅威の本質を理解し、防御対象のリスクを正確に報告し、何に注力すべきかを決定するために、独自のツールを構築する必要に迫られています。

このミッションを支援するために、Sophos AI は、全体的なマルウェア感染の広がりを推定するための、疫学に着想を得た一連の統計モデルを構築するプロジェクトに乗り出しました。そこで、1 億のエンドポイントからデータを収集する堅牢なデータ収集パイプラインとベイズ統計手法を組み合わせています。これによって、「現場」でのモデルのパフォーマンスの全体像を構築するため、これらの難しい問題に取り組むことができます。

たとえば、「毎週、実際にどれだけのマルウェアが顧客に影響を与えているのか？ そのうち、どの程度の割合で検知できているのか？」という質問を考えてみましょう。

すべてのファイルの中で、どのファイルがマルウェアで、どのファイルが無害であるかを把握していれば、答えるのは簡単です。しかし、実際には 2 つの問題があります。

1. どのエンドポイント製品でも、一部のマルウェアはどうしても検知されず、また偽陽性（マルウェアとしてフラグが立てられた正規のファイル）の発生は避けられません。
2. 無害なファイルと悪意のあるファイルの数を比べると、無害なファイルが圧倒的に多いため、手動で分析するのはおそらく不可能です（悪意のあるファイルを 1 つ見つけるために、エンドポイント製品が無害と判断した何千ものファイルを徹底的に分析する必要があります）。

これらの問題に対処するため、ソフォスはベイズ統計学に注目しました。簡単に言うと、私たちが構築しているのは、データを「生成できる」モデルです。このモデルは、パラメーター（「実際にどのくらいのマルウェアが存在するのか？」）について推測し、その推測をエンドポイントで検知される数のシミュレーションに変換できる数学的プログラムです。

次に、さまざまな推測を試して、どのシミュレーションが実際に観測された結果と一致するかを確認します。そこから逆算して、注目するパラメーターの中でもっともらしい値を見つけます。

たとえば、エンドポイントでの検知数が 2,000 であり、特定の週におけるモデルの真陽性率と偽陽性率を正確に推定できていると想定します。0% 、2% 、5% などマルウェア率を使用して世界のシミュレーションを行い、エンドポイントの検知率がどのように予想されるかを確認します。マルウェア検知数が 2,000 に近くなるマルウェア感染率があれば、それが妥当な値となるはずです。

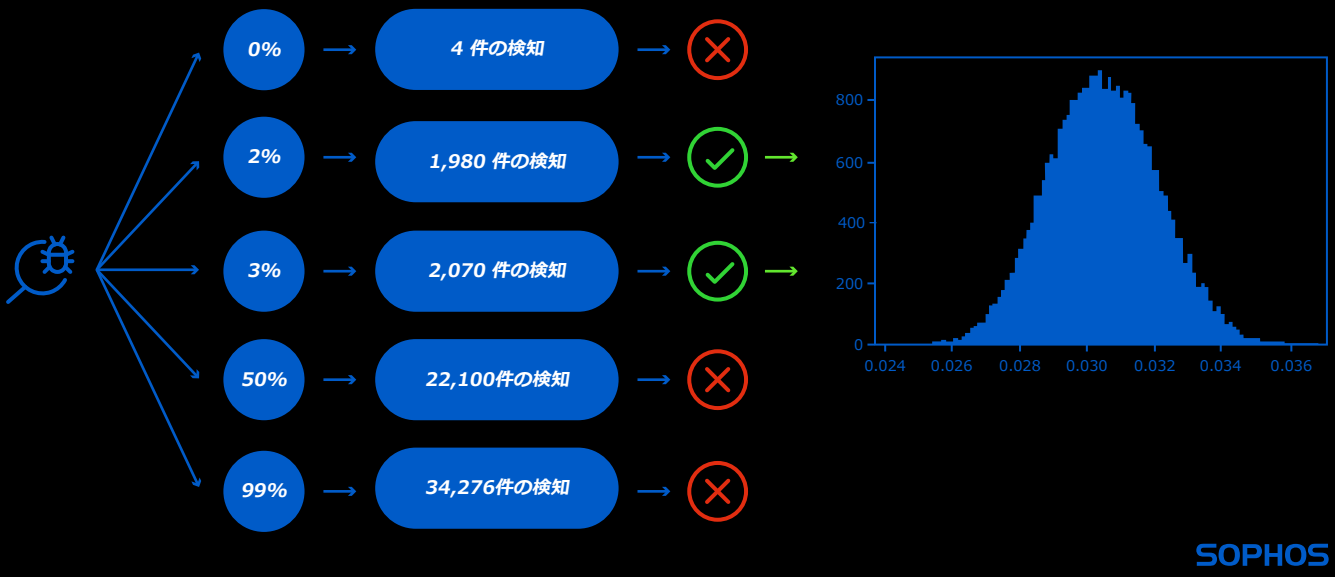


図 28: マルウェア率を提案し、サンプリングし、シミュレーションが観測された現実の値と一致するかどうかを確認し、一致した率を集計し、これを繰り返します。
出典：Sophos AI

このプロセスを何百万回も繰り返して、マルウェア感染率の妥当な値の分布を構築することができます。また、ベイズ統計手法を使用しているので、エラーバーは推定値に「織り込み済み」です。この例の場合、「ファイル全体に占めるマルウェアの割合は？」という質問に対する可能性が最も高い答えは、モデルによると 3% を少し上回る値になりますが、約 2.75% から約 3.35% の範囲であれば、妥当性がかなり高いと言えます。

また、この値（「顧客のエンドポイント全体に占めるマルウェアの割合は？」の答え）を把握できれば、偽陰性（検知漏れ）や偽陽性（誤検知）についても簡単に推定できます。5 月の 1 週間における、ディープラーニング ML ベースのマルウェア検知システムのデータを使用して（シグネチャベース、挙動ベース、ヒューリスティックのオプションはオンにしません）、真陽性、偽陽性、真陰性、偽陰性の完全なマトリクスを完成させることで、モデルのパフォーマンスを把握できます。この場合、一定の偽陰性がある一方で、偽陽性の数は少なく、ゼロに向かって傾いています。また、真陽性の数は多く、161,000（サンプル内の陽性の合計数）に向かって傾いています。

数値の規模を見ると、これら 3 つの数値に比べて、真陰性 (ML が無害と判断した無害なファイル）の数が圧倒的に多いことがわかります。

疫学に着想を得たこのツールによって、大量の PE ファイルの中に潜むごく少数のマルウェアを（見つけたわけではないとしても）推定できます。

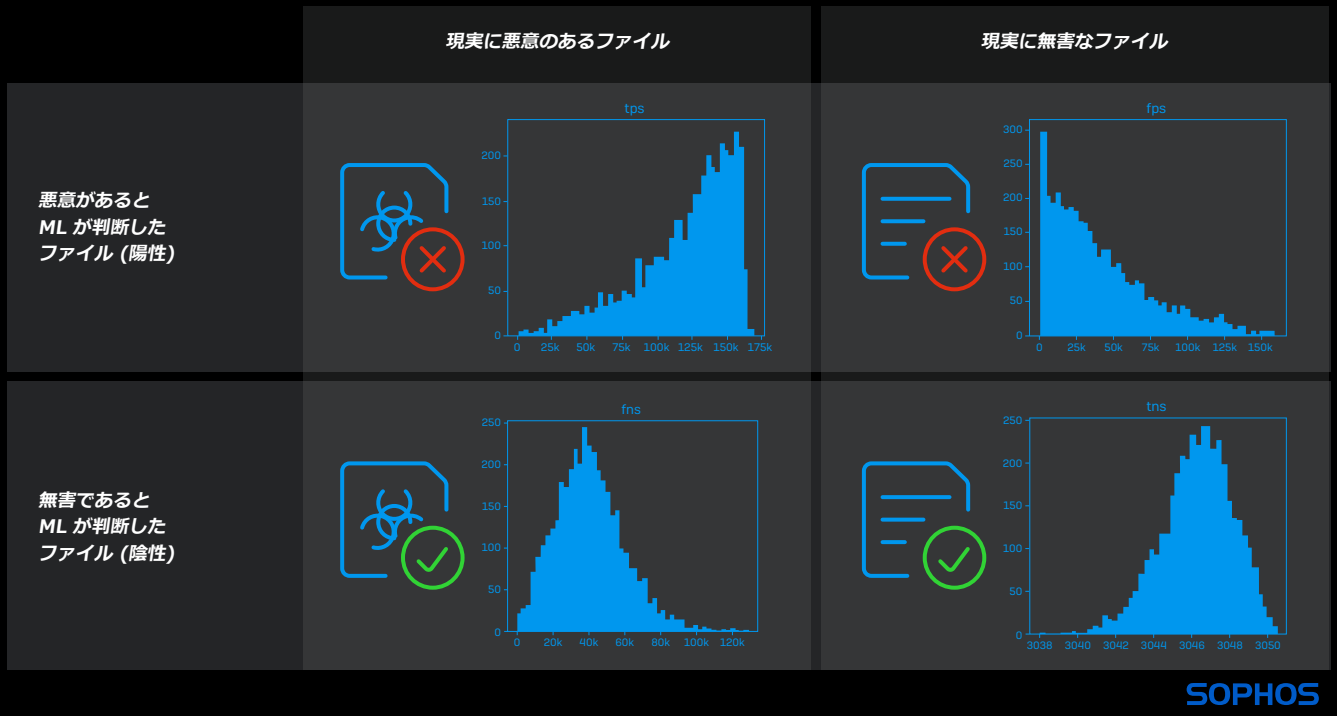


図 29: 2020 年 5 月上旬における ML モデルの真陽性と偽陽性の分析。出典：Sophos AI

ソフォス株式会社営業部
sales@sophos.co.jp

20-11-01 EN (DD)

SOPHOS