※この日本語は参考訳です。原文は英文であり、参考訳に齟齬があるときは英文が優先されます。

ESET サイバーセキュリティ脅威レポート 2022 年 T3（第 3 三半期）

目次

3 序文

4 エグゼクティブサマリー

5 特集記事

8 ESET Research Lab からの最新情報

11 統計と傾向

12 脅威状況の概要

13 検出されたマルウェアトップ 10

14 情報窃取型マルウェア

17 ランサムウェア

20 ダウンローダー

22 暗号通貨の脅威

25 ウェブに関する脅威

28 電子メールに関する脅威

31 Android に関する脅威

34 macOS と iOS に関する脅威

36 IoT セキュリティ

38 エクスプロイト

41 ESET Research チームの貢献

序文

ESET 脅威レポート T3 2022 号へようこそ!

2022 年、ウクライナへのいわれのない不当な攻撃は世界に衝撃を与え、同国とその国民に壊滅的な影響をもたらしました。この戦争は、エネルギー価格やインフレからサイバースペースまであらゆるものに影響を与え続け、ESET の研究者とアナリストは 1 年を通して広範囲に渡って監視しています。

サイバースペースで見られる影響の中で、ランサムウェアのシーンは最も大きな変化を経験しました。侵入当初から、ランサムウェアの運営者の間で、この侵略行為を支持する者と反対する者とに分かれているのが見受けられます。また、ランサムウェアを模倣し、被害者のデータを暗号化して復号化キーを提供するつもりのないワイパーを展開するなど、攻撃者の破壊的な手口はますます増えています。

この戦争は、露出した RDP サービスに対するブルートフォース攻撃にも影響を与え、2022 年にはこの攻撃は急降下しました。この低迷の要因としては、戦争以外にも、リモートワークの減少、企業の IT 部門による設定や対策の改善、Windows 11 に組み込まれたブルートフォースブロックの新機能などが考えられる。2022 年に検出された RDP 攻撃のほとんどは、ロシアの IP アドレスから発信されています。

RDP 攻撃が減少したとはいえ、2022 年第 3 四半期のネットワーク攻撃ベクトルでは、パスワード推測が最も好まれていました。また、2021 年 12 月から Log4J の脆弱性の対策が行われているにもかかわらず、外部からの侵入ベクトルランキングで 2 位となりました。

一方では暗号通貨為替レートの急落、他方ではエネルギー価格の高騰により、様々な暗号脅威が影響を受けました。ESET 製品によってブロックされた暗号通貨をテーマにしたフィッシングサイトは、T3 に 62%増加し、FBI は最近、新たな暗号投資スキームの急増について警告を発しました。

12 月は、多くの祝日があるため、オンラインショップを装ったフィッシングが増加しました。これは、オンラインでプレゼントを購入する人々が、サイバー犯罪者にとって非常に有利なターゲットであるためです。また、モバイルゲーム開発者がクリスマスシーズン前に新作を発表すると、攻撃者は、その宣伝効果を利用して、改変した不正なバージョンをサードパーティのアプリストアにアップロードしました。その結果、2022 年の T3 では、Android アドウェアの検出数が大幅に増加していることが確認されています。

また、Android プラットフォームでは、様々なオンラインフォーラムで入手できるアクセスしやすいスパイウェアキットやアマチュア攻撃者が使用するスパイウェアが、年間を通じて増加しました。また、T3 および 2022 年全体では、インフォスティーラー全体の検出数は減少傾向にありましたが、バンキングマルウェアは例外で、前年比では検出数が倍増しています。

2022 年の最後の数ヶ月は、ESET の興味深い調査結果で賑わいました。ESET のリサーチャーは、日本の著名な政治団体を狙った MirrorFace のスピアフィッシング・キャンペーンや、ウクライナの複数の組織を標的とし、Sandworm の痕跡を残す RansomBoggs という新しいランサムウェアを発見しています。また、ESET の研究者は、悪名高い Lazarus グループが行った、偽の求人情報を記載したスピアフィッシング・メールで被害者を狙うキャンペーンも発見し

ています。サプライチェーン攻撃に関しては、ダイヤモンド産業で使用されているイスラエルのソフトウェア・スイートのユーザーを狙う、新たなワイパーとその実行ツールが発見されましたが、いずれも APT グループ「Agrius」によるものであるとしています。

いつものように、ESET の研究者は様々なカンファレンスで専門知識を共有する機会を複数設け、AVAR や Ekoparty などに出演し、前述の ESET Research の発見のほとんどについて技術的な側面を深く掘り下げて説明しました。今後数ヶ月間、Botconf や RSA Conference などでの ESET の講演にご招待させていただきます。洞察に満ちた読み物であることを祈っています。

Roman Kováč

リサーチ部門　最高責任者

エグゼクティブサマリー

特集記事

MirrorFace の仮面を剥ぐ。日本の政治団体を標的とした Operation LiberalFace ESET の研究者は、参議院選挙の数週間前に日本の政治団体を標的としたスピアフィッシングキャンペーンを発見し、その過程で、これまで知られていなかった MirrorFace のクレデンシャルステーラーを発見しました。

ESET Research Lab からの最新情報

RansomBoggs。ウクライナを標的とした新しいランサムウェア ESET の研究者は、ウクライナを標的とした新しいランサムウェア「RansomBoggs」を発見し、このキャンペーンは悪名高い APT グループ「Sandworm」と多くの特徴を共有していることを明らかにしました。

ファンタジーサプライチェーン攻撃で展開された Agrius の新型ワイパー ESET の研究者は、イスラエルのソフトウェア開発者を悪用し、ダイヤモンド業界を含む被害者に Agrius の新型ワイパー「Fantasy」を展開するサプライチェーン攻撃を分析しました。

統計と傾向

カテゴリー	T2 2022/ T3 2022	T3 2022 のキーポイント
全体的な脅威の検出数	-13.2% ↓	ほとんどの監視対象カテゴリで検知数が減少
情報窃取型マルウェア	-11.9% ↓	銀行業務用マルウェアの検出数が前年同期比で倍増
ランサムウェア	-1.9% ↓	ランサムウェアを模倣したワイパーがウクライナを狙う
ダウンローダー	-44.8% ↓	MSIL ダウンローダーがリード、Emotet はほぼ静観
暗号通貨の脅威	-24.8% ↓	暗号通貨マルウェアはさらに減少、詐欺が盛んに
ウェブに関する脅威	-10.0% ↓	暗号通貨をテーマにしたフィッシング詐欺が増加中
電子メールに関する脅威	-17.4% ↓	T3 の減少にもかかわらず、前年比 30%増
Android	+56.5% ↑	広告を利用した Android の脅威が大幅に増加
macOS	-5.5% ↓	PUA を除く検出カテゴリで減少
RDP 攻撃	-15.9% ↓	RDP 攻撃は 1 日平均 8900 万回で減少を維持

特集記事

MirrorFace の正体を暴く。日本の政治団体を標的とした「Operation LiberalFace

Dominik Breitenbacher

ESET の研究者は、参議院選挙の数週間前に日本の政治団体を標的としたスピアフィッシング・キャンペーンを発見し、その過程で、これまで知られていなかった MirrorFace の認証情報盗用ソフトを発見しました。

2022 年 7 月に行われる日本の参議院選挙[1]のわずか数週間前に、ESET リサーチャーは、その選挙の候補者を標的としたスピアフィッシング・キャンペーンに気づきました。ESET リサーチは、この活動を行った APT グループを MirrorFace と追跡し、このキャンペーンを Operation LiberalFace と名付けました。私たちの調査により、このキャンペーンでは特定の政党のメンバーが特に重視されていることが明らかになりました。

MirrorFace は、日本に拠点を置く企業や組織を標的とする中国語を話す脅威行為者です。この脅威者は APT10 に関連しているのではないかという憶測もありますが、ESET はこの脅威者を既知の APT グループに帰属させることができません。そのため、ESET では、この脅威を MirrorFace と名付けた別個の組織として追跡しています。特に、MirrorFace と、日本国内の標的のみに使用される同社独自のマルウェア「LODEINFO」は、メディア、防衛関連企業、シンクタンク、外交機関、学術機関などを標的としていることが報告されています[2]。MirrorFace の目的は、諜報活動や目的のファイルの流出です。

これらの指標から、Operation LiberalFace を MirrorFace と判断しています。

- 私たちの知る限り、LODEINFO マルウェアは MirrorFace によってのみ使用されています。
- リベラルフェイス作戦のターゲットは、従来のミラーフェイスのターゲットと一致している。
- 第 2 段階の LODEINFO マルウェアのサンプルは、MirrorFace のインフラの一部として内部で追跡している C&C サーバに接触しました。

Operation LiberalFace で送信されたスピアフィッシングメールの 1 通は、日本の特定の政党の広報部からの公式通信を装い、参議院選挙に関連するお願いが記載されており、著名な政治家の代理として送信されたとされています。MirrorFace は 2022 年 6 月 29 日に攻撃を開始しました。悪意のある添付ファイルを含むスピアフィッシングメールの件名は、<redacted>SNS 用動画 拡散のお願い（機械翻訳です。[重要】<redacted>SNS 用動画拡散のお願い)でした。）

この悪質なメールは、受信者に対し、党の PR をさらに強化し、選挙での勝利を勝ち取るために、添付された動画を自身のソーシャルメディアプロファイル（SNS - Social Network Service）で配信するよう求めていました。さらに、メールには、動画の公開戦略について明確な指示が記載されています。

2022 年 7 月 10 日に参議院選挙が行われたことから、このメールは MirrorFace が政治団体を攻撃する機会を伺っていたことを明確に示しています。また、メールの具体的な内容から、特定の政党の議員が狙われたことがわかります。

MirrorFace は、このキャンペーンで別のスピアフィッシングメールも使用しており、添付ファイルのタイトルは【参考】220628<redacted> 発・<redacted>選挙管理委員会宛文（添書分）.exe（機械翻訳）になっていました。[【参考】220628<redacted>省から<redacted>選挙管理委員会宛の文書（添書）.exe)。添付されたおとり文書は、参議院選挙にも言及しています。

ESET リサーチが分析したすべてのスピアフィッシングメールには、標的を欺き、良性に見せるためのデコイ文書を開く悪意のある添付ファイルが含まれており、さらに感染したマシン上に LODEINFO が展開されました。LODEINFO は、継続的に開発されている MirrorFace バックドアです。JPCERT/CC は、2019 年 12 月頃に登場した LODEINFO の最初のバージョン[3]（v0.1.2）について報告しており、その機能は、スクリーンショットのキャプチャ、キーロギング、プロセスの殺害、ファイルの流出、追加のファイルおよびコマンドの実行を可能にします。それ以降、その各バージョンに導入されたいくつかの変更が確認されています。

LODEINFO の検出に加えて、MirrorFace は、私たちが MirrorStealer と名付けた、これまで文書化されていないマルウェアを使用して、ターゲットの認証情報を盗んでいたことも発見しました。このマルウェアが公表されたのは、私たちの研究が初めてです。MirrorStealer は、ブラウザや電子メールクライアントなどの様々なアプリケーションから認証情報を盗み出します。興味深いことに、対象となるアプリケーションの 1 つは、Becky![4]は、現在、日本でのみ利用可能なメールクライアントです。MirrorStealer は、盗んだデータを流出させる機能を持っていないため、他のマルウェアに依存することになります。

MirrorFace のオペレータは、LODEINFO コマンドを使用して、侵害されたマシンの画面をキャプチャし、ネットワークに接続されているコンピュータのリストと、利用可能なドメインのリストを取得しました。また、LODEINFO は、MirrorStealer によって収集された認証情報、および被害者のブラウザクッキーを流出させるために使用されました。

また、様々な種類の文書や保存された電子メール（.eml ファイル）も、感染したマシンから流出しました。このオペレーターは、.doc*、.ppt*、.xls*、.*xps といった拡張子を持つファイルなど、一般的な文書タイプに興味を示していました。MirrorFace は、ジャストシステムが開発した日本語ワープロ「一太郎」[5]の文書である.jtd という拡張子を持つファイルにも興味を示していたことは重要なポイントです。

私たちが観察した最後のステップは、第 2 段階の LODEINFO を配信することでした。オペレータは、感染したマシンに複数のバイナリを配信し、そのうちの 1 つが JsSchHlp.exe でした。オリジナルの JsSchHlp.exe は、先に述べた日本語ワープロ一太郎のメーカーである JUSTSYSTEMS CORPORATION によって署名された良性のアプリケーションです。しかし、このケースでは、MirrorFace のオペレータは、マイクロソフトのデジタル署名検証の既知の問題[6]を悪用して、JsSchHlp.exe のデジタル署名に RC4 暗号データを付加していました。この問題のために、Windows は修正された JsSchHlp.exe を有効な署名であるとみなしています。

JsSchHlp.exe は、DLL の検索順序のハイジャックの影響を受ける可能性もあります。したがって、実行時に、侵害されたマシンに配信された DLL もロードされます。そして、この悪意のあるローダーは、JsSchHlp.exe から付加されたペイロードを読み取り、復号して実行します。このペイロードは、第 2 段階の LODEINFO ですが、オペレータは第 2 段階

の LODEINFO を C&C サーバと適切に通信させることができていないように見えます。そのため、第 2 段階の LODEINFO を利用した際の運営者のさらなる動きは不明なままです。

MirrorFace のオペレータは、対象マシン上で行われた特定の活動から、LODEINFO に対して手動または半手動でコマンドを発行しましたが、やや不注意な方法で、痕跡を残し、さまざまなミスを犯したと思われます。例えば、LODEINFO にコマンドを発行する際、いくつかのエラーやタイプミスがありました。

cmd /c dir "c:\use\"

を LODEINFO に変換するはずだった。

cmd /c dir "c:\users"

次の観察は、侵害の痕跡を除去するためにいくつかのクリーンアップを実行したにもかかわらず、盗まれた認証情報を含むログである %temp%31558.txt を削除するのを忘れていたことである。このように、少なくともこの痕跡は侵害されたマシンに残っており、オペレータがクリーンアッププロセスにおいて徹底していなかったことを示しています。

ESET リサーチは、12 月に開催された AVAR 2022 カンファレンス[7]で、このキャンペーンとその背後にいる APT グループに関する詳細を初めて明らかにしました。

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

Worok

Worok：全体像

ESET の研究者は、これまで知られていなかったサイバーレスポンスグループを発見し、Worok と命名しました。少なくとも 2020 年から活動しているこのグループは、主にアジアの様々な有名企業や地方自治体に対して標的型攻撃を実施しています。したがって、運営者の主な目的は情報窃盗であると考えられます。

Worok は、既存のツールを利用してターゲットを危険にさらすだけでなく、独自のツールも開発しています。その中には、CLRLoad と PNGLoad という 2 つのローダーや、PowHeartBeat というバックドアも含まれています。

CLRLoad は、2021 年に使用された C++で書かれた第一段階のローダーで、2022 年には、ほとんどの場合、PowHeartBeat に置き換えられました。PNGLoad は第 2 段階のローダーで、今回は C#で書かれており、PNG 画像に隠された悪意のあるペイロードを再構成するためにステガノグラフィーを使用します。

PowHeartBeat は、PowerShell で書かれたフル機能のバックドアで、圧縮、エンコード、暗号化などの様々な技術を使って難読化されています。このバックドアは、コマンド/プロセスの実行やファイル操作など、さまざまな機能を備えています。

WeLiveSecurity のブログ記事[9]。

SparklingGoblin

決して一人歩きはしない。バックドア「SideWalk」に Linux の亜種が登場

ESET リサーチは、APT グループ SparklingGoblin が使用する複数のカスタムインプラントの 1 つである SideWalk バックドアの Linux 亜種を発見しました。SparklingGoblin は、主に東アジアと東南アジアをターゲットにしており、特に学術分野に重点を置いています。

2021 年 2 月、SideWalk の Linux 版が、過去に SparklingGoblin の標的になっていた香港の大学に対して展開され、初めてその動作を確認しました。SideWalk Linux は、Windows 版とのいくつかの類似点と、いくつかの技術的な新しさを示しています。その共通点とは、カスタマイズされた ChaCha20 暗号化アルゴリズム、ソフトウェアアーキテクチャ、設定、デッドドロップ・リゾルバの実装などが同じであることです。Windows 版 SideWalk とは対照的に、Linux 版ではデバッグ用のシンボルが含まれており、一部の固有の認証キーやその他のアーティファクトが暗号化されていないため、検出と分析が非常に容易になっています。

WeLiveSecurity のブログ記事[10]。

APT-C-50

国内子猫キャンペーンが新マルウェア「FurBall」でイラン国民をスパイ活動

ESET の研究者は、APT-C-50 グループが行っている Domestic Kitten キャンペーンで使用されている Android マルウェア「FurBall」の新バージョンを確認しました。Domestic Kitten キャンペーンは、イラン国民に対してモバイル監視活動を行うことで知られており、この新しい FurBall バージョンもそのターゲットに変わりはありません。

この悪質な Android アプリケーションは、英語からペルシャ語に翻訳された記事や書籍を提供する正規のサイトを模倣した偽サイトを介して配信されます。模倣サイトの目的は、ペルシャ語で「アプリケーションをダウンロードしてください」と書かれたボタンをクリックした後に、Android アプリケーションをダウンロードできるようにすることです。ボタンには Google Play のロゴがありますが、このアプリは Google Play ストアから入手できるものではなく、攻撃者のサーバーから直接ダウンロードされるものです。

このバージョンの FurBall は、以前のバージョンと同じ監視機能を備えていますが、脅威の主体がクラス名とメソッド名、文字列、ログ、およびサーバー URI をわずかに難読化しました。この亜種の機能は変わっていないため、このアップデートの主な目的は、セキュリティソフトウェアによる検出を回避することにあるようです。このマルウェアは、連絡先へのアクセスというたった 1 つの侵入許可を要求していますが、これは、インストールプロセス中に潜在的な被害者の疑いを引き付けず、レーダーを潜り抜けるためと思われます。また、これは、テキストメッセージによるスピアフィッシングに続く連絡先収集の第一段階である可能性もあります。

WeLiveSecurity のブログ記事[11]。

Bahamut

サイバー傭兵集団「Bahamut」、偽の VPN アプリで Android ユーザーを標的にする

ESET の研究者は、Bahamut APT グループが実施した、Android ユーザーを対象としたキャンペーンを発見しました。2022 年 1 月から活動しているこのキャンペーンは、偽の Secure VPN ウェブサイトを通じて、2 つの正規 VPN アプリのトロイの木馬化したバージョンを配布していました。私たちは、少なくとも 8 つのバージョンの Bahamut スパイウェアを発見しました。

このマルウェアは、連絡先、SMS メッセージ、通話ログ、デバイスの位置情報、録音された電話など、機密データを流出させることが可能です。また、Signal、Viber、WhatsApp、Telegram、Facebook Messenger などの非常に人気の高いメッセージングアプリでやり取りされるチャットメッセージも積極的にスパイすることが可能です。

スパイウェアのコード、つまりその機能は、これまでの Bahamut Android のキャンペーンと同じであることがわかりました。その中には、ローカルデータベースにデータを収集してからオペレーターのサーバーにデータを流出させるという、モバイルサイバースパイパーアプリではほとんど見られない戦術が含まれています。

このキャンペーンは目立たないようにしています。ウェブサイトの URL は、潜在的な被害者にアクティベーション・キーとともに届けられる可能性が高いのですが、ウェブサイトでは提供されていないのです。残念ながら、私たちは有効なキーを入手することができませんでした。さらに、私たちの遠隔測定データでは、このキャンペーンのインスタンスを確認していないため、このキャンペーンは高度に標的化されていると考えています。

WeLiveSecurity のブログ記事[12]。

ScarCruft

韓国海域を泳ぐのは誰？ScarCruft のイルカに会いに行こう

ESET リサーチチームは、主に韓国の政府機関や軍事組織を対象とする APT グループである ScarCruft が使用する、これまで報告されていないバックドアを分析しました。Dolphin と名付けたこのバックドアは、ドライブやポータブルデバイスの監視、目的のファイルの流出、キーロギングやスクリーンショットの取得、ブラウザからの認証情報の窃取など、幅広いスパイ機能を備えています。

2021 年、ScarCruft は、北朝鮮に焦点を当てた韓国のオンライン新聞サイトをホストとする水飲み場攻撃を実施しました。被害者は複数のコンポーネントで侵害され、その中には BLUELIGHT と名付けられたバックドア（Volexity [13]と Kaspersky [14]が報告）が含まれていました。当時、BLUELIGHT はこの攻撃の最終的なペイロードであると考えられていましたが、私たちは、BLUELIGHT を介して特定の被害者に展開された、より洗練された別のバックドアを発見しました。このバックドアは、実行ファイルに含まれる PDB パスのテキストに基づき、Dolphin と名付けられました。

Dolphin は、選択されたターゲットに展開された後、侵害されたシステムのドライブを検索し、興味深いファイルを Google Drive に流出させます。Dolphin の以前のバージョンで見つかった 1 つの珍しい機能は、被害者の Google と Gmail アカウントの設定を変更してセキュリティを低下させる機能で、おそらく脅威者の Gmail アカウントへのアクセスを維持するためと思われます。

WeLiveSecurity のブログ記事[15]。

Lazarus

オランダとベルギーで Amazon をテーマにした Lazarus キャンペーンを実施

ESET リサーチは、Lazarus APT グループがオランダとベルギーのターゲットに対するスピアフィッシングキャンペーンで使用した悪意のあるツール一式を分析しました。2021 年後半に行われたこのキャンペーンは、オランダの航空宇宙企業の従業員とベルギーの政治ジャーナリストを対象に、Amazon をテーマにした悪質な文書を含むスピアフィッシングメールを送信していました。

オランダの社員は LinkedIn Messaging 経由で、ベルギーのジャーナリストは電子メールで、それぞれ仕事の依頼を受けました。攻撃は、これらの文書が開かれた後に開始されました。ドロッパー、ローダー、HTTP（S）バックドア、HTTP（S）アップローダーなど、複数の悪意のあるツールがシステム上に配置されました。

攻撃者が配信した最も注目すべきツールは、Dell の正規ドライバの脆弱性 CVE-2021-21551 を悪用したことにより、カーネルメモリを読み書きする能力を獲得したユーザーモードモジュールでした。この脆弱性は Dell DBUtil ドライバに影響し、Dell は 2021 年 5 月にセキュリティアップデートを提供しています。本脆弱性の悪用は、これまでで初めて記録されたものです。

WeLiveSecurity のブログ記事[16]。

POLONIUM

POLONIUM、イスラエルを標的にした不気味なマルウェアを公開

ESET の研究者は、POLONIUM APT グループがイスラエルで展開した、これまで文書化されていなかったカスタムバックドアとサイバースパイラルツールを分析しました。POLONIUM は、2022 年 6 月に Microsoft [17]によって初めて文書化されたサイバースパイグループです。マイクロソフトによると、このグループはレバノンに拠点を置き、イランの情報セキュリティ省に所属する他のアクターと活動を連携させています。

POLONIUM のツールセットは、7 つのカスタムバックドアーで構成されています。OneDrive と Dropbox のクラウドサービスを悪用して C&C を行う CreepyDrive、攻撃者自身のインフラから受け取ったコマンドを実行する CreepySnail、Dropbox と Mega ファイルストレージサービスをそれぞれ利用する DeepCreep と MegaCreep、攻撃者のサーバーからコマンドを受信する FlipCreep、TechnoCreep、PapaCreep の計 7 つのカスタムバックドアが搭載されています。また、スクリーンショットの撮影、キーストロークの記録、ウェブカメラ経由のスパイ、リバースシェルのオープン、ファイルの流出など、ターゲットをスパイするためのカスタムモジュールも複数開発されているとのことです。

POLONIUM がカスタムツールに導入した多数のバージョンと変更は、グループのターゲットをスパイするための継続的かつ長期的な努力を示しています。そのツールセットから、POLONIUM が機密データの収集に関心を持っていることが推測されます。このグループは、破壊工作やランサムウェアのような行為には関与していないようです。

WeLiveSecurity のブログ記事[18]。

Sandworm

RansomBoggs ウクライナを標的とした新たなランサムウェア

ESET の研究者は、ウクライナの複数の組織を標的としたランサムウェア攻撃の新風を発見し、そのキャンペーンは APT グループ「Sandworm」と多くの特徴を共有していることを明らかにしました。私たちは、.NET フレームワークで開発

されたこのマルウェアを「RansomBoggs」と名付けました。このマルウェアは新しいものですが、その展開方法は、Sandworm に起因するとされる過去のいくつかの攻撃と酷似しています。

RansomBoggs が被害者のマシンに侵入すると、ランダムな鍵を生成し、CBC モードの AES-256 を使ってファイルを暗号化し、暗号化されたファイルに.chsch の拡張子を付けます。その後、鍵は RSA 暗号化され、aes.bin に書き込まれます。オペレータはデータ復号と引き換えに金銭を要求していないため、これはファイルコーダがワイパーとして使用されているケースである。

RansomBoggs は、Sandworm が実行したウクライナの CaddyWiper と Industroyer2 の両攻撃で使用されたものとほぼ同じ PowerShell スクリプトを介して、被害者のドメインコントローラから配布されました。

WeLiveSecurity のブログ記事[19]。

ツイッターのスレッド[20]

Agrius

ファンタジー：サプライチェーン攻撃で展開される新型 Agrius ワイパー

ESET リサーチは、Agrius APT グループに起因する新たなワイパーとその実行ツールを発見しました。私たちは、Agrius のオペレーターが、イスラエルのソフトウェア開発者を悪用して、同グループの新しいワイパー「Fantasy」と、新しい横移動および Fantasy 実行ツール「Sandals」を展開するサプライチェーン攻撃を行ったと確信しています。Fantasy は、南アフリカ、イスラエル、香港の被害者を標的としていました。

このキャンペーンで、Agrius はまず南アフリカのダイヤモンド産業の組織にクレデンシャル・ハーベスティング・ツールを配備しました。数週間後、Fantasy と Sandals を使用したワイプ攻撃を開始し、まず南アフリカのターゲットを攻撃し、イスラエルのターゲットに続き、香港で終了しました。このキャンペーンは 3 時間以内に終了し、ESET の顧客はその時間内に Fantasy をワイパーとして識別し、その実行をブロックする検知によって既に保護されていました。

Sandals は、C#/.NET で書かれた 32 ビット Windows 実行ファイルで、SMB 経由で同じネットワーク内のシステムに接続し、Fantasy wiper を実行するバッチファイルをディスクに書き込み、PsExec 経由でそのバッチファイルを実行するために使用します。

Fantasy ワイパーも C#/.NET で書かれた 32 ビット Windows 実行ファイルで、それぞれ fantasy45.exe と fantasy35.exe というファイル名からその名が付けられています。これは、ランサムウェアとして書き換えられる前に、当初ランサムウェアを装っていた以前の Agrius ワイパー、Apostle と多くの点で類似しています。Fantasy はランサムウェアとして偽装する努力をしません。

WeLiveSecurity のブログ記事[21]。

統計と傾向

ESET テレメトリから見る 2022 年の T3 における脅威の状況

脅威環境の概要

T3 2022 年の脅威動向のまとめ。

2022 年第 3 四半期は、第 2 四半期と同様に、脅威の全体的な減少が見られました。ESET 遠隔測定では、脅威の検出数が全体で 13.2%減少し、トレンドチャートでは、HTML/Phishing.Agent のアクティビティの増加により、9 月 14 日にわずか 1 つのスパイクが発生したことが確認されました。しかし、1 年を通してのデータでは、一時的な数の減少が見られたかもしれませんが、実際には総検出数は前年比 13%増となり、増加したことが明らかになっています。

T3 でも、あるカテゴリーが隆盛を極めた。Android カテゴリは、検出数で 57%という著しい成長を記録しました。これは、アドウェアの検出数が 163%増加し、HiddenApps の検出数が 83%増加したことによります。

他のいくつかのカテゴリでは、脅威全体の検出数と同様の現象が見られ、これらのカテゴリの検出数は T3 では減少しているものの、年々増加を記録しています。例えば、「ダウンローダ」カテゴリーは、2021 年から 2022 年の間に 71%の伸びを示しました。一方、Emotet の検出数は、日本でのキャンペーンと新しい情報収集モジュールの追加を除けば、T3 で 84% の急減を記録し、大幅に減少しています。

同様に、T3 ではインフォステーラーの検出数が 12%減少しましたが、バンキングマルウェアの検出数は 1 年間成長を続け、2021 年から 2022 年にかけて 100%以上増加しました。

エモテに話を戻すと、2022 年の T1 で大規模なキャンペーンを行った結果、T3 では 17%減少した電子メールの脅威が前年比 30%増加しました。

2021 年から 2022 年にかけて、Web 脅威全体の検出数は 10.6%減少したにもかかわらず、そのフィッシングのサブカテゴリーは T3 において唯一成長し、フィッシングサイトのブロック数は T2 比で 115%も増加したのです。

macOS カテゴリでは、ESET 遠隔測定は 5.5%の微減にとどまりました。Potentially unwanted applications (PUAs) は、これらの検出の 52%を占め、T2 と比較して 3%増加しました。

ランサムウェアの検出数に関しては、年々増加することはなく、2021 年から 2022 年にかけて 20%減少しています。しかし、2022 年 T3 には、Azov ランサムウェア、Somnia ワイパー、CryWiper など、ロシア・ウクライナ戦争に関連したランサムウェアを模倣したワイパーの利用が増加しました。

エクスプロイトのカテゴリでは、2021 年に賑わいを見せた RDP パスワード推測攻撃が、2022 年には 49%減少しています。攻撃試行の 1 日平均は、T1 では 10 億件前後で推移していましたが、T3 では約 1 億件に急減しています。一方、SQL 攻撃は、T3 に 9%増加し、逆転した。

現在では予想されているように、暗号通貨脅威の検出数は減少の一途をたどり、2021 年から 2022 年にかけて 45%も減少しました。クライムウェアの割合が減少する一方で、暗号通貨関連の詐欺は増加傾向にありました。

IoT セキュリティの脅威の分野では、Mozi ボットネットに新たに加わったボット数が 25%減少し、ZHtrap ボットネットが突然死し、Mirai ベースのボットは 11%増加しましたが、攻撃の検出数は 6%減少しています。

いくつかの順位が入れ替わっただけで、マルウェア検出数トップ 10 に劇的な変化はありませんでした。HTML/Phishing.Agent は、T3 でも 2022 年全体でもトップに君臨しています。T3 では、HTML/Phishing.Outlook が 9 位から 16 位に転落し、最も多く検出されたプログラムから外れることになりました。また、T2 で 14 位だった DOC/Fraud トロイの木馬が 6 位に上昇し、空席となったリストを占めた。

全世界で検出されたマルウェアトップ 10

HTML/Phishing.Agent トロイの木馬

HTML/Phishing.Agent は、フィッシングメールの添付ファイルによく使用される悪意のある HTML コードの検出名です。実行形式の添付ファイルは通常、自動的にブロックされたり、疑いを持たれやすいため、攻撃者は他のファイル形式ではなく、これを使用する傾向があります。このような添付ファイルを開くと、ウェブブラウザ上で銀行や決済サービス、ソーシャルネットワークの公式サイトなどを装ったフィッシングサイトが開かれます。このウェブサイトは、認証情報やその他の機密情報を要求し、攻撃者に送信します。

Win/Exploit.CVE-2017-11882 トロイの木馬

この検出名は、Microsoft Office のコンポーネントである Microsoft Equation Editor に見つかった脆弱性 CVE-2017-11882[22]を悪用した特別に細工されたドキュメントを表しています。このエクスプロイトは一般に公開されており、通常、侵害の第一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、エクスプロイトが起動され、そのシェルコードが実行されます。その後、追加のマルウェアがコンピュータにダウンロードされ、任意の悪意あるアクションが実行されます。

HTML/Phishing トロイの木馬

HTML/Phishing トロイの木馬は、電子メールや電子メールの添付ファイル内の悪意のある URL のスキャンに基づいて収集された一般的なマルウェアの検出を表します。電子メールまたはその添付ファイルにブロックリストされた URL が含まれている場合、HTML/Phishing.Gen の検出がトリガーされます。

MSIL/TrojanDownloader.Agent トロイの木馬

MSIL/TrojanDownloader.Agent は、Windows プラットフォーム向けに書かれ、.NET Framework を使用する悪質なソフトウェアの検出名です。このマルウェアは、さまざまな方法を使用して他のマルウェアをダウンロードしようとします。

通常、最終的なペイロードにつながる URL または URL のリストが含まれています。このマルウェアは、より複雑なパッケージの最初の層として機能し、被害者のシステムへのインストールを担当することがよくあります。

JS/Agent トロイの木馬

この検出名は、様々な悪意のある JavaScript ファイルを対象としています。これらは、静的な検出を避けるために、しばしば難読化されています。これらは通常、訪問者のドライブバイ・プロテクションを達成する目的で、侵害された、しかしそれ以外は正当な Web サイトに配置されます。

DOC/Fraud トロイの木馬

DOC/Fraud の検出は、主に電子メールの添付ファイルを通じて配布される、さまざまな種類の不正なコンテンツを含む Microsoft Word ドキュメントを対象としています。この脅威の目的は、例えば、被害者に認証情報や機密データを開示するよう説得することで、被害者の関与から利益を得ることです。受信者は、宝くじの当選や非常に有利な融資の申し出があったかのように騙されるかもしれません。この文書には、被害者が個人情報を入力するよう求められる Web サイトへのリンクが含まれていることがよくあります。

DOC/TrojanDownloader.Agent トロイの木馬

この分類は、インターネットからさらにマルウェアをダウンロードする悪意のある Microsoft Office ドキュメントを表します。この文書は、請求書、フォーム、法的文書、またはその他の一見重要な情報に偽装されていることがよくあります。また、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たり、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に受信者の注意をそらすためのおとり文書として機能することもあります。

LNK/Agent トロイの木馬

LNK/Agent は、Windows の LNK ショートカットファイルを利用して、システム上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、良性とみなされ、疑いを持たれる可能性が低いため、攻撃者の間で人気があります。LNK/Agent ファイルは、ペイロードを含まず、通常、より複雑な他のマルウェアの一部となっています。LNK/Agent は、システム上の主要な悪意のあるファイルの永続性を実現するため、または侵害ベクターの一部として使用されることがよくあります。

HTML/ Fraud トロイの木馬

HTML/詐欺の検出は、被害者を巻き込んで金銭やその他の利益を得る目的で配布される、さまざまな種類の HTML ベースの詐欺的なコンテンツを対象としています。これには、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が含まれます。このようなメールでは、受信者が宝くじの当選に騙され、その後、個人情報の提供を要求されることがあります。もうひとつよくあるのが、「419 詐欺」としても知られる悪名高いナイジェリア王子詐欺など、いわゆる前金詐欺 [23]である。

VBA/TrojanDownloader.Agent トロイの木馬

VBA/TrojanDownloader.Agent は、通常、ユーザーを操作してマクロの実行を可能にしようとする、悪意を持って細工された Microsoft Office ファイルを対象とした検出です。実行されると、同梱の悪意のあるマクロは、通常、追加のマルウェアをダウンロードし、実行されます。悪意のある文書は、通常、受信者に関連する重要な情報を装って、電子メールの添付ファイルとして送信されます。

情報窃取型マルウェア

2022 年、バンキングマルウェアの検出数が倍増。

2022 年の T3 テレメトリーデータは、ほとんどのモニターカテゴリーで減少していることが特徴です。インフォスティーラーも例外ではなく、T3 では 12%近く減少し、2022 年全体では 2021 年に比べて 10%近く減少しています。インフォスティーラーは、T3 期間中、緩やかではありますが、着実に減少しており、劇的な検出の急増や減少は見受けられませんでした。

Infostealer のサブカテゴリの中で、この報告期間中に減少が見られなかったのはバンキングマルウェアで、T3 の数字は T2 の数字とほぼ同じでした。それでも、前年比の検出数は 2 倍以上、107%も増加しています。

この現象は、Magecart としても知られる Web スキマーJS/Spy.Banker の蔓延によって引き起こされました。このマルウェアは、2022 年に検出されたバンキングマルウェアの圧倒的多数を占めました。年間を通じて、このマルウェアファミリは、バンキングマルウェアの検出数の約 4 分の 3 を一貫して占めています。また、JS/Spy.Banker は、T3（9.5%）と 2022 年全体（8%）の両方で、最も検出された情報窃盗犯の第 3 位となり、情報窃盗犯全体のトップ 10 に入った唯一のバンキングマルウェアとなりました。ただし、ハッキングされた Web サイトに潜むこのオンラインスクリプトの検出は、当該 Web サイトへのユニークビジット数に基づいているため、遠隔測定では、ダウンローダーや電子メールの添付ファイルとして配布される他のほとんどの Infostealer カテゴリのマルウェアよりもはるかに高い値を示す可能性があることに注意する必要があります。

2 位の Win/ClipBanker は 8.6%増で、2022 年 T3 に ESET テレメトリーが登録したバンキングマルウェアの 4.7%を占めた。

バンキングマルウェアとして 3 番目に多く検出されたのは、中南米のバンキング型トロイの木馬「Grandoreiro」で、バンキングマルウェアの検出数の 4%を占めています。JS/Spy.Banker などと比較すると、この割合はそれほど印象的ではないかもしれませんが、Win/Spy.Grandoreiro は 2022 年に大きく成長し、2021 年と比較してその数はほぼ 6 倍になっています。T3 では、ラテンアメリカ以外の地域でも拡大を続けており、検出数の大部分はスペインからもたらされています。

LATAM のバンキング型トロイの木馬[24]といえば、その多くがかなり好調な年末を迎えています。Grandoreiro だけでなく、Casbaneiro、Mispadu、Mekotio といった他のいくつかのトロイの木馬の検出が、2022 年の 11 月と 12 月に急増しました。これらのトロイの木馬の中で最も流行しているスクリプトから Delphi ダウンローダーへの移行が見られ、検

出回避を向上させるためと思われます。Delphi 実行ファイルを使用する場合、脅威者は VMProtect と Themida を多用し、通常非常にシンプルでカスタムメイドのスクリプト難読化に比べ、非常に優れたコード保護を提供します。

銀行業務用マルウェアは、T3 で減少しなかった唯一の Infostealer サブカテゴリでしたが、Cryptostealer サブカテゴリは、48.7%と最も減少したカテゴリとなりました。これは、詐欺やフィッシングとは対照的に、「伝統的な」暗号通貨関連のクライムウェアの脅威が継続的に減少していることをさらに際立たせています。

T2 2022 年にテレメトリーに登場した PowerShell/PSW.Coinstealer は、T3 では 31.5%で最も検出されたクリプトステーラーとなることに成功した。Win/PSW.Delf は 24.5%で 2 位、Win/Spy.Agent は 22.2%で 3 位となりました。Cryptostealer に関する詳しい情報は、暗号通貨の脅威のセクションでご覧いただけます。

テレメトリーで Infostealer の大部分を占める Spyware サブカテゴリーは、T3 では 14.3%減と減少傾向が続いています。その 2022 年の検出数も 2021 年に比べて減少し、合計で 15%減少しています。

スパイウェアは、その数は減少したものの、特にそのファミリーの多くがオンラインですぐに利用できることから、非常に一般的なマルウェアの一種として存続しています。私たちの遠隔測定では、MSIL/Spy.AgentTesla として知られている悪名高い Agent Tesla は、広く利用されている唯一のスパイウェアではありません。最近では、これらのファミリのもう 1 つである RedLine Stealer が何度もニュースを賑わせています。9 月には、このマルウェアが、ビデオゲーム出版社の 2K Games を襲い、悪質な実行ファイルを含む偽のサポートメールを同社の顧客に送りつけたことが報告されました[25]。また、ゲームに関連した別のキャンペーン[26]では、RedLine は、YouTube の悪質な動画を通じて自己拡散する不正プログラムのバンドルに含まれており、「ファイナルファンタジー」、「FIFA」、「レゴスターウォーズ」といったゲームのファンを狙っていました。遠隔測定データによると、RedLine が検出されたのは、ペルー、ポーランド、トルコの 3 カ国が中心でした。

スパイウェアの検出数は、T3 期間の初めの 9 月 6 日にピークを迎え、トルコとチェコ共和国において攻撃の試行回数が増加したことが記録されています。Win/Spy.Weecnaw は、リモートアクセス型のトロイの木馬で、T3 期間中に 151.4%増加し、大きな伸びを記録しています。このトロイの木馬の L バージョンは、PDF の請求書ドキュメントを装った実行ファイルとして電子メールで配布されていました。

2022 年全体と同様に、T3 で最も多くの検出数を記録した 2 つのスパイウェアファミリーは、通常の容疑者であった。MSIL/Spy.AgentTesla」と「Win/Formbook」です。また、T3 と 2022 年の両方で、最も多く検出された情報窃盗犯でもあります。Agent Tesla は、T3 でスパイウェアの 26.1%（情報窃盗犯の 15.7%）を占め、Win/Formbook トロイの木馬は、スパイウェアの 16.7%（情報窃盗犯の 10%）に相当しました。この 2 つのファミリーは、年間を通じて検出数が減少する傾向にありました。

T2、T3 での減少を見ると、Agent Tesla の時代は終わったと言いたくなりますが、長期的なトレンドは全体的にほぼ安定しています。一時的に検出数が減少したのは、配布ベクトルが変化したためと考えられます。

スパイウェアの 3 位とインフォスティーラの 4 位は、MSIL/Spy.Agent で、スパイウェアの 11.3%、インフォスティーラの 6.8%が検出された。このマルウェアファミリーは、T3 でも減少傾向にあり、T2 と比較して 24%減少しています。

バックドアは、インフォステーラの検出数の 28% 以上を占めていたが、2022 年第 3 四半期には 9.6% 減少し、そのトレンドチャートには顕著な上昇は見られなかった。バックドアの前年比減少率は、14.3%に対して 13%と、スパイウェアの減少率より若干低いものの、ほぼ同じでした。

T3 で infostealer のトップ 10 に入ることができたバックドア・ファミリーは 3 つだけでした。その中で最も順位が高かったのは PHP/Webshell で 5.4%（バックドアでは 18.4%）でした。T3 では検出数が 5.8%減少したにもかかわらず、2022 年には 2021 年よりも 7.6%も検出数が増えています。6.2%で 2 番目に検出数の多いバックドアファミリの ASP/Webshell は、T3、2022 年ともにそれぞれ 15.6%、27%減少しています。T3 では、1.8%でインフォステアトップ 10 全体の 8 位ということでした。

インフォステアトップ 10 では 1.5%、バックドアトップ 3 では 5.2%の検出率で、いずれも締め切られました。Win32/Rescoms.B の亜種は、10 月 24 日に急増し、その攻撃のほとんどはトルコで捕捉されました。

2022 年 T3 に最も多くの infostealer 攻撃試行を登録した国は、6%の米国で、僅差で 5.9%のスペイン、5.8%の日本が続いています。2022 年全体のデータを考慮した場合、不戦勝はスペイン（6.6%）、2 位は日本（6.5%）、3 位はトルコ（6.4%）となっています。

トレンドと展望

Agent Tesla、Magecart、Fareit、Formbook などのマルウェアは、2023 年においても好調を維持すると思われます。これらのマルウェアはすべて、利益を得るために製品を更新し続けることに強い意欲を持つ作者による、高度な情報窃盗に分類されます。これらのアプリケーションの中核は、多かれ少なかれ安定しており、その開発の中心は、新しく高度なコード難読化および検出回避技術であり、この傾向は今後も続くと思われます。

Agent Tesla や Fareit のようなスパイウェアは、成功の確率を上げるために、できるだけ多く伝播しようとします。しかし、銀行業務用マルウェアに関しては、多要素認証やその他の金融取引の安全確保手段により、銀行口座から直接お金を盗むことが難しくなっているため、今後もその成長が続くとは限りません。サイバー犯罪者は、暗号窃盗の方が簡単であり、取引の追跡も困難であるため、暗号窃盗に頼るかもしれません。しかし、暗号通貨市場のボラティリティが高いため、こうした試みが実を結ぶかどうかは未知数です。

ESET 脅威検出担当ディレクター Jiří Kropáč

ランサムウェア

検出数が停滞する中、ロシア・ウクライナ戦争に関連して、ランサムウェアを模倣したワイパーが複数出現しました。

ここ数年、ランサムウェアはその収益性の高さから広まりました。しかし、ロシアのウクライナ侵攻は、その破壊的な可能性をも浮き彫りにしました。紛争双方の脅威者がランサムウェアの亜種を使用して敵対組織を攻撃し、復号化キーを提供する意思のない暗号化によってデータを効果的に消去したためです。

2022 年 T3 月、いくつかの新種が、この「ランサムウェアを模倣したワイパー」のカテゴリーに当てはまるか、少なくともその端に位置するものであった。10 月には、「Azov Ransomware」[27]と呼ばれるワイパーが拡散を開始しました。このソフトウェアは、一度に 666 バイトのデータチャンクを上書きし、回復の見込みがない状態にします。また、Azov は、発見された 64 ビット実行ファイルのほとんどをバックドアし、さらに拡散される危険性を高めています。身代金要求文の中で、作成者はウクライナに対する欧米の支援の欠如を批判し、欧米の人々に抗議活動を始めるよう求める政治的メッセージを送っていますが、それでもこのマルウェアはロシアの組織を標的にしていないため、偽旗作戦である可能性があります。

11 月には、ウクライナの複数の組織が Somnia wiper に感染しました[28]。CERT-UA は、このマルウェアを「From Russia with Love」として知られるグループの仕業であるとしています。この見解は、Somnia の第一段階の実行ファイルが投下した画像に、グループ名と、隣国に対するロシアの侵略の象徴として有名な「Z」の文字が表示されていることからも裏付けられます。

12 月、おそらく Somnia 攻撃の報復として、ロシアの政府機関や裁判所に向けて CryWiper [29]が起動し、そのデータとシステムを破壊しました。CryWiper は、戦争勃発後、ロシアを標的とした破壊的なマルウェアとしては、2022 年 3 月の RURansom [30]を唯一の前身とし、2 番目のものです。

ESET の調査では、T3 2022 年にウクライナの組織を標的とした RansomBoggs [20]という新しい.NET ランサムウェアも見つかっています。これは、初期のバージョンでは復号化機能を備えていたものの、それが呼び出されていなかったため、ワイパー・カテゴリの端に位置するものでした。しかし、作者は後にこの機能を追加しましたが、特に冷酷なロシア系 APT グループである Sandworm に起因することから、このマルウェアの被害者がこのマルウェアの作者によって救済される可能性は低いことが示唆されます。この帰属は、RansomBoggs と Sandworm の初期のマルウェア CaddyWiper [31]の配布に使用された、ほぼ同一の POWERGAP PowerShell スクリプトに基づいており、どちらも Active Directory Group Policy [32] を介して展開されます。

このカテゴリに属する別のマルウェアである Prestige ランサムウェアは、ESET の最新の APT Activity Report [33]でも言及されているように、ウクライナとポーランドの物流会社を標的として検出されています。

ランサムウェアの一般的な傾向として、T3 では検出数が安定しており、T2 2022 年と比較して 2%しか減少していない。前年比の検出数の傾向はかなりダイナミックで、2021 年から 2022 年の間に 20%も減少しています。国際的な法執行機関の協力と活動の増加、ウクライナ戦争による混乱、身代金の支払いを制限する規制の強化など、いくつかの要因が考えられますので、攻撃者の金銭的リターンを減少させることができました。

2022 年 T3 の地理的分布を見ると、中国が最も多く、次いで米国、ロシア、ウクライナ、日本となっています。ただし、年間データでは、2022 年のランサムウェア攻撃全体のうち、ロシアが 8%でトップ、米国が 7%未満で続き、4 位のウクライナは 4%未満となっています。

T3 2022 年のトップ 10 を見ると、特に注目すべき株は Win/Filecoder.STOP と Win/Filecoder.Hive である。前者は 9 月 20 日と 11 月 3 日に複数の国で同時にスパイクし、後者は 9 月 1 日にナミビアと米国の組織への侵入を試み、11 月 3 日には米国を狙いました。遠隔測定で最後に急増したランサムウェアは、11 月 29 日にペルーで発生した Win/Filecoder.AvosLocker による攻撃の試みによるものです。

T3 2022 では、公開されている HiddenTear コードをベースにした MSIL/Filecoder の亜種が大量に発生しました。これらは通常、クリーンなソフトウェアに注入されます。AGP 亜種の場合も同様で、作者はコードの不正な目的を隠すために古典的なスネークビデオゲームを使用しました。

しかし、2022 年のこの 4 ヶ月間、一部のランサムウェアの被害者に朗報ももたらされました。LockerGoga [34]、RanHassan [35]、Zeppelin [36]の各ランサムウェアに感染した人々は、現在、すべて自由に復号化できるようになりました。オランダの警察は、民間企業のパートナーとともに、Deadbolt として知られる NAS を標的としたギャングを騙し[37]、復号化キーを手渡させ、この犯罪を当局に報告したオランダの被害者の 90%にものぼる人々を支援したのです。

T3 2022 年には、複数のランサムウェアの関連会社が逮捕されました。REvil ギャングのウクライナの関係者が拘束され、Kaseya のケースを含むいくつかの攻撃への関与で起訴されました[38]。また、このグループとつながりのある他の 2 人の関係者もルーマニアで逮捕されました。また、LockBit ギャングとつながりのあるロシア系カナダ人の逮捕にも成功しました[39]。カナダで逮捕され、米国に送還されたネットウォーカーの関係者[40]のケースでは、今後 20 年間刑務所に収監される判決が下されています。

復号化ツールや法執行機関の活動が活発化しているにもかかわらず、ランサムウェアは、犯罪者にとって金銭的に魅力的なモデルであることに変わりはありません。CISA が発表した Cuba [41]と Hive [42]のランサムウェア運営者への身代金支払額の推定値は、前者では 101 人の被害者から 6000 万ドル、後者では 1300 人の被害者から 1 億ドルにも達しています。

米国金融犯罪取締ネットワーク（FinCEN）は、2021 年の統計を調べた報告書[43]を発表し、1200 件以上のランサムウェア関連の事件が記録され、8 億 8600 万米ドルの被害があったことを明らかにしました。また、そのデータ分析によると、記録された攻撃の 75%は、ロシア、そのプロキシ、またはその代理で行動する人物との関連性があることが示されています。

高額な収入を得る可能性のあるランサムウェアは、犯罪者を引きつける磁石のように作用し、2022 年の T3 には、数多くの新しいランサムウェア・ファミリーを立ち上げるに至ったのです。このリストには、Linux 版の DarkAngels [44]、Conti の二重人格者 MONTI [45]、DagonLocker という MountLocker の新しい亜種 [46]、Vohuk、ScareCrow、AERST [47]が含まれています。

ランサムウェアのトレンドに関して、T3 2022 では、注目すべき点がいくつかありました。このプロセスは、対象となるファイルの一部にのみ影響を与え、復号器と復号化キーがなければ復元できないようにします。この変更の理由は、暗号化プロセスを高速化し、検出と防止のための窓を縮小するためです。

APT の世界では、他の脅威者や国を指し示す偽の証拠を仕込むことは、目新しいことではありません。しかし、犯罪ソフトの分野では、このアプローチはそれほど頻繁ではありません。Yanlouwang ランサムウェア[49]の流出した通信を調査したところ、この犯罪の詳細が判明し、さらにその運営者がこれまで考えられていた中国系ではなく、ロシア系であることを証明することができました。

過去のレポートでは、ロシアの組織を標的にし、高額な身代金を強要することに躊躇しない数少ないランサムウェア集団、OldGremlin [50]について紹介しました。このグループによる複数の業界へのさらなる攻撃は、2022 年を通して記録されており、1690 万米ドルという身代金強奪の新記録を打ち立てました。

トレンドと展望

2022 年のロシアのウクライナ侵攻は、ランサムウェアのアクターたちを侵略の支持者と反対者に二分し、楔を打ち込むことになりました。この対立は、場合によっては一味のソースコードや私的な会話を含む壊滅的な情報漏えいにつながった一方で、攻撃者たちがますます攻撃的な手法を展開し、犠牲者を侮辱し、時にはデータを破壊する動機にもなりました。

しかし、このようなイデオロギー的な戦いは、日々のランサムウェアの開発にあまり影響を与えなかった。ほとんどの脅威者は、二重の恐喝スキームを継続し、身代金を支払う余裕のある企業や組織を危険にさらしました。一般ユーザは、NAS デバイスの所有者を唯一の例外として、ランサムウェアのシーンにほとんど関心を持たないままでした。素人のランサムウェアについては、2022 年に多発し、その大部分は Python で書かれていました。

2023 年、飽和状態にあるランサムウェアは、イデオロギーの違いや意見の相違もあり、個々のランサムウェアギャングの間で緊張が高まり、さらに熾烈な競争状態になると予想されます。防御側としては、このような衝突によって脅威者が集中力を失い、解読者の作成に活用できるようなミスを犯したり、最悪の場合、逮捕や起訴につながったりすることを期待しています。

ESET シニア検出エンジニア Igor Kabina

ダウンローダー

T3 2022 年に Emotet が 84%減と閑古鳥が鳴くようになると、MSIL ダウンロードが主役となった。

「ダウンローダー」カテゴリの T3 2022 では、興味深い展開がありました。T1 および T2 では、Emotet が ESET 遠隔測定における検出数の大半を占め、トレンドを生み出すマルウェア群でした。しかし、今回は、MSIL/TrojanDownloader.Agent の亜種が検出数の 37%を占めてトップに立ちました。MSIL/TrojanDownloader.Agent の活動は、T3 期間を通じて非常に安定しており、11 月と 12 月の最終週のみ、目に見えて減速したことが記録されています。

MSIL/TrojanDownloader.Agent の最も一般的な亜種は、Agent Tesla のダウンローダーを表す NKC でした。この悪名高い雇われスパイウェアは、そのオペレータが被害者のデータや機密情報を流出させ、キーストロークを記録し、カメラやマイクロフォンを制御することを可能にします。この活動の多くは、9 月中旬から 10 月初旬にかけて、日本（14%）、トルコ（14%）、スペイン（10%）で検出されました。

これに続く他の主要な亜種、すなわち OFZ、NDX、OHG、OFQ、NHO は、T3 2022 年に見られたこのファミリーの検出数の 10%以上を総称して占めています。これらの亜種は、暗号化された DLL インジェクタ（JPG または BMP ファイルを装う）をダウンロードし、Agent Tesla、Fareit、または MSIL/Agent.CFQ トロイの木馬による侵害につながるいくつかの悪質なキャンペーンにおいて重要な役割を担っています。この活動の多くは、9 月と 12 月に、日本（14%）、チェコ共和国（14%）、トルコ（11%）で観測されています。

Emotet も完全に沈黙したわけではなく、アップデート [51] で、情報セキュリティ・コミュニティが「hwinfo」と名付けた新しいモジュールを追加しています。これは、感染したデバイスに関する追加情報を取得するように設計されており、Emotet のオペレータは、別のデータ取得モジュール「systeminfo」が配信される前に、ボット候補を吟味できるようになっています。両方のモジュールが満足のいくデータを返した場合、他の Emotet モジュールをダウンロードすることができます。収集した情報に基づいて、ボットネット・オペレーターは、被害者のターゲットをより正確に定めることができ、また、セキュリティ研究者によって埋め込まれたボットの検出を向上させることができます。

トレンドと展望

2022 年、Emotet は、主に上半期にマルスパムの大波を起こし、本格的に復活した。Emotet の復活に水を差したのは、Microsoft が VBA マクロをインターネットからデフォルトで無効化したことでした。Emotet のお気に入りの攻撃ベクトルをカットしたことで、Emotet のオペレーターは、LNK や XLL ファイルなどのターゲットを侵害する新しい方法を探すことになりました。最新のキャンペーンに基づき、彼らは、兵器化された Office ファイル、特にスプレッドシートを狙うことにしました。

2022 年後半は Emotet のキャンペーンが 1 回しか行われませんでしたが、11 月にはマルウェア自体にいくつかのアップデートが行われました。T2 では、Google Chrome に保存されているクレジットカード情報を流出させることができる新しいスティラーモジュールを追加し、古いスプレッダーモジュールを返却しました。また、10 月には、新しい「hwinfo」モ

ジュールが、感染したマシンに関する追加情報を取得するようになり、追加モジュールを送信する前に、オペレータがマシンを吟味するのに役立つという改善も行われました。

このことは、Emotet が作者によってまだ活発に開発されていることを示しています。彼らはおそらく、2023 年に将来性がないと思われるプロジェクトにそれほど多くの時間を投資することはないでしょう。特に、別の脅威グループが Emotet とそのインフラを買収しようとしている、あるいはすでに買収しているというソーシャルメディアからの噂を信じるのであれば、このことは、必ずしも彼らがコントロールを維持することになるとは限りません。

ESET マルウェアリサーチャー Jakub Kaloč

Emotet は 2022 年の最初の 4 カ月で活動を活発化させたものの、T2 では約 30%のパワーを失い、この傾向は 2022 年の T3 まで続き、さらに 84%も低下しました。この報告期間で ESET の遠隔測定が上昇した唯一の注目すべきキャンペーンは、11 月 2 日から 11 月 14 日の間に発生し、日本（41%）、イタリア（7%）、ブラジル（5%）が、ほとんどの攻撃に直面したトップ 3 のターゲットとなりました。

これらの攻撃では、ほぼ独占的に、スパムメールに添付された兵器化された文書やスプレッドシートが使用されました。T1 および T2 2022 で Emotet オペレータがテストした悪意のある LNK ファイルや VBA マクロなど、他の侵入ベクトルの使用は、T3 2022 を通してごくわずかでした。最終的なペイロードについては、Conti の消滅後、Emotet は、Quantum および BlackCat [52]を含むいくつかのランサムウェア・アズ・ア・サービスのギャングにとって主要な配信メカニズムとなっています。

2022 年の最後の 4 ヶ月間、Emotet の活動が少なかったことは、検出されたダウンローダーの種類にもその痕跡を残しています。T3 2022 では、MSIL の検出が 42%のシェアで最も多く、T2 2022 と比較して 19%ポイントの急増となりました。2 番目に多いダウンローダーの種類は、ほぼ Emotet によってのみ使用される武器化 Office ファイル（DOC）で、ブロックされたインシデントの 19%を占め、25%ポイント低下しています。かつて首位だった VBA マクロは 3 位にとどまりましたが、3 ポイント上昇し 11%になりました。

暗号通貨の脅威

長期的な自由落下にあるビットコイン為替レートは、暗号通貨の脅威の検出を引きずり続けている。

暗号通貨の脅威は、開始時と同じように、2 桁の減少で 2022 年を終えました。T3 2022 年に 23.6%減少した Cryptominers のサブカテゴリは、一方では暗号通貨為替レートの急落、他方ではエネルギー価格の高騰の影響を受けました。T2 2022 年に一時的に急増した Cryptostealers は、48.7%の減少を記録しています。2022 年第 3 四半期は 24.8%減少し、2021 年と比較すると半減している（45.3%減）。

暗号通貨関連の脅威のうち、クライムウェアの部分は全盛期を過ぎたように見えますが、暗号通貨をプレゼントする詐欺は急速に人気を集めています。Group-IB が明らかにしたように[53]、2022 年の上半期だけで、これらの詐欺の数は 2021 年全体と比較して 3 倍に増加しています。それに加えて、FBI は 10 月 3 日に、いわゆる豚の屠殺を行う暗号通貨投資詐欺の増加について警告する公共サービスアナウンスを発表[54]しました。これらの詐欺は、詐欺師が被害者（すなわち「豚」）の信頼を獲得した上で、暗号投資口座に定期的に入金するよう誘いかけるというものです。被害者は通常、偽のウェブサイトやアプリで投資を追跡することができます。これは、被害者との連絡を断ち、暗号通貨を持って姿を消すことを意味します。

T3 2022 年におけるクリプトマイナーの脅威の検出傾向を見ると、検出のピークを迎えて下降線をたどっています。これは 9 月 15 日に発生したもので、潜在的に望ましくないアプリケーションである Win/CoinMiner のいくつかの亜種の活動が急増したことが原因でした。テレメトリーデータによると、その日に最も目立った亜種は、Win64/CoinMiner ファミリーの IZ、QG、RH の亜種でした。このファミリーは一般的に主にロシアで活動しており、それはスパイクが発生した日にも当てはまりました。

前回と同様、Win/CoinMiner PUA は、23.3%減少したにもかかわらず、T3 において最も多く検出されたクリプトマイナーのファミリーでした。潜在的に不要なマイナーには、暗号通貨を入手するためにユーザーが進んで自分のマシンにインストールするソフトウェアも含まれているため、この減少は、一般消費者の間で暗号通貨の人気が低下していることと関連しています。

トップ 3 の他の 2 つのランクも同じで、13.3%の Win/CoinMiner トロイの木馬が占め、13%の JS/CoinMiner PUA がそれに僅差で続きました。この 3 つのファミリーは、年間統計でもトップ 3 を占めており、唯一の変化は、JS/CoinMiner PUA が Win/CoinMiner トロイの木馬をぎりぎり抑えて 2 位となったことです。

T2 2022 と比較して変化は少なく、T3 2022 の PUA：トロイの木馬比率は 67%から 33%、Desktop：In-browser 比率（Web ブラウザに潜むクリプトマイナーのうち実行ファイルとして配布されるものの割合）は 82%から 18%となっています。また、T3 におけるクリプトジャッキングのドメイン数は、T2 との関係でほぼ横ばいで、4%しか減少していない。

T3 と 2022 年全体の両方でアクセス数トップのクリプトジャッキングドメインは webminepool[.]com で、JavaScript のマイニングコードを入れてウェブサイトからお金を稼ぐ方法を訪問者に約束しています。これは基本的に、2019 年に閉

鎖された、クリプトジャッキング操作における横行する悪用で知られるサービス、Coinhive の別バージョンです。両方のリストに登場したもう 1 つのそのようなドメインは、T3 で 3 位、2022 年に 6 位だった moneromine[.]rocks です。

T2 での Cryptostealer 検出数の急増は例外であり、T3 ではほぼ同数の 49%の減少となり、過去の 50%の増加がすぐに帳消しになったようです。この減少は、このサブカテゴリでほとんど見られなかった成長の原因である PowerShell/PSW.CoinStealer にも影響を及ぼしました。T3 では 42.3%減少したものの、Win/Spy.Agent トロイの木馬の暗号通貨窃盗に焦点を当てた亜種に代わって、31.5%を占めて最も検出された暗号窃盗犯となりました。ESET の遠隔測定データによると、PowerShell/PSW.CoinStealer は、ペルー、インド、バングラデシュで多く確認されています。これらの国々では、T3 でのクリプトシーラー検出総数の半分以上を占めています。2022 年全体のトップ暗号ストール犯の統計では、トロイの木馬 PowerShell/PSW.CoinStealer は、T1 の終わりに遠隔測定に現れただけにもかかわらず、2 位（暗号ストール犯の 20.2%）にランクインしています。

T3 の 2 位は再び Win/PSW.Delf（24.5%）で、T2 と比較すると全体的に安定した検出数となっています。2022 年全体のチャートでは、19.4%で 3 位でした。Win/PSW.Delf トロイの木馬、特にその OSF 亜種は、10 月 5 日の T3 クリプトステーラー検出ピークにも関与していました。

Win/Spy.Agent トロイの木馬、より正確には、スパイウェアの検出数でより多く見られるこのマルウェアファミリのいくつかの暗号化された亜種は、63%減少し、暗号化された盗聴者の 22.2%を占めて 3 位で 1 年を終えました。興味深いことに、このトロイの木馬の検出数は大幅に減少したものの、T3 では（数値的には）増加傾向にあり、その数は期間の後半に回復しています。この急増の時期に、ペルー、メキシコ、ボリビアで、その検出のほとんどを登録しました。T3 では 63%減少したものの、Win/Spy.Agent は 31.7%で 2022 年のトップリストの 1 位に留まりました。

T3 2022 年に最も暗号通貨の脅威を登録した国はペルー（8.2%）、次いでロシア（7.2%）、ポーランド（4.6%）となっています。年間の統計では、ロシアが 8.5%で 1 位、ペルーが 7.5%で 2 位、米国が 4.5%で 3 位となりました。

トレンドと展望

クリプトマインダーの衰退は 2023 年まで続く可能性が非常に高い。暗号通貨のマイニングは、サイバー犯罪者にとってあまり面白いものではなくなり、大量のコンピュータを占拠しても、収益性がなくなっています。イーサリアムを狙うのは、プルーフ・オブ・ステーク方式を採用しているため、もはや完全にアウトです。

悪意のあるスクリプトのブロックやプラグインの審査など、ウェブブラウザのセキュリティは向上しており、その結果、インブラウザのクリプトマイナーやクリプトステーラーが減少しているのである。一方、暗号通貨関連の詐欺やフィッシングはルネッサンスを迎えており、2023 年もおそらく増加し続けるでしょう。

ESET シニア検出エンジニア Igor Kabina

ウェブに関する脅威

暗号通貨をテーマにしたフィッシング詐欺が増加、全体的な Web 脅威は減少傾向。

年初からの傾向を引き継ぎ、Web の脅威は 2022 年に減少に転じた。T3 では、ブロックされたすべての Web 脅威の数は 10%減少し、ユニークブロック URL の数は 5.9%と減少幅が小さくなっています。一方、2021 年の統計と 2022 年の統計を比較すると、より急激に減少したのはユニーク URL ブロックであり、全ブロックが 10.6%減少したのに比べ、25.7%減少しています。

Web 脅威のトレンドチャートでは、11 月のブロック数は、フィッシングを除くすべてのサブカテゴリで全体的に減少しており、このサブカテゴリは T3 終了時に開始時の値を上回った唯一のカテゴリでした。このカテゴリーは、11 月 21 日に Web 脅威全体のトレンドチャートで見られた、フィッシング URL のブロック数が 300 万を超えるスパイクの原因ともなっています。T3 期間中に ESET がブロックしたフィッシングサイトの数は、T2 期間の 2 倍以上、具体的には 114.6%増加しています。

T3 ではユニークフィッシング URL のブロック数が急増していない（8%弱）にもかかわらず、年間統計では 2022 年に当社製品がブロックしたユニークフィッシングサイトの数は 2021 年より 80%多く、合計 1300 万以上となったことが判明しました。同時に、2022 年のフィッシングサイトの総ブロック数は、2021 年とほぼ同等に推移しています。

2022 年を通してそうであったように、ESET はマルウェアのサブカテゴリで最大のブロック数の減少を記録しました。今回は全体で 21.7%減少し、T2 の 1 日平均 120 万ブロックから T3 では 100 万ブロック弱となりました。前年同期比では、30%減少しています。T3 のユニークな悪意のある URL の数は 5.5%の微増を示していますが、2022 年には前年比 35.9%減少しています。

T3 2022 年、ESET 製品は、マルウェアをホストする正規の Web サイト（マルウェアオブジェクトに分類）に、T2 とほぼ同じ割合で遭遇しました：すべてのブロック数は基本的に変わらず、ユニークブロック数は 5%の微減にとどまりました。しかし、年間では、全ブロック数が 29.5%、ユニークブロック数が 25.2%減少しており、確実に減少しています。

T3 における詐欺サイトのブロックは、そのようなウェブサイト全体で 14.4%、ユニークな詐欺 URL で 15%減少している。2021 年と比較すると、これらのウェブサイトのブロック数全体はあまり変化していませんが、ユニークブロックは 29.4%減少しています。

当社製品が最も多くブロックしたマルウェア、詐欺、フィッシングのドメインは、前ページの表で確認することができます。

GeoIP トラッキングによると、T3 2022 年に最も多くの有害なドメインをホストしたのは米国で、33.4%を占めました。他の国でのホスティングはずっと少なかったのです。Web ベースの脅威で 2 番目に選ばれたドイツは、10%で米国に大きく差をつけました。ドイツは、フィッシング、マルウェア、詐欺のウェブサイトの 5%をホストしている第 3 位の中国の 2 倍の数字でした。

これらの脅威が最も多く標的とした国を見ると、残念ながら 1 位は日本で、全 Web 脅威攻撃の 13.7%に直面したことがわかります。次いでロシアが 12%で、3 番目に多かったのはポーランドで 4.4%でした。

ESET のフィッシングフィードによると、最も多く見られたフィッシングサイトのカテゴリは、T2 と比較して大きな変化はありませんでした。金融、ソーシャルメディア、配送と続き、それぞれ前期とほぼ同じ割合のフィッシング URL で、最もなりすまされているリストの上位を占めた。ソーシャルメディア関連のフィッシングサイトは、Facebook に似せたものが多く、金融分野で最もなりすまされた企業は、Bancolombia でした。配送関連では、T3 で USPS に代わって DHL がなりすましサービスの第 1 位となった。

ユニーク URL 数に基づく上位のフィッシング・カテゴリーでより大きな変化があったのは、やや下位のランクです。暗号通貨をテーマにしたフィッシングサイトは、62%増加し、第 5 位にランクアップしました。これは、暗号通貨の脅威のセクションで述べた暗号通貨をテーマにした詐欺やフィッシングの人気の上昇と一致しています。

このカテゴリでは、ESET 製品は、特に、オーストラリアの暗号通貨取引所 CoinSpot のふりをし、ユーザーの認証情報を要求するウェブサイトをブロックしていました。また、ドメインに「tesla」という単語が含まれ、不正なビットコインプレゼントを宣伝し、Tesla CEO の Elon Musk の写真を目立つように表示している Web サイトもいくつかありました。そのようなウェブサイトの例としては、reytesla[.]com、teslaevents[.]net、および tesla-crypto[.]top があります。

当然ながら、「ショッピング」カテゴリも T2 と比較して大幅に増加している。9 位から 7 位へと 84%も上昇したのは、年末年始に贈答品を購入する人を狙ったサイバー犯罪のためです。

カタールで開催される 2022 年ワールドカップのような時事問題は、フィッシングの誘い水として悪用され続けました。ESET が、ワールドカップ開催前から発生していた様々な詐欺の事例を紹介する記事の中で警告しているように、「うますぎる話」には常に注意が必要であり、特に多くの人の注目を集める大きなイベント時には用心することが必要です。ワールドカップに関連するフィッシングサイトとしては、大会の公式サイトになりすまし、試合のチケットを販売するサイトや、大会の特別企画と思われる割引や無料のデータプランを約束するサイトなどが見受けられました。

ホモグリフ攻撃ブロックは、2022 年 T2 と比較すると 58%増加した。しかし、2021 年と比較すると、2022 年のホモグリフドメインの全体数は 52%減少しています。Hotmail になりすましたドメインは、T3 でも 2022 年全体でも最も多くなっています。なりすましドメイン上位の 1 位は変わらなかったものの、T3 には 2 つの新参者がいました。1 つは、トルコの金融会社 Oyak Yatirim を模倣した oyakyatırım.com[.tr で、i をドットなしの i に置き換えています。2 つ目のドメインは、金融分野の別のトルコ企業、Türkiye İş Bankası で、こちらも i をドットなしの i に置き換え、ısbank[.]com というアドレスでなりすましました。

電子メールに関する脅威

電子メールの脅威は、T3 では 17%減少しましたが、年間では大幅に増加しました。

T3 2022 年は、電子メールの脅威がさらに減少し、T2 の 10%減に続いて、カテゴリ全体でも 17%減となりました。しかし、1 年単位で見ると、このようなマイナスの数値にもかかわらず、電子メールの脅威は依然として大きな危険性を持っており、前年比で約 30%も増加しています。

地理的な観点から見ると、2022 年第 3 四半期に配信された脅威メールのほとんどは、日本（12%）、スペイン（8%）、トルコ（7%）の受信トレイに着弾しています。この 3 カ国は、年間統計でも上位を占めていますが、この 12 カ月間に耐えなければならなかった攻撃の割合は、日本が 46%、トルコが 22%、スペインが 21%と、はるかに高い割合になっています。

T3 2022 年の電子メールの脅威のトップは、HTML/Phishing.Agent で、10 ポイント増加し、全検出数の 31%を占めました。その最も一般的な亜種である HTML/Phishing.Agent.AUW は、悪意のある HTML 添付ファイルで、ローカル IT 部門の偽のプロンプトを表示し、受信者にパスワードの提供または変更を要求します。被害者をおびき寄せるために、メッセージの件名には「IT HelpDesk:この件名は、T3 の悪意ある電子メールに最も頻繁に見られたものです。

2 番目に多く検出された Win/Exploit.CVE-11882 のシェアは、T3 2022 年に 17%から 13%に縮小しました。この減少は世界的に見られ、おそらく悪意のあるインフラの撤去や、運営者が活動を放棄したことが原因だと思われます。

この脅威の最も頻度の高い亜種を見ると、2022 年を通じて C と F の亜種がリードしていました。過去 12 カ月間のこれらの亜種の地理的分布は、トルコ、ポーランド、スペインで最も密集していました（10%、9%、8%）。

MSIL/TrojanDownloader.Agent は、T3 2022 で 3 番目に多く見られた脅威ですが、そのシェアはわずかに増加し、その活動のほとんどは、トルコ、日本、スペインで記録されています。通常、これらの脅威は、危険な添付ファイルを配信し、JPG または BMP ファイルを装った暗号化された DLL インジェクタをダウンロードさせる悪意のあるメッセージです。実行されると、最終的なペイロードが配信され、多くの場合、Agent Tesla、Fareit、または MSIL/Agent.CFQ トロイの木馬が配信されます。

上半期にカテゴリ全体に顕著な影響を及ぼした Emotet ボットネットは、T3 では小規模なキャンペーンを行っただけで、検出傾向の上昇を引き起こすことはありませんでした。このボットネットの不活性化は、武器化された Office ファイル（DOC/TrojanDownloader.Agent）の減少に反映されており、T2 の 17% から T3 2022 年には 5% に減少しています。

ブランド別フィッシング脅威のうち、トップ 10 に入ったのは「HTML/Phishing.Microsoft」だけでした。2%で、9 位にランクインしています。HTML/Phishing.Outlook は、2022 年第 2 四半期には上昇傾向にありましたが、2022 年の最後の 4 カ月でその数は激減し、わずか 1.3%で 12 位にまで落ち込んでいます。続くブランド固有の脅威である WeTransfer、Adobe、DHL は、いずれも検出率が 1%を下回っています。

マルスパマーが最も興味を示したトピックは、偽の支払情報であり、次いで偽の出荷や銀行のメッセージであった。T3 では、COVID-19 のルアーもさらに減少しています。パンデミックの規制やロックダウンがなければ、旅行がマルスパムのおとりとしてますます人気が高まっています。

T3 2022 年に ESET テレメトリーが報告した代表的な添付ファイル名は、Offer.docx と Offer - contextual advertising.docx でした。どちらも DOC/Fraud.ATU として検出される長期間の詐欺で、偽の広告サービスに被害者を誘い込もうとするものです。また、同一の WhatsApp、Telegram、Skype の連絡先情報を提供していることから、同じ作者から発信されているようです。

T3 2022 年に最も多く見られた悪意のある添付ファイルの種類は、引き続き Windows 実行ファイルであり、そのリードは 5 ポイント増の 52%になりました。2 位のスクリプトファイルは、2 倍の 10%ポイント上昇し、検出された電子メールの脅威の 33%に見られました。Emotet のアクティビティが低いため（ダウンローダーの項を参照）、Office ファイルは逆に 19%から 10%に減少しています。

トレンドと展望

このアプローチが成果を上げる限り、電子メールは、マルウェアの主要な配布経路の 1 つであり続けることが予想されます。私たちのデータで確認されたように、電子メールは現在もそうであり、おそらく長期的にはそうであり続けるでしょう。

電子メールによる脅威の拡散に使用される主な誘い文句も、一般的な発注書、出荷通知、銀行決済を装ったものが大半で、これまでとほとんど変わらないものと思われます。さらに、COVID-19 のパンデミック、ウクライナ戦争、2022 年カタール・ワールドカップなど、世界のニュースやソーシャル・メディアのトレンドトピックが加わることもあります。

ESET 脅威検出担当ディレクター Jiří Kropáč

スパムは、T1、T2 の 6%、7%の伸びと比較すると、2022 年 T3 は 12%増加し、より高いギアにシフトしていることがわかる。この時期は、ネットショッピングが盛んになり、セールも頻繁に開催されるためか、迷惑メールの量は 8 月末にピークに達し、2022 年末までほぼ同じペースを維持した。この上昇傾向は、前年との差も 14.5%に達している。

米国は 19%で、スパムの最大の発信国としての首位を維持し、中国が 16%、日本が 11%でそれに続いています。送信された全メールに占めるスパムの割合（T3 2022）を見ると、中国が 77%で引き続き首位でした。2 位はロシアで 33%、3 位はシンガポールで T2 の 41%から T3 では 26%に改善されました。

ESET が保護するエンドポイントに到達する前に、インターネットメールサービスプロバイダを含む他のレベルでメールトラフィックが一般的にフィルタリングされるため、ESET によるスパムの可視化は限定的であることに留意してください。

Android に関する脅威

2022 年の T3 では Android の検出数が 50%以上増加。全検出数の 7 割近くが、様々な広告でお金を稼ごうとするものでした。

T3 では、Android の脅威の検出数が全体として 56.5%と顕著に増加し、その中でもアドウェアと HiddenApps が最も大きな割合を占めています。12 月末にトレンドチャートが減少したとはいえ、T3 ではアドウェアが大幅に増加（163.2%増）しています。Android の検出数トップ 10 では、AdDisplay.MobiDash PUA、AdDisplay.Fyben PUA、Snaptube PUA がこのカテゴリを代表する存在となっています。

これらの検出されたものはすべて、ほとんどがサードパーティのストアに存在し、正規のアプリと一緒に梱包されているため、Potentially Unwanted Applications（PUA）としてフラグが立てられます。ユーザーは特定のアプリを望んでいるのに、その代金が広告を見ることによって支払われることを警告されないのです。アドウェアの成長の背景には、特に Fyben があります。T2 と比較して、T3 では 1100%以上も成長しています!この検出は、主にモバイルゲームに詰め込まれており、T3 は、開発者がクリスマス商戦に乗るためにゲームの新バージョンやアップデート版をリリースする時期と重なるため、この検出が大きく伸びたのかもしれません。ESET 遠隔測定では、ウクライナ、メキシコ、ブラジル、ロシア、トルコで Fyben の検出が最も多く見られました。

モバイルゲームの開発者は、これらの国でゲームを提供していない場合があります。そのため、これらの国に住む人々は、簡単に入手できる非公式のストアやウェブサイトでゲームを探します。

T3 では、HiddenApps の検出率も 82.9%と大幅に増加しました。このタイプの Android の脅威は、自身のアイコンを隠してこっそり広告を表示する不正なアプリを表し、経験の浅いユーザーの手にかかるとアンインストールが困難になることがあります。トップ 10 では、5 位に Android/Hiddad がランクインしており、Fyben と同様にゲームアプリに関連したカテゴリとなっています。

オンライン広告を経由してサイバー犯罪者に利益をもたらしているもう一つのカテゴリは、クリッカーです。これらは、HiddenApps ほど侵入的ではなく、バックグラウンドで広告を開き、クリックするだけで、消費者が実際に広告を見ることなく、広告主からお金を現金化するものです。そのため、クリッカーの被害者は、デバイスに何かインストールしてはいけないものをインストールしたという目に見える兆候はありませんが、クリッカーはデバイスのパフォーマンスやインターネットの使用状況に影響を与える可能性があります。また、クリッカーは標準的なポップアップ広告を表示するケースもあります。このカテゴリーは、T3 では検出数が 20.9%減少しています。しかし、広告を離れて生活するすべてのカテゴリーの検出数を合算すると、Android の全検出数に占める割合は 69.2%になります。

トレンドと展望

2022 年初頭、私たちは、今年の残りは、サイバー犯罪者が暗号通貨を換金するためのマルウェア（クリプトマイナー、ランサムウェア、バンキングマルウェア）が Android の脅威シーンを席巻すると考えていました。しかし、暗号通貨

市場の急激な変化により、サイバー犯罪者は、非常に迅速にそのやり方を変え、新しい環境に適応することができることがわかりました。

広告で稼ぐマルウェアや PUA の普及は、他の種類の脅威の普及が減少していれば、何かポジティブなこととして受け止められるかもしれません。しかし、そうではありません。スパイウェアも、さまざまなオンラインフォーラムで入手できるアクセスしやすい市販の Android スパイウェアキットのおかげで存在感を増しており、アマチュア攻撃者たちが利用しています。また、2023 年には、ChatGPT と呼ばれる新しい AI チャットボットが、Android の脅威の全体像にどのような影響を与えるかを見ることになるでしょう。マルウェアの作成者はすでにそれを使って新しいツールを開発し始めていますが、今のところ Android 向けに作られたものには気づいていません。

さらに、サイバー傭兵や APT グループは、知名度の高いターゲットや脆弱な市民グループから情報を収集するために、高度な標的型スパイウェアを開発し続けており、この鍋に追加しているのです。このことは、攻撃者たちが、スマートフォンを標準的なコンピュータとして扱い、地獄のように収益化し、地政学的な理由からその所有者をスパイできることを完全に理解したことを示しています。

ESET シニアマルウェアリサーチャー Lukáš Štefanko

また、クリッカーは通常、有用な正規アプリに詰め込まれ、大手の公式ストアを含む様々なデジタルストアに配置されます。例えば、2022 年 10 月、McAfee [56]は、Google Play ストアでクリッカーのマルウェアが詰め込まれた 16 のアプリを発見しました。これらのアプリは、累積ダウンロード数が 2000 万を超え、タスクマネージャ、Instagram のプロファイルダウンローダ、通貨換算器、釜山市のバス時刻表などの様々な韓国関連のサービスなどの機能を約束していました。ESET の遠隔測定によると、これらのクリッカーの検出のほとんどは日本で発見されたもので、当社の製品は、これらのアプリをすべて Android/Clicker.OW の亜種として検出しています。

このカテゴリが 3 桁の増加率に達していた今年の他の時期と比較すると、T3 ではスパイウェアの検出数は 14.9%とわずかな増加にとどまりました。トップ 10 では、このカテゴリの代表として、トロイの木馬 Android/Spy.Agent が 7 位にランクインしています。11 月末、カタールで FIFA ワールドカップ 2022 の試合が始まる頃、ESET の研究者は、ワールドカップを誘い水とする進行中の Android RAT キャンペーンを発見しました[57]。このキャンペーンは、RAT を配布するウェブサイトへのリンクを持つ Facebook ページを通じて広がっており、ESET の製品では、Android/Spy.Agent.BOC として検出されます。ダウンロードされた RAT は、ワールドカップのニュースやライブ放送を提供し、SMS メッセージ、通話履歴、連絡先リスト、写真、クリップボードの内容、特定の拡張子を持つファイルの流出、電話の録音、写真の撮影など、悪意のある機能を幅広く備えています。

ESET の研究者は、ハック・フォー・ハイヤーグループの Bahamut が行った Android キャンペーンも発見しています[12]。このキャンペーンは、2022 年 1 月から数ヶ月間活動し、偽の SecureVPN ウェブサイトを通じて悪意のあるアプリを配布していました。正規の VPN アプリをトロイの木馬化したものは、感染したデバイスから連絡先、SMS メッセージ、デバイスの位置情報、録音された電話などを流出させました。また、Signal、Viber、WhatsApp、Telegram、

Facebook Messenger などのメッセージングアプリで交わされたチャットも、キーロギングによってスパイされました。ESET 製品は、この脅威を Android/Spy.Bahamut.M.として検出します。

ESET の研究者は、StrongPity APT グループ[58]が行ったキャンペーンを特定し、見知らぬ人同士の暗号化されたコミュニケーションを提供するランダムビデオチャットサービス「Shagle」になりすましたウェブサイトを通じてこのバックドアを配布していることを突き止めました。バックドアは Shagle アプリとして表示されていますが、実際は正規の Telegram アプリをトロイの木馬化し、完全に機能させたものです。

ESET の研究者は、APT-C-50 グループが使用する新バージョンの Android 向け不正プログラム「FurBall」[11]も確認しています。FurBall は、イラン市民に対するモバイル監視活動を行う同グループの「Domestic Kitten」キャンペーンの一部です。2021 年 6 月以降、この FurBall の亜種は、翻訳された記事、雑誌、書籍を提供するイランのウェブサイトの模倣品を通じて、翻訳アプリとして配布されました。このマルウェア（ESET 製品では Android/Spy.Agent.BWS として検出）は、目立たないように、連絡先にアクセスするのみで、おそらくテキストメッセージによるスピアフィッシングでその収集を追跡するために、機能が制限されています。

検出数がわずかに増加したもう一つのカテゴリは、Android バンキングマルウェアで、3.5%の増加でした。このカテゴリの検出数の大部分を占めているのは、Cerberus や Hydra といった有名な Android バンキングマルウェアのファミリです。また、Xenomorph（ゼノモーフ）[59]は、残念ながら、現在も Android 端末に侵入し、Google Play にさえも登場しています。Zscaler [60]は、ライフスタイルのアプリに埋め込まれたバンキング型不正プログラムを発見しました。また、BitDefender は、ファイルマネージャを装った同種のマルウェアを Google Play で検出しています（BitDefender[62]）。

T3 では、他のすべての Android カテゴリで検出数が減少しました。SMS トロイの木馬は 34.2%、ランサムウェアは 15.5%、ストーカーウェアは 13.6%、ScamApps は 13.1%、クリプトミナーは 7.1%減少しています。

T3 で ESET テレメトリーが Android の脅威を最も多く検出した国は、ブラジル（8.5%）、ウクライナ（7.6%）、メキシコ（7.3%）、ロシア（6.6%）、トルコ（5%）および米国（4%）であった。しかし、2022 年全体で見ると、Android の検出数が最も多かったのは、ウクライナ（9.3%）とロシア（9.2%）でした。

macOS と iOS に関する脅威

macOS の検出数は、2022 年第 3 四半期も微減で、その半分以上を Potentially Unwanted Applications が占めています。

T3 2022 年、ESET 遠隔測定では、ほぼすべての種類の macOS 検出数が減少し、T2 と比較して 5.5%減少しました。唯一の例外は、Potentially Unwanted Applications (PUA)で、検出数は 3.3%とわずかに増加し、引き続き最も広く普及している macOS 検出の種類となっています。T3 2022 では、PUA は全 macOS 検出数の 52%を占め、トップ 10 には、OSX/Mackeeper、OSX/GT32SupportGeeks、そして新たに OSX/BuhoCleaner がランクインしています。

一般的に PUA はマルウェアではありません。macOS デバイスのクリーニングなど、有用な機能が約束されているため、ユーザーが自発的にインストールします。しかし、PUA は macOS のパフォーマンスに悪影響を与える動作を行う可能性があり、macOS のプロセスやファイルに対して広範な権限とアクセスを持つため、実際のマルウェアが侵入する可能性が高くなります。また、サイバーセキュリティ・ベンダーは、怪しいマーケティング手法を採用している場合があり、エンドユーザ・ライセンス契約を見つけるのが困難な場合があります。 サイバーセキュリティ・ベンダーは通常、この種のソフトウェアにフラグを付けるかどうかを顧客に選択させることができます。

macOS の検出傾向グラフでは、2022 年 12 月末にかけて PUA の検出数およびすべての macOS の検出数が最も低下していますが、これは一時的な低下に過ぎないと確信しています。この減少は、マルウェア運営者を含む世界中の人々がさまざまな宗教的・文化的な祭りを祝い、単純にコンピュータの使用頻度が下がる特定の時期であるため、私たちは毎年の現象を示していると考えています。

macOS で 2 番目に多く検出されたカテゴリのアドウェアは、15.4%の減少を記録しています。このカテゴリーは、OSX/Pirrit、OSX/Bundlore、OSX/Genieo、OSX/MaxOfferDeal、VSearch が macOS 脅威トップ 10 リストで代表されています。これらの脅威は、侵入型広告を表示し、アドウェアを正規のアプリケーションにバンドルし、インターネット検索を傍受します。T3 では、潜在的に安全でないアプリケーション（PUsA）の検出数が 20.6%と最も減少し、トロイの木馬は 3.4%とわずかに減少しています。

ESET 遠隔測定では、T3 2022 年に米国（20.7%）、日本（11.7%）、フランス（7.7%）、ドイツ（5.6%）、英国（4%）で macOS 検出数が最も多く記録されました。これらすべての国で、macOS の検出数は T2 2022 年と比較して減少していますが、ドイツは例外で、検出数は 21%増加しています。

macOS の脅威の検出数が全体的に減少しているにもかかわらず、様々なグループが、このプラットフォームのユーザに対する新たな脅威を開発したり、クロスプラットフォーム型のマルウェアを展開し続けていることが、ESET の研究者によって以前に示されています。Talos 社 [63]の研究者たちは、リモート管理機能を持つ Insekt というクロスプラットフォームのマルウェアを展開できる Alchimist という新たな攻撃フレームワークを発見しています。ReversingLabs（64）は、サイバーセキュリティ企業である SentinelOne のソフトウェア開発キットを装った悪意のあるモジュールを使用した、新たなサプライチェーン攻撃を発見しています。このモジュールは SentinelOne 社とは無関係ですが、被害者をおびき寄せるためにその名前を悪用しています。研究者が名付けた SentinelSneak の目標は、開発者関連の機密ファイルを流出させることです。

VirusTotal において、トレンドマイクロ社[65]は、オープンソースアプリケーションのトロイの木馬化バージョンに埋め込まれた KeySteal と名付けられたキーチェーン窃盗マルウェアを発見しました。Keychain は、パスワードやアカウント情報を保存する macOS のアプリケーションです。トレンドマイクロの研究者は、KeySteal を実際に目撃しておらず、ESET 製品は OSX/Spy.GogoKChain.A の亜種として検出しますが、ESET テレメトリでもこの脅威に関するヒット数はゼロであり、KeySteal が狭い範囲のキャンペーンで使用されたことを意味する可能性があります。

マルウェアや同様の脅威のほか、脆弱性やバグも、macOS ユーザーにとって懸念材料となっています。macOS Ventura 13.0 のバグ [66] は、セキュリティ製品がスキャンを行うために必要なアクセスを妨害するため、Ventura の新しいバージョンにアップグレードすることが推奨されています。macOS 13.0 を実行しているデバイスでは、ESET 製品が、システムが完全に保護されていない旨の警告を表示します [67]。

ユーザーができるだけ早くシステムを更新すべき理由は、このバグだけではありません。Intego 社による Virus Bulletin のプレゼンテーションで明らかにされ[68]、その後 Apple 社の文書で確認されたように[69]、同社は、同じバグを古いバージョンで常にパッチするとは限らないのです。例えば、ある脆弱性が活発に悪用され、Apple がバージョン 13.X でパッチを適用した場合、12.X などの以前のバージョンでは対処されない可能性があります。

ある意味、Apple は複雑なメッセージを送っています。米国機関との綱引き[70]の後、同社はついに、写真、メモ、そして最も重要な iCloud バックアップに追加の保護を提供する iCloud サービスのエンドツーエンド暗号化保護を拡張することを決定しました。Advanced Data Protection for iCloud と呼ばれるこの機能は、ユーザが有効にする必要があり [71]、iOS 16.2 を搭載した iPhone、iPadOS 16.2 を搭載した iPad、macOS 13.1 を搭載した Mac、その他の Apple デバイスで利用可能で、より優れた保護の恩恵を受けたい場合は、オペレーティングシステムのアップグレードが必要な別の理由となっている。

IoT セキュリティ

Mozi ボットネットは墓場に片足を突っ込み、ZHtrap は死滅した。Mirai ベースのボットネットは、規模は拡大したものの、活発ではなくなりました。

2022 年 T3、ZHtrap ボットネットが突然店じまいしました。ESET の遠隔測定によると、この 4 ヶ月間で新しいボットと攻撃の数は 97%減少し、ペイロードサーバーのほぼ半分が消滅しました。テイクダウンが報告されていないにもかかわらず、その検出数は T1 および T2 2022 年の数万から T3 2022 年にはほぼゼロになり、ZHtrap は我々のレーダーから事実上姿を消しました。

この迅速な終わり方は、かつて IoT デバイスの主要な脅威であった Mozi ボットネットがほとんど氷河期のように衰退していったのとは対照的です。2021 年に作成者が中国当局に逮捕[72]された後、Mozi は自動操縦され、1 年を通じて数十万台の新しいデバイスに広がりました。

この事実は変わりませんが、2022 年 T2 にはペースを落とし始め、2022 年 T1 の 49 万 8000 台の新規デバイスに蔓延したのに対し、38 万 3000 台にとどまり、23%減速しています。2022 年の T2 から T3 にかけてもこの傾向は続き、Mozi は 289,000 台の新しいデバイスにのみ広がり、さらに 25%減速しています。この傾向が続けば、2023 年末には Mozi が埃をかぶるかもしれない。

しかし、今のところ、ゾンビ・ボットネットはまだ飢餓状態にあるように見えますが、オペレーターがいないため、「新鮮な脳みそ」に向けることができる人がいません。そのためか、新しいボットの 45%と 42%が検出された中国とインドで、ほぼ独占的に新しい犠牲者を出しています。T3 2022 年の 280 万件の攻撃のうち、30%が米国、6.5%がドイツ、6%が英国を狙ったもので、T2 2022 年とほぼ同じでした。

残念ながら、すべての IoT ボットネットが死んでしまうわけでも、墓場に向かうわけでもありません。ボットネットの作成者は、何年も前の Mirai マルウェアのスピンオフを使用して、侵害されたデバイスの新しいネットワークを構築し、不正な目的のために使用またはレンタルすることが可能です。ESET の遠隔測定では、Gafgyt、BotenaGo、Dofloo、Tsunami、そして最近では Zero が、このグループに含まれています。

これらの Mirai ベースのボットネットによってボット化されたデバイスの数は、T3 2022 年に 11%増加し、ほぼ 20 万台となりました。ボットネットは、エジプト（63%）、米国（7%）、中国（4%）で最も肥沃な土地を発見しました。ターゲットとなる IoT デバイスを奴隷化したこれらのネットワークは、T2 と T3 2022 の間で 20%減少し、主にドイツ（15%）、米国（11%）、日本（6%）の 83,000 の IP アドレスをターゲットとしました。

エジプトの Mirai ボットは、1100 万件の検出数のうち 28%を占め、攻撃数に関しても主導権を握っていました。米国のデバイスは 15%で 2 番目に活発で、韓国のデバイスが 13%でそれに続きました。攻撃波の大部分は、米国（24%）、ドイツ（8%）、英国（7%）で発生しています。良いニュースは、1100 万件の検出により、Mirai ベースのボットネットの活動が 2022 年の T2 より 6%減少したことです。

Mirai ベースのボットネットのキャンペーンで使用された 800 台のペイロードサーバーの 3 分の 1 は米国で、8%はブラジルで、さらに 8%はドイツで観測されました。注目すべきは、T2 2022 年にはトップ 10 にも入らなかったブラジルが、

T3 2022 年には 2 番目に多く利用されたサーバー拠点となったことです。それと対照的なのがオランダで、T2 2022 年には Mirai ベースのボットネットのサーバーの 11%をホストしていましたが、T3 2022 年には 7%にとどまり、2 位から 4 位に下降しています。

69%を占め、MVPower DVR デバイスの 2017 年 EDB-41471 [73]バグは、Mirai ベースのボットネットがさらなる拡散のために悪用する欠陥のナンバーワンにとどまりました。2 番目に悪用された脆弱性は、検出された事例の 11%で使用された ZyXEL ルータにおける 2017 年のコマンドインジェクション（CVE-2017-18368 [74]）、次いで 8%のインシデントで見られた Linksys E シリーズルータにおける 2014 年の脆弱性 EDB-31683 [75]でした。

年末には、現代自動車、ジェネシス（76）、日産自動車、インフィニティ（77）、テスラ・モデル Y（78）などの自動車がハッキングされ、ドアのロックや解除、エンジンの始動、ホーンやヘッドライトなどの機能を制御する攻撃に対して脆弱であることが判明した。

ヨーロッパ全土で行われた車上荒らしの一味に対する捜査で 31 人の容疑者が大量逮捕[79]されたことは、この種の攻撃がもはや理論上のものではなく、犯罪者がすでに実戦配備していることを示しています。解体された犯罪組織は、脆弱なキーレスエントリーとスタートシステムを悪用して、車に乗り込み、車を走らせたのです。

IoT のセキュリティが何年も欠けているため、いくつかの先進国は、最も一般的な欠点に対処するための規制メカニズムを検討しています。2022 年の T3 では、米国ホワイトハウスが民間と政府のパートナーを招いて、米国人がスマートデバイスのセキュリティをより理解できるような自主的なラベルプログラムの開発 [80] を目指した会議を開催しました。その一歩先として、ドイツとシンガポールが、既に存在する IoT セキュリティラベルを互いに承認することに合意[81]しています。

透明性の向上と政府が定めた規格により、本章の前半で紹介した IoT ボットネットの主な餌である、安全でない、修正不可能なデバイスの時代が終わることを期待したいところです。

トレンドと展望

2022 年のデータを振り返ってみると、Mozi ボットネットが消滅しつつあるという私たちの予測は正しかったと言えます。ボットネットの作成者やその秘密鍵に関する新たな動きはなく、新たなエクスプロイトも追加されておらず、アクティビティの著しい増加も観察されていないことから、このボットネットが息切れしていることはほぼ間違いないと思われます。しかし、現時点では、このボットネットに代わる IoT 分野のリーダー的存在となりそうなものは見当たらないため、「誰がこのボットネットに取って代わるのか」という疑問が残ります。

しかし、そのような後継者を生み出す可能性のある脅威分野の 1 つが、Mirai ベースのボットネットです。これらの悪意のあるネットワークは、運営者によって活発に管理されており、悪用された古い脆弱性の長いリストを頻繁に更新し、さらに規模を拡大するのに役立つ新しいエクスプロイトを追加しています。2023 年の IoT 分野において、Mirai ベースのボットネットが主要な脅威であり続けると予想される理由もここにあります。

また、来年は、産業用 IoT がサイバー犯罪者の間でますます人気のターゲットになりつつあり、ハニーポットを使って反射型攻撃やその他の DDoS 攻撃に使われていることが示唆されていることから、産業用 IoT にも注目したいと思います。

ESET マルウェアリサーチャー Milan Fránik

エクスプロイト

RDP パスワードの推測は依然として減少していますが、SQL 攻撃はペースを上げています。Log4J 脆弱性の検出と悪用の試みは引き続き増加しています。

2021 年、公衆向け RDP に対するブルートフォース攻撃は、サイバー犯罪者の活動の中でも最も活況を呈し、この先も変化の兆しがない分野でしたが、2022 年の最初の 10 日間だけで、急降下しています。

その急激な減少は、RDP の数値がほぼ安定する 2022 年 5 月まで続いたが、T2 から T3 の 2022 年の間にも 16%の減少を示した。ブロックされたパスワードの 1 日平均推測数は、T1 では 10 億以上だったのが、T2 では 1 億 500 万、T3 では 8900 万になった。

統計的に見ると、パスワードの推測件数は、2021 年の 2880 億件から 2022 年には 1460 億件を下回り、前年比 49%減少しています。しかし、検知の多い最初の 10 日間を差し引くと、その減少幅はさらに大きくなり、63%にも達します。

この大きなトレンドの変化の要因としては、リモートワークの減少、企業の IT 部門による設定と対策の改善、ロシアのウクライナへの侵略、Windows 11 に搭載されたブルートフォースブロックの新機能などが、前回のレポートでの仮説として残っています。

RDP に対するブロックされた攻撃を少なくとも 1 回報告したユニーククライアントの 1 日平均を見ると、T3 2022 年は 7 万件と最も低い数字となり、T2 2022 年の 7 万 3000 件から 4%減少、T1 2022 年の 10 万 2000 件から 31%減少していることがわかります。

地理的な観点から見ると、2022 年の攻撃の大部分（55%にも及ぶ）は、ロシアの IP アドレスから発生しています。2 番目に有力な発信元はドイツで 14%、次いで米国で 6%でした。これらの接続を受ける側は、ほとんどがフランス、スペイン、ドイツの IP で、それぞれ 14%、13%、7%でした。

T3 2022 に限って言えば、ロシアの IP が依然としてトップですが、32%に留まり、次いで米国が 10%、不明な地域の IP が 7%となっています。T3 2022 の最も顕著なターゲットについては、米国が 11%でトップ、次いでポーランドが 10%、スペインが 8%となっています。なお、VPN、レンタルサーバー、プロキシサービスの利用が、上記の地理的データに影響を与えている可能性があることを強調しておく必要がある。

当初、公開された SQL と SMB サービスに対するパスワード推測のブロック数は、1 月にこの 3 つがほぼ同時に崩壊したため、RDP に続くものと思われました。

しかし、SMB は最初の落ち込みの後、安定し、2022 年の残りの期間も堅調に推移しました。攻撃数は 3 億 5600 万（T1 2022）→3 億 2400 万（T2 2022）→3 億 200 万（T3 2022）となり、9%と 7%の減少を占めた。それでも、2022 年全体の数値は 9 億 8300 万件となり、2021 年と同じ水準になりました。SMB 攻撃で最も大きな割合を占めた国は、メキシコ、フランス、米国でした。

公衆向けの SQL サービスを狙った攻撃の検出数は、1 月に新境地を開いたものの、再び増加に転じ、1 年を通じて顕著な上昇を示しました。SQL 攻撃の絶対数は、T1 2022 年の 8 億 7200 万件から T2 2022 年の 6 億 2000 万件へと 29%減少したものの、T3 2022 年の 6 億 7100 万件へと 10%増加した。

前年比の状況を見ると、SQL に対する攻撃は 42%急降下し、絶対数は 37 億件から 21 億件に減少しています。地域別では、2022 年の SQL のパスワード推測の多くは、トルコ、マレーシア、米国のサービスに向けられていました。

主要な悪用されるネットワーク攻撃ベクトルは、2022 年第 2 四半期と比較してほとんど変化がありませんでした。パスワードの推測は依然として最も好まれる侵入手段であり、過去 4 カ月で 41%から 44%へと 3 ポイントシェアを伸ばしています。

Log4J 脆弱性[82]は、シェアを 2 ポイント落としたとはいえ、外部侵入ベクトルランキングで 2 位にランクインしています。2021 年 12 月からこの欠陥に対するパッチが提供されているにもかかわらず、この欠陥に対する攻撃の絶対数は、T2 から T3 2022 年の間に 9%増加しました。Log4J のエクスプロイト試行のほぼ 40%が米国で、8%が英国で、6%がオランダでブロックされました。

また、この 4 ヶ月の間に、カナダ、米国、日本のエネルギー企業を狙う Lazarus APT グループ [83] や、米国政府を狙うイランの脅威者 [84] など、サイバー犯罪者や巧妙な脅威者によってこの欠陥が悪用されたことがさらに報告されました。Log4J ライブラリの新規ダウンロードの 4 分の 1 が脆弱なインスタンスであると報告されており[85]、この常習的欠陥の「人気」はさらに上昇しそうです。

より好ましい点として、Spring4Shell[86]の攻撃は、2022 年 5 月の顕著な減少以降、回復していないことが挙げられます。4 月に公表された時点では、この CVSS 9.8 の脆弱性は Log4Shell の追随者となる可能性があると見られていましたが、2022 年の最後の 4 カ月間で 8%の減少を示し、最も悪用されている侵入ベクトルの中で 7 位に転落しています。このままでは、Spring4Shell が脚光を浴びる時代は終わりそうです。

トレンドと展望

年初に RDP パスワードの推測が大幅に減少したとはいえ、この分野のサイバー攻撃はまだ死滅しているとは言い難い。最初の 3 ヶ月を省いても、毎日平均 1 億回の攻撃試行回数に達しており、これは決して小さな数字ではありません。

2023 年に向けては、アカウントロックアウトのポリシーを内蔵した Windows 11 と Windows Server 2022 のシェアが拡大しているため、マイクロソフトのサービスに対する攻撃の成功率は低下していくと考えられます。また、マイクロソフトは、古いけれどもまだサポートされている OS にも保護を追加していますが、オンにするかどうかは管理者に委ねていることも忘れてはなりません。それを踏まえて、今後数ヶ月、数年の間にパスワードの推測件数は減少すると思われます。

ESET シニアマルウェアリサーチャー Ladislav Janko

ESET Research チームの貢献

ESET Research チームの専門家による最新の取り組みと成果

近日発表

RSA Conference 2023

100 ドル以下でネットワークをクラッキングできた（かもしれない）[87]

脆弱性を突いたり、スピアフィッシング攻撃をしたりして、ネットワークのログイン情報を取得するのは大変な作業です。オンラインで購入できるのに、なぜ悩むのでしょうか？このプレゼンテーションでは、ESET の専門セキュリティ・リサーチャーの Cameron Camp と ESET のチーフ・セキュリティ・エバンジェリストの Tony Anscombe が、これまで認識されていなかった企業のネットワーク管理慣行に、小規模企業だけでなく大規模多国籍企業にも広く問題があることを示す ESET の新しい調査結果を説明します。詳細については、RSA 開催間近にお知らせします。

Botconf 2023

Asylum Ambuscade:クライムウェアかサイバースパイか？[88]

Asylum Ambuscade は、ロシア・ウクライナ戦争が始まった直後の 2022 年 2 月下旬に欧州の政府関係者を標的にしたことから、研究対象となった脅威グループです。ウクライナの機関やその同盟国を攻撃する数十種類の脅威主体がセキュリティコミュニティによって捕捉されていますが、Asylum Ambuscade は他のものと何が違うのでしょうか。ESET のシニアマルウェアリサーチャーの Matthieu Faou によるプレゼンテーションでは、このグループがどのようにクライムウェア関連の活動に従事し、戦争の初期にはサイバースパイ活動も開始したかが紹介されます。Asylum Ambuscade は、ヨーロッパの外交官をスパイして戦争に関連する情報を盗み出す一方、世界中の銀行顧客や暗号通貨トレーダーを危険にさらしてきました。この地域の他のグループとは異なり、Asylum Ambuscade は、カスタムクライムウェアのようなツールキットを使用して、高価値のスパイ対象を狙いに行きます。プレゼンテーションでは、同グループの侵害チェーン、被害者学、TTP、および犯罪ソフトウェアグループが諜報活動に従事する理由について説明します。

曲者ぞろいの RedLine での生活。悪名高い情報窃盗犯のバックエンドを分析する[85]

RedLine Stealer は、マルウェア・アズ・ア・サービス（MaaS）モデルで動作する情報窃取型マルウェアとして広く知られています。フォーラムや Telegram で販売され、アフィリエイトは、Stealer のサンプルを生成し、C&C サーバとして機能し、盗まれた情報を管理するコントロールパネルを購入することができます。ある調査の際、私たちは MaaS インフラの第 3 層を形成するモジュール、すなわちコントロールパネル自体のバックエンドサーバを発見しました。このバックエ

ンドサーバは、これまで公に文書化されたことはありませんでした。ESET のマルウェア研究者 Alexandre Côté Cyr による本発表では、RedLine の普及状況と特徴、LoadBalancer および DbController モジュールを含む C#で書かれたバックエンドサーバソフトウェアの共通技術分析、仮想ネットワーク内のコントロールパネルとバックエンドのデモを紹介します。

講演されたプレゼンテーション

AVAR 2022

Lazarus が Windows のシステム監視に宣戦布告[89]

2021 年後半から、Lazarus グループのマルウェア作者は、Windows の監視機能を可能な限りオフにし、ほとんどの監視ツール、セキュリティソリューション、イベントロギングを効果的に無効にできる新しいマルウェアを改良してきました。ESET マルウェアリサーチャーの Peter Kálnai と ESET マルウェアアナリストの Matěj Havránek は、プレゼンテーションで、2022 年第 2 四半期に発見され、当時新たに追加された目隠し機能を含むこの不正モジュールの最新バージョンに焦点を当てました。彼らは、これらのメカニズムがどのように動作し、モジュールが実行されるとマルウェアがシステムにどのような変更を加えるかを実演しました。セキュリティ製品の開発者にとって、このセッションの内容が、自社の実装を再評価し、ソリューションの自己防衛力を高めるきっかけとなることを期待します。

韓国の海を泳いでいるのは誰？ScarCruft のイルカを紹介[90]

ScarCruft は、APT37 または Reaper とも呼ばれ、少なくとも 2012 年から活動しているスパイ集団で、主に韓国を対象としています。昨年、ScarCruft は、韓国の新聞社サイトに対して水飲み場攻撃を行いました。この攻撃は、これまで最終的なペイロードとして BLUELIGHT バックドアを搭載していると公言されていました。しかし、ESET のマルウェア研究者である Filip Jurčacko が講演で説明したように、ESET Research は、感染した特定のマシンに BLUELIGHT を介して展開された Dolphin という、より高度な第 2 のバックドアを発見したのです。講演では、Dolphin バックドアとその機能に関する技術的な説明を行い、ScarCruft の活動を追跡しようとする脅威ハンターに役立つ情報を提供するとともに、ESET の研究者が最初の発見後に観察した複数の Dolphin バージョンの進化を紹介しました。

MirrorFace の仮面の裏側。日本の選挙を妨害するマルウェア「LODEINFO」[7]

2022 年 7 月の日本の参議院選挙までの数週間、ESET の研究者が MirrorFace として追跡している APT グループは、日本の政治団体に対してスピアフィッシングキャンペーンを開始しました。被害者が悪意のある添付ファイルにアクセスすると、2019 年から使用されている、日本の団体に限定した LODEINFO マルウェアが実行され、脅威アクターが攻撃の次のステージに移行するための扉を開くことができました。ESET のマルウェア研究者である Dominik Breitenbacher は、発表の中で、LODEINFO マルウェアで日本の事業体を独占的に狙う脅威アクターである MirrorFace APT グループを紹介し、日本の政治団体に対するこのキャンペーンの詳細について説明しました。ブライ

テンバッハーは、その分析の過程で、これまで詳細が公表されていなかった MirrorFace の戦術と手順を発掘しました。また、過去数年間における LODEINFO マルウェアの進化についても説明がありました。

MAIMLA：人工知能を再び機械学習させる[91]

機械学習は数十年前からサイバーセキュリティ業界を変革してきましたが、多くの人が注目するようになったのは、「人工知能」といったバズワードが話題にのぼるようになってからです。次世代」セキュリティ・ベンダーの登場により、この技術自体は「銀の弾丸」のようなマーケティングの層に埋没し、脅威の検知に対する真の貢献が見えなくなってしまったのです。ESET のシニア機械学習エンジニアであるフィリップ・マザンは、このノイズに切り込もうと、ESET が 1990 年代から機械学習を導入し、それがいかに当社の多層アーキテクチャの重要な要素になっているかをプレゼンテーションで紹介しました。Mazán は、現実問題として、自然言語処理手法が、管理者にとって最悪の悪夢の 1 つである破壊的なランサムウェア攻撃を軽減するのに役立つことを実証しました。また、敵対者が遺伝的アルゴリズムや自動化アルゴリズムを使用して、悪意のある製品の新しい亜種を作成する方法についても説明しました。この講演の最後のセクションでは、参加者は、予見可能な将来において、機械学習技術を活用する可能性のある脅威について説明を受けました。

SparklingElf、SparklingGoblin の Linux マルウェアに最近供給、APT41 と新たな関係[92]。

ESET の研究者である Thibaut Passilly と Vladislav Hrčka は、SparklingGoblin APT グループに属するモジュール型 Windows バックドアである SideWalk の Linux 亜種を発見し、元々は StageClient という名前であったことを発表しました。また、このバックドアは、モジュール式 Linux RAT である Specter IoT ボットネットマルウェアと機能が大きく重複していることも発見しました。このことから、これらのマルウェアの作者は、これらのツールが同じ脅威要因によるものであることは疑いようがないことがわかりました。ESET の研究者は、プレゼンテーションの中で、StageClient と Specter の関連性を説明し、SparklingGoblin APT グループを聴衆に紹介し、StageClient と SideWalk のコードの類似性を説明しました。また、StageClient と同時に発見された Linux ユーザランドのルートキットが、ステルス性を実現するために、どのようにプロセスへ自身を注入し、ファイルやネットワーク接続を隠しているのかについても説明しました。

Ekoparty 2022

ウクライナの過去と現在のサイバー戦争[93]。

過去 8 年間、ウクライナは数多くの APT グループによる膨大なサイバー攻撃の標的になってきました。ESET の主要マルウェア研究者である Robert Lipovsky 氏は、同国の電力網に対する攻撃など、最も顕著な試みを中心に、講演の参加者に説明しました。Industroyer2」です。このマルウェアは、停電を引き起こすために特別に設計された唯一のマルウェアの新バージョンで、ロシアの侵攻が続く中、ウクライナに展開されました。2016 年の初代 Industroyer と同様、このサイバー攻撃の目的は大規模な停電を引き起こすことでしたが、今回、攻撃者は失敗しました。Lipovsky

氏は、攻撃がどのように展開され、なぜ失敗したのかを概説し、リバースエンジニアリングしたコードを用いて、最初のバージョンからコードがどのように進化してきたかを示しました。また、悪名高い NotPetya ワームから、ESET が侵入のわずか数時間前の 2022 年 2 月 23 日に発見した HermeticWiper キャンペーン、そして 5 月に展開された破壊的なワイパーである CaddyWiper まで、Sandworm APT グループによる破壊的ワイパーキャンペーンの進化に焦点を当てたプレゼンテーションが行われました。また、攻撃者が ESET をどのように荒らしてきたかも公開されました。

MITRE ATT&CK EVALUATIONS

2023 年 4 月、ESET は MITRE Engenuity ATT&CK®評価の次ラウンドに参加し、Turla APT グループが適用する戦術、技術、手順（TTP）に焦点を当てる予定です。このロシア系サイバースポンジグループは、12 年以上にわたって活動を続けており、Linux や Windows のインフラから機密情報を搾取することを目的とした高度な標的型キャンペーンを実行しています。

このグループは、世界中の多くの政府、特に外交機関に侵入し、ESET Research が過去数年間 [96] [97] にわたって記録した [94] 大規模なマルウェアを運用しています [98]。このグループは、標的を絞った侵入と革新的なステルス技術で知られています。足場を固め、被害者を列挙した後、Turla は、メモリ内またはカーネルへのインプラントを通じて、最小限のフットプリントで持続します。私たちが発表した研究[99]に加え、この脅威者に関連する MITRE ATT&CK Enterprise Matrix にいくつかの貢献[100]をしています。

ESET の Turla のような APT グループに関する研究は、経済、スパイ、地政学、犯罪などの目的で同じグループが使用する TTP を可視化することで、多くの組織や国家が潜在的な攻撃を阻止するために直接または間接的に役立っています。

ESET は、今回も検知と保護の両方の評価ラウンドに参加し、結果は公開され、参加者と共同で作成されます。しかし、この評価では、競合分析や製品の順位付け、「勝者」の決定は行いません。その代わり、この評価では、MITRE ATT&CK の知識ベースの言語と構造を通じて、各ベンダーの脅威検知へのアプローチを示し、コミュニティが個々のニーズに最も適したサイバーセキュリティ製品を評価できるようなツールを提供する予定です。

その他の貢献

ESET の研究者は、複数の Lenovo ノートブックの UEFI ファームウェアに 3 つの脆弱性を発見し [101] 、Yoga、IdeaPad、および ThinkBook の各種デバイスに影響を及ぼしました。これらの脆弱性はすべてメーカーに報告され、アクティブな開発サポートが行われているデバイスは修正されています。Lenovo は、セキュリティ勧告 [102] で、影響を受けるデバイスのリストとファームウェアのアップデート手順を提供しており、ESET Research は、最新バージョンのファームウェアにアップデートすることを強く推奨しています。

この脆弱性により、UEFI Secure Boot を無効にしたり、工場出荷時の Secure Boot データベース（forbidden signature database (dbx)を含む）をオペレーティングシステムから簡単にリストアすることが可能になります。UEFI

Secure Boot を無効にすると、署名されていない UEFI アプリを直接実行できるようになりますが、工場出荷時のデフォルトの dbx を復元すると、Secure Boot を有効にしたまま、既知の脆弱なブートローダを使用して Secure Boot を迂回することができるようになります。ESET 脅威レポート T2 2022 [103]で述べた前回の発見（CVE-2021-3971、CVE-2021-3972）と同様に、この脆弱性はコードの欠陥によって引き起こされたものではありません。影響を受けるドライバは、製造工程でのみ使用される予定でしたが、誤って製品版に含まれていました。

報告された脆弱性は、特殊な NVRAM 変数を作成するだけで、悪用することができます。

CVE-2022-3430 [104]

この脆弱性は、DXE ドライバ WmiSetupUnderOsDxe に存在し、NVRAM 変数 L05WSBD をチェックし、その値に基づいてアクションを実行します。UEFI Secure Boot を無効にするには、攻撃者は L05SecureBootData.Action の値を 2 に設定します。

CVE-2022-3431 [105]

この場合、変数の値は関係ありません。DXE ドライバ BootOrderDxe は、NVRAM 変数 BootOrderSecureBootDisable または BootOrderDualBootMode が存在すると、単に UEFI Secure Boot を無効化します。

CVE-2022-3432 [106]

本脆弱性は、BdsDxe DXE ドライバに関連します。このドライバーは、NVRAM 変数 L05SecBootSmm の値を取得し、値が 0 の場合、UEFI Secure Boot を無効化します。値が 1 の場合、セキュアブートを有効にし、工場出荷時のキー/データベースを復元します。

Lenovo の脆弱性に加えて、ESET の研究者は、Acer のノートパソコンにもう 1 つ同様の脆弱性を発見しました。Lenovo のケースと同様に、OS から直接 NVRAM 変数を作成することで UEFI Secure Boot を無効化することが可能です。影響を受ける Acer モデルのリストは、Acer のウェブサイト [107] で入手でき、同社によると、アップデートは、重要な Windows アップデートとして配布されます。代わりに、更新された BIOS バージョンもダウンロード可能です [108]。

CVE-2022-4020 [109］

この脆弱性は、DXE ドライバ HQSwSmiDxe に存在します。このドライバは、NVRAM 変数 BootOrderSecureBootDisable の有無を確認します。この変数が存在する場合、ドライバはセキュアブートを無効化します。

クレディッツ

チーム

Peter Stančík, Team Lead

Klára Kobáková, Managing Editor

Aryeh Goretsky

Branislav Ondrášik

Bruce P. Burrell

Hana Matušková

Nick FitzGerald

Ondrej Kubovič

Zuzana Pardubská

序文

Roman Kováč, Chief Research Officer

貢献者

Dušan Lacika

Dominik Breitenbacher

Igor Kabina

Jakub Kaloč

Jakub Souček

Ján Šugarek

Jean-Ian Boutin

Jiří Kropáč

Ladislav Janko

Lukáš Štefanko

Marc-Étienne M.Léveillé

Martin Červeň

Martin Lackovič

Michal Malík

Milan Fránik

Miroslav Legéň

Patrik Sučanský

Vladimír Šimčák

Zuzana Legáthová

Zoltán Rusnák

本レポートのデータについて

本レポートに記載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ーデータに基づくものです。特に明記されていない限り、対象プラットフォームに関係なく検出されたデータを含んでいます。

さらに、より詳細なプラットフォーム別のセクションおよび暗号通貨の脅威のセクションで言及されている場合を除き、潜在的に望ましくないアプリケーション [110]、潜在的に安全でないアプリケーション [111]、アドウェア [112] の検出はデータから除外されています。

このデータは、提供される情報の価値を最大化するために、既知のバイアスをすべて軽減することを意図して処理されています。

本レポートのほとんどのグラフは、絶対的な数値を示すのではなく、検出傾向を示している。これは、特に他の情報源からのテレメトリーデータと直接比較した場合、データが様々な誤解を招きやすいためである。しかし、有益と思われる場合には、絶対値や桁数を記載しています。