サイバーセキュリティ脅威レポート 2020年第1四半期

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

目次

序文

2020 年最初の ESET 四半期脅威レポートをご覧いただきありがとうございます。2020 年の第 1 四半期には、私たちの生活は新型コロナウイルス（COVID-19）の流行による大きな影響を受け、世界の多くの国が封鎖（ロックダウン）され、前例のない制約を受けています。

新型コロナウイルスの感染が拡大する中で、多くの企業はテレワークを急遽導入せざるを得なくなりましたが、これが多くの新しい問題を生み出す結果になりました。リモートアクセスやビデオ会議アプリケーションの需要の急増にサイバー犯罪者が便乗しており、社会の仕組みの変化から抜け目なく利益を得ようとしています。

サイバー犯罪者は、感染症の流行を取り巻く人々の懸念を悪用することを一切躊躇しません。2020 年 3 月には、人々が抱いている新型コロナウイルスの流行に対する恐れや情報の渇望を悪用した詐欺やマルウェア攻撃が急増しました。

都市がロックダウンされている状況の中でも、ESET のアナリスト、検出エンジニア、およびセキュリティスペシャリストは、今四半期の動向を注視し続けています。クリプトマイナーや Android マルウェアなどの一部のタイプの脅威は、前四半期と比較して検出数が減少しましたが、Web の脅威やストーカーウェアなどの脅威は増加しました。新型コロナウイルスのロックダウンの影響と考えられますが、特に Web の脅威は、検出された脅威全体で最大の増加が確認されています。

ESET Research Lab も、脅威の調査を継続しています。2020 年第 1 四半期には、新しい暗号化モジュールである Stantinko の難読化手法を分析し、ブラジルの銀行組織を標的とする高度なトロイの木馬 Guildma の詳細な仕組みを解明しました。さらに、悪名高い Winnti Group と Turla による新しい攻撃や、10 億台以上の Wi-Fi デバイスの暗号化に影響する、これまで知られていなかった脆弱性 KrØØk も検出しました。

ロックダウンが新たな日常となる前は、ESET Research Lab の専門家は世界中のセキュリティ会議やイベントに参加し、研究の成果を共有していました。今年 2 月には脆弱性 KrØØk の調査結果を発表し、RSA Conference 2020 では Linux マルウェアの検出に関するワークショップを主催、BlueHat IL で 2 回講演を行っています。

ESET の研究者を檀上で見ることはしばらくできないかもしれませんが、ESET のブログ、WeLiveSecurity、および ESETresearch の Twitter で調査結果をご確認いただけます。また、これらの四半期毎の脅威レポートもぜひご参照ください。

本レポートが皆さまのお役に立てれば幸いです。健康を維持しながら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

KrØØk：10 億台以上の Wi-Fi 対応デバイスの暗号化に影響を及ぼす深刻な脆弱性

Miloš Čermák および Robert Lipovský 著

ESET の研究者は、攻撃者が脆弱なデバイスから送信された一部のワイヤレスネットワークパケットを解読可能となる新しい脆弱性を発見しました。

ESET の研究者は、これまで知られていなかった脆弱性が Wi-Fi チップに存在することを発見し、この脆弱性を KrØØk と名付けました。この重大な脆弱性には、CVE-2019-15126 が割り当てられており、脆弱なデバイスはすべてゼロ値の暗号鍵を使用してユーザーの通信の一部を暗号化します。この脆弱性を利用した攻撃が成功すると、攻撃者は脆弱なデバイスから送信された一部のワイヤレスネットワークパケットを解読可能となります。

Broadcom および Cypress の Wi-Fi チップを搭載し、パッチが適用されていないデバイスが、KrØØk の影響を受けます。これらは、スマートフォン、タブレット、ラップトップ、IoT ガジェットなど、Wi-Fi 対応デバイスで現在最も多く使用されている一般的な Wi-Fi チップです。

さらにクライアントデバイスだけでなく、Broadcom チップを搭載した Wi-Fi アクセスポイントやルーターもこの脆弱性の影響を受けるため、この脆弱性の影響を受けないデバイスやパッチが適用されているクライアントデバイスから構成されている環境であってもこの脆弱性の影響を受けます。

パッチを適用する前に ESET が実施したテストでは、Amazon（Echo、Kindle）、Apple（iPhone、iPad、MacBook）、Google（Nexus）、Samsung（Galaxy）、Raspberry（Pi 3）、Xiaomi（RedMi）の一部のクライアントデバイスと、Asus および Huawei の一部のアクセスポイントが、KrØØk に対して脆弱でした。控えめに見積もっても、合計で 10 億台を超える Wi-Fi 対応デバイスとアクセスポイントがこの脆弱性の影響を受けます。さらに、ESET がテストをしていない他の多くの製品のベンダーも、この問題の影響を受けるチップセットをデバイスで使用しています。

この脆弱性は、AES-CCMP 暗号化を使用した WPA2-Personal プロトコルと WPA2-Enterprise プロトコルの両方に影響します。

KrØØk は、2017 年に Mathy Vanhoef 氏によって発見された ***KRACK***（Key Reinstallation Attacks）[1] と関連しています。調査の初期段階で、KRACK 攻撃に関するテストで確認された、すべてゼロ値の暗号鍵の「再インストール」が KrØØk の原因に関連していることがわかりました。この調査は「***AKRACK による Amazon Echo と Kindle への影響***」という ESET の過去の調査から続いています [2]。

ESET は、この脆弱性をチップメーカーの Broadcom と Cypress に開示しました。その後、両社はこの問題を世界に公開し、更新プログラムをリリースしています。また、***ICASI*** (Industry Consortium for Advancement of Security on the Internet) [3] と協力し、影響を受けるデバイスメーカーやその他のチップメーカーなど、すべての関係者が KrØØk について知ることができるよう手配しました。

ESET がこれまでに収集した情報によると、大手メーカーのデバイス用のパッチはすでに公開されています。デバイスの所有者として自分を保護するためには、携帯電話、タブレット、ラップトップ、IoT デバイス、Wi-Fi アクセスポイントおよびルーターなど、Wi-Fi 対応デバイスに対し、最新の更新プログラムを適用してください。デバイスメーカーの担当者は、KrØØk の脆弱性パッチについて、チップメーカーに直接お問い合わせください。

この調査に多大な貢献をした同僚の Juraj Bartko と Martin Kalužnik に感謝します。また、報告した問題について積極的に協力いただいた Amazon 社、Broadcom 社、Cypress 社と、影響を受ける多くのベンダーに周知いただいた ICASI の支援にも深く感謝申し上げます。

セキュリティブログ記事 [4] | KrØØk ホワイトペーパー [5] | KrØØk ウェブサイト [6] | RSAC 2020 presentation [7]

KrØØk の脆弱性

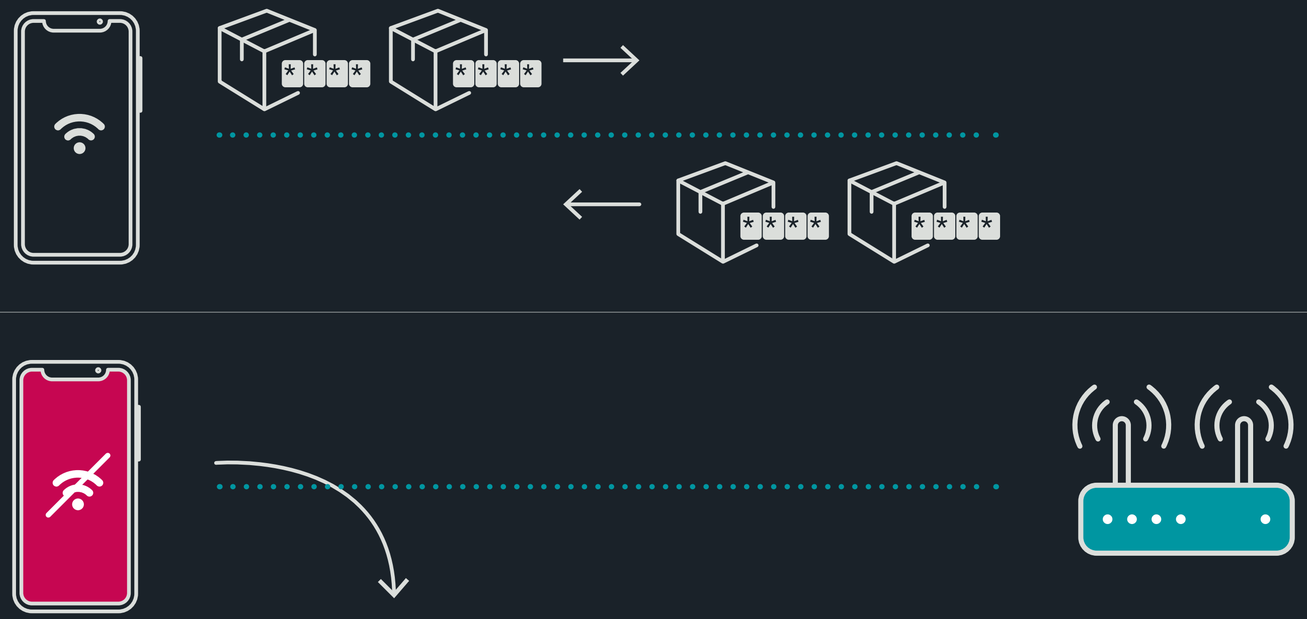
KrØØk は、アソシエーション解除後に現れます。ステーションの WLAN セッションの関連付けが解除されると、ワイヤレスネットワークインターフェイスコントローラー（WNIC）の Wi-Fi チップに保存されているセッションキー（TK）がメモリから消去され、ゼロに設定されます。アソシエーション解除後にデータが送信されることはないため、これは設計上、予想される動作です。ただし、チップの TX（送信）バッファーに残されたすべてのデータフレームは、すべてゼロのキーで暗号化された後に送信されていました。

その結果、攻撃者はパッチが適用されていないデバイスの、暗号化されたワイヤレスネットワークトラフィックに侵入することが可能になります。

幸い、このバグによる影響を制限するいくつかの要素があります。

最初に、この脆弱性は、無線 LAN（Wi-Fi）レイヤーの暗号化に関するものであり、オンラインバンキング、電子メール、および HTTPS で始まる Web サイトを保護している暗号規格：TLS には通用しません。つまり、KrØØk を利用した攻撃を成功させたい場合、Wi-Fi オープンネットワークにおける通信を狙う必要があります。

次に、この脆弱性は Wi-Fi に関連していることから、Wi-Fi 信号の近くにいなければ攻撃を実行することはできません。ただし、Wi-Fi のパスワードを知らなくても攻撃は可能です。



コンセプト概念図：KrØØk によってすべてゼロのキーで暗号化された後に送信される

ESET Research Lab からの最新情報

世界各国にある ESET Research Labs の
最新調査結果

クリプトマイニング

クリプトマイニング（暗号通貨採掘）を行う Stantinko ボットネット

ESET の研究者は、50 万台の強力な Stantinko ボットネット [8] を操るサイバー犯罪者が 2012 年以降活動しており、主にロシア、ウクライナ、ベラルーシ、カザフスタンのユーザーを標的に、乗っ取ったコンピュータに対し、仮想通貨モネロ（Monero）を採掘するモジュールを拡散していることを突き止めました。*Stantinko ボットネット* [8] は、それ以前にはクリック詐欺、広告の挿入、ソーシャルネットワーク詐欺、パスワードの盗み出しの攻撃を行っていました。

セキュリティブログ記事 [9]

独自の難読化技術を実装する Stantinko の新しいクリプトマイナー

ESET の研究者は、Stantinko の新しいクリプトマイニングモジュールを調査した結果、検出と分析を防止するためのいくつかの難読化手法を発見しました。ESET の研究者は、サイバーセキュリティ業界全体が、高度な脅威に対する保護機能を強化できるように、これらの手法を解き明かし、難読化手法のいくつかを解除するためのアプローチ、特に文字列の難読化と制御フローの難読化について詳しく調査し説明しています。

セキュリティブログ記事 [10]

バンキングマルウェア

ラテンアメリカの金融機関を標的とする Guildma

ESET の研究者は、ブラジルの金融機関を標的とするトロイの木馬（バンキングトロイ）である Guildma を分析しました。Guildma は広く拡散しており、新しい実行方法と高度な攻撃手法により、ブラジルで深刻な影響を及ぼしています。

Guildma は、金融機関を標的とすることに加えて、電子メールアカウント、オンラインショップ、ストリーミングサービスの認証情報も盗み出します。ラテンアメリカで多く見られる他のバンキングトロイと同様に、Guildma は多数のバックドア機能を実装し、正規のツールを悪用します。また、その機能が多くのモジュールに分割されています。このマルウェアは、悪意のあるファイルが添付されたスパムメールにより拡散しており、ESET の分析では、他のラテンアメリカのバンキングトロイと比較して被害は少なくとも 10 倍になっています。

セキュリティブログ記事 [11]

APT グループの動向

ESET の調査で明らかになった APT（持続的標的型攻撃）グループとその攻撃

Winnti Group

Winnti Group は、少なくとも 2012 年から活動していますが、ビデオゲームおよびソフトウェア業界に大規模なサプライチェーン攻撃を仕掛けています。また、また、ヘルスケアおよび教育業界のさまざまな標的を攻撃していることも分かっています。

Winnti Group、香港の大学を標的に

Winnti Group が香港の 2 つの大学に対して攻撃を実行したことを ESET が発見しました。今回、ESET の研究者は、ShadowPad バックドアの新しい亜種を検出しました。ShadowPad は、Winnti Group が主要な攻撃ツールとして使用しているバックドアです。新しいこの亜種は、新しいランチャーを使用して展開され、多くのモジュールを埋め込みます。Winnti マルウェアも、ShadowPad バックドアが検出される数週間前にこれらの大学で検出されました。

香港の大学を中心に、香港全体で市民による抗議活動が激化する中で、この攻撃が実行されました。

ESET は、2 つの大学についてこの攻撃が実行されセキュリティが侵害されたことが確認していますが、さらに 3 つ以上の大学がこの攻撃の影響を受けた兆候も確認しています。攻撃者は、被害者のマシンから情報を盗むことを目的としていました。

ESET は、攻撃を大学に連絡し、必要な情報とセキュリティ侵害を修復するために支援を行いました。

2019 年 11 月に、これらの大学で見つかった ShadowPad と Winnti の両方には、これらの大学名を含む攻撃 ID と C&C の URL が含まれていることから、標的型攻撃であることが分かります。

ESET マルウェアリサーチャー、Mathieu Tartare

ESET の研究者は、最近、アジアのビデオゲーム業界を標的にしたサプライチェーン攻撃について説明したブログ [13] に続いて、Winnti Group が使用している攻撃ツールに関する最新情報を説明したホワイトペーパー [12] を公開しました。さらに、Microsoft SQL Server をターゲットとする skip-2.0 という名前の新しいバックドアに関するブログ [14] も公開しています。

セキュリティブログ記事 [15]

Turla

Turla（別名：Snake）は、複雑なマルウェアを使用することで知られる悪名高いスパイグループです。Turla の活動は、少なくとも米軍のコンピュータに侵入した 2008 年から続いていると考えられています。

水飲み場型攻撃で悪用されるアルメニアの Web サイトから配信される新たなバックドア Turla

ESET の研究者は、いくつかの有名なアルメニアの Web サイトを標的とした水飲み場型攻撃を発見しました。この攻撃は、偽の Adobe Flash アップデートを使用するソーシャルエンジアリングの手法でユーザーを騙して、これまで検出されていなかった 2 つのマルウェアを配信します。ESET では、これらの 2 つのマルウェアを NetFlash および PyFlash と命名しました。

Turla は、この攻撃で政府機関に属する 2 つの Web サイトを含む少なくとも 4 つのアルメニアの Web サイトを乗っ取っています。このことから、標的には政府関係者や政治家が含まれていることが考えられます。ESET は、一般に情報を公開する前に、アルメニアの CERT にこの問題を通知し、分析結果を伝えています。

ESET のテレメトリ（監視チームデータ）から、次の Web サイトが乗っ取られていることが判明しました。

- armconsul[.]ru：ロシアのアルメニア大使館の領事局
- mnp.nkr[.]am：アルツァフ共和国自然保護天然資源省
- aiisa[.]am：アルメニア外交政策および安全保障問題研究所
- adgf[.]am：アルメニア預金保険基金

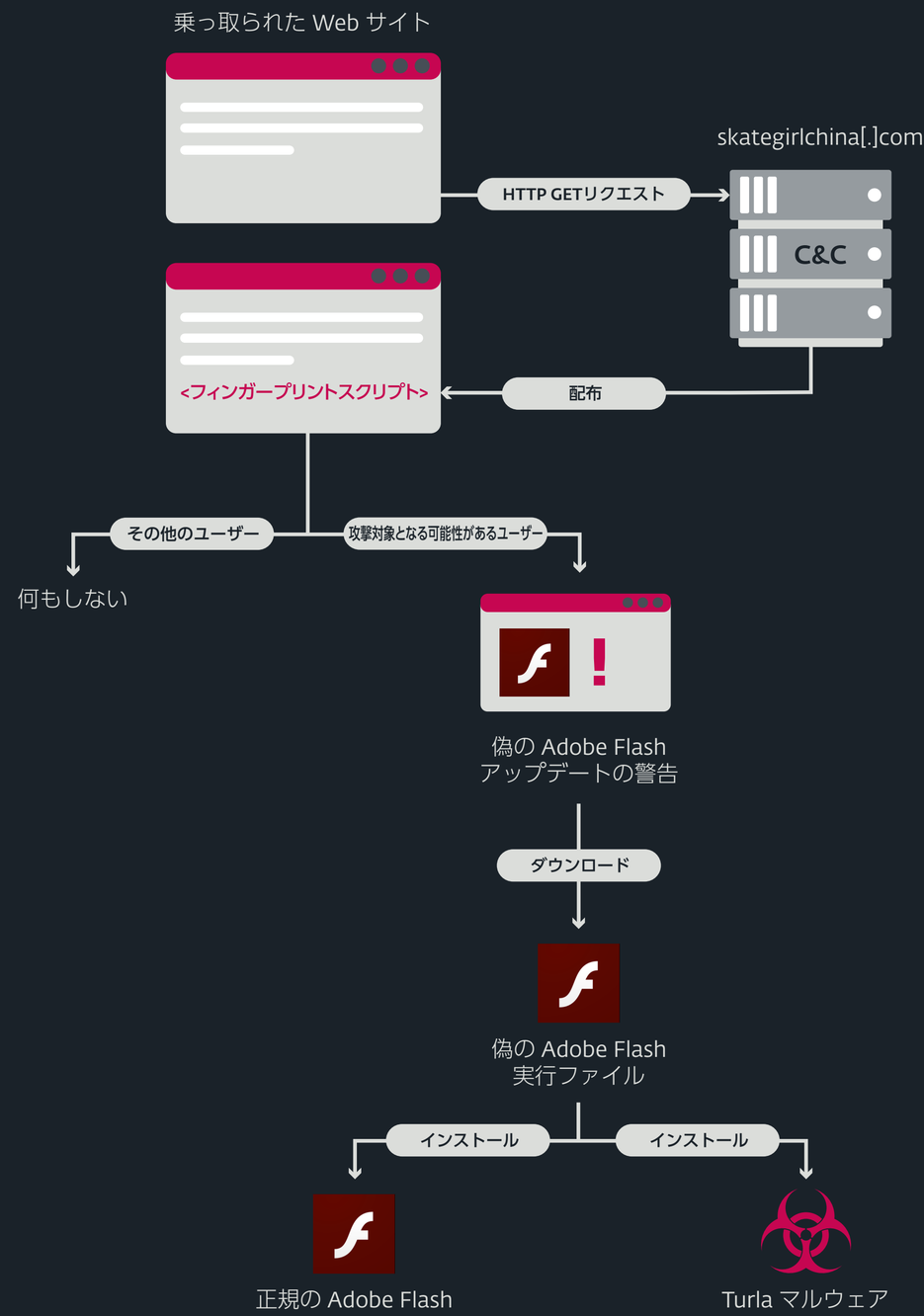
Web サイトにアクセスしたユーザーが重要な標的であれば、サーバーから偽の Adobe Flash のアップデート画面を表示する JavaScript コードが送られます。ESET テレメトリのデータは、この攻撃は、ごく一部のユーザーだけが Turla のオペレータによって重要な標的と見なされたことを示しています。

ESET マルウェアリサーチャー、Matthieu Faou

重要な標的であれば、偽の Adobe Flash 更新ポップアップウィンドウの警告が表示され、悪意のある Flash インストーラーをダウンロードするように誘導されます。悪意のある実行ファイルがダウンロードされ、ユーザーが手動で実行すると、Turla マルウェアの亜種と正規の Adobe Flash プログラムがインストールされます。

右側のスキームは、初期のセキュリティ侵害プロセスの概要を示しています。

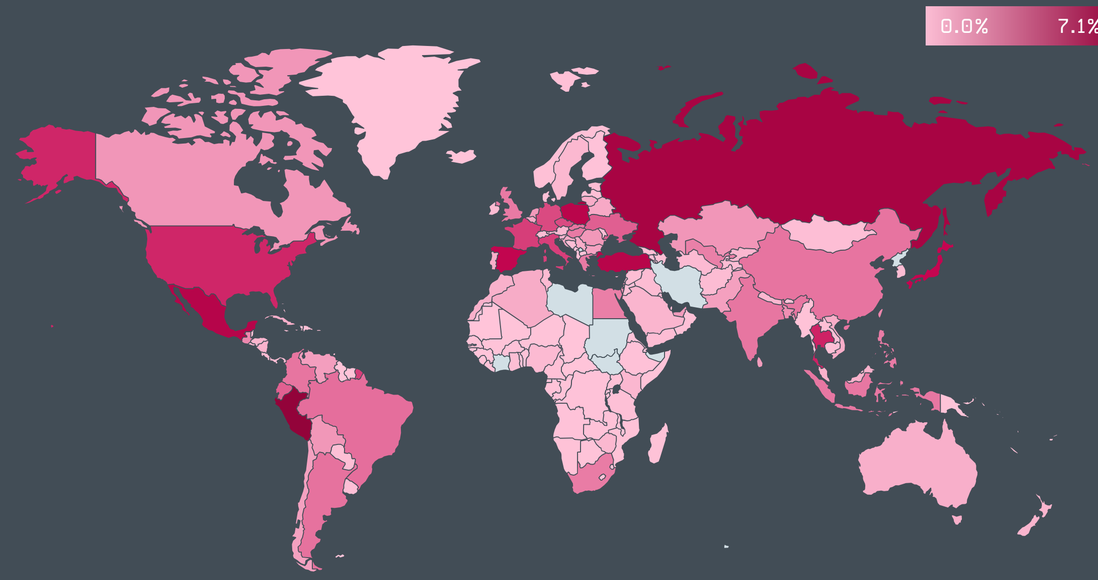
セキュリティブログ記事 [16]



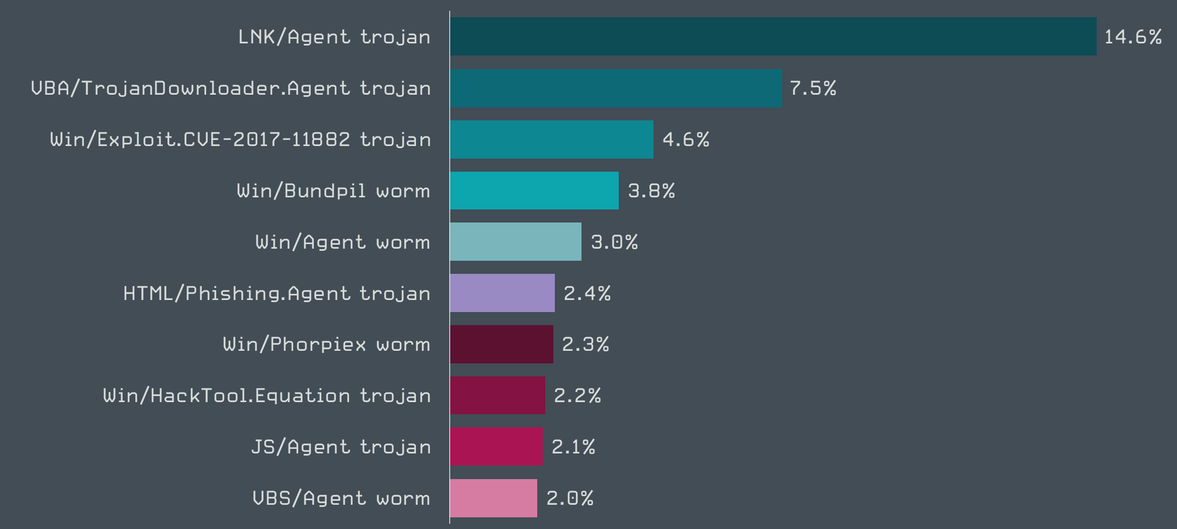
水飲み場攻撃の概要

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 1 四半期の脅威状況



2020 年第 1 四半期のマルウェア検出率



2020 年第 1 四半期に検出されたマルウェアトップ 10（% はマルウェア検出率）

検出されたマルウェアトップ 10

LNK/Agent トロイの木馬 2019 年 Q4：1 位↔ 2020 年 Q1：1 位

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できるように、セキュリティを侵害する方法として頻繁に使用されます。

VBA/TrojanDownloader.Agent トロイの木馬、2019 年 Q4：2 位↔ 2020 年 Q1：2 位

VBA/TrojanDownloader.Agent の検出名は、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。

Win/Exploit.CVE-2017-11882 トロイの木馬、2019 年 Q4：4 位↑ 2020 年 Q1：3 位

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*** [17] 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。

日本における VBA/TrojanDownloader.Agent 及び Win/Exploit.CVE-2017-11882 の攻撃はグローバルの傾向と同じくして多大な数を観測しています。

イーセットジャパン　テクノロジー＆セキュリティエバンジェリスト、中川菊徳

Win/Bundpil ワーム、2019 年 Q4：3 位↓ 2020 年 Q1：4 位

Win32/Bundpil は、リムーバブルメディアを介して拡散するワームです。これは、最大級のボットネットのひとつである Wauchos の一部であり、***Gamarue*** [18] または Andromeda としても知られています。Bundpil は、Wauchos の常駐化を支援し、ネットワークでグローバルに削除できないようにするために設計されました。ドメイン生成アルゴリズムが含まれており、DNS 要求を変更できます。

Win/Agent ワーム、2019 年 Q4：5 位↔ 2020 年 Q1：5 位

この検出名は、自己複製が可能なさまざまな悪意のある実行ファイルに使用されます。これらの実行ファイルに共通する特徴は、すべての利用可能なドライブに拡散し、常駐化する能力です。ユーザーを騙してこれらの悪意のあるファイルを実行させるために、システムで検出された無害なフォルダやファイルを偽装するように、ファイル名が変更されることがあります。また、通常、C&C サーバーとの通信、追加ファイルのダウンロードと実行、キーロギングなどの基本的なバックドア機能も含まれています。

HTML/Phishing.Agent トロイの木馬、2019 年 Q4：35 位↑ 2020 年 Q1：6 位

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。通常、実行ファイル形式の添付ファイルは自動的にブロックされるか、ユーザーが警戒するため、攻撃者は実行ファイルなどの代わりに HTML コードを使用する傾向があります。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。

Win/Phorpiex ワーム、2019 年 Q4：6 位↓ 2020 年 Q1：7 位

Win/Phorpiex は、主に他のマルウェアのダウンロード、スパムの配信、DDoS 攻撃の実行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、ユーザーをだましてダウンロードおよび実行させるために、Web または FTP サーバーフォルダーに保存されている正規のファイルを自分自身のコピーと置換します。このワームは、IRC チャネルを介して通信します。

Win/HackTool.Equation トロイの木馬、2019 年 Q4：7 位↓ 2020 年 Q1：8 位

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、漏えい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。

JS/Agent トロイの木馬、2019 年 Q4：16 位↑ 2020 年 Q1：9 位

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。

VBS/Agent ワーム、2019 年 Q4：8 位↓ 2020 年 Q1：10 位

VBS/Agent の検出名は、多くの場合リムーバブルドライブを介し、さまざまな常駐化手法を使用して、あるシステムから別のシステムに拡散する悪意のある Visual Basic スクリプト（VBS）に使用されます。これらのスクリプトの目的は、セキュリティを侵害したシステムの情報を収集し、それをリモートマシンに送信し、通常はさらに複雑な他のマルウェアをダウンロードして実行することです。

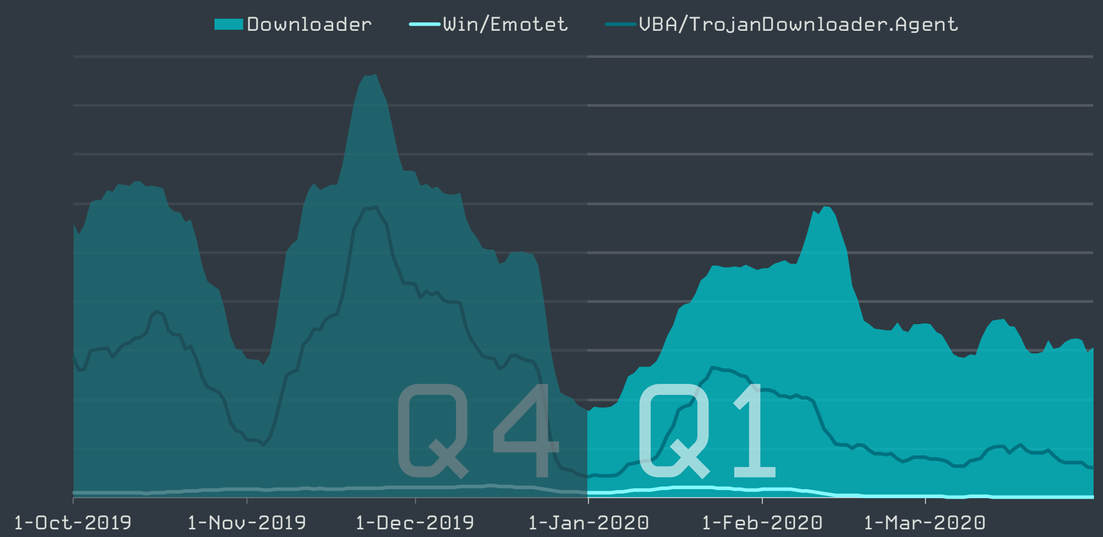
ダウンローダー

2020 年の第 1 四半期は、ダウンローダーの活動は低調であったものの、悪名高いトロイの木馬である Emotet とその拡散のメカニズムが更新されており、注意が必要となっています。

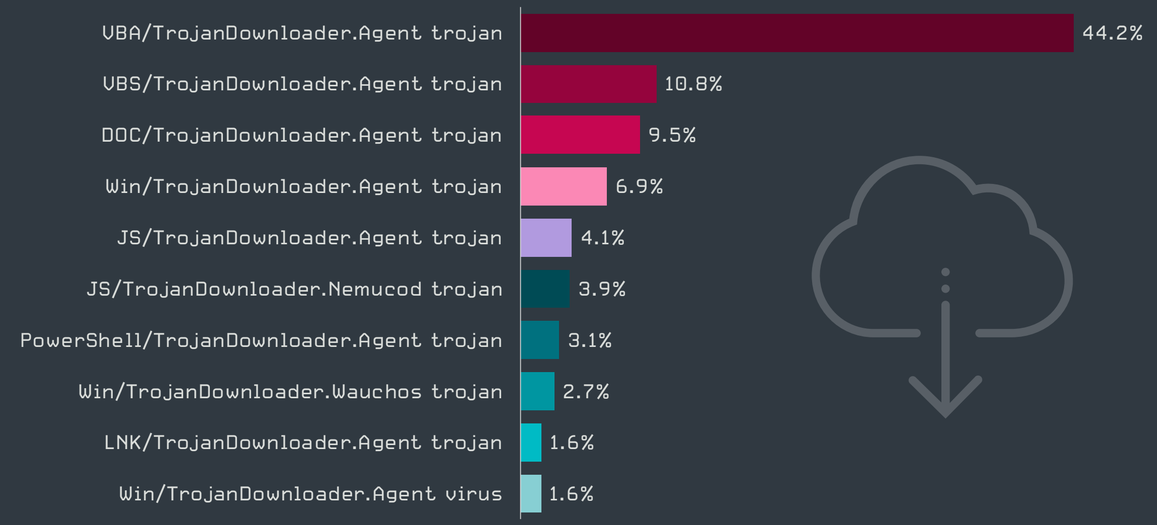
2020 年第1四半期のダウンローダーファミリーは、2019 年第 4 四半期と比べて、かなり勢いを失っており、全体数では 35% 以上減少しました。ESET のテレメトリでは、年末に最も大きな低下が見られます。これは、これまで攻撃が増加するクリスマスシーズンから、攻撃数が減少する傾向にある年初に移行したという理由で説明できます。***Emotet の攻撃が「一時期停止したこと」*** [19] もこの急落の一因となった可能性があります。VBA/TrojanDownloader.Agent は Emotet と連携していることが多いことには注意が必要です。

2020 年第 1 四半期の最大の急上昇は、2 月 10 日頃に観測されました。これは、西半球における新型コロナウイルスの発生状況によって説明できます。マルウェアを操る攻撃者は、スペイン、ポルトガル、チェコ共和国、台湾、ドイツの順番で、主にヨーロッパの国々を標的に、市民の間で高まる新型コロナウイルスに対する緊張と恐れに便乗し、悪意のある添付ファイルを拡散しました。

ダウンローダーファミリーのレベルでは、VBA/TrojanDownloader.Agent が第 4 四半期から最も多く検出されています。その検出数は、2 番目に検出数の多い VBS/TrojanDownloader.Agent の 4 倍でした。VBA/TrojanDownloader.Agent はスパム攻撃で配信されており、主に悪意のある Microsoft Office ファイルを介して拡散します。これらのマクロが有効にされているドキュメントを開くと、通常、PowerShell を使用して、ハッキングされた Web サイトから Win/Emotet バイナリがダウンロードされます。



2019 年第 4 四半期から 2020 年第 1 四半期のダウンローダーの検出傾向、7 日間の移動平均線



2020 年第 1 四半期のダウンローダーファミリートップ 10（% はダウンローダー検出率）

2020 年第 1 四半期の Win/Emotet の傾向は特に注目に値します。研究者は、***ワームモジュールを使用する検体を特定しています*** [20]。この検体はセキュリティで保護されていない近隣の Wi-Fi ネットワークに拡散し、Wi-Fi に接続しているユーザーに感染します。2018 年 4 月に ESET 製品はこの Wi-Fi モジュールを検出していますが、ESET のテレメトリでは非常に限られた数しか検出されていません。

> ***この Wi-Fi モジュールの普及率が低いことは、Emotet を悪用しているサイバー犯罪者が、このモジュールを隠そうとしており、おそらく標的型攻撃を実行するためにその利用を控えている可能性があります。***
>
> **ESET マルウェアアナリスト、Zoltán Rusnák**

この Wi-Fi ワームモジュールは、2020 年 2 月上旬に大きく更新されました。2018 年の元のバージョンは、Emotet バイナリと、近隣の Wi-Fi ネットワークにブルートフォースアクセスを試行しネットワーク共有にアクセスするように設計された別の悪意のあるバイナリが含まれる自己解凍型のアーカイブでした。この Emotet の Wi-Fi 感染拡大機能が更新され、ブルートフォース攻撃の後に別のステップを追加し、遠隔の C&C サーバーから第 2 ステージのマルウェアをダウンロードし、Emotet バイナリ自体をダウンロードしてデバイスで実行し、より柔軟に更新できるようになっています。

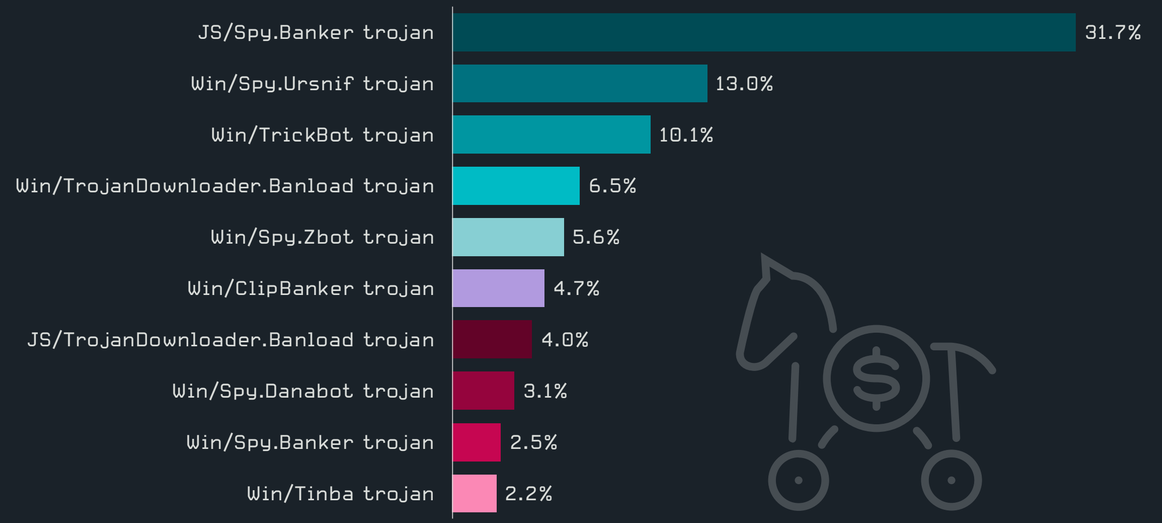
バンキングマルウェア（銀行を標的とするマルウェア）

ESET のテレメトリ（監視チームデータ）によると、2020 年第 1 四半期にバンキングマルウェアの検出はわずかに増加していますが、その中でも、Win/Spy.Ursnif が 2019 年第 4 四半期と比較して最大の増加を示しました。

グローバルなバンキングマルウェアは、2019 年 12 月に検出数が大幅に落ち込みましたが、2020 年第 1 四半期の検出数はわずかに増加傾向に転じました。JS/Spy.Banker は、検出されたすべてのバンキングマルウェアの 3 分の 1 以上を占めており、このカテゴリで最も多く検出されています。この検出名は、ユーザーのブラウザから銀行取引やクレジットカードの機密情報を盗むために使用されるさまざまな悪意のあるスクリプトに使用されます。

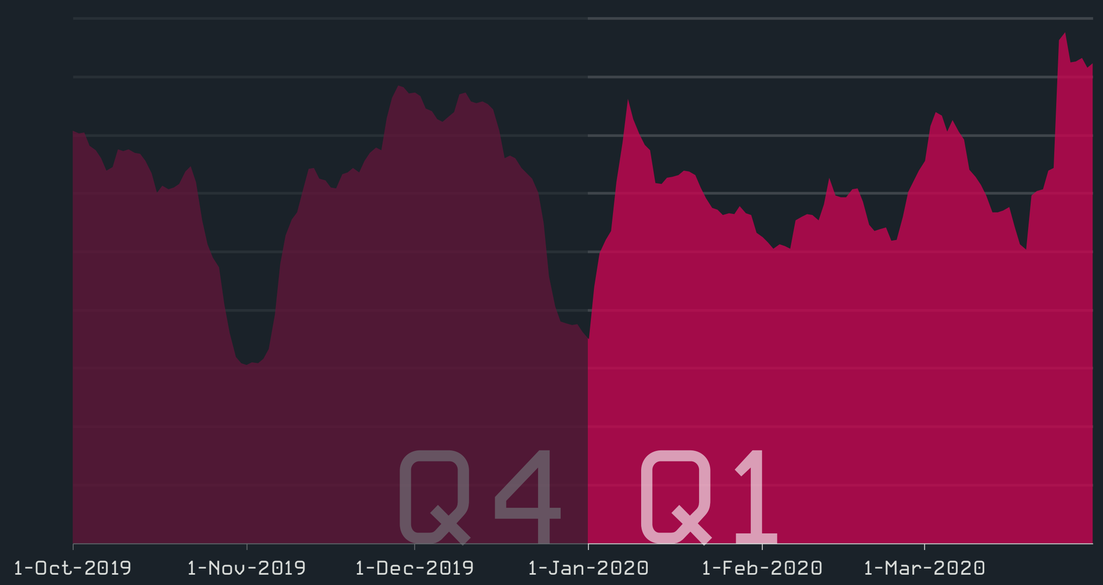
2019 年第 4 四半期と 2020 年第 1 四半期を比較した場合、最も大きな変化が見られたバンキングマルウェアは、Win/Spy.Ursnif であり最も拡散していました。2019 年第 4 四半期には検出率は 5.9% でしたが、2020 年第 1 四半期には 13% に大幅に増加しています。

日本においてもバンキングマルウェアの流通を確認しており、その半数を Ursnif が占めました。アタックベクターについては、グローバルでの配布方法と同類で添付ファイルを偽装する手法が主に使われていました。　**イーセットジャパン　テクノロジー&セキュリティエバンジェリスト、中川菊徳**



2020 年第 1 四半期のバンキングマルウェアトップ 10（% はバンキングマルウェア検出率）

Ursnif は、Gozi マルウェアの亜種としても知られています。Ursnif は、大規模な組織を標的に現在も非常に多く悪用されているバンキングトロイであり、主に認証情報とデータの盗み出しを実行します。



2019 年第 4 四半期から 2020 年第 1 四半期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

Ursnif は、悪意のあるリンクや添付ファイルのある電子メールやエクスプロイトキットを介して拡散します。2020 年第 1 四半期に検出が増加したのは、今年の初めに、悪意のあるファイルが添付されたスパムが急増したことに関連しています。これらのスパムメッセージは 2020 年の法改正に関する内容であると謳っており、実行可能な添付ファイルが PPT や PDF ファイルに偽装されていました。

ESET が特定したラテンアメリカのバンキングトロイには、多くの共通点が見られます。Delphi で記述されており、バックドア機能を実装し、通常、非常に長い実行チェーンを介して配信されます。銀行取引関連の情報を盗むために、通常、ソーシャルエンジニアリングと偽のポップアップウィンドウを組み合わせて使用します。他のバンキングトロイで一般的に使用される Web インジェクションは使用されません。　**ESET マルウェアアナリスト、Jakub Souček**

最も一般的なバンキングマルウェアの系統の他に、特に注意が必要なのは、ラテンアメリカを標的とするバンキングトロイです。ESET の研究者がこれらの脅威を調査したところ、多くの共通の特性があり相互に関連している 10 以上のマルウェア系統を特定しました。2020 年第 1 四半期に、ESET は、ブラジルを標的としたバンキングトロイである ***Guildma*** [11] の分析結果を発表しました。

これらの共通するラテンアメリカのバンキングトロイを組み合わせると、2020 年第 1 四半期に検出されたバンキングマルウェアの 7% 以上を占めており、Win/Spy.Mekotio、Win/Spy.Amavaldo、Win/Spy.Grandoreiro が最も多く検出されています。

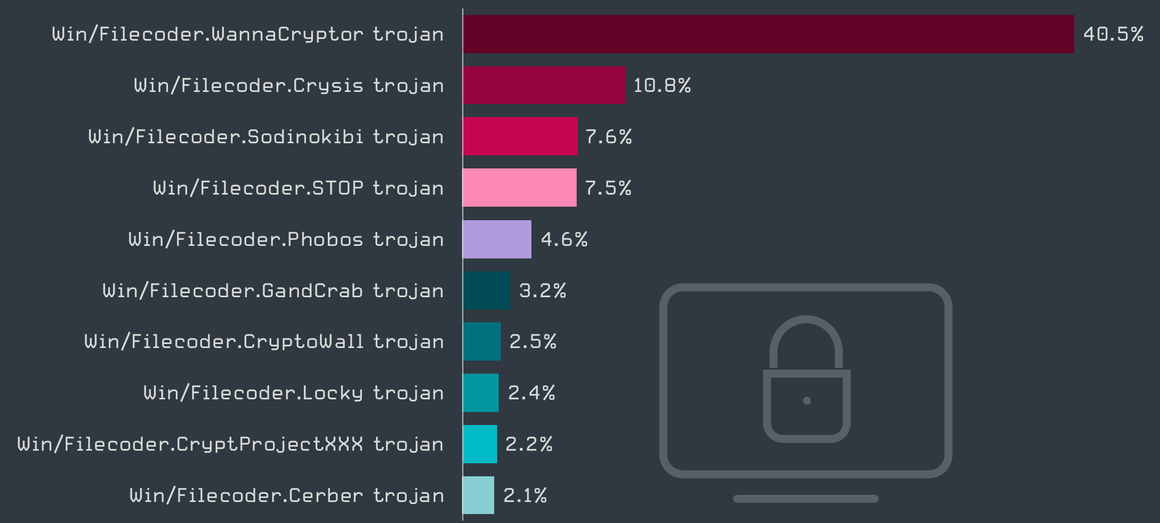
ランサムウェア

ランサムウェアを運用しているサイバー犯罪者（オペレータ）は、新しい戦略として攻撃のためにユーザーの個人情報を Web に公開する「晒し」を行うようになりましたが、新型コロナウイルスの世界的な流行が続いている間は、医療関係機関への攻撃を控えると宣言している組織もいます。

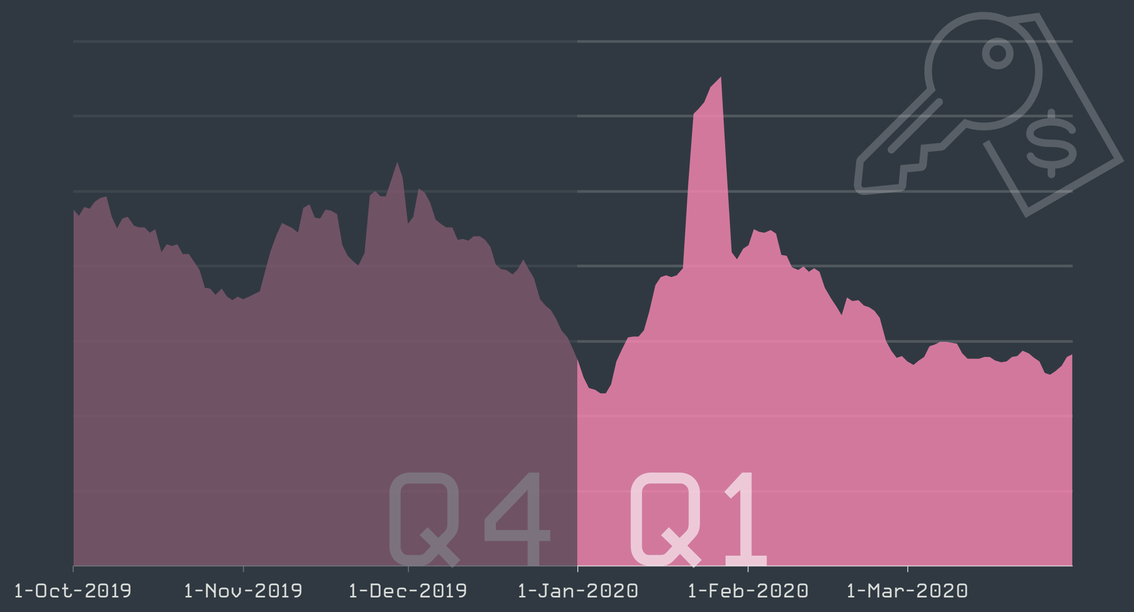
ESET による検出結果では、2020 年第 1 四半期におけるランサムウェアの活動は全体的に減少しています。ランサムウェアの活動は年末の後は低調なスタートでしたが、2020 年 1 月に最も多くの活動が確認されています。

ESET のテレメトリ（監視チームデータ）によると、1 月に検出が上昇した理由は 2 つの大規模なキャンペーンです。1 つは Crysis ファミリのキャンペーン（1 月のすべての Filecoder[1] 検出の 12.9%）、もう 1 つは Sodinokibi ファミリによる南アフリカのユーザーを標的としたキャンペーン（1 月のすべての Filecoder 検出の 13.4%）です。後者のマルウェア系統は親プロセスとして powershell.exe を使用します。これは、Sodinokibi のオペレータが PowerShell を使用して悪意のある電子メールの添付ファイルを介してペイロードを配信し、ランサムウェアを実行していることを示しています。

WannaCryptor は、2017 年 5 月に発生し、検出数がピークに達してからほぼ 3 年経過しているにもかかわらず、2020 年の第 1 四半期を通じて検出されたランサムウェアのトップに立っています。第 1 四半期に検出された WannaCryptor のほとんどは、トルコ、タイ、インドネシアなどの修正パッチが適用されていないデバイスが多い地域で検出されており、既知の検体が拡散されたことが原因になっています。



2020 年第 1 四半期のランサムウェアファミリートップ 10（% はランサムウェア検出率）



2019 年第 4 四半期から 2020 年第 1 四半期のランサムウェアの検出傾向、7 日間の移動平均線

ESET のテレメトリ（監視チームデータ）から、GandCrab の古い亜種の検出についても同様の状況になっていることがわかります。GandCrab の一部は、2018 年までさかのぼりますが、第 1 四半期のキャンペーンを実行しているオペレータは、電子メールを使用して、GandCrab の亜種を主にドイツ、日本、イタリアのユーザーに拡散しています。

音楽のヒットチャートと同じように、上位のランキングは大きく変動します。さまざまなファミリの検出率が大きく上下に変動しています。WannaCryptor が最も多く検出されていますが、その後に、Crysis、Sodinokibi、STOP、Phobos ファミリが続きます。これらランサムウェアの順位は常に入れ替わっています。2020 年 2 月にもトップ 10 に初めて Nemty がランクインしました。Nemty が実環境で最初に検出されたのは、2019 年 8 月です。しかし、Nemty は翌月すぐに Cerber に置き換えられました。

3 月の終わりには、DeathRansom オペレータによる特異な活動が確認されました。GandCrab ランサムウェアの古いバージョン（5.1）の動作を模倣し始めたのです。この変化における最も顕著な特徴は、GandCrab の身代金メモを使用していることです。異なるのは、TOR リンクに「gandcrab」という文字列が含まれないことです。元のサイバー犯罪者の「証拠」が、現在の DeathRansom ページに存在しておらず、さらに、DeathRansom のランディングページは、GandCrab で使用されていたページとは異なります。

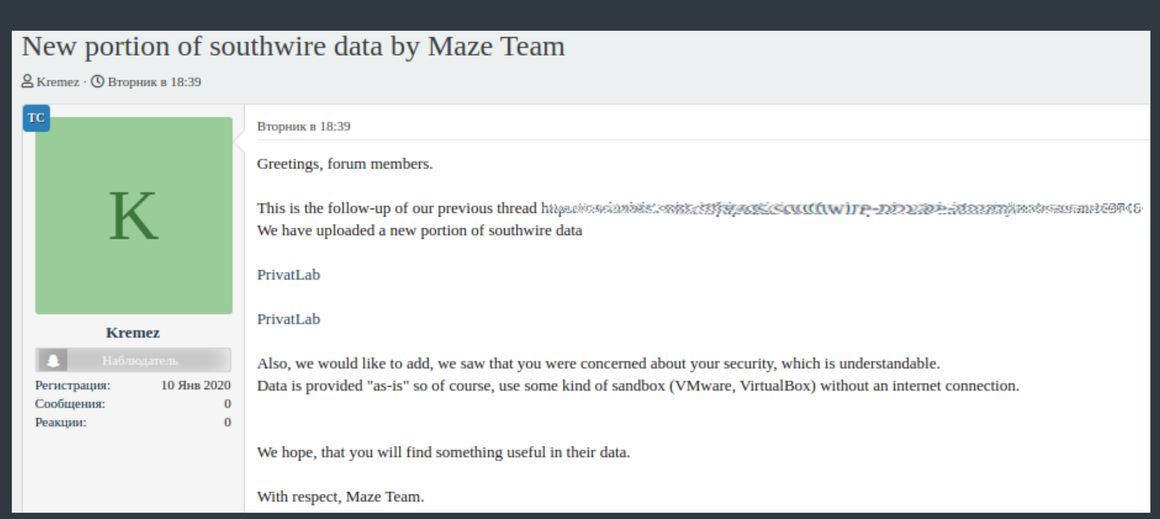
[1] ESET は、攻撃の標的がファイルまたはディスクボリュームかどうかに応じて、ランサムウェアを Filecoder および Diskcoder カテゴリに分類します。

2019 年の第 4 四半期の終わりにかけて重要な新しい傾向が出現しました。身代金が支払われない限り、ランサムウェアのオペレータは、ユーザーの機密データを盗み出し、公開すると脅迫したのです。この手法（「晒し」または「ドキシング」とも呼ばれます）は、ユーザーデータの暗号化とは別に行われます。

機密データがオンラインに漏洩した場合に、業務の停滞、経済的損失、評判へ失墜、当局への報告や罰金（GDPR または他の法律による）、競争力の低下など、さまざまな問題に対処しなければならなくなることから、攻撃者はこの手法によって被害者に金銭を支払うように強い圧力を掛けています。

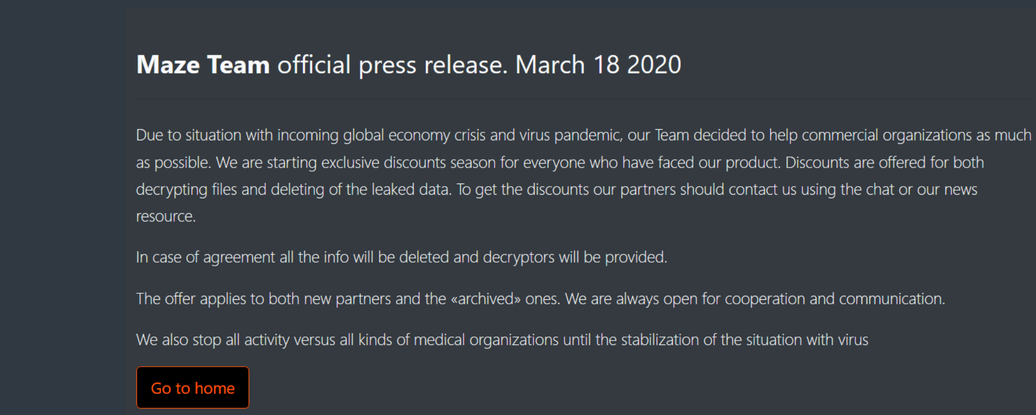
「晒し」は当初、Maze ランサムウェアのオペレータによって使用されていました。しかし、他のランサムウェアオペレータも、その有効性に気が付き、2020 年第 1 四半期から追随するようになりました。DoppelPaymer、Sodinokibi、RobinHood、Nemty などのランサムウェアも晒しを採用していることから、注意が必要です。

Maze による晒しの最初の被害を受けたのは、米国の電線およびケーブル製造業者の Southwire 社です。Maze のオペレータは 120 GB のデータを盗み、約 900 台のデバイスを暗号化し、以前の状態に復元するために 600 万ドルを要求しました。Southwire が支払いを拒否すると、Maze はデータをオンラインに投稿し始めました。Southwire 社は、漏えいしたデータをホスティングしているプロバイダに対して予防措置を求め、法的な措置を講じています。



Maze オペレータによるロシアのハッキングフォーラムへの投稿（画像の出典：BleepingComputer.com [21]）

2020 年第 1 四半期に重要な転機となったのは、西欧諸国における新型コロナウイルス（COVID-19）の感染拡大です。一部のランサムウェアファミリのオペレータ（Maze や DoppelPaymer など）は、感染症流行の影響を悪化させないために、*保健機関や医療機関を攻撃対象にしないとする声明を発表しました* [22] 。ただし、Ryuk など一部のランサムウェアファミリは通常どおり攻撃を続けています。



新型コロナウイルスのパンデミックを受けた Maze オペレータによる「プレスリリース」（画像の出典：@CryptoInsane [23]）

> ***一部のランサムウェアオペレータは、医療機関を攻撃しないことを決定しましたが、他の標的への攻撃を停止しているわけではありません。2020 年の第 1 四半期にもこれらのオペレータによる攻撃例がかなり数に上っています。***
>
> **ESET シニア検出エンジニア、Igor Kabina**

2020 年 *2 月中旬の US-CERT のアラート* [24] で、注意するべきランサムウェア関連の事例が説明されました。天然ガスの圧縮施設を標的にしたこのサイバー攻撃では、スピアフィッシングのリンクが使用され IT ネットワークに最初にアクセスされ、そこから運用・制御技術（OT）ネットワークにアクセスされました。その後、両方のネットワークがランサムウェアに感染しました。このインシデントにより、生産性と収益が低下しましたが、業務の運用が中断することにはなりませんでした。US-CERT は、被害を受けた企業が IT ネットワークと OT ネットワークの間に堅牢なセグメンテーションを実装していれば、このインシデントは阻止できた可能性があると述べています。

2020 年第 1 四半期は、ランサムウェアオペレータの収益が一部解明されました。*RSA 2020 Conference の FBI 特別捜査官 Joel DeCapua 氏による講演* [25] によると、暗号化のランサムウェアである Filecoder を使用している攻撃者は、過去 6 年間に少なくとも 1 億 4,000 万ドルを稼ぎ出しています。少なくともこの金額は、身代金メモに記載されていたビットコインウォレットで確認された入金の合計です。これらのほぼすべての金額は、Ryuk（6,100 万ドル以上）と Crysis/Dharma（約 2,450 万ドル）のウォレットに送金されています。

DeCapua 氏はまた、圧倒的な数の事例で、RDP が業務を危険にさらすために使用されている主要な攻撃方法であることを重ねて述べています。FBI のデータによると、ランサムウェア攻撃の最大 80% は、RDP の資格情報にブルートフォース攻撃を仕掛けてネットワークに侵入して成功しています。DeCapua の講演は *YouTube* [26] で視聴できます。

クリプトマイナー

2020 年第 1 四半期に観測された最も注目するべきクリプトマイニングの傾向は、その活動が継続的に減少していることです。クリプトマイナーは、望ましくない可能性があるアプリケーション（PUA）として分類されており、その活動は最も大きく後退しています。

ESET のセキュリティ製品は、望ましくない可能性があるアプリケーション（PUA）またはトロイの木馬としてクリプトマイナーを検出します。トロイの木馬として検出されるクリプトマイナーは、ユーザーの同意なしに、あるいはユーザーに気が付かれることなく暗号通貨を採掘（マイニング）するように構成されたものです。クリプトマイナーのトロイの木馬と PUA の比率は、2019 年第 4 四半期には 52 対 48 でしたが、PUA が減少したことで、2020 年第 1 四半期の比率は 60 対 40 に増加しました。

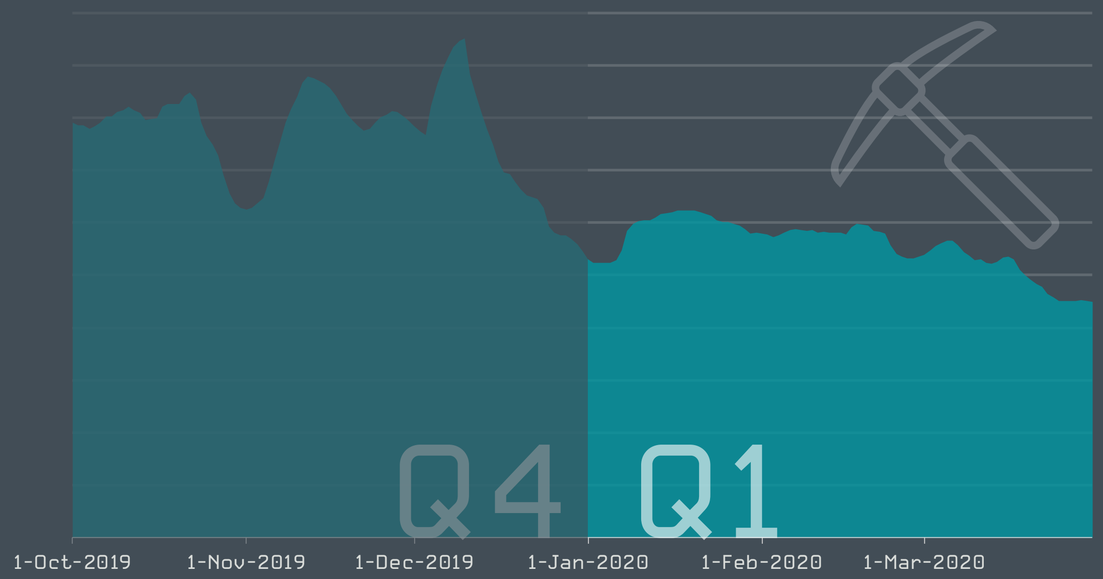
下のグラフに示すように、悪意のあるクリプトマイナーの全世界における検出数は徐々にではありますが減少傾向にあります。この傾向は、2019 年の初めから継続しています。

> ***暗号通貨の為替レート下落に伴い、攻撃者の利益も減少しています。結果として、マイニングに必要だったユーザーのデバイスへの興味も減少しています。***
>
> **脅威自動化検出・機械学習部門ヘッド、Juraj Jánošík**

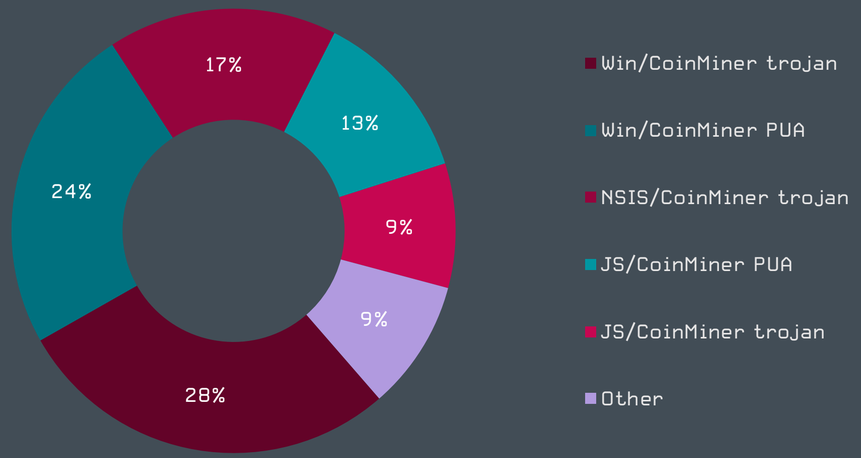
2019 年第 4 四半期および 2020 年第 1 四半期に見られるクリプトマイナーの活動の減少は、ビットコインや他の暗号通貨価格が下落していることに加えて、クリプトマイニングへの対処を目的とした活動「*Operation Goldfish Alpha*」[27] に起因している可能性があります。この活動は国際刑事警察機構（インターポール）が実施しており、ASEAN 地域で 20,000 台以上のハッキングされたルーターを特定しました。これは、クリプトマイニングマルウェアの世界的な感染の 18% を占めると報告されています。インターポールによると、2019 年 11 月下旬までに、感染したデバイスの数は 78% 減少しました。

JS/CoinMiner として検出されるブラウザ内マイニングに使用される悪意のある JavaScript は、2019 年 3 月に発生した*悪名高いマイニングサービス Coinhive* [28] が終焉したあとは、回復していません。JS/CoinMiner は、2019 年第 1 四半期には 30% 程度のシェアでしたが、2020 年第 1 四半期のシェアは 10% をわずかに上回っている程度で、これは 2019 年第 4 四半期と比べてもほぼ変化はありません。

一部のアナリストは、Android のコインマイナー（トロイの木馬と PUA の両方）は増大すると予測していましたが、実際にはそうなっていません。



2019 年第 4 四半期から 2020 年第 1 四半期のクリプトマイナーの検出傾向、7 日間の移動平均線



2020 年第 1 四半期のクリプトマイナー検出トップ 10

スパイウェアとバックドア

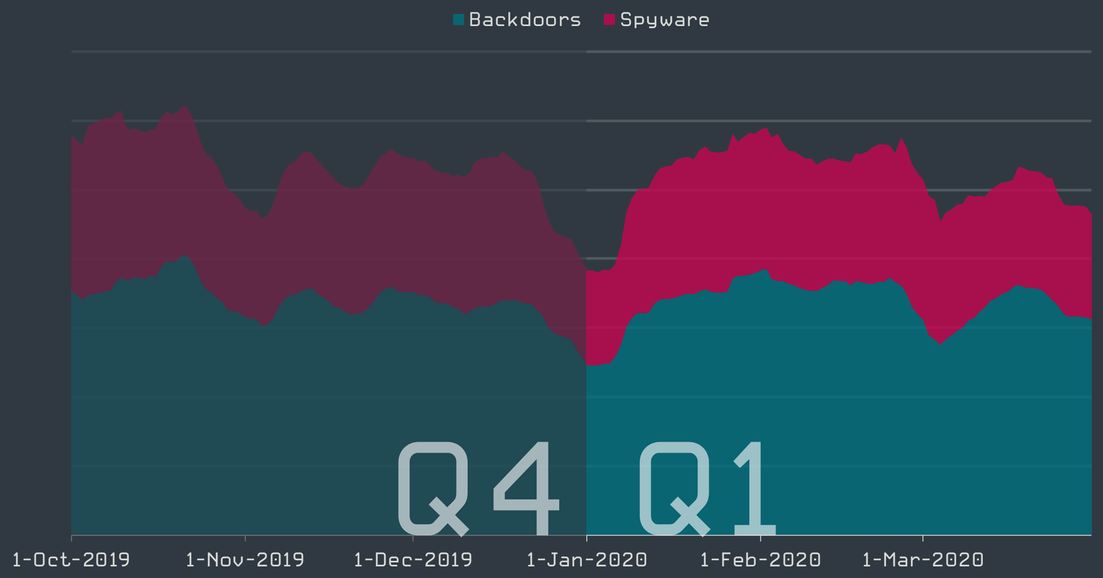
ESET のテレメトリ（監視チームデータ）によると、2020 年第 1 四半期には、スパイウェアとバックドアの検出数に大きな変動は見られず、Win/HoudRat がこのカテゴリでは最も多く検出されています。

例年、年初には検出数が低下する傾向にあります。今年もこの期間を除くと、スパイウェアとバックドアの検出は 2019 年の第 4 四半期と 2020 年の第 1 四半期でほぼ横ばいでした。バックドアは、スパイウェアの約 2 倍検出されています。

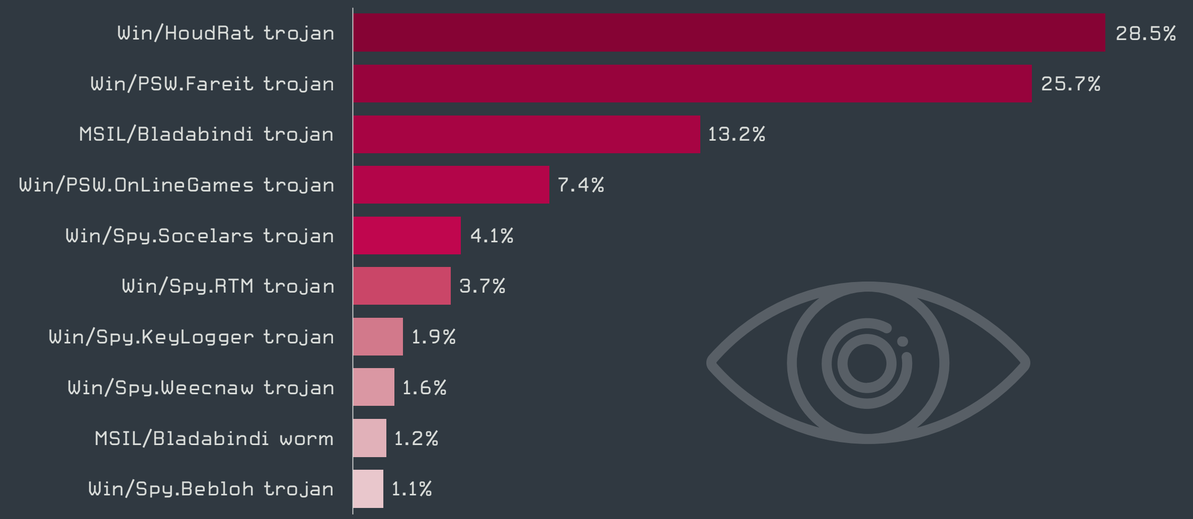
本レポートのスパイウェアのカテゴリは、データの盗み出し、パスワード収集、キーロギング機能を備えたトロイの木馬とワームの検出で構成されます。バックドアは、リモートアクセス型トロイの木馬（RAT）とも呼ばれ、ユーザーの気が付かないうちにコンピュータにリモートからアクセスするアプリケーションとして定義され、別の検出カテゴリとして追跡されています。

2020 年第 1 四半期のスパイウェアのカテゴリで最も多く検出されたマルウェアファミリは Win/HoudRat であり、検出されたすべてのスパイウェアのほぼ 3 分の 1 を占めています。HoudRat は、人気のあるオンラインストア、支払ポータル、および広範に使用されている Web ブラウザから認証情報を盗むために使用される複雑なマルウェアです。自身を拡散するためにリムーバブルメディアを利用します。

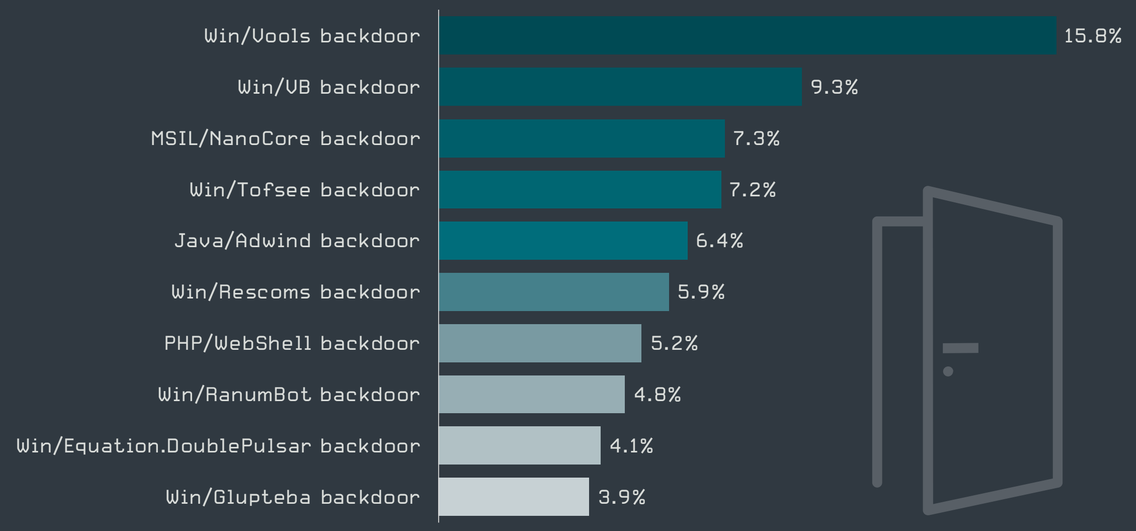
バックドアのランキングでトップになっているのは、Win/Vools であり、検出されたすべてのバックドアの約 16% を占めています。このマルウェアは、Microsoft サーバーメッセージブロック（SMB）の脆弱性を利用して、脆弱なコンピュータに拡散します。侵入に成功すると、Vools はユーザーの機密情報を収集し、リモートサーバーに送信します。



2019 年第 4 四半期から 2020 年第 1 四半期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 1 四半期のスパイウェアファミリートップ 10（% はスパイウェア検出率）



2020 年第 1 四半期のバックドアファミリートップ 10（% はバックドア検出率）

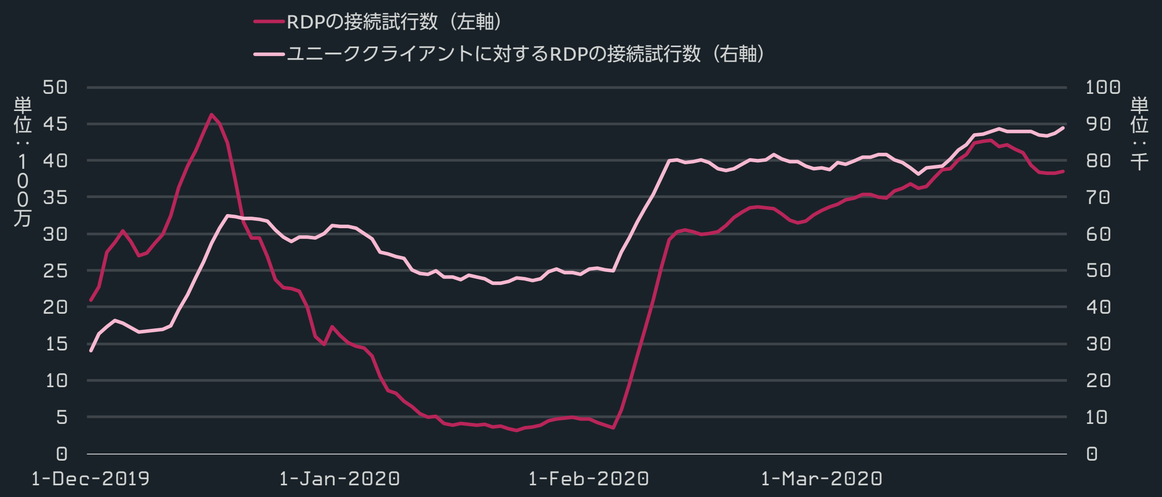
エクスプロイト

テレワークを行うユーザーが増加しており、外部から簡単にアクセスできるネットワークトラフィックが増加している環境はサイバー犯罪者の恰好の攻撃となることから、ネットワークセキュリティに注目が集まっています。

悪名高い EternalBlue エクスプロイトによって試行された攻撃の数は、2020 年第 1 四半期まで減少し続けており、2019 年第 2 四半期に記録した***過去最高の攻撃数*** [29] と比較すると半減しました。EternalBlue エクスプロイトは、これまでで最も厄介なランサムウェアである WannaCryptor（別名 WannaCry）の元凶です。このエクスプロイトが悪用され始めてからほぼ 3 年が経過しているにもかかわらず、EternalBlue は、現在でも毎日、何十万もの攻撃で利用されています。

2020 年第 1 四半期に攻撃試行数が減少した別の脆弱性は ***BlueKeep*** [30] でした。このリモートデスクトップサービスに存在する「ワームとして自己増殖を可能にする」深刻なリモートコード実行の脆弱性は、2019 年 5 月に修正パッチが適用された後に公開されました。初期の頃に、BlueKeep の活動は急増しましたが、攻撃数は減少し始め、その傾向は 2020 年第 1 四半期まで続いています。

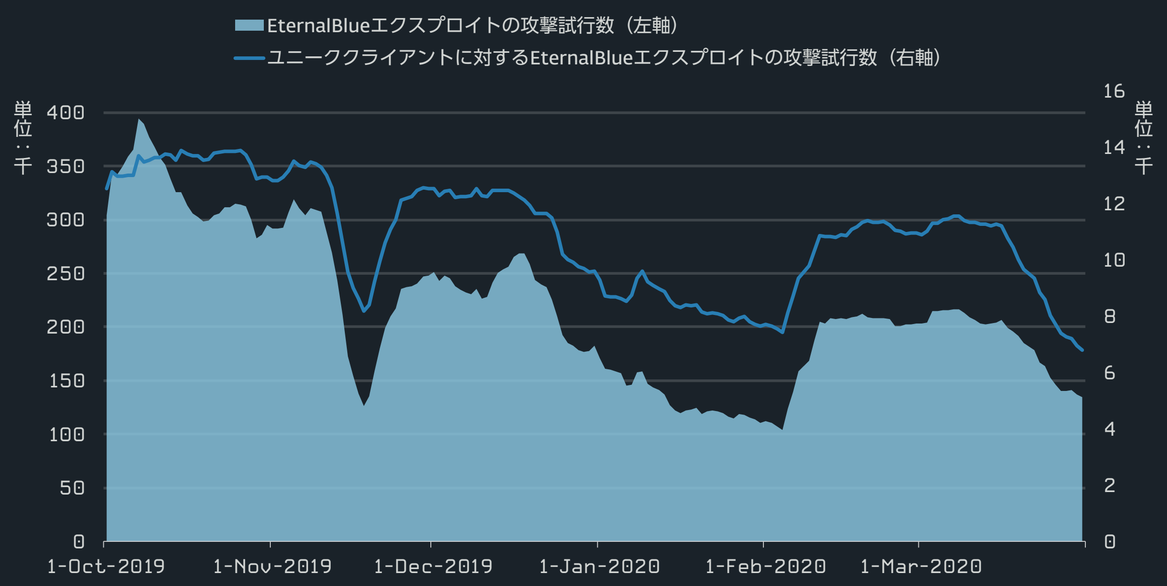
ネットワークセキュリティの観点では、リモートデスクトッププロトコル（RDP）は依然として重大な問題の 1 つです。ESET では大規模なパスワード推測攻撃を確認しています。このような攻撃は、最近、新型コロナウイルスによって引き起こされているロックダウンによって明らかに増加しています。RDP のセキュリティに関しては、この ***ESET アドバイザリ*** [31] を参照してください。



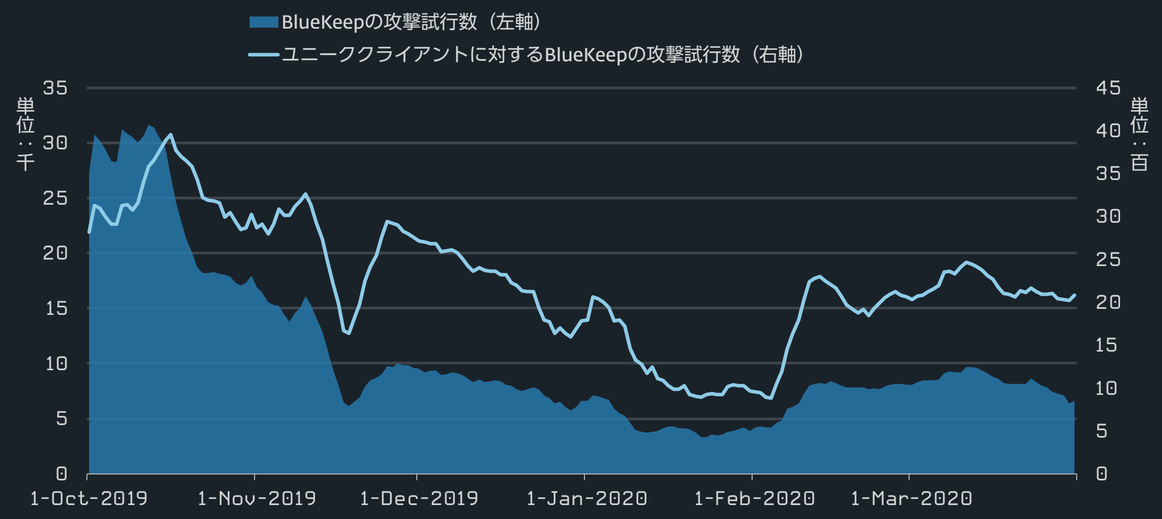
2019 年第 4 四半期から 2020 年第 1 四半期の RDP の接続試行の検出傾向、7 日間の移動平均線 [2]

日本に関する攻撃データを参照しても、攻撃数はかなりの数を計上しており、この古典的な RDP に対する攻撃が、攻撃者にとっていまだポピュラーであることがわかります。

イーセットジャパン　テクノロジー＆セキュリティエバンジェリスト、中川菊徳



2019 年第 4 四半期から 2020 年第 1 四半期のエクスプロイトの攻撃試行の検出傾向、7 日間の移動平均線



2019 年第 4 四半期から 2020 年第 1 四半期の BlueKeep の攻撃試行の検出傾向、7 日間の移動平均線

[2] 2019 年 12 月より前のデータは、方法論の変更されたために利用できません。2 月上旬の増加は、一連の攻撃試行を分類するしきい値を低く設定したことが原因の 1 つです。

Mac に関する脅威

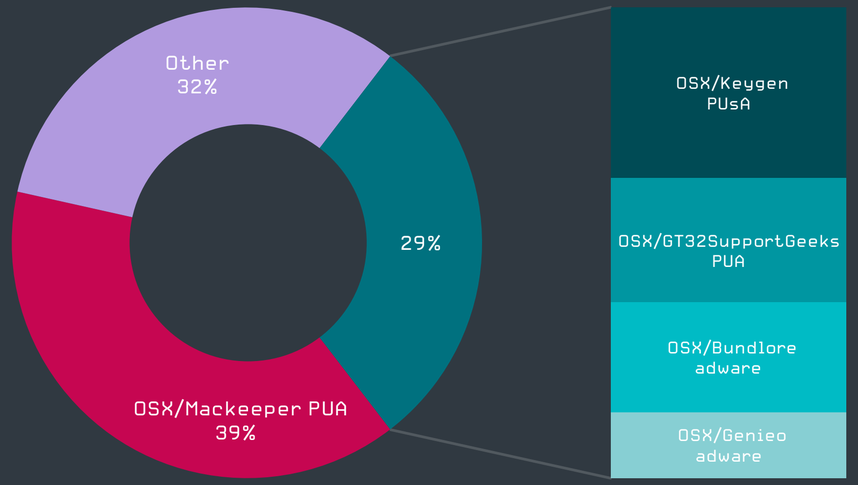
ESET のテレメトリ（監視チームデータ）によると、2020 年第 1 四半期における Mac の脅威は横ばいになっています。

2020 年第 1 四半期では、1 月に macOS の脅威検出数が若干増加しましたが、その後、2019 年の平均をわずかに下回る状態に戻りました。2020 年第 1 四半期に ESET 製品によって検出された Mac の脅威では、望ましくない可能性があるアプリケーション（PUA）のカテゴリが最も多く、続いて潜在的に危険なアプリケーション（PUsA）、アドウェア、トロイの木馬が続いています。

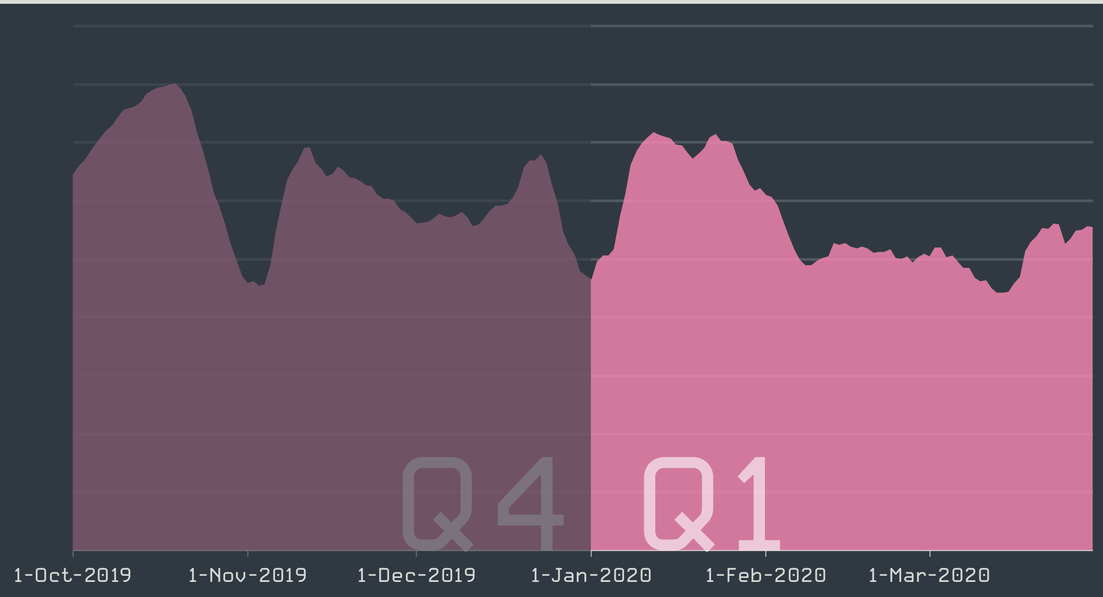
Mac コンピュータ（macOS オペレーティングシステムを搭載しているコンピュータ）は、Windows または Linux デバイスと比較するとマルウェアによる攻撃を受けることが少なくなっています。Apple 社の「ウォールドガーデン（壁に囲まれた庭）」戦略は、セキュリティ以外の理由から批判されることもありますが、マルウェアが Mac に侵入することを困難にしています。macOS セキュリティの重要な要素は、コードが Apple によって署名されているかどうかをチェックするゲートキーパーと呼ばれる仕組みです。このコードチェックに失敗したアプリは、ユーザーが明示的に許可しない限り、インストールされません。

典型的な攻撃シナリオは、ソーシャルエンジニアリングによって、ユーザーをだまして Mac にマルウェアをインストールさせる手法です。

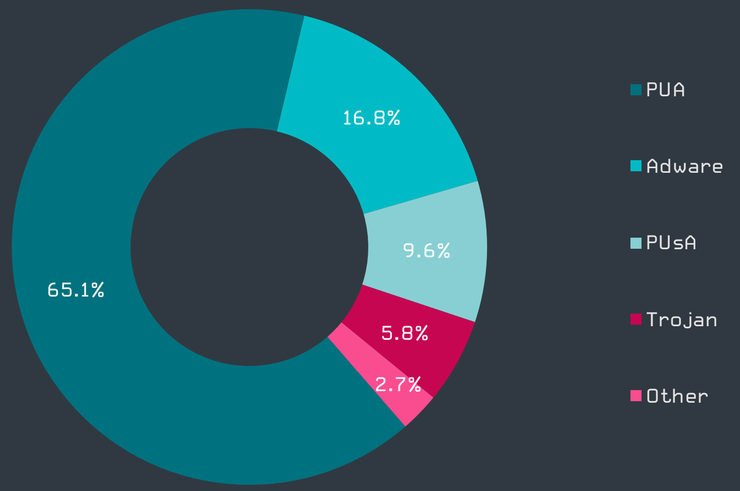
ESET シニア検出エンジニア、Miroslav Legéň



2020 年第 1 四半期の Mac の脅威検出トップ



2019 年第 4 四半期から 2020 年第 1 四半期の Mac の脅威検出傾向、7 日間の移動平均線



2020 年第 1 四半期の Mac の脅威検出カテゴリトップ

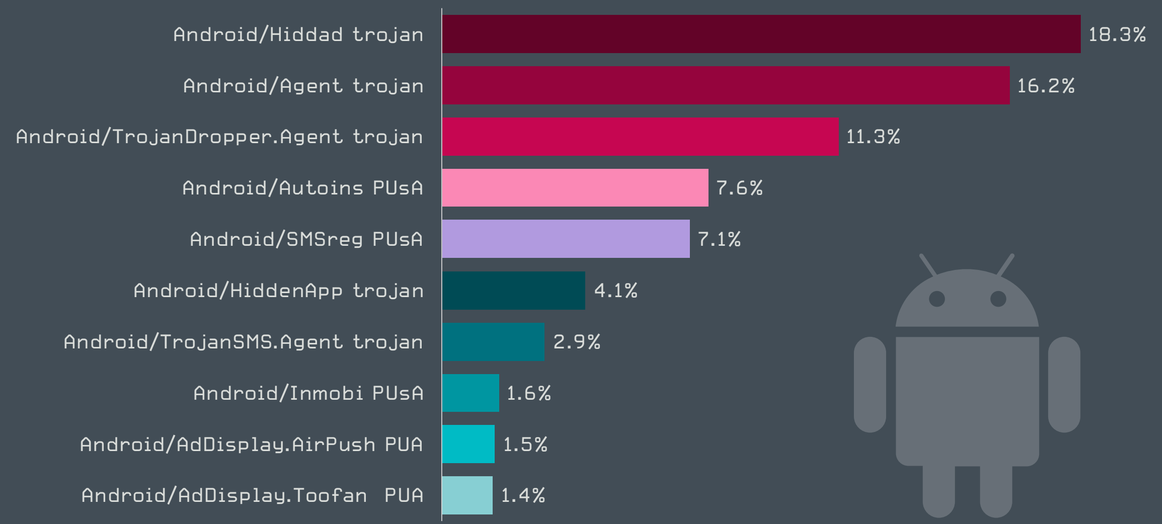
Android に関する脅威

Android の脅威では、広告を表示するアプリが最も多く検出されていますが、今、最も注意が必要なのはストーカーウェアです。

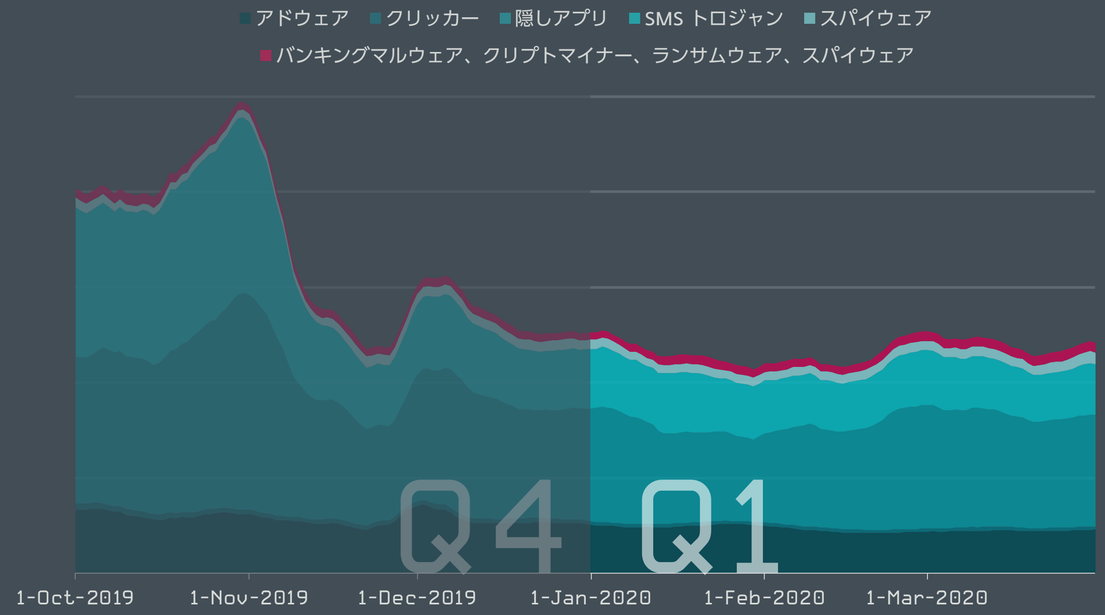
全体的な Android の脅威検出レベルは 2020 年第 1 四半期を通じて横ばいでしたが、2019 年第 4 四半期の前半と比較すると著しく低くなっています。隠しアプリである Android/Hiddad は、検出されたマルウェアファミリの中で常に 1 位になっています。隠しアプリは、Android/HiddenApp などとともに、依然として Android の脅威の中で最も多く検出されているカテゴリです。これらのアプリの主な機能は、インストール後にアイコンを非表示にし、フルスクリーン広告をユーザーに表示することです。これらの疑わしいアプリは通常、Google Play ストアに入り込み、魅力的なゲームや写真編集アプリになりすましています。

「隠しアプリ」のカテゴリに含まれるアプリはアドウェアの動作を表示しますが、そのステルス機能は従来のアドウェアとは一線を画しており、普及が進んでいます。これらの理由から、ESET では、一般的なアドウェアカテゴリとは別に「隠しアプリ」として追跡しています。

ESET マルウェアリサーチャー、Lukáš Štefanko



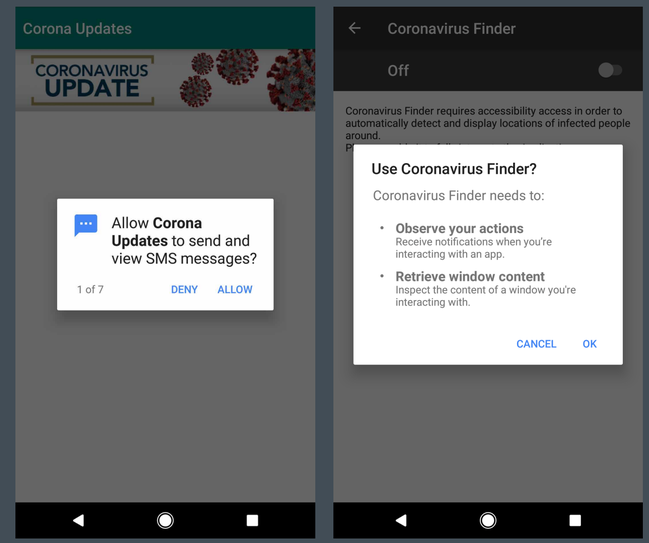
2020 年第 1 四半期の Android の脅威トップ 10（% は Android の脅威検出率）



2019 年第 4 四半期から 2020 年第 1 四半期の Android の脅威カテゴリ別検出傾向、7 日間の移動平均線

Android エコシステムは、2020 年第 1 四半期に始まった新型コロナウイルスの世界的な流行の影響を受けています。狡猾なサイバー犯罪者は、新型コロナウイルスに関連する感染予防商品や機器および治療法に関する情報を渇望する Android ユーザーの心理を悪用し始めています。

ESET の研究者は、症状の特定、感染マップ、感染経路の追跡アプリケーション、給付金など、新型コロナウイルスに便乗にした偽情報を悪用して配布されている悪意のあるアプリの存在を確認しました。この方法で配布された悪意のあるアプリの中には、さまざまなバンキングトロイ、ランサムウェア、SMS ワーム、スパイウェア、アドウェアが含まれています。



新型コロナウイルスを悪用した Android マルウェアが許可を求める例

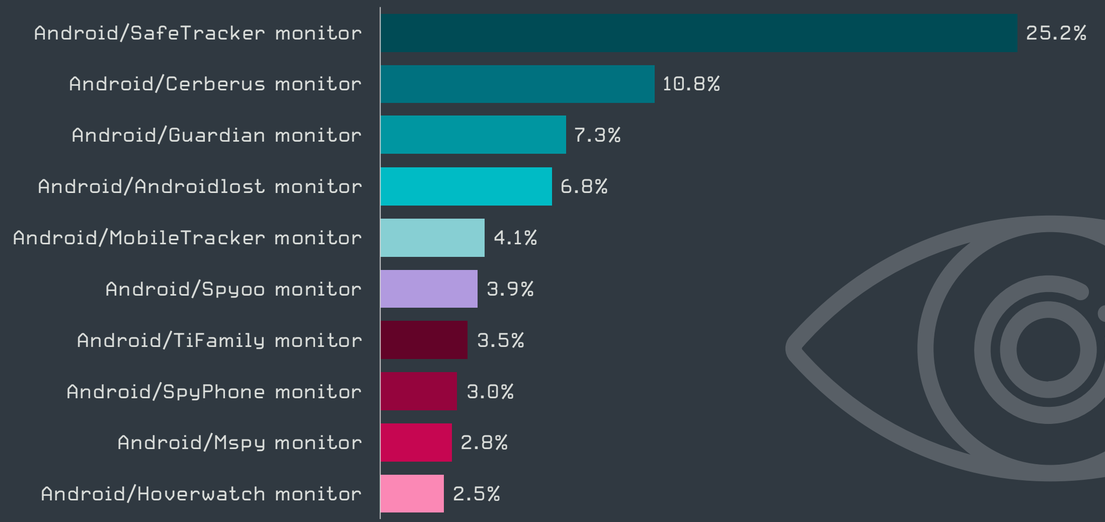
ストーカーウェア

ストーカーウェアのカテゴリ（配偶者ウェアやスパウズウェアとも呼ばれます）の検出数は、2019 年第 4 四半期と比較して約 3 倍に増加しています。

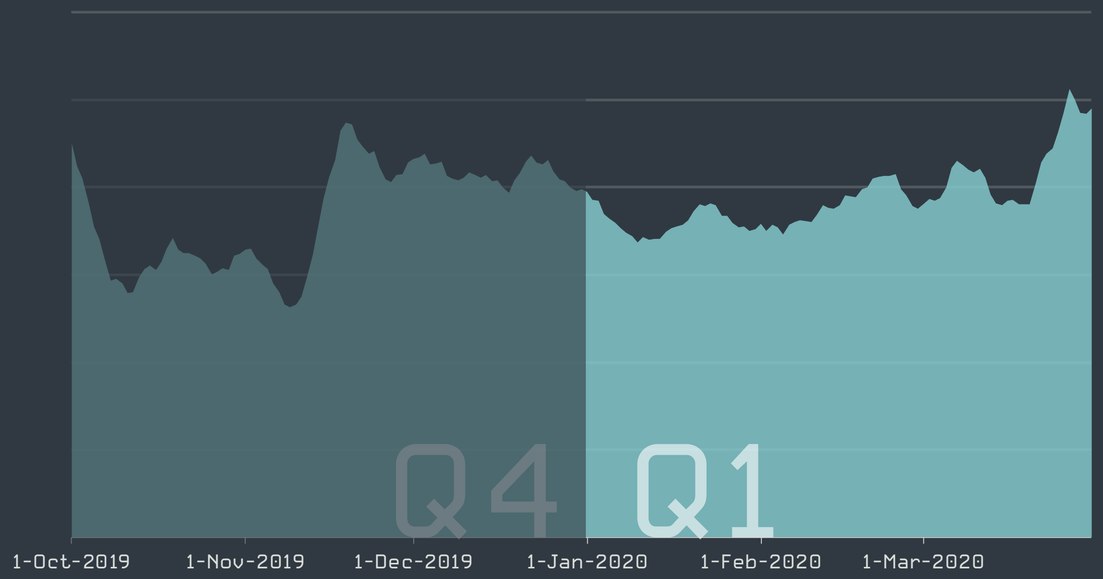
ESET は、Android の脅威であるストーカーウェアカテゴリを、技術的には同じカテゴリに属する望ましくない可能性があるアプリケーション（PUA）とは別に扱っています。ストーカーウェアは、2 つの機能を持つテクノロジーの典型です。正規の目的で利用される場合もありますが、違法な目的のために悪用されることも多いツールです。

通常、ストーカーウェアは、子供、学生、または従業員を見守ることができるツールとして販売されていますが、実際には、これらのアプリは、アプリの機能に疑いを持たない配偶者や恋人をスパイするために使用されることが多く、時には悲劇的な結果をもたらすこともあります。このため、ESET はこれらのアプリを望ましくないアプリケーション（PUA）のカテゴリとは別に分類し、顧客の設定に関わらずその性質について警告しています。

ストーカーウェアアプリにはさまざまなタイプがあり、ESET の研究者は約 100 のストーカーウェアファミリに注目しています。これらのうち、上位 4 つを除くすべてのストーカーウェアの検出率は 5% 未満であり、検出された主要なストーカーウェアファミリがこのカテゴリの 25% 以上を占めています。



2020 年第 1 四半期の Android ストーカーウェアファミリートップ 10（% は Android ストーカーウェア検出率）



2019 年第 4 四半期から 2020 年第 1 四半期のストーカーウェア検出傾向、7 日間の移動平均線

ストーカーウェアアプリは、不正な目的で使用されて脅威になるだけでなく、セキュリティを考えずに開発されている傾向があります。ESET の研究者は、これらのアプリが暗号化されず、セキュリティ保護されていないチャネルを介してバックエンドサーバーと通信しているケースを多く確認しています。

> ***ストーカーウェアアプリを開発しているサイバー犯罪者は、明らかにセキュリティをまったく考慮しておらず、ほぼすべての努力を積極的なマーケティング活動に費やしています。***
>
> **ESET マルウェアリサーチャー、Lukáš Štefanko**

そのため、安全でないストーカーウェアアプリケーションによって、違法に監視されるリスクだけでなく、情報が漏えいするリスクにも晒されます。ストーカーウェアアプリがデバイスにインストールされると、そのユーザーの個人情報が漏洩する恐れがあります。

Web に関する脅威

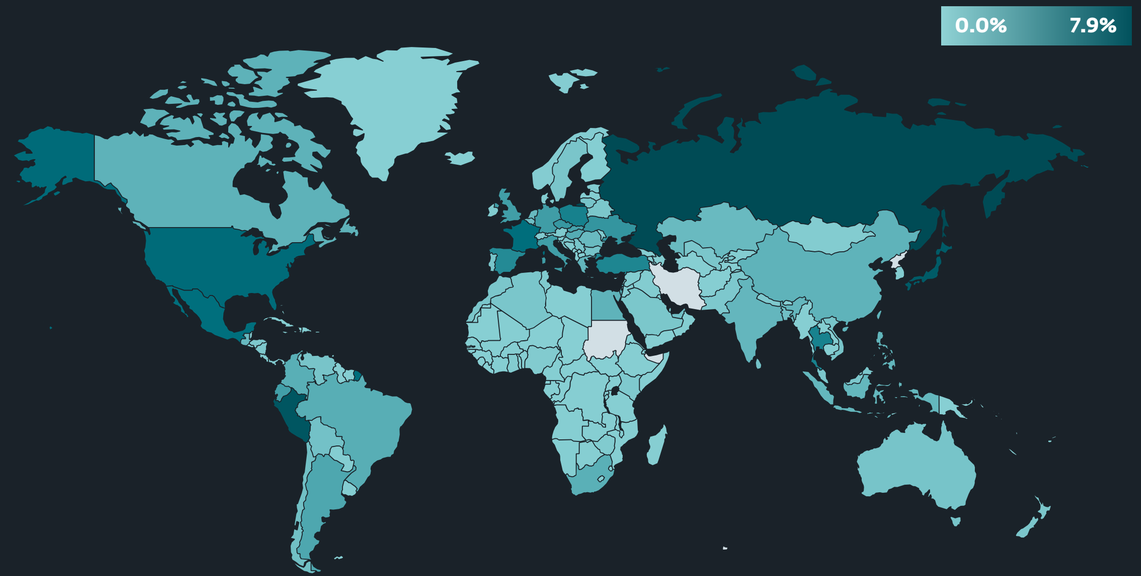
ESET のテレメトリ（監視チームデータ）によると、2020 年の第 1 四半期には Web の脅威が全体的に増加し、新型コロナウイルスの世界的な流行に関連する情報がユーザーを引き付けるために頻繁に使用されています。

2019 年第 4 四半期と比較して、2020 年第 1 四半期にブロックされた悪意のある不正な Web サイトの数は 21% 増加しました。年初に、これらのサイトの検出数は急増し、2020 年 1 月中旬にピークに達し、四半期の終わりにはわずかに減少しました。ただし、ブロックされた URL に注目すると、反対の傾向が見られ、2019 年第 4 四半期から 2020 年第 1 四半期に 33% 減少しています。

傾向データは、ブロックされた脅威のタイプに基づいてカテゴリ別に分類されます。

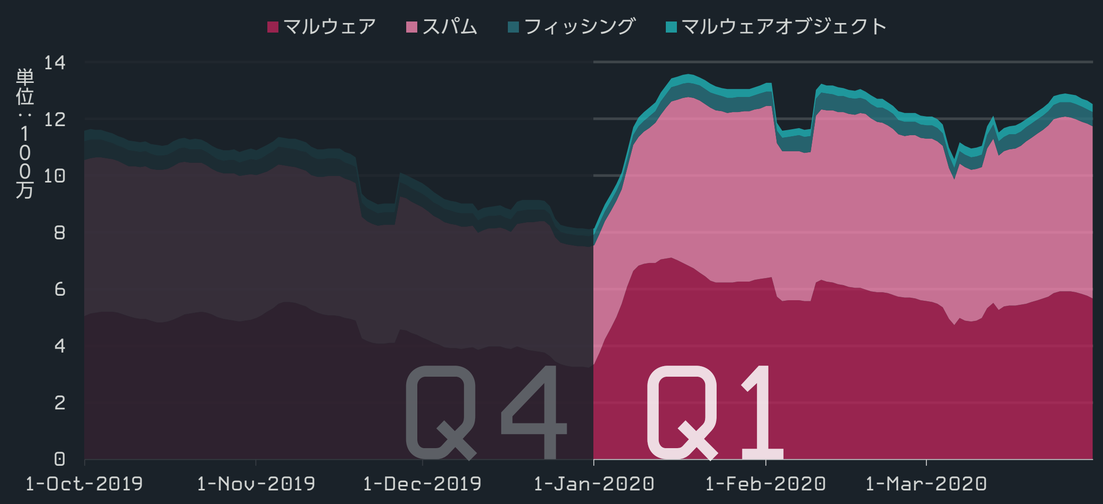
- **マルウェア**：マルウェアを配信することが知られている Web サイト
- **詐欺**：詐欺コンテンツを含む Web サイト
- **フィッシング**：機密データを収集するために使用される Web サイト
- **マルウェアオブジェクト**：正規の Web サイト（クラウドストレージサービスなど）でありながら、悪意のあるコードをホスティングするサイト

「マルウェア」カテゴリの Web サイトが全体的には最も多くブロックされていますが、URL でブロックされたものの多くは「詐欺」カテゴリに属しています。「フィッシング」のカテゴリでは、URL でブロックされた攻撃数が最大で約 20 件程度になっています。

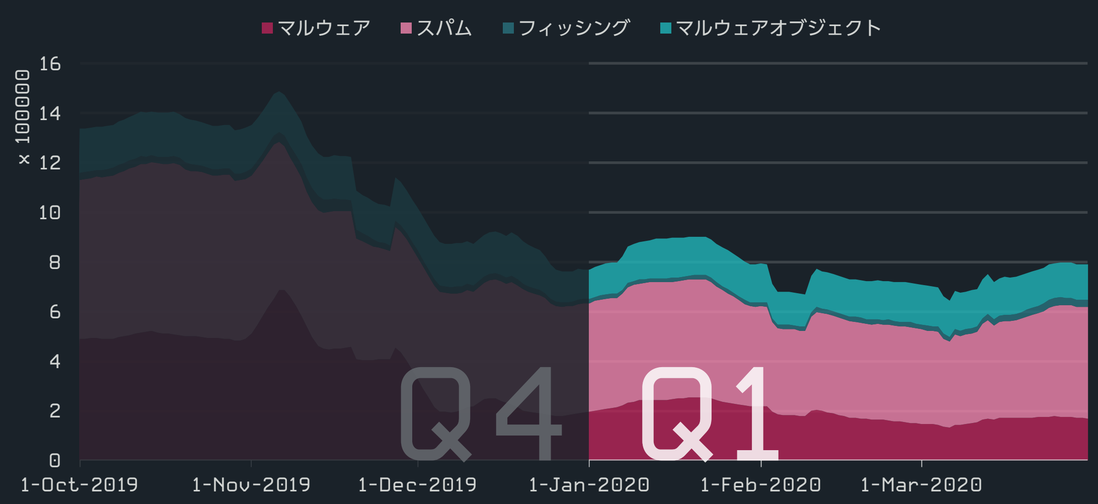


2020 年第 1 四半期の Web の脅威ブロック率

ESET のテレメトリ（監視チームデータ）によると、ロシア、ペルー、日本、米国、フランスの ESET の顧客が Web の脅威を最も多くブロックしています。検出数が最も多いドメインを次ページの表に示します。



2019 年第 4 四半期から 2020 年第 1 四半期のブロックされた Web の脅威傾向、7 日間の移動平均線



2019 年第 4 四半期から 2020 年第 1 四半期のブロックされた URL の傾向、7 日間の移動平均線

	マルウェア	スパム	フィッシング
1	adobviewe[.]club	r.remarketingpixel[.]com	d18mpbo349nky5.cloudfront[.]net
2	fingahvf[.]top	ofhappinyer[.]com	mrproddisup[.]com
3	deloplen[.]com	ak.imgfarm[.]com	attacketslovern[.]info
4	runmewivel[.]com	plugins.zonainst[.]xyz	gleaminist[.]info
5	webunstop[.]net	maranhesduve[.]club	update.updtbrwsr[.]com
6	cozytech[.]biz	rudy.adsnative[.]com	update.updtapi[.]com
7	d3qjtdfpbrj6c.cloudfront[.]net	version.zonainst[.]xyz	static.oceanreefs[.]xyz
8	linkangood[.]com	glotorrents[.]pw	update.brwsrapi[.]com
9	videomore[.]club	postlnk[.]com	update.mrbrwsr[.]com
10	hardyload[.]com	koindut[.]com	update.savebrwsr[.]com

2020 年第 1 四半期のブロックされたマルウェア、スキャム、フィッシングドメイントップ 10

ホモグラフ攻撃

ホモグラフ攻撃は、URL 内の文字（フォントデザイン用語のグリフ（字形））を、似たように見える文字、または視覚的にはまったく同じであるが、異なるアルファベットに属しているためコンピュータでは異なる文字として認識される文字に置き換える手法を悪用するものです。これらの攻撃は、罠を見破ることが難しい為、ユーザーにとって非常に危険な攻撃です。

価値が高く標的になりやすいドメイン（銀行、金融機関、決済プラットフォーム、人気の高い電子メールサービス、信頼されるメディア）を保護するために、ESET 製品は厳密な検査を実行しています。保護対象の URL の文字を他のアルファベットの類似文字テーブルと照合し、詐欺が検出された場合は顧客に警告します。

ESET のテレメトリ（監視チームデータ）によると、2020 年の第 1 四半期に最も多く「ホモグラフ攻撃」のような手法で偽装されたドメインは apple.com であり、その次に instagram.com と blockchain.com が続きました。検出された apple.com のホモグラフのほとんどは、教育的な目的のために作成された悪意のないドメインのものでした。

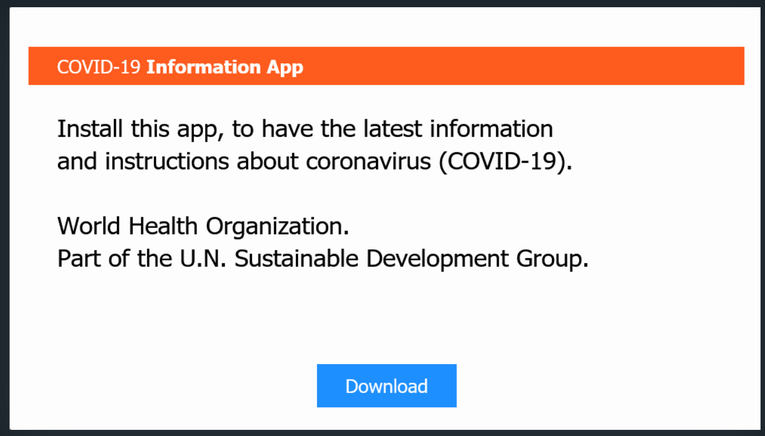
ただし、instagram.com および blockchain.com を偽装したドメインは悪意があるものです。

2020 年第 1 四半期に最も多くホモグラフ攻撃に狙われたブランド

ユーザーを攻撃するための擬似餌として悪用される新型コロナウイルスの流行

3 月中旬に、新型コロナウイルスに便乗した Web 攻撃が急増しました。マスクやほかの個人用感染予防商品を販売すると謳った詐欺のオンラインストアから、危険なマルウェアを配信する Web サイトも発生しました。

マルウェアを配信する Web サイトのカテゴリでは、ESET の監視チームは、ユーザーを騙して「新型コロウイルス情報アプリ」なるアプリをダウンロードさせようとする世界保健機関（WHO）を装った悪意のある Web サイトを検出しました。このサイトから、ダウンロードされるのは情報アプリではなくマルウェアです。ESET では、ペイロードを頻繁に変更しながら、ダウンローダー、スパイウェア、ランサムウェアなどの悪意のあるさまざまなマルウェアを配信する Web サイトを確認しています。



ユーザーにマルウェアのダウンロードを促す WHO を装った悪意のある Web サイト

ドメイン名にコロナウイルス関連の文字列が含まれる Web サイトについては、2020 年 3 月中旬に急増しており、3 月 1 日と 3 月 16 日の検出を比較すると 60 倍に増加しています。これらの脅威は、米国、ロシア、およびウクライナの ESET の顧客の間で最も検出されており、これらの国を合わせると、新型コロナウイルス関連の Web 脅威の検出全体の 70% を占めています。

マルウェアカテゴリでは、HTML/ScrInject.B（ブラウザで他の URL にリダイレクトして別のマルウェアをインストールする悪意のあるコード）を配信している coronavirus[.]zone が最も多くブロックされました。フィッシングカテゴリで最も流行しているのは chasecovid19v[.]com であり、詐欺 Web サイトのカテゴリで、最も多くブロックされたのは survivecoronavirus[.]org でした。

日本にも、流行早期の段階から、ファイル名：COVID-19 UPDATE.exe としたマルウェアスパム着弾をかなりのボリュームで確認しています。

イーセットジャパン　テクノロジー＆セキュリティエバンジェリスト、中川菊徳

電子メールに関する脅威

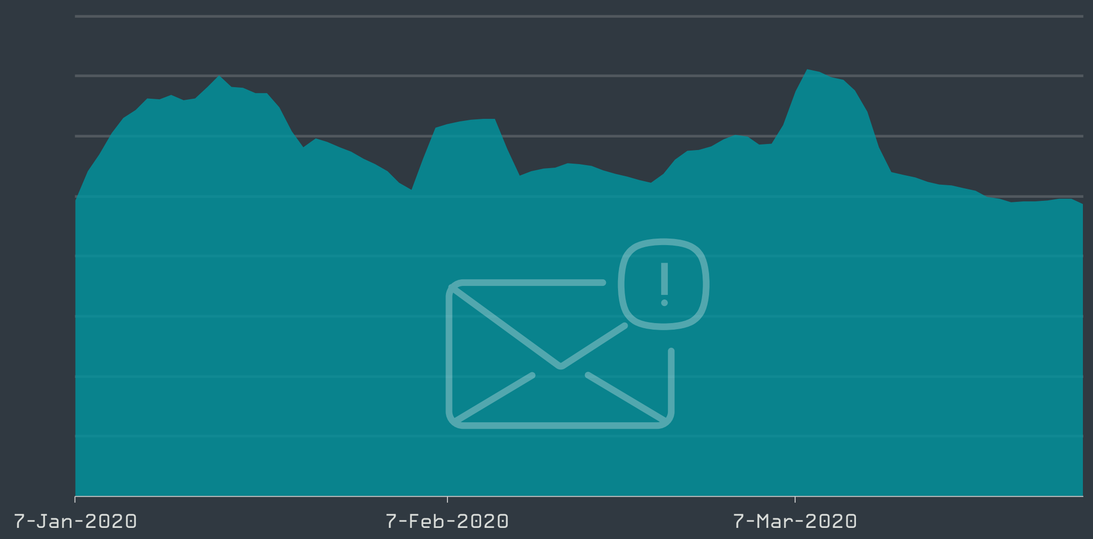
2020 年第 1 四半期のスパム攻撃については大きな変化はありませんでした。2020 年 3 月に若干上昇し、新型コロナウイルスに便乗にした迷惑メールが増加しました。

2020 年第 1 四半期には、大きな混乱をもたらす大規模なスパム攻撃は発生していません。ESET のテレメトリ（監視チームデータ）では、スパムの検出数は比較的安定したレベルを示しています。いくつかの小さなピークが確認されており、最大のスパム数が検出されたのは 2020 年 3 月の第 2 週でした。

第 1 四半期に検出された迷惑メールの内、約 5 分の 1 は米国から送信され、続いてポーランド、フランス、日本、ドイツから送信されています。送信者の国を特定できなかったメールは、スパム全体の 13% を占めました。各国で送信されたすべてのメールとスパム数の比較を見ると、ベトナム、リトアニア、アルゼンチン、中国、インドでその比率が高くなっており、送信された全メールの半分以上をスパムが占めています。

このデータを読み解く場合には、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メールが到達する前に、インターネットメールサービスプロバイダなどでフィルタリングされている可能性があり、すべてのスパムトラフィックを捉えていない可能性があることを考慮しなければなりません。しかし、ESET のソリューションでスパムトラフィックが検出されているということは、他のスパム対策ソリューションをすり抜けている可能性があり、その脅威が潜在的に高いことを示しています。

ESET のクライアントベースは分散しており地理的なデータに偏りがあることには注意してください。スパムメールの発信国は、送信側の情報ではなく、メール自体の情報から判断していることをご理解ください。



2020 年第 1 四半期のスパム検出傾向、7 日間の移動平均線

	国	ブロックされた全スパムにおける送信国の割合
1	アメリカ	18.4%
2	不明	12.9%
3	ポーランド	6.6%
4	フランス	5.9%
5	日本	5.2%
6	ドイツ	4.5%
7	ロシア	4.0%
8	リトアニア	3.8%
9	中国	3.4%
10	インド	3.1%

2020 年第 1 四半期に送信されたスパム配信数国別ランキング

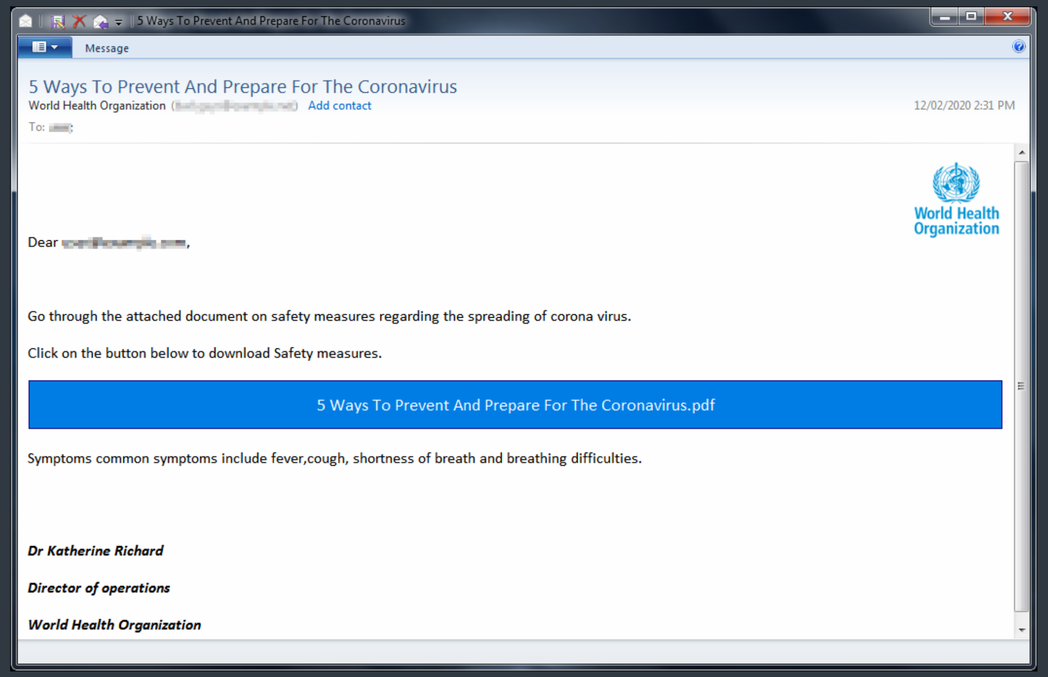
	国	国別の送信された全電子メールにおけるスパムの割合
1	ベトナム	71.7%
2	リトアニア	70.6%
3	アルゼンチン	57.2%
4	中国	56.1%
5	インド	54.3%
6	ブラジル	43.9%
7	インドネシア	40.5%
8	コロンビア	34.5%
9	韓国	31.5%
10	フランス	25.4%

2020 年第 1 四半期にメールによって送信されたスパム配信数国別ランキング

新型コロナウイルスに便乗するスパム

新型コロナウイルスの発生だけではこの世に渦巻く災厄が十分ではないかのように、サイバー犯罪者達はこの危機に関連する情報の錯綜、恐れ、感染予防商品の供給不足に便乗して利益を得ようと躍起になっています。2020 年 3 月には、新型コロナウイルスに便乗する膨大な数のスパム、マルウェアの拡散、機密情報のフィッシング、偽の製品（マスク、コロナウイルスの自然療法、またはコロナウイルスワクチンの成分のリストなど）に関連する攻撃が検出されました。

スパマーは無防備なユーザーに悪意のあるリンクや添付ファイルを開かせるために、世界保健機関（WHO）になりすました攻撃も複数見つかっています。新型コロナウイルスの流行に関する主要な情報源である WHO は、WHO の Web サイトでなりすましについて*注意を喚起しています* [32]。

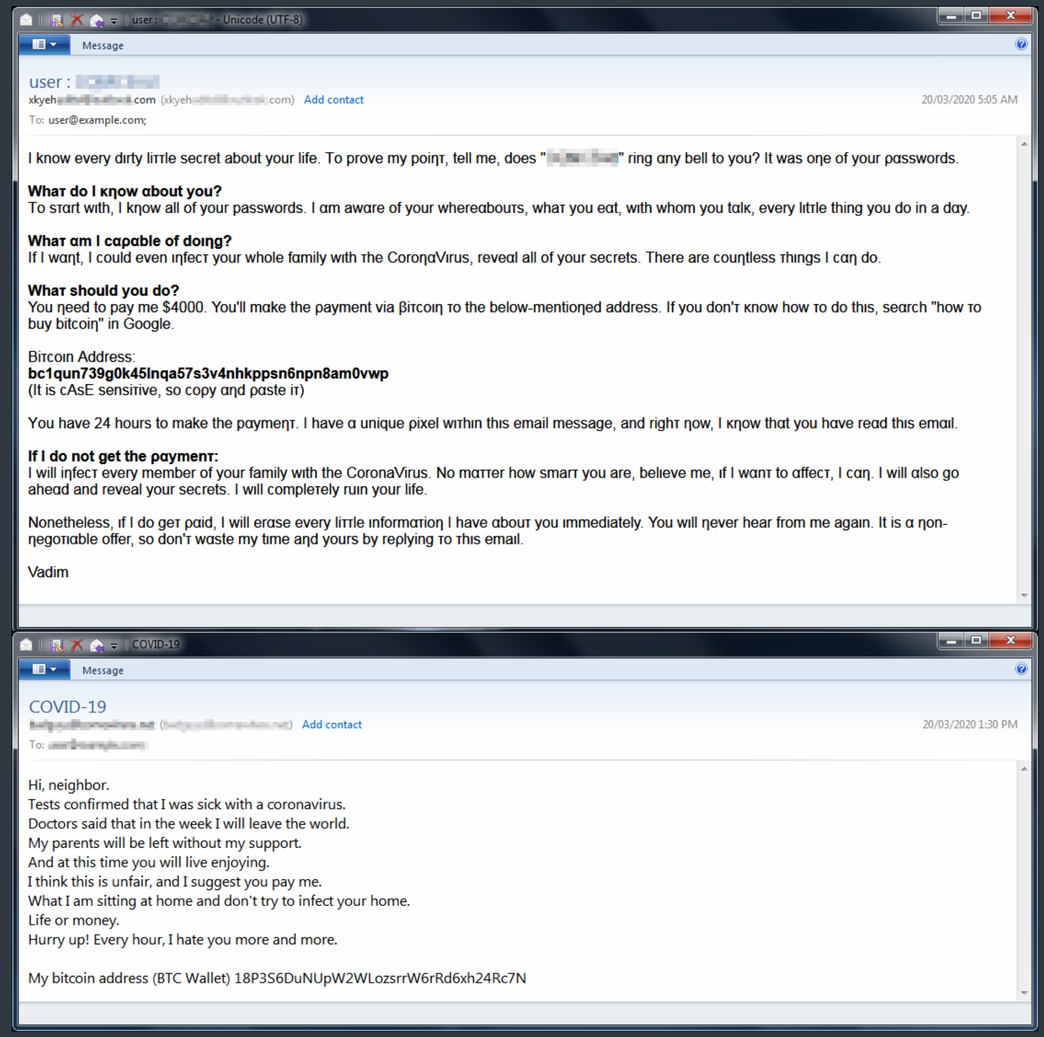


WHO を装ったスパムメール

恐ろしいことに、恐喝メールを送りつけて金銭を得ているサイバー犯罪者は、このコロナウイルスの危機から利益を得ようとしており、身代金が支払われなければ電子メールの受信者とその家族に新型コロナウイルスを感染させると脅迫しています。

右上のスクリーンショットに示すスパム攻撃では、犯罪者は恐喝目的で実行された*過去のセクストーション詐欺メールのテンプレートを利用し* [33]、新型コロナウイルスの流行に合わせてカスタマイズしています。

スパム対策エンジンを回避するために、スパマーは標準のラテン文字に非常によく似たギリシャ語のアルファベットの文字をメールのテキストに組み込んでいます。たとえば、小文字の a ではなく α（小文字のアルファ）が使用されています。また、近隣の住人から電子メールが送信されているとして受信したユーザーを脅迫するサイバー犯罪者もいます。これは、金銭を払わなければ、簡単に感染させることができる近くの人物を装って威圧する手法です。



新型コロナウイルスに便乗したスパムメール

ほとんどの脅迫目的の電子メール攻撃と同様に、これらの電子メールの内容の主張は根拠はありません。他のスパムメールと同じように無視してください。

IoT セキュリティ

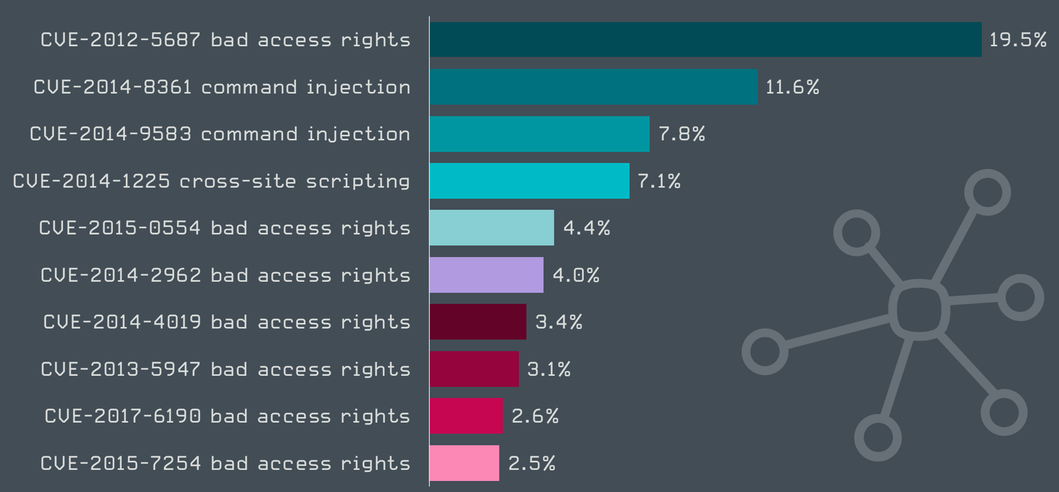
攻撃者によるアクセス制御の迂回を可能にする数年前の脆弱性が、IoT デバイスで最も多く検出される欠陥リストの上位にランクインしています。

モノのインターネット（IoT）と呼ばれるデバイスでは、脆弱性や構成の問題が発生することが多くあり、悪用される恐れもあります。ESET のルーター脆弱性スキャナーモジュールは、この四半期に世界中で 10 万台以上のルーターをスキャンし、パスワードや情報漏えい、ディレクトリトラバーサルなどの不正アクセスにつながる可能性のある脆弱性が、IoT の問題における主なタイプであることを示しています。

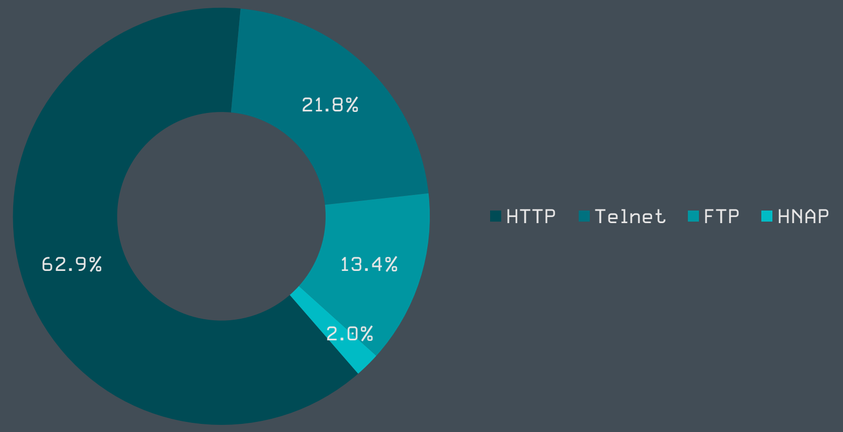
ESET のスキャナーによって検出された上位 10 の IoT 脆弱性の 7 つがこのタイプの問題であることから、この見解が正しいことが証明されています。注目すべきなのは、IoT の脆弱性リストでトップ 10 にランキングしている脆弱性の古さです。ESET のテレメトリ（監視チームデータ）によると、トップ 10 のすべての脆弱性が 2017 年以前に発見されたものであり、発見された年が 2014 年にまでさかのぼる脆弱性も 10 件中で 5 件もあります。

IoT デバイスの問題の原因となっている主要な脆弱性である ***CVE-2012-5687*** [34] はさらに古く、2012 年 10 月に最初に報告されたものであり、7 年以上前から存在していますが、検出されたすべての脆弱性の 19% を占めています。古いコマンドインジェクションの脆弱性も蔓延しており、ランキングの第 2 位（CVE-2014-8361 が 12%）と第 3 位（CVE-2014-9583 が 8%）を占めています。

ESET のテレメトリ（監視チームデータ）は、ホスティングされているサービスが強度の低いパスワードやデフォルトのパスワードで保護されているケースがどれだけあったかについても有用な情報を提供しています。このようなパスワードの問題との関係性は、HTTP が使用されている場合に特に有意であると考えられ、HTTP が使用されている場合、63% でパスワードの問題が検出されています。続いて telnet を使用する場合が 22%、FTP を使用する場合が 13% でした。



ESET のルーター脆弱性スキャナーモジュールによって検出された脆弱性トップ 10（% は脆弱性検出率）



2020 年第 1 四半期にホスティングされているサービス強度の低いパスワード

IoT セキュリティの欠陥がネットワーク全体のセキュリティを大幅に低下させる恐れがあることを示す重大な事例のひとつが、***KrØØk の脆弱性*** [5] です。

KrØØk は、すべてゼロの WPA2 ペアワイズセッションキーで暗号化されるワイヤレスネットワークデータとして現れ、Wi-Fi のアソシエーションが解除（「切断」）される後に脆弱なチップ上で発生します。このようなアソシエーション解除（および再アソシエーション）は、信号の干渉やアクセスポイント間のローミングなど、さまざまな（正当な）理由で自然に発生します。したがって、理論的には、アソシエーション解除の直前に送信キューに入っていた少量のデータを復号でき、誰でもネットワークデータを盗聴できます。もちろん、これは受動的なアプローチであるため、目的のデータを取得するために運という要素が必要になります。

攻撃を効率化させる場合、標的となるデバイスでアソシエーション解除を手動で何度も繰り返すことで、KrØØk の脆弱性を悪用し、対象となる（機密性の高い）データを傍受する確率を大幅に高めることができます。

Wi-Fi に対して一般的に使用されている他の攻撃手法と比較すると、KrØØk は攻撃者にとって大きな利点があります。攻撃を実行するためには Wi-Fi 信号の範囲内にいる必要はありますが、WLAN に認証してアクセスする必要はありません。つまり、Wi-Fi のパスワードを知らなくても攻撃が可能になります。

ESET シニアマルウェアリサーチャー、Robert Lipovský

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

講演

RSA Conference 2020

KrØØk：Amazon Echo など 10 億台以上の Wi-Fi デバイスに影響する脆弱性 [7]

ESET の Robert Lipovský と Štefan Svorenčík が、RSA Conference 2020 で初めて KrØØk を発表しました。これは、Apple、Google、Samsung のデバイスを含む 10 億台を超える Wi-Fi 対応デバイスの暗号化に影響を与える、これまでに知られていなかったセキュリティの脆弱性です。

Linux マルウェアの検出の重要性 [35]

ESET の研究者である Marc-Étienne M.Léveillé は、実践的な技術ワークショップで、Linux システムの管理者がサーバーサイドの Linux の脅威を分析および理解するためのトレーニングの必要性について説明しました。彼のチュートリアルは、Linux の専門家がこのような脅威を安全かつ効果的に研究できる環境を作成することを目的としています。

BlueHat IL

世界で最も危険な攻撃者の TTP（戦術、手法、手順） [36]

ESET マルウェアリサーチャーである Robert Lipovský は、Sednit（別名：APT28）と Telebots（別名：Sandworm）の TTP を中心に、歴史上最も重大なサイバー攻撃の分析から得られた教訓について説明しました。

Attor：GSM フィンガープリンティングを実行するスパイプラットフォーム [37]

ESET のマルウェアリサーチャーである Zuzana Hromcová が、価値の高い対象への標的型攻撃で使用される新しいスパイプラットフォームである Attor を紹介しました。Attor の特徴的な機能は、高度なモジュール方式のアーキテクチャ、複雑なネットワーク通信方法、GSM デバイスのフィンガープリントを取得する独自のプラグインです。

MITRE ATT&CK への貢献

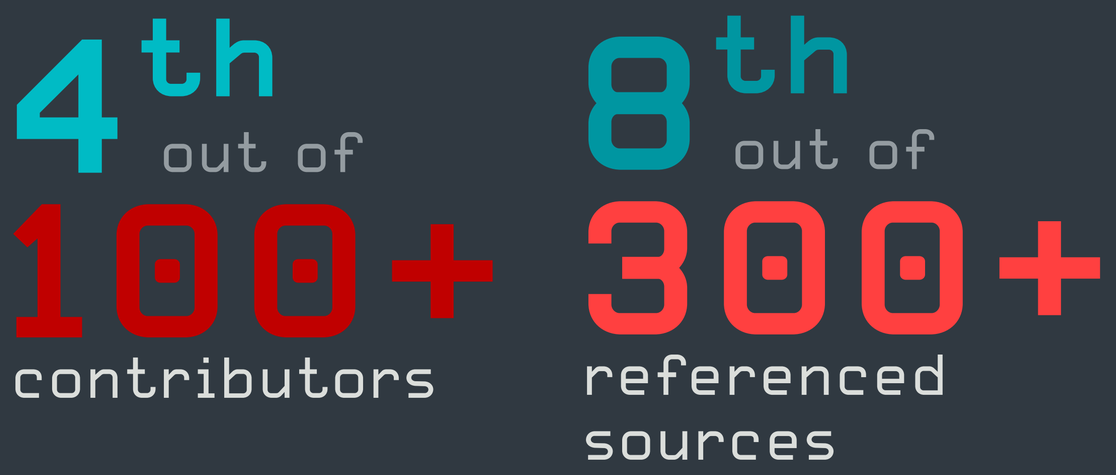
ESET の研究者は、調査結果を公開し、カンファレンスで発表しているほかに、定期的に ***MITRE ATT&CK®*** [38] にも貢献しています。MITRE ATT&CK® は、サイバー攻撃者の戦術と手法に関するナレッジベースであり、全世界からアクセス可能です。

2020 年 4 月の時点で、ESET は ATT&CK ***エンタープライズマトリクス*** [39] の貢献者のトップ 5 に入っており、***モバイルマトリクス*** [40] に最初に情報を提供し、最も貢献している組織のひとつとなっています。ESET は、両方のマトリックスで最も頻繁に参照されている情報ソースのひとつです。

この四半期レポートの執筆時点では、エンタープライズマトリクスには 100 以上の寄稿者と 300 の参照ソースがあり、モバイルマトリクスには 6 つの寄稿者と 100 以上の参照ソースがあります。

脅威インテリジェンスコミュニティの貢献は、MITRE ATT&CK® ナレッジベースを充実させるために重要な役割を果たしています。サイバースペースをより安全にするためには共同作業が必要であり、実環境で検出されたサイバー攻撃者の戦術と手法についての外部ソースからの報告は、防御する側の組織とって ATT&CK を貴重な資産にするために役立っています。

MITRE ATT&CK 担当、Adam Pennington



ESET はエンタープライズマトリクスの貢献者トップ 5、さらに参照される情報ソーストップ 10

ESET は、既存のカテゴリに情報を追加するだけではなく、エンタープライズとモバイルの攻撃手法、攻撃グループ、ソフトウェアカテゴリについても情報を提供して貢献しています。

「エンタープライズへの攻撃手法」カテゴリで、ESET が果たした大きな貢献の 1 つは、Turla グループが使用しているバックドア ***LightNeuron*** [42] を分析して判明した独自の***トランスポートエージェント (T1505)*** [41] です。LightNeuron は、常駐化するために悪意のある Microsoft Exchange トランスポートエージェントを実装します。

「ソフトウェア」カテゴリでは、Sednit（別名：APT28）が使用している UEFI ルートキットである ***LoJax (S0397)*** [43] に関する情報を ESET が提供しています。これは、ESET によって***検出された*** [44] 実環境で使用された初の UEFI ルートキットです。

「グループ」カテゴリにおける ESET の貢献の 1 つは、***Machete（G0095）*** [45] です。Machete は、ラテンアメリカ諸国で警戒が必要となっているサイバースパイ集団であり、ESET の研究者によって、1 年間にギガバイトレベルの機密データが盗まれたと***報告されています*** [46]。

ESET による Android の脅威調査も ATT&CK に組み込まれています。「モバイル」カテゴリには、さまざまな種類のデータを盗み出す Android マルウェアで使用されている ***Input Injection（T1516）*** [47] と ***Access Notifications（T1517）*** [48] の手法が含まれています。

ATT&CK の Web サイトでは ESET の関連情報が掲載されていますが、WeLiveSecurity ブログにある ESET Research のページでも、サイバー攻撃者の手法と ATT&CK ナレッジベースの対応表を***参照できます*** [49]。

その他の貢献

ESET の研究者は、マルウェアの調査・研究に関連するコミュニティで広く使用されているツールである YARA のコードベースにも貢献しています。2020 年第 1 四半期に、ESET は 2 つのプルリクエストをメインコードベースにマージしています。

最初に受け入れられたプルリクエスト [50] は、ESET のマルウェアリサーチャーである Peter Kálnai と Michal Poslušný による調査に基づいており、YARA の Rich Header 機能を拡張して、バックエンドデータをより明確に示し、Rich Header を完全に利用できるようにしました。

2 番目の貢献 [51] は、ESET のマルウェアリサーチャーである Anton Cherepanov が主導したものであり、PDB 文字列を解析するための新機能を追加して、YARA の PE モジュールを改善しました。この新機能により、PDB パスに特定のキーワードが含まれる Windows マルウェアを特定・検出できるより優れた YARA ルールを作成できます。

クレジット

チーム

Peter Stančík, Lead
Klára Kobáková, Managing Editor

Aryeh Goretsky
Bruce Burrell
Nick FitzGerald
Ondrej Kubovič
Petr Blažek

序文

Roman Kováč, Chief Research Officer

貢献者

Igor Kabina
Jakub Souček
Ján Šugarek
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Martin Abrahámek
Martin Červeň
Martin Lackovič
Mathieu Tartare
Matthieu Faou
Milan Fránik
Miloš Čermák
Miroslav Legéň
Miroslav Rolko
Patrik Sučanský
Robert Lipovský
Zoltán Rusnák
中川 菊徳

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）* [52]、*潜在的に危険なアプリケーション* [53]、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.krackattacks.com/#paper

[2] https://www.eset.com/jp/blog/welivesecurity/alexa-how-amazon-echo-kindle-got-kracked/

[3] https://www.icasi.org/

[4] https://www.eset.com/jp/blog/welivesecurity/krook-serious-vulnerability-affected-encryption-billion-wifi-devices/

[5] https://www.eset.com/fileadmin/ESET/JP/Blog/download/ESET_Kr00k-whitepaper_J_200501.pdf

[6] https://www.eset.com/jp/blog/welivesecurity/kr00k/

[7] https://www.rsaconference.com/usa/agenda/kr00k-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wifi-devices

[8] https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/

[9] https://www.eset.com/jp/blog/welivesecurity/stantinko-botnet-adds-cryptomining-criminal-activities/

[10] https://www.welivesecurity.com/2020/03/19/stantinko-new-cryptominer-unique-obfuscation-techniques/

[11] https://www.welivesecurity.com/2020/03/05/guildma-devil-drives-electric

[12] https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf

[13] https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/

[14] https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

[15] https://www.eset.com/jp/blog/welivesecurity/winnti-group-targeting-universities-hong-kong/

[16] https://www.eset.com/jp/blog/welivesecurity/tracking-turla-new-backdoor-armenian-watering-holes/

[17] https://nvd.nist.gov/vuln/detail/CVE-2017-11882

[18] https://www.welivesecurity.com/2017/12/04/eset-takes-part-global-operation-disrupt-gamarue/

[19] https://www.bleepingcomputer.com/news/security/emotet-malware-restarts-spam-attacks-after-holiday-break/

[20] https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/

[21] https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/

[22] https://www.welivesecurity.com/2020/03/23/good-bad-plain-ugly/

[23] https://twitter.com/CryptoInsane/status/1240668834190839808

[24] https://www.us-cert.gov/ncas/alerts/aa20-049a

[25] https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17627/2020_USA20_SEM-M03H_01_Feds-Fighting-Ransomware-How-the-FBI-Investigates-and-How-You-Can-Help.pdf

[26] https://youtu.be/LUxOcpIRxmg

[27] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-led-action-takes-aim-at-cryptojacking-in-Southeast-Asia

[28] https://www.welivesecurity.com/2019/02/28/coinhive-cryptocurrency-miner-to-call-it-a-day-next-week

[29] https://www.eset.com/jp/blog/welivesecurity/eternalblue-new-heights-wannacryptor/

[30] https://www.welivesecurity.com/2019/05/22/patch-now-bluekeep-vulnerability/

[31] https://www.welivesecurity.com/2019/12/17/bluekeep-time-disconnect-rdp-internet/

[32] https://www.who.int/about/communications/cyber-security

[33] https://www.welivesecurity.com/2018/07/26/i-saw-what-you-did-or-did-i/

[34] https://nvd.nist.gov/vuln/detail/CVE-2012-5687

[35] https://www.rsaconference.com/usa/agenda/hunting-linux-malware-for-fun-and-flags

[36] https://www.bluehatil.com/abstracts#collapse-Tactics

[37] https://www.bluehatil.com/abstracts#collapse-GSMFingerprinting

[38] https://attack.mitre.org/

[39] https://attack.mitre.org/matrices/enterprise/

[40] https://attack.mitre.org/matrices/mobile

[41] https://attack.mitre.org/techniques/T1505/

[42] https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

[43] https://attack.mitre.org/software/S0397/

[44] https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf

[45] https://attack.mitre.org/groups/G0095/

[46] https://www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

[47] https://attack.mitre.org/techniques/T1516/

[48] https://attack.mitre.org/techniques/T1517/

[49] https://www.welivesecurity.com/

[50] https://github.com/VirusTotal/yara/pull/1135

[51] https://github.com/VirusTotal/yara/commit/a72945ce44ce70bd7193e94c16e8bef580e35038

[52] https://help.eset.com/glossary/en-US/unwanted_application.html

[53] 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。詳細情報については、*www.eset.com/jp* をご覧ください。

ENJOY SAFER TECHNOLOGY™

WeLiveSecurity.com
@ESETresearch
ESET GitHub