

脅威レポート

2022年第2三半期

[WeLiveSecurity.com](https://www.welivesecurity.com)

[@ESETresearch](https://twitter.com/ESETresearch)

[ESET GitHub](https://github.com/ESET)

目次

3 エグゼクティブサマリー

4 特集記事

7 ESET Research Lab からの最新情報

9 統計と傾向

10 脅威環境の概要

11 全世界で検出されたマルウェアトップ10

(以降のサブセクションは「ダウンローダー」を除いて英語での提供となります)

12 Infostealers

14 Ransomware

16 ダウンローダー

18 Cryptocurrency threats

20 Web threats

23 Email threats

26 Android

29 macOS and ios

31 IoT security

34 Exploits

37 ESET RESEARCH CONTRIBUTIONS

序文

2022年T2（第2三半期）のESET脅威レポートをご覧くださいありがとうございます。

この4ヶ月間は、北半球の多くの人にとって夏休みの時期でした。また、一部のマルウェアオペレーターは、この時期に活動を一時的に休止し、攻撃手法を見直し、新たな攻撃を仕掛けるための準備期間にしていたようです。ESETのテレメトリ（監視データ）によると、広範な影響を及ぼしているEmotetダウンローダーのオペレーターも8月は休暇としていたようです。Emotetを操っている犯罪組織は、マイクロソフトがインターネットから入手した文書に含まれるVBAマクロをデフォルトで無効化する対策を取ったことを受けて、別の方法で武器化したMicrosoft OfficeファイルやLNKファイルを悪用するキャンペーンに力を注いでいます。

2022年T2は、RDP（リモートデスクトッププロトコル）攻撃がさらに減少しましたが、これはロシアとウクライナの戦争、新型コロナウイルスの感染者の減少に伴うリモートワークからのオフィス回帰、そして企業環境全体でセキュリティ対策が進んだことなどが要因と考えられます。RDP攻撃は減少していますが、引き続きロシアのIPアドレスからのRDP攻撃が最多になっています。2022年T1には、ロシアが最も多くランサムウェアの標的となりました。戦争に端を発した政治的または思想的な動機による攻撃も行われました。しかし、後で説明するように、政治色の強いハッカーによる攻撃（ハクティビズム）の波はT2に減少し、ランサムウェアオペレーターは米国、中国、イスラエルに目を向けるようになりました。

ホームユーザーを標的とする脅威では、宅配に便乗したフィッシング詐欺の検出数が6倍に増加しました。これらの多くの詐欺では、DHLとUSPSになりすまし、配送先住所の確認を求めるフィッシングメールが送り付けられています。Magecartと呼ばれるWebスキミング攻撃は2022年T1に3倍に増加し、オンラインショッピング利用者のクレジットカード情報を盗み出す重大な脅威であり続けています。暗号通貨の為替レートの急落は、オンラインの脅威にも影響を与えています。暗号通貨に関連するフィッシング詐欺が倍増し、クリプトスティーラも増加していることからわかるように、犯罪者は暗号通貨のマイニング（採掘）ではなく窃取することを重視するようになっています。

この4ヶ月間で、いくつかの脅威の調査や研究についても重要な成果が得られました。ESETのリサーチャーは、これまで検出されていなかったmacOSバックドアを発見し、サイバー犯罪組織ScarCruftに帰属することを特定しました。また、APTグループであるSandwormが使用しているArguePatchマルウェアローダーのアップデート版の発見、トロイの木馬化したアプリケーションに含まれていたLazarusペイロードの発見、Lazarusの「Operation In(ter)ception: イン(ター)セプション作戦」がmacOSデバイスを利用する暗号通貨業界のユーザーにスパイフィッシングを実行していた事例を特定するなどの成果を上げました。また、LenovoのUEFIファームウェアに存在するバッファオーバーフローの脆弱性を特定したほか、Salesforceの偽のアップデートをテーマに関心を集める新たなキャンペーンも特定しています。

この数ヶ月間、Virus Bulletin、Black Hat USA、RSA、CODE BLUE、SecTor、REcon、LABSCon、BSides Montrealなどのサイバーセキュリティコンファレンスにおいて、OilRig、APT35、Agrius、Sandworm、Lazarus、およびPOLONIUMが展開しているキャンペーンについて、ESETが分析した情報を公開しました。また、ESET Researchは、Wslinkと命名した独自のローダーを解析し、悪意のある脅威やキャンペーンの帰属（攻撃を実行している組織）を特定する方法について説明しながら、UEFI脅威の将来について解説しました。今後も、開催されるRSAやEkopartyなどの多くのカンファレンスでESETは講演を行いますので、ぜひご参加ください。

本書が読者の皆様に貴重な知見をもたらすことを願っています。

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

macOS を標的とする CloudMensis スパイウェアの詳解

ESET のリサーチャーは、クラウドストレージを C&C チャネルとして使用し、侵害した Mac からドキュメント、キーボードへの入力、画面キャプチャを取得するこれまで特定されていない macOS マルウェア「CloudMensis」を発見しました。

ESET Research Lab からの最新情報

Sandworm、ArguePatch の新バージョンを使用してウクライナを攻撃

ESET Research は、Sandworm が使用している ArguePatch マルウェアローダーのアップデート版を発見しました。ArguePatch はこれまで、ウクライナのエネルギー企業を標的とした攻撃「Industroyer2」や、データを完全に破壊するワイパー型マルウェア「CaddyWiper」などの複数の攻撃で使用されています。

イン(ター)セプション作戦の戦略の変化：標的となる暗号通貨プラットフォーム

ESET Research は、Lazarus のイン(ター)セプション作戦が macOS を標的とし、Coinbase 暗号通貨プラットフォームの求人情報を悪用していたことを特定しました。

統計と傾向

カテゴリ	2022 年 T1 から 2022 年 T2 の比較	2022 年 T2 の重要ポイント
脅威全体の検出数	-9.1% ↓	ほぼすべての監視対象カテゴリで検出数が減少
情報窃取型マルウェア	-14.3% ↓	JS/Spy.Banker (別名 Magecart) は、依然として最も多く検出されたバンキングマルウェアになっている
ランサムウェア	-24.1% ↓	政治的な動機によるランサムウェア攻撃は減少傾向
ダウンローダー	-31.0% ↓	Emotet は、配信方法を変えながら活動を継続
暗号通貨の脅威	-16.0% ↓	クリプトスティーラが初めて増加。ほぼ 50% の増加を確認
Web に関する脅威	-6.0% ↓	宅配に関連するフィッシング詐欺の被害が急増
電子メールに関する脅威	-10.2% ↓	悪意のある添付ファイルにおける Office ファイルの割合が倍増
Android	+9.5% ↑	Android スパイウェアは T1 から増加を続ける
macOS	-15.1% ↓	アドウェアのカテゴリの検出数が大幅に減少
RDP 攻撃	-89.4% ↓	T1 に急激に減少した RDP 攻撃がさらに減少

特集記事

macOS を標的とする CloudMensis スパイウェアの詳解

Marc-Étienne M.Léveillé

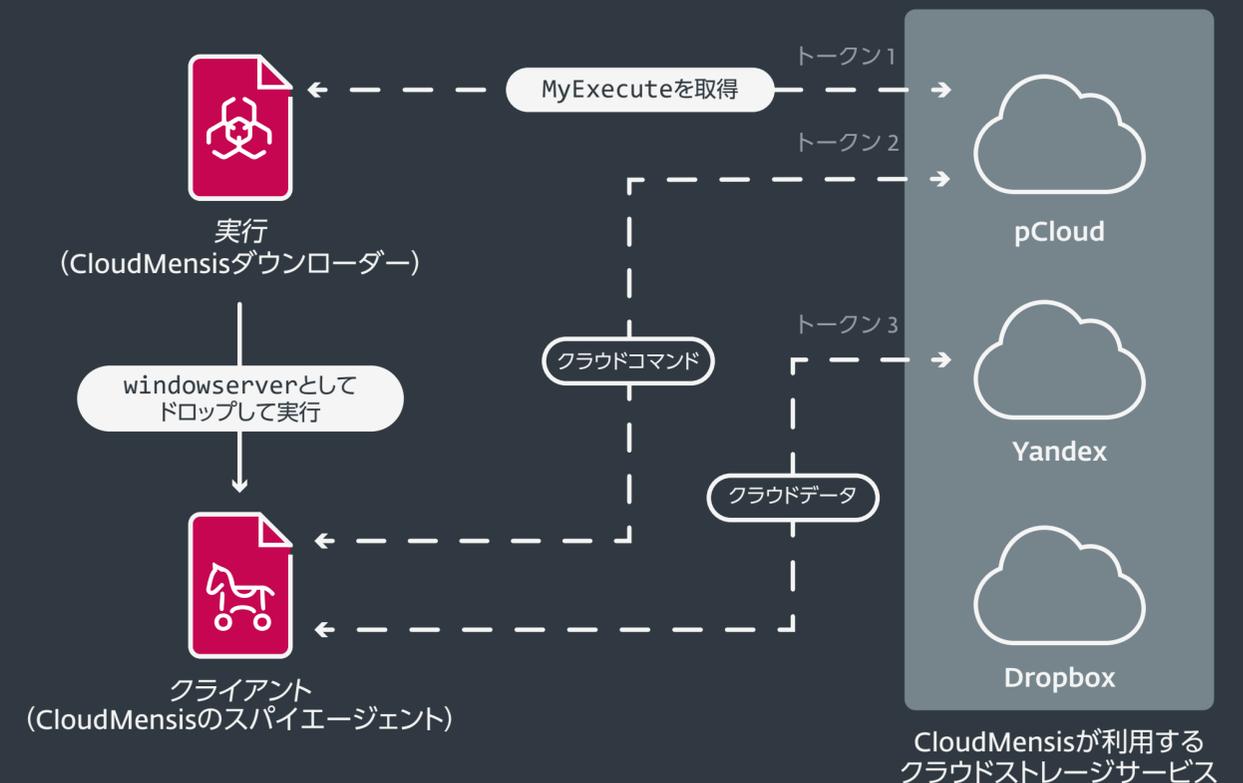
CloudMensis は今回初めて特定されたスパイウェアです。クラウドストレージを C&C チャネルとして使用し、感染させた Mac からドキュメント、キーボードへの入力、画面キャプチャを取得します。

ESET のリサーチャーは、新しい macOS バックドアを発見し、CloudMensis と命名しました。CloudMensis は、主にパブリッククラウドのストレージサービスを使用してマルウェアのオペレーターと通信します。ドキュメント、キーボードへの入力、および画面キャプチャを外部に送信していることから、標的の Mac から情報を収集することがこのマルウェアの目的であることは明白です。

CloudMensis は Objective-C で開発された macOS を標的とするマルウェアです。ESET Research が分析した検体は、Intel と Apple の両方のシリコンアーキテクチャで動作するようにコンパイルされています。

CloudMensis の標的となったユーザーのセキュリティが最初に侵害された方法はこれまでのところ不明です。CloudMensis は、コード実行権限と管理者権限を獲得すると、第一段階のマルウェアを実行し、さらに多くの機能を実行できる第二段階のマルウェアをクラウドストレージサービスから取得します。

注意が必要なのは、CloudMensis はクラウドストレージプロバイダから第二段階のマルウェアを取得するときに、一般ユーザーがアクセス可能なリンクは使用しておらず、ドライブから MyExecute ファイルをダウンロードするアクセストークンを使用していることです。今回分析した検体は、第二段階のマルウェアを保存して配信するために [pCloud](#) [1] を使用していました。



CloudMensis がクラウドストレージサービスを利用する仕組み

スパイエージェントコンポーネント

CloudMensis の第二段階では、より大規模なコンポーネントが実行されます。このコンポーネントには侵害した Mac から情報を収集する多くの機能が詰め込まれています。攻撃者はこの段階で、ドキュメント、スクリーンショット、メールの添付ファイル、他の機密データを取得しようとしています。

CloudMensis は、オペレーターからコマンドを受信し、ファイルを外部に送信する両方の目的でクラウドストレージを使用しています。pCloud、Yandex Disk、Dropbox の 3 つのストレージプロバイダが使用されています。解析した検体の構成には、pCloud と Yandex Disk の認証トークンが含まれていました。

CloudMensis のスパイエージェントコンポーネントが最初に実行する操作の 1 つは、構成のロードです。この構成には、以下の内容が含まれます。

- 使用するクラウドストレージプロバイダと認証トークン
- ランダムに生成されるボット ID
- Mac に関する情報
- CloudMensis が使用する各種ディレクトリへのパス
- マルウェアのオペレーターが重視するファイル拡張子

分析した検体で見つかったファイル拡張子のデフォルトリスト（以下の図を参照）から、このオペレーターは標的ユーザーの Mac からドキュメント、スプレッドシート、音声録音ファイル、写真、メールメッセージに関心があることがわかります。このオペレーターが収集していた特異なファイル形式として、音声圧縮用に特別に設計された音声コーデックである Adaptive Multi-Rate（拡張子 `.amr` と `.3ga`）を使用した音声録音も含まれていました。このリストにあるファイル拡張子には、韓国語圏のユーザーに人気のあるワードプロセッサである [Hangul Office](#) [2]（現 Hancom Office）のドキュメントである `.hwp` と `.hwp` ファイルも含まれていました。

```
471 aDocDocxXlsXlsx db '*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.hwp;*.hwp;*.csv;*.pdf;*'
471 ; DATA XREF: __cfstring:cfstr_DocDocxXlsXlsx+o
471 db '*.rtf;*.amr;*.3gp;*.m4a;*.txt;*.mp3;*.jpg;*.eml;*.emlx',0
4F8 aHwModel db 'hw_model' @ ; DATA XREF: __cfstring:cfstr_HwModel+o
```

CloudMensis のデフォルト構成にあるファイル拡張子

macOS に搭載されているセキュリティフレームワーク（TCC）の回避

2018 年にリリースされた macOS Mojave (10.14) 以降、スクリーンキャプチャ、カメラ、マイク、キーボードイベントなど一部の機密情報へのアクセスは、TCC（Transparency, Consent, Control）というセキュリティフレームワークで保護されるようになりました。アプリケーションが特定の機能にアクセスしようとする、macOS はアプリケーションの要求が正当かどうかをユーザーに確認し、ユーザーはそのアクセスを許可または拒否できます。最終的に、TCC のルールは Mac のデータベースに保存されます。このデータベースは SIP（システム整合性保護）によって保護されており、TCC デモンだけが変更できます。

CloudMensis は、2 つの手法によって TCC を回避し（つまり、ユーザーによる確認を回避し）、画面にアクセスできるようになり、リムーバブルストレージをスキャンして目的のドキュメントを見つけて、キーボードイベントを記録します。SIP が無効になると、TCC データベース（`TCC.db`）は改ざんから保護されなくなります。このケースでは、CloudMensis は、機密情報を使用する前に自身に権限を付与するためのエントリを追加します。SIP が有効で、Mac が 10.15.6 より前のバージョンの macOS Catalina を実行している場合、CloudMensis は TCC デモン（`tccd`）の脆弱性を攻撃し、CloudMensis が書き込めるデータベースをロードします。この脆弱性は、[CVE-2020-9934](#) [3] として知られており、2020 年に [Matt Shockley](#) [4] によって詳細が報告されています。

C&C サーバーとの通信

CloudMensis の構成には、オペレーターと通信するための、いくつかのクラウドサービスプロバイダへの認証トークンが含まれます。構成の各エントリは、異なる目的で使用されます。これらのエントリは、CloudMensis がサポートするクラウドストレージプロバイダに対応しています。分析した検体は、Dropbox、pCloud、Yandex Disk に対応していました。

コマンド

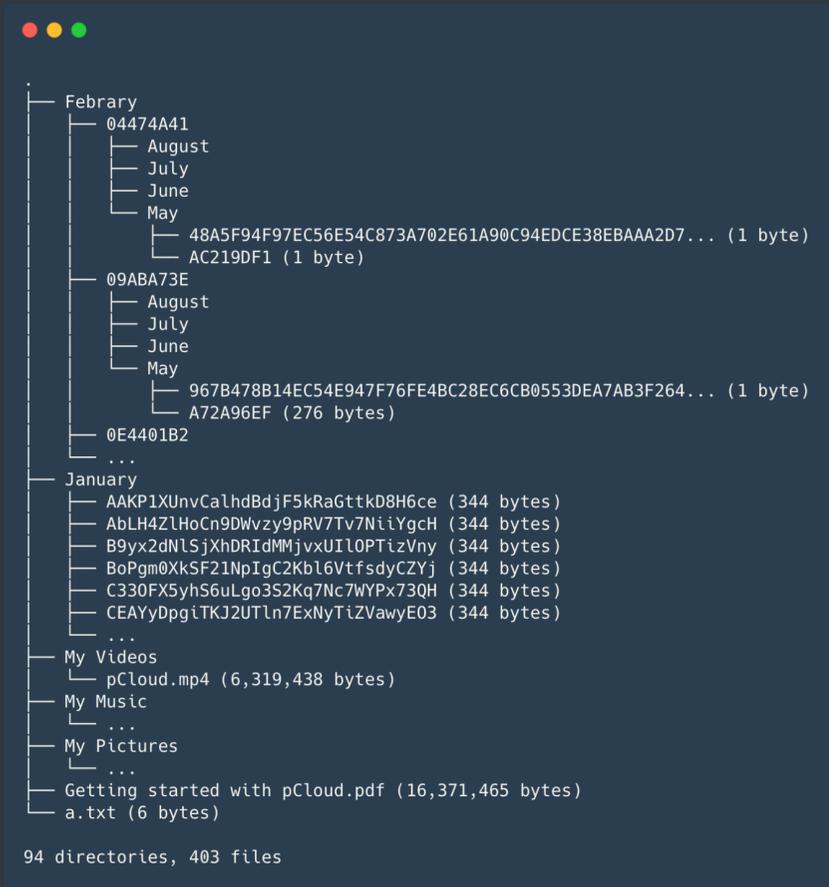
ESET が解析した CloudMensis の検体には、39 個のコマンドが実装されていました。いくつかのコマンドは、引数を指定して使用する必要があります。オペレーターは、これらのコマンドを使用して次の操作を実行できます。

- クラウドストレージプロバイダと認証トークン、オペレーターが重視するファイル拡張子、クラウドストレージのポーリング頻度などの CloudMensis の設定値の変更
- 実行中のプロセスの一覧表示
- 画面キャプチャの取得の開始
- メールメッセージと添付ファイルの一覧表示
- リムーバブルストレージにあるファイルの一覧表示
- シェルコマンドの実行と、クラウドストレージへの出力のアップロード
- 任意のファイルのダウンロードと実行
- クラウドストレージのメタデータ

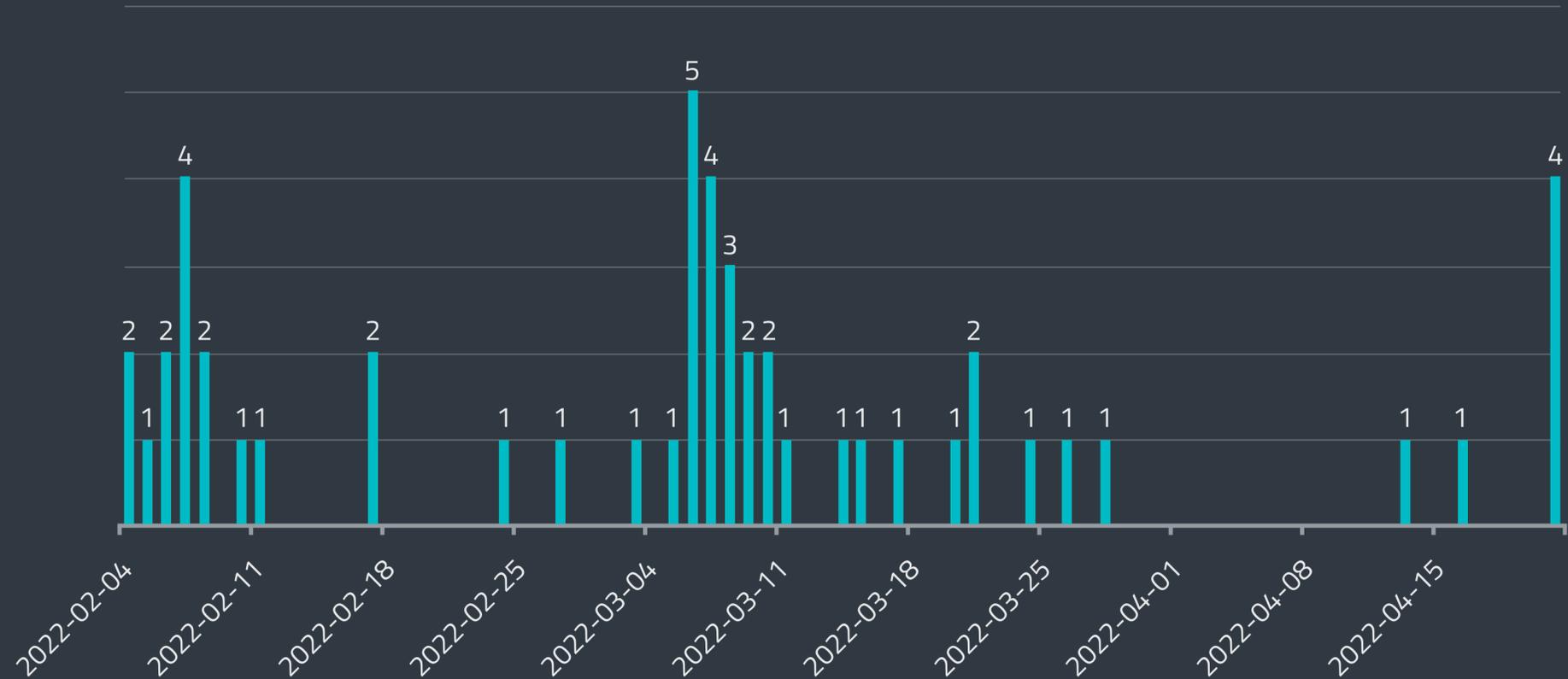
CloudMensis が使用するクラウドストレージのメタデータから、運用に関する重要な情報が見えてきます。次のページの図は、2022 年 4 月 22 日時点における、CloudMensis が最初にレポートを送信し、ボットにコマンドを送信するために使用しているストレージのツリービューを示しています。

このメタデータから、このマルウェアがどのように運用されてきたのかを時系列で理解できます。最初に、pCloud のアカウントは 2022 年 1 月 19 日に作成されました。4 月 22 日のディレクトリ一覧では、51 個のユニークなボット ID が、コマンドを受け取るためにクラウドストレージでサブディレクトリを作成していることがわかります。これらのディレクトリは、マルウェアが最初に起動したときに作成されるため、次ページのチャートに表示されているように、この作成日から最初に侵害された日付を特定できます。

このチャートは、最初の侵害が 2 月 4 日であり、2022 年 3 月上旬に侵害が急増していることを示しています。侵害の最後のピークは、CloudMensis が VirusTotal にアップロードされ、CloudMensis を実行したサンドボックスによって発生した可能性があります。



CloudCmd ストレージのディレクトリー一覧のツリービュー



/February (sic) にあるサブディレクトリの作成日

結論

CloudMensis は、Mac ユーザーにとって脅威ですが、配信の対象が非常に限定されていることから、標的型攻撃で利用されている可能性があります。このマルウェアファミリーのオペレーターは、攻撃者が重視している標的ユーザーのみに CloudMensis を展開しています。このマルウェアのオペレーターは、macOS に実装されているセキュリティ対策を回避するためにいくつかの脆弱性を利用しており、スパイ活動を成功させるために大きな労力を費やしています。ESET の調査では、このグループが利用している未公開の脆弱性（ゼロデイ）は発見されていません。このため、セキュリティ対策の回避を防ぐために、Mac で公開されているすべてのパッチを適用して最新の状態にすることが推奨されます。

Apple は最近、自社製品のユーザーを攻撃するスパイウェアが存在することを認めており、iOS、iPadOS、macOS において、コード実行やマルウェアの展開に頻繁に悪用されてきた機能を無効化する「[ロックダウンモード](#)」[5] を発表しました。

[WeLiveSecurity のブログ](#) [6]

CloudMensis ブログを公開した後に ESET Research は、CloudMensis マルウェアが、[RokRAT](#) [7] の Windows 亜種と同様の機能と特徴を有していることを発見しました。RokRAT については、Cisco Talos が Group 123 に所属していると断定しています。Group 123 は、[ScarCruft](#) [8]、APT37、Reaper としても知られるサイバー犯罪組織です。

ESET のリサーチャーは、RokRAT と CloudMensis は APT グループである ScarCruft に所属すると考えています。ScarCruft は少なくとも 2012 年から活動しており、[北朝鮮のスパイ組織であることが疑われています](#) [9]。主に韓国を対象に活動していますが、その他のアジア諸国も標的にしています。ScarCruft が使用しているツールセットは、ダウンローダー、データ流出ツール、スパイ活動に使用されるバックドアなど多岐にわたります。

帰属を示す指標として、使用されているファイル拡張子リストの一致、マルウェア検体に残されたパスなどの開発工程で使用された情報の類似性、C&C（コマンド & コントロール）サーバーとして使用するクラウドサービスプロバイダの共通性などが挙げられます。

[Twitter で公開した帰属に関連する詳細情報](#) [10]

ESET Research は、今後開催される [AVAR 2022](#) で ScarCruft グループに関する講演を行います。

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

UEFI の脅威

Lenovo UEFI ファームウェアに存在するバッファオーバーフローの脆弱性

ESET のリサーチャーは、複数の Lenovo ノートブックの UEFI ファームウェアに 3 つのバッファオーバーフローの脆弱性が存在することを発見しました。ThinkBook シリーズのいくつかのモデルを含む 70 以上のノートブックの機種が影響を受けました。ESET は、これらのすべての脆弱性について 2 月 18 日に Lenovo に報告しました。Lenovo は脆弱性が存在することを認め、[セキュリティアドバイザリ \[11\]](#) の中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方法を公開しました。

このトピックに関する詳細については、[\[ESET Research チームの貢献について\]](#)のセクションを参照してください。

[Twitter のスレッド \[12\]](#)

macOS の脅威

Salesforce のアップデートを偽装して macOS に展開される Sliver

ESET Research は、Salesforce のアップデートを偽装して、macOS と Windows 向けのマルウェア [Sliver] を展開する新たなキャンペーンを発見しました。以前、SentinelOne が特定および文書化した [13] 新型コロナウイルスに便乗したキャンペーンでも、今回発見された macOS に対するマルウェアと非常に類似する攻撃チェーンが確認されています。

Sliver は Cobalt Strike に似たフレームワークであり、多くの悪意のあるキャンペーンで使用されています。ESET が特定したキャンペーンでは、Bash スクリプトをダウンロードして実行する追加の Go Mach-O 実行ファイルを使用して Sliver が展開されています。また、Windows 版では、Go 言語で記述されたダウンローダーが使用されています。

SentinelOne が説明したスクリプトとは異なり、macOS に Sliver を展開するこのシェルスクリプトには、「新型コロナウイルスに便乗する」マルウェアは含まれず、Sliver マルウェアのみをインストールします。Sliver は、必要に応じて追加のマルウェアを展開することが可能です。

偽装された Salesforce アップデートのダウンロードページには、macOS のセキュリティ機能を無効にする方法が記載された PDF へのリンクが含まれていました。さらに、攻撃を受けたユーザーの Salesforce の認証情報は、ダウンロードページにアクセスするときにフィッシングされたと考えられます。

[Twitter のスレッド \[14\]](#)

Sandworm

Sandworm、ArguePatch の新バージョンを使用してウクライナを攻撃

ESET Research は、Sandworm APT グループが使用しているマルウェアローダーの「ArguePatch」のアップデート版を発見しました。ArguePatch は、ウクライナのコンピューター緊急対応チーム（CERT-UA）が命名したものであり、ESET 製品は、この亜種を Win32/Agent.AEGY として検出します。ArguePatch は、以前、ウクライナのエネルギー企業を標的とした Industroyer2 攻撃や、データ消去型のマルウェアである CaddyWiper などのいくつかの攻撃で使用されています。

Industroyer2 の攻撃時には ArguePatch は検出を逃れるために、リモートデバッグソフトウェアである HexRays IDAPro のパッチが適用されたバージョンを使用していました。ArguePatch のアップデート版では、マルウェアのオペレーターは HexRays IDAPro でなく、デジタル署名が削除されコードが上書きされた ESET の正規の実行ファイルを使用しています。

ArguePatch の新しい亜種は、指定した時間に次の攻撃段階を実行する機能を備えています。この新機能は、Windows のスケジュールタスクの設定を不要にすることで防御側による検出を回避することを目的としていると考えられます。

これは、Sandworm がウクライナを標的とする大規模な攻撃に使用しているツールを今も更新し続けていることを示しています。

[Twitter のスレッド](#) [15]

[WeLiveSecurity のブログ](#) [16]

Lazarus

トロイの木馬化された一般のアプリケーションに潜む Lazarus のペイロード

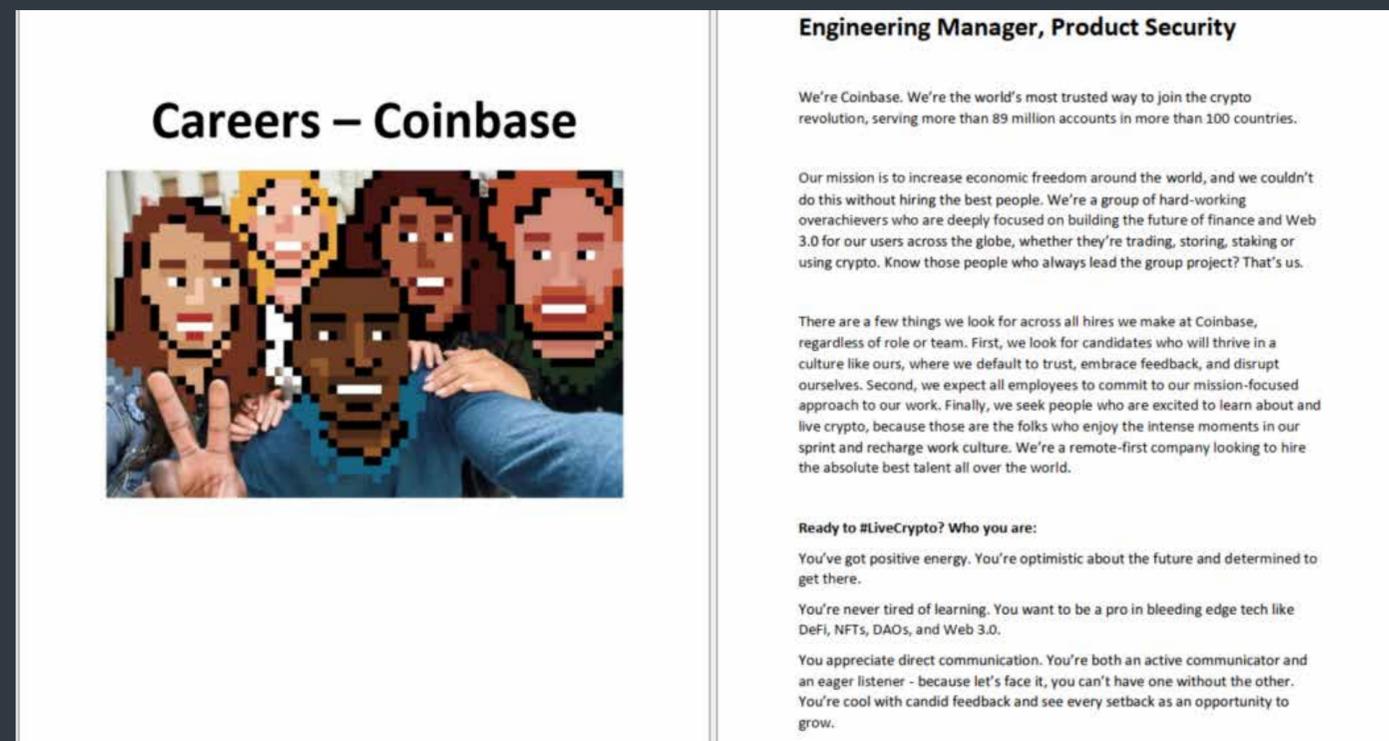
ESET のリサーチャーは、2022 年 5 月に APT グループである Lazarus が一般的なアプリケーションをトロイの木馬として悪用していることを確認しました。ESET は最初に、Windows の実行ファイルである mozilla.cp1 についてツイートし、2020 年 11 月に VirusTotal に提供しました。このファイルは、トロイの木馬化された sqlite v3.31.1 ライブラリで、RAR で圧縮されたファイルをユーザーのシステムから外部に送信するペイロードが埋め込まれています。

11 月下旬に ESET は、Lazarus がペイロードの 1 つを KMSAuto フォルダに保存して、一般的な Windows アクティベーションツールのように見せかけていたことを報告しました。KMSAuto はクラックツールであり、ユーザーは通常、KMSAuto がある場所をセキュリティ製品のスキャン対象外に設定しているため、Lazarus ペイロードを隠ぺいする格好の場所となっています。ペイロード自体は VMProtect で保護された実行ファイルであり、メモリからダンプすると RAT であることがわかります。これは、トロイの木馬として実行される DeFi アプリによって配信されます。

[Twitter のスレッド](#) [17] [18]

イン(ター)セプション作戦の戦略の変化：標的となる暗号通貨プラットフォーム

ESET Research は、Lazarus が macOS を対象としてイン(ター)セプション作戦を実行している事例を発見しました。Coinbase の求人情報を装った署名付きの Mach-O 実行ファイルがブラジルから VirusTotal にアップロードされていました。Lazarus は、LinkedIn や偽の求人情報を足掛かりに標的を攻撃する手法を利用してきましたが、暗号通貨業界を標的としてスパイフィッシングを実行したことはありませんでした。



イン(ター)セプション作戦で使用された Coinbase の偽の求人情報

このマルウェアは、Intel と Apple のシリコンプロセッサをサポートする Mach-O 実行ファイルとして構築されており、[ESET が検出した別のマルウェア](#) [19] と酷似しています（このマルウェアも Lazarus に帰属すると考えられます）。この新しい検体は、おとりの PDF 文書と、悪意のある 2 つの実行ファイルの合計 3 つのファイルをドロップします。最初の実行ファイルである FinderFontsUpdater.app が、2 番目の実行ファイルである、safariFontAgent を実行します。safariFontAgent はダウンローダーです。ダウンローダーが次の攻撃のためのマルウェアを取得する C&C サーバーは、ESET がこの脅威を分析したときには応答していませんでした。

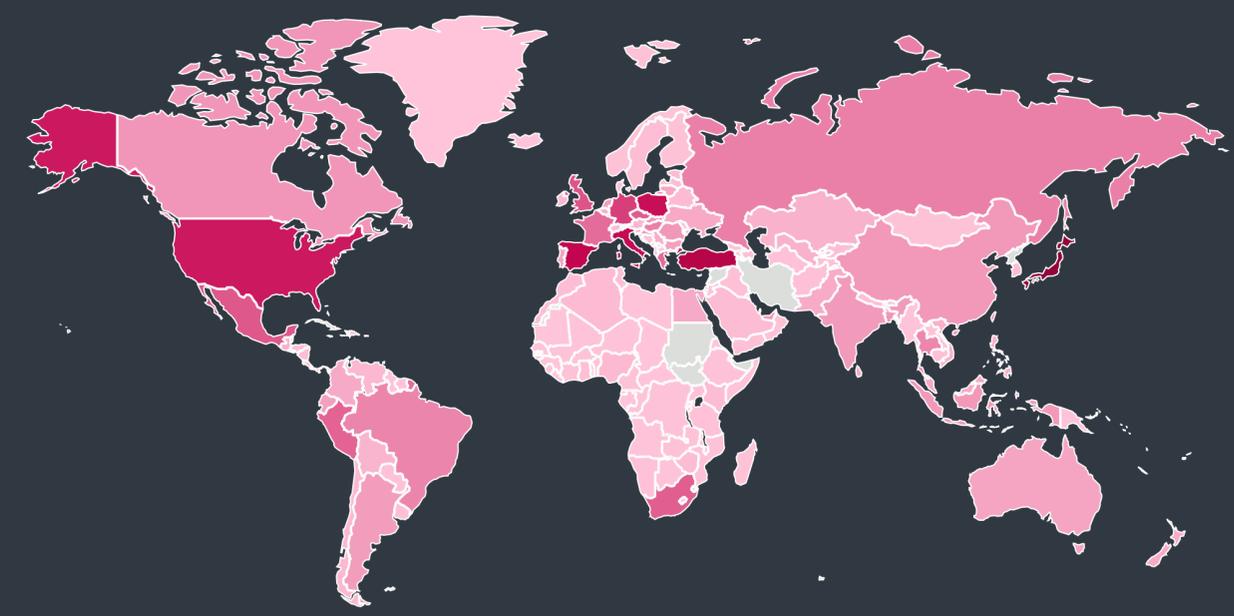
このバンドルは、2022 年 2 月に Shankey Nohria という開発者に発行された証明書を使用して署名されています。しかし、この申請は公証されていなかったため、Apple は 8 月 12 日に証明書を取り消しています。

また、この脅威は Windows も対象としており、同じおとり文書をドロップします。この文書の内容は、Malwarebytes のリサーチャーによって[公開](#) [20] されています。

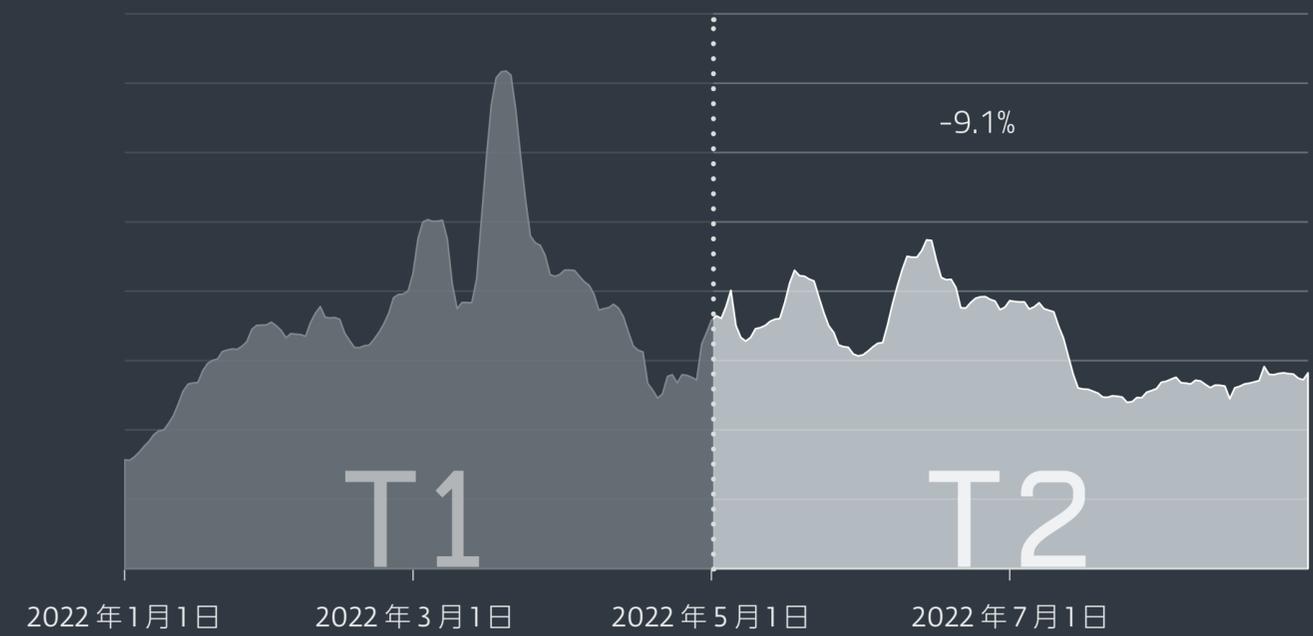
[Twitter のスレッド](#) [21]

統計と傾向

ESET のテレメトリ（監視データ）から見た
2022 年 T2 の脅威環境



2022 年 T2 におけるマルウェア検出の世界的な分布



2022 年 T1 ~ 2022 年 T2 の脅威の検出傾向、7日移動平均線

脅威環境の概要

2022年 T2 の脅威動向の概要。

2022年の脅威環境を見ると、ほぼすべての監視対象のカテゴリが減少しており、脅威全体の検出数は9.1%減少しました。検出された脅威の合計数がピークになったのは6月14日でしたが、これはEmotetマルウェアであるDOC/TrojanDownloader.Agentによるものです。

Emotetの活動については「[ダウンローダー](#)」のセクションでも説明しています。T2においてもEmotetの多くの活動が見られましたが、検出数は31%減少しています。また、Emotetが用いている攻撃手法がVBAマクロからDOCやLNKファイルへと移行していることも確認されています。

「[エクスプロイト](#)」のカテゴリでもT2には変化がありました。Log4ShellやSpring4Shellなどの新しいエクスプロイトが増加した一方で、RDP攻撃の試行は89%減少しました。

ランサムウェアの数は過去2年間で最も減少し、このカテゴリの検出数は24%減少しました。T1はロシアがウクライナに侵攻したことにより、ロシアが最も多くの標的となりましたが、T2ではランサムウェアオペレーターは再び米国に目を向けています。

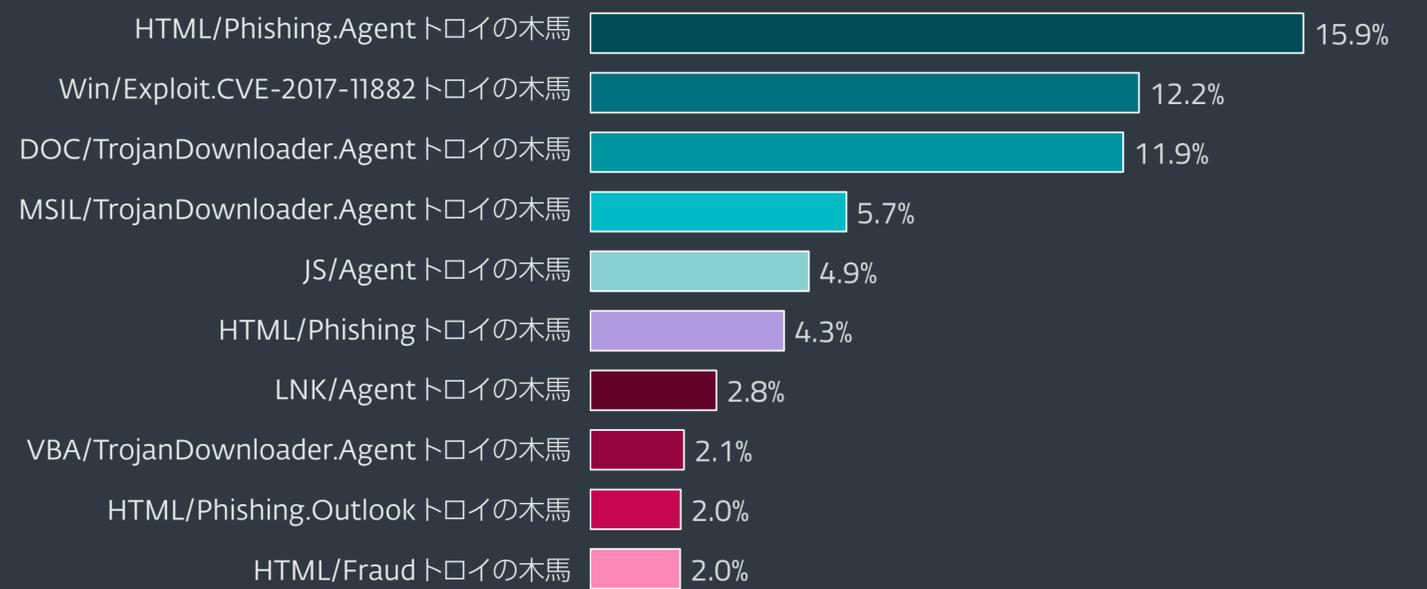
予想されたように、ビットコイン価格が下落したことにより、「[暗号通貨の脅威](#)」はT2に18.9%減少しました。少し意外だったのは、これまで減少し続けていたクリプトスティーラーのサブカテゴリがT2に約50%増加したことです。

一方で「[Webに関する脅威](#)」は、他のカテゴリほど急減していませんが、T2は減少傾向にあり、増加した脅威はユニークフィッシングURLのみでした。ESETのフィッシングフィードでは、宅配に関するフィッシングが6倍になり劇的に急増しています。

「[メールの脅威](#)」はT1に統計を取り始めてから最も大きく増加しましたが、T2では一転して15%の減少となりました。しかし、メールの脅威の1つであるHTML/Phishing.Outlookが急増し、最も多く検出されたマルウェアのトップ10に初めてランクインしました。

また、「[情報窃取型マルウェア](#)」のカテゴリも減少傾向にあり、今期は検出数が14.3%減少しました。これまで最も多く検出されていたサブカテゴリ「スパイウェア」の検出数が21.7%減少したことが、このカテゴリ全体が減少した原因です。

「[macOS](#)」のほぼすべてのサブカテゴリも減少しており、カテゴリ全体では15.6%減少しました。監視対象の脅威の検出数のほぼ半数を占めたのは、PUA（望ましくないアプリケーション）でした。



2022年 T2 のマルウェア検出率トップ10（マルウェア検出数に占める割合）

「[IoTセキュリティ](#)」のカテゴリでは、Mozi ボットネットの勢いがT2に失われ、23%減少しています。一方で、他のMiraiベースのボットネットの活動は61%増加しました。

「[Android](#)」のカテゴリは、全体としての検出数が増加した（9.5%）唯一のカテゴリでした。最も増加したサブカテゴリはスパイウェアでしたが、中でも最も検出数が増加したのは「[隠しアプリ](#)」でした。

マルウェアの検出数トップ10のいくつかのマルウェアの順位は上下しています。唯一の大きな変化は、検出数が大幅に減少した（29%減）MSIL/Spy.AgentTeslaがトップ10リストのランク外になったことと、検出数上位の脅威ランキングに新たにトロイの木馬のHTML/Phishing.Outlookが入ったことです。今回新しくトップ10にランクインしたHTML/Phishing.Outlookは、2022年T1からT2の間に66.1%も増加しています。

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 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。exe 形式の添付ファイルは通常、自動的にブロックされたり、攻撃が疑われたりする可能性が高いため、攻撃者はこのような形式のファイルを使用する傾向があります。このような添付ファイルが開かれると、銀行、決済サービス、ソーシャルネットワーキングの公式 Web サイトを偽装したフィッシングサイトが Web ブラウザに表示されます。これらの Web サイトでは認証情報または他の機密情報を入力するようにユーザーに要求し、入力した情報が攻撃者に送信されます。

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

↘ DOC/TrojanDownloader.Agent トロイの木馬

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 Office 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。

↗ 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記述された、.NET Framework を使用した悪意のある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で他のマルウェアのダウンロードを試みます。通常は、最終的なペイロードをダウンロードするための URL や URL のリストが含まれています。このマルウェアは、さらに複雑なパッケージの最初のレイヤーとして機能していることが多く、標的となったシステムへのインストールを担います。

↘ JS/Agent トロイの木馬

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。

→ HTML/Phishing トロイの木馬

HTML/Phishing トロイの木馬は、メールやメールの添付ファイルに含まれる悪意のある URL をスキャンして収集した、一般的なマルウェアの検出結果です。メールや添付ファイルにブラックリストに登録されている URL が含まれている場合、HTML/Phishing.Gen が検出されます。

→ LNK/Agent トロイの木馬

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

→ VBA/TrojanDownloader.Agent トロイの木馬

この検出名は通常、ユーザーを騙して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。

↗ HTML/Phishing.Outlook トロイの木馬

HTML/Phishing.Outlook は、マイクロソフトのメールサービス Outlook.com のログイン情報を窃取するフィッシングメールの検出名です。このマルウェアが検出されるメールメッセージには、通常、Outlook.com のログインページを偽装する HTML の添付ファイルが含まれています。これらのフィッシングのフォームには、標的ユーザーのメールアドレスがあらかじめ入力されていることが多く、できる限り手間をかけずにログイン情報を入力できるようにしています。

↘ HTML/Fraud トロイの木馬

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、HTML 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](#) [23] です。

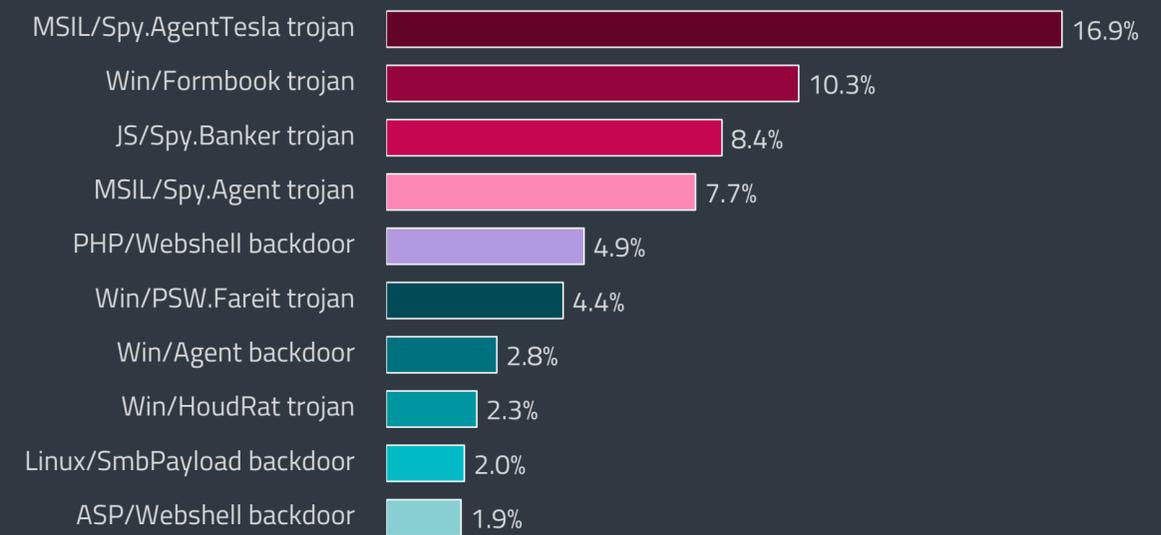
INFOSTEALERS

JS/Spy.Banker continued its reign in the Banking malware subcategory; Agent Tesla numbers dropped.

As is the case for most of our categories in T2 2022, the number of Infostealer detections decreased compared to T1. They went down by 14.3%, caused by a decline in their strongest subcategory, Spyware, which lost 21.7% in T2. Backdoors seem to have stabilized, for now, only having 2% fewer detections than in the previous period. Meanwhile, banking malware continued its growth from T1, this time increasing by 9.9%. Rather unexpectedly, the biggest growth among Infostealer subcategories was exhibited by the smallest one, Cryptostealers. In T2 2022, it managed an unprecedented gain of 49.7%.

Despite the substantial decrease in detections, Spyware was still the most prevalent Infostealer subcategory, responsible for 58.6% of detections in the category. Spyware's decline might have been helped by the drop in MSIL/Spy.AgentTesla detections, which were down by 24.6% in T2. We still registered a considerable spike in detections in this subcategory on June 6, caused by the aforementioned Agent Tesla alongside the Win/Formbook trojan. On that date, the highest number of attack attempts conducted by both malware families was seen in Turkey.

Looking at the chart of the top 10 Infostealer threats, half of them are in the Spyware subcategory. As usual, MSIL/Spy.AgentTesla was in the lead with 16.9% of all Infostealers and 28% of Spyware – even the drop in numbers did not succeed in dethroning it as the most prevalent there. It introduced a new distribution method in T2 when it started *spreading* [24] via weaponized Windows compiled



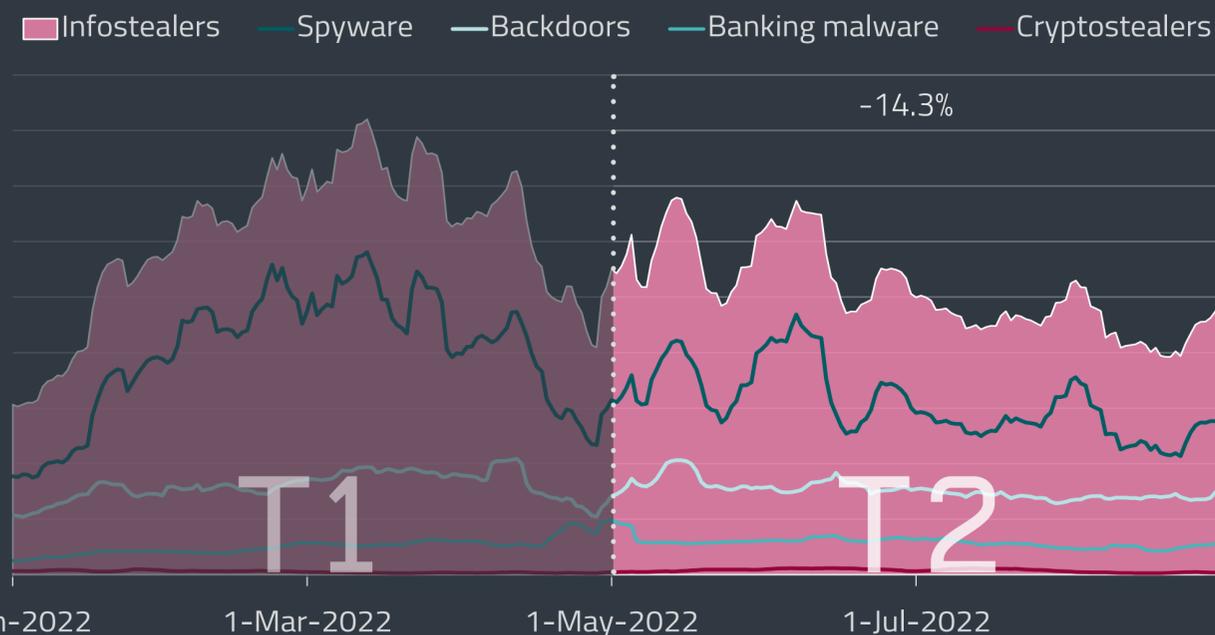
Top 10 infostealer families in T2 2022 (% of Infostealer detections)

HTML Help files, which use the `.chm` extension, attached to phishing emails impersonating the shipping company DHL.

The Win/Formbook trojan also managed to keep its second place despite losing an even higher percentage of its detections than Agent Tesla (36.7%, to be precise). It constituted 10.3% of Infostealer detections and 17.1% of Spyware detections. The MSIL/Spy.Agent trojan actually grew by 14.4%, but still remained the third most detected spyware, with 12.8%, and the overall fourth most detected in the Infostealer category, with 7.7%.

In addition to somewhat recovering from their decline, the Backdoor subcategory increased its overall share of Infostealer detections, going from 25.5% in T1 to 29.1% in T2. Backdoor numbers peaked on May 12 when we saw increased activity from the Win32/Agent.TJS backdoor, caught mostly in the Czech Republic.

This time, four backdoors managed to claim places in the Infostealer top 10, as opposed to three in T1. PHP/Webshell kept a steady trend and remained the most prevalent backdoor with 16.5%, which is 5% of all Infostealers. Even a 7.2% decrease could not budge the Win/Agent family from its second place in the subcategory, which it earned with 9.2% (2.8% of Infostealers). T1's third-place holder, ASP/Webshell, was fourth this time, narrowly replaced by the Linux/SmbPayload backdoor with 6.5% of Backdoor and 2% of Infostealer detections.



Infostealer detection trend in T1 2022 – T2 2022, seven-day moving average

While the rates of banking malware detections increased by 9.9% in T2, they showed a clear, albeit gentle, downward trend across the period. Detections in this subcategory constituted 10.8% of the Infostealer category. Banking malware detections peaked on June 9, with the largest amount of hits recorded in the United States and attributed to JS/Spy.Banker. The second most detected malware family on that day was the notorious Qbot, which also had its T2 peak at that time.

JS/Spy.Banker's dominance from T1 continued in T2. This web skimmer, better known as Magecart, constituted three-fourths of all Banking malware detections, leaving far behind the rest of the families in the subcategory. *From January up until almost the end of May* [25], Magecart led a very successful campaign, during which it compromised more than 300 restaurants, stealing at least 50,000 credit card records in the process. It was also the third most detected among the Infostealers, with 8.4%, and the only banking malware to get into the overall top 10.

```
jQuery(document).ready(function () {
  if (!new RegExp("onepage|nexwaycheckout|checkout|onestep|firecheckout|onestepcheckout").test(window.location)) return;
  setTimeout(function () {
    jQuery(function ($kk) {
      $kk(document).on("change", "form", function () {
        gresos_v = null;
        a = [
          'select[name="ops_cc[year]"',
          'input[name="ops_cc[cardno]"',
          'input[name="cc_number"',
          'input[name="cc_cv2"',
          'input[name="ops_cc[cvc]"',
        ]
      });
    });
  });
});
```



Website compromised by JS/Spy.Banker and the malicious skimmer code linked to the page

However, it is important to note that web skimmers such as JS/Spy.Banker are distributed and detected in a different way from most of the Infostealer top 10. Since they constitute online scripts that are lying in wait on hacked or unpatched websites (mostly hosted on WordPress and Magento), their detection statistics are based on the number of visits to these websites and might not reflect

the actual level to which the skimmers in question have spread. The only other members of the Infostealer top 10 that work similarly to JS/Spy.Banker are PHP/Webshell and ASP/Webshell. The rest of the most-detected families are distributed via email attachments or as downloader payloads.

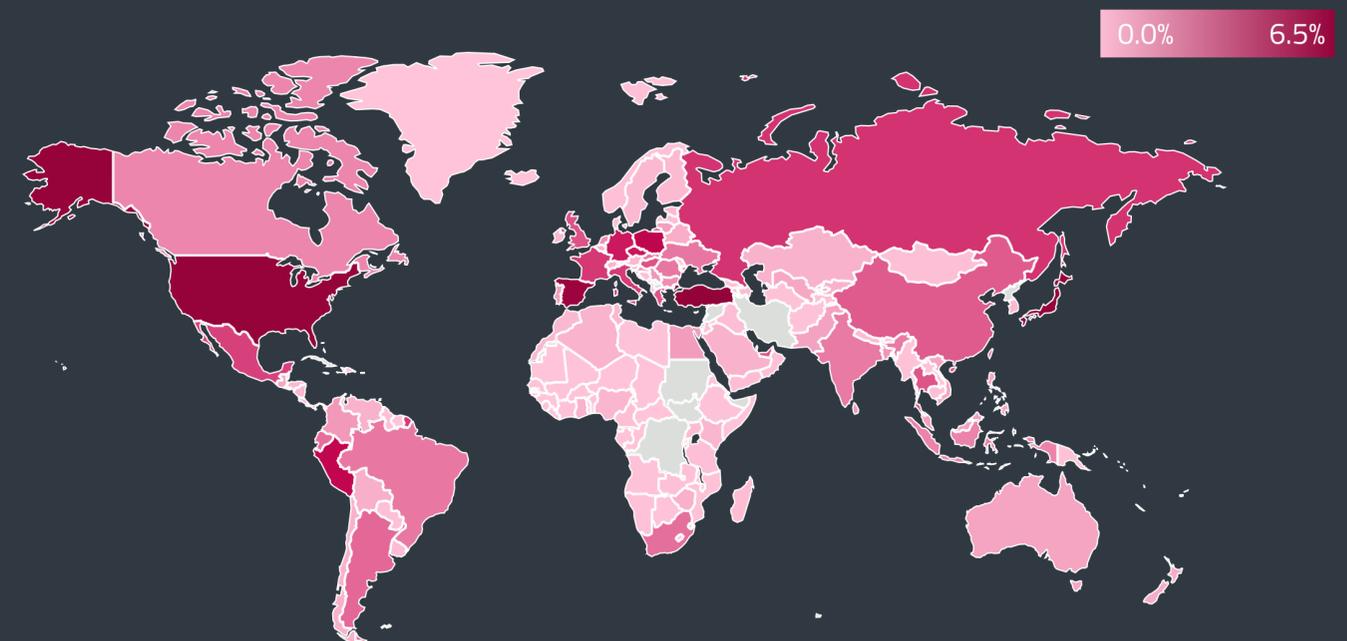
EXPERT COMMENT

The most prevalent variant of JS/Spy.Banker was JS/Spy.Banker.KJ. It is quite an interesting piece of malware because the part of the code that downloads the skimmer itself is rather short, uses only a handful of common JavaScript functions, and mostly does not use complex obfuscation. This means the malicious code blends in with the original code quite seamlessly, making the infested web page appear safe. This posed a challenge in differentiating between a legitimate site and a skimmer-infested site, showing the resourcefulness of the malware's creators.

Radim Raszka, ESET Detection Engineer

As we already mentioned in the opening paragraph, the Cryptostealers subcategory unexpectedly grew by 49.7% in T2. This development was caused by a staggering increase in PowerShell/PSW. Coinstealer detections, which gained a new variant in T2. More details regarding Cryptostealers can be found in the *Cryptocurrency threats* chapter of this report.

Concerning the geographical distribution of Infostealer detections, the top three countries in the list faced almost the same amount of attack attempts: Turkey 6.5%, and both Japan and the United States 6.3%.



Global distribution of Infostealer detections in T2 2022

RANSOMWARE

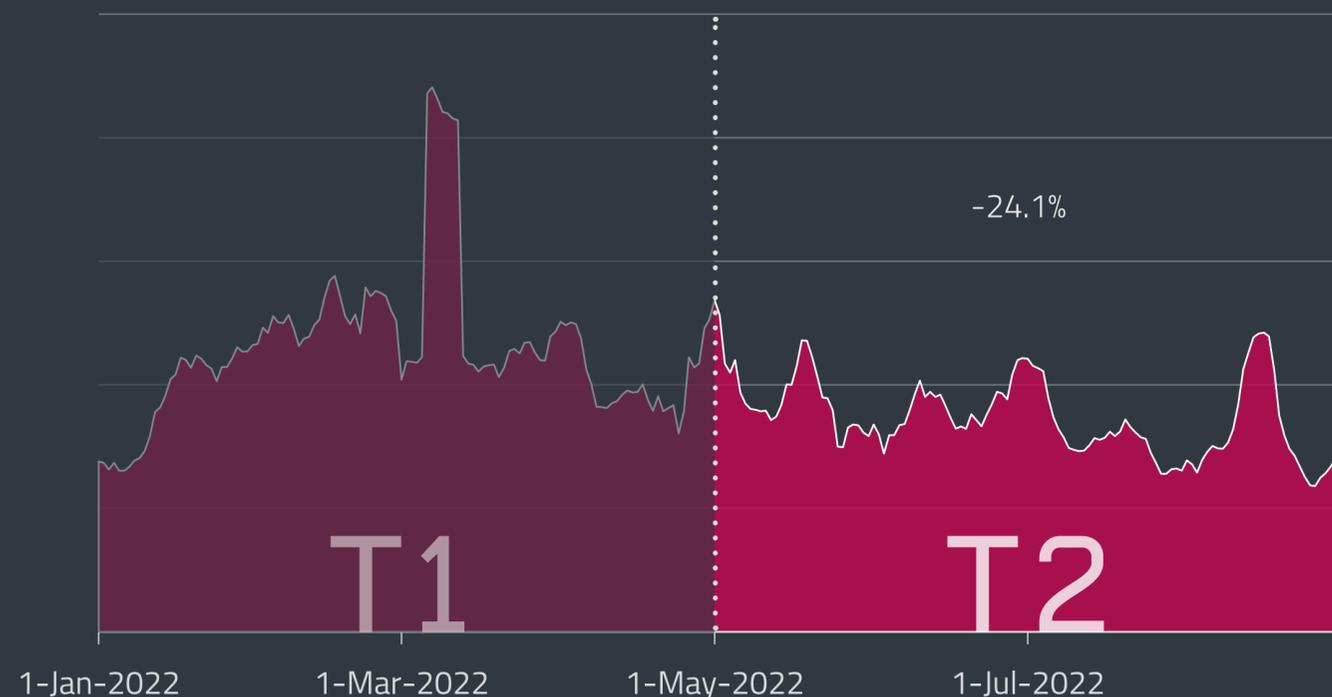
Ransomware detections dropped by a quarter in T2 2022. Politically loaded messages related to the Russian war against Ukraine receded in new variants.

The Ransomware category dropped by more than 24% in T2 2022, which is the most significant decrease since the beginning of 2021 when ransomware detections declined by 27%.

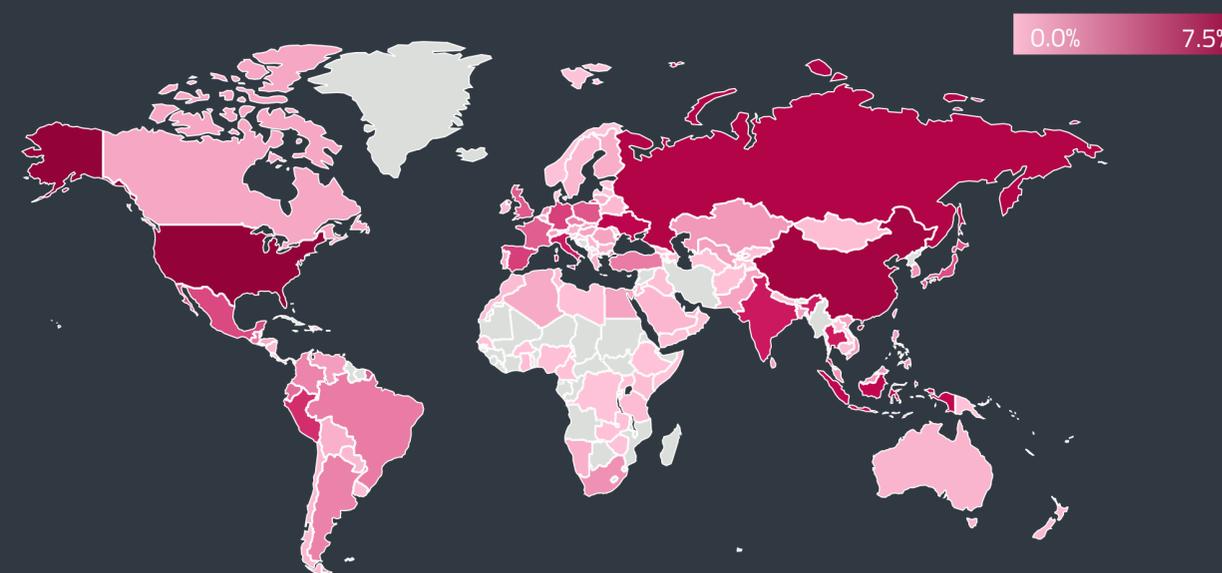
This detection trend shows several upticks, first on May 18, caused by Lockbit attacks in Guatemala, accounting for 59% of all detections on that day. Another peak in telemetry appeared on June 28 due to the spread of Win/Filecoder.WannaCryptor.D (24%) in Peru and the distribution of multiple old variants of MSIL/Filecoder (16.5%) in Ukraine. The last and the largest spike was observed on August 12, caused primarily by well-known variants of Win/Filecoder and MSIL/Filecoder, with 45% of detections that day coming from the United States.

Russia was replaced by the United States in being the country most targeted by ransomware in T2 2022, reporting 7.5% of all such attacks. It was followed by China with 6% and Israel with 5.5%.

Coming in at fourth and fifth place were Russia and Ukraine; both faced roughly the same number of ransomware attacks. The difference compared to T1 2022 was the decreased number of attacks with politically loaded messages. Russia was most commonly targeted by years-old Win/Filecoder variants and ransomware families that lock victims' screens. In contrast, Ukraine was hit mostly by derivatives of HiddenTear, the first open-source ransomware, detected by ESET as AK and Y variants of MSIL/Filecoder.



Ransomware detection trend in T1 2022 – T2 2022, seven-day moving average



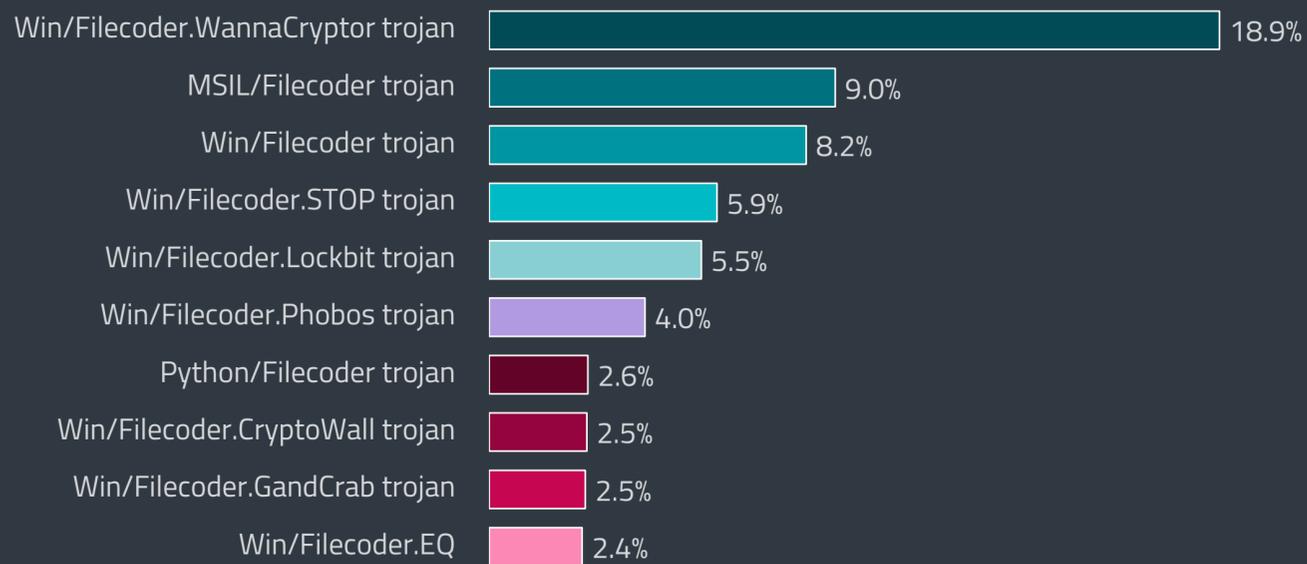
Global distribution of Ransomware detections in T2 2022

In the Ransomware top 10, the most interesting change was probably the increased prevalence of Python/Filecoder. While in T1 2022 it ranked tenth, in T2 2022 it moved up to seventh place, accounting for 2.5% of all detections in the category. The detection covers amateurish attempts to create ransomware. Names such as `test.pyc` used for some of the recently seen binaries and the use of hardcoded private keys such as `1881**ANARCHY_rtxDATA__ANARCHY1881***` support this hypothesis.

```
privkey = "1881**ANARCHY_rtxDATA__ANARCHY1881***"  
enc_key = hashlib.md5(privkey.encode("utf-8")).hexdigest()  
enc_key = enc_key.encode("utf-8")
```

Hardcoded private key as seen in some amateurish Python/Filecoder variants

T2 2022 brought several new trends to the ransomware scene. Lockbit (3.0) started the first ever [ransomware bug bounty](#) [26] program, offering researchers and (un)ethical hackers anything between USD 1000 and USD 1 million in Monero for findings related to their operation. The sought-after items include flaws in malware, vulnerabilities in the leak site, or "brilliant ideas" for improvements. The highest sum is reserved for anyone who can identify the person running Lockbit's affiliate program, currently known by the nickname "LockBitSupp". In an interesting turn of events, it was this actor who [publicly claimed](#) [27] that one of the gang's victims – Entrust – was behind the DDoS attacks that were hitting Lockbit's leak sites.



Top 10 ransomware families in T2 2022 (% of Ransomware detections)

Another trend observed in T2 2022 is the shift of skilled ransomware writers towards the Rust programming language. The first to make the move were the [BlackCat](#) [28] creators, followed by [Hive](#) [29]. The latest addition to this currently exclusive club is the T2 newcomer [Luna](#) [30]. Using Rust offers malware operators several advantages, including improved evasion of security solutions and improved [error resistance](#) [31].

In the past couple of years, one of the most prevalent red team tools (ab)used by the ransomware gangs has been Cobalt Strike. However, in T2 2022 some of the ransomware groups switched to [Brute Ratel](#) [32] because of its lower detection rates by EDR and security solutions.

The last four months saw some curious ransomware-related cases. For example, a victim in the automotive industry experienced what it meant to have initial access to their network sold on the black market. Its systems were hit by [three different ransomware gangs](#) [33] in just two weeks. Another uncommon approach has been seen in cases caused by a new ransomware family called Zeppelin. [CISA and the FBI](#) [34] warned that victims targeted by this gang could see their data encrypted several times during a single compromise.

But ransomware actors are also facing increased pressure from authorities. Due to ransomware attracting so much attention, new regulations are being passed, sanctions imposed, and the willingness of victims to pay the ransom decreasing. A mixture of these factors is forcing the threat actors to refocus from high-profile victims to mid-sized organizations and to lower the demanded [ransoms](#) [35]. A new [report](#) [36] by the British think tank RUSI even suggests that increased attention on ransomware is pushing perpetrators to look for new hunting grounds, primarily in the Global South, where attacks are less laborious and the risk of prosecution is lower.

An illustrative case of making the life of ransomware gangs harder is the [USD 10 million reward](#) [37] offered for information about “individual(s) who hold a key leadership position in the Conti ransomware... group”. But even victims may not come out unscathed, as shown by the [Colonial Pipeline](#) [38] case. The US regulator has proposed to fine the company nearly USD 1 million for “control room management failures” that complicated recovery from the 2021 ransomware compromise.

Despite the growing law-enforcement and regulatory activity, many new ransomware actors appeared on the scene in T2 2022. Reminding the world of the 2017 WannaCryptor (aka WannaCry) incident, [CISA and the FBI](#) [39] warned that North Korean threat actors cooked up a new ransomware family called Maui. About a week later Microsoft attributed another newcomer [HolyGhOst](#) [40] to hackers from the same country. QNAP NAS devices have another threat to worry about too, namely [Checkmate](#) [41]. A new free-to-use ransomware builder [Redeemer](#) [42] (version 2.0) may also worsen the situation as it opens the doors for unskilled actors who want to try their luck in the game.

There were also some “rebrands” during this period. Chaos ransomware builder has been used to create another family called [Yashma](#) [43]. And we have to mention Conti, which after catastrophic leaks saw its minions [dissolved](#) [44] into several other gangs, including Hive, BlackBasta, BlackCat, and BlackByte.

The list of high-profile victims in T2 2022 is also quite long. It includes a [Foxconn factory in Mexico](#) [45] hit by Lockbit, the [government of Costa Rica](#) [46] that saw its systems attacked by Conti, building materials manufacturer [Knauf Group](#) [47] hit by Black Basta, and the already mentioned security giant [Entrust](#) [48].

In the happy corner, there were multiple families that ceased their activity or actors behind them were arrested. In the case of [Thanos](#) [49], its creator, seller and also operator – a Venezuelan doctor – was arrested by the authorities. [AstraLocker](#) [50] closed up shop with decryptors now available. Victims of the newcomer [Yashma](#) [51] can also decrypt their files using a new decryptor.

The final bit of good news comes from the [No More Ransom](#) [52] initiative – where ESET is an associate partner – which in its six years of existence has helped 1.5 million ransomware victims to decrypt their files and save around USD 1.5 billion.

EXPERT COMMENT

The growing proportion of Python ransomware families can have multiple explanations. First, Python is easy to use even for unskilled malware writers. As a scripting language, it also allows threat actors to obfuscate and change their code and create new variants that can evade detection. Second, technically advanced ransomware actors are abandoning the mass-spreading model mostly tracked by our telemetry and are increasingly focusing on big-game hunting and RaaS schemes, letting the rookies claim a bigger portion of their former market. Last but not least, there are very many “test” projects related to encryption on GitHub that can be easily reused as part of a new ransomware strain.

Igor Kabina, ESET Senior Detection Engineer

ダウンローダー

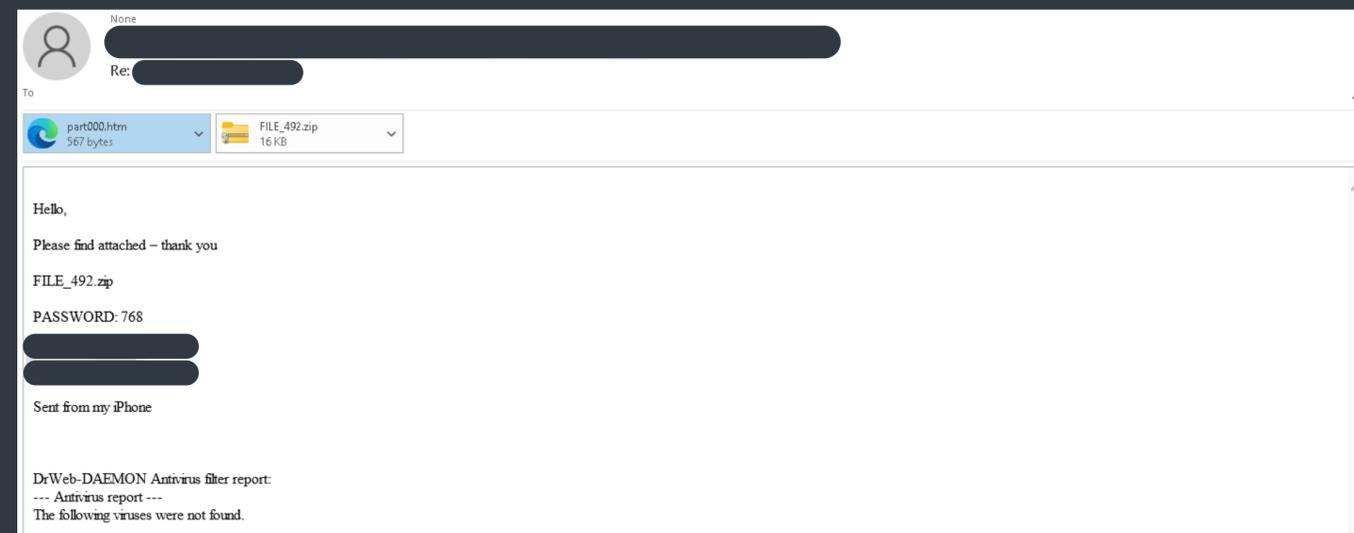
2022年T2は、Emotetのオペレーターは攻撃の手を緩めましたが、それでも「ダウンローダー」のカテゴリにおいてEmotetは圧倒的な強さを保ったままでした。

2022年第T1の終わりまでにEmotetの攻撃が100倍に増加しました。EmotetはT2には新しい攻撃方法を模索するようになりました。2022年T2には、Emotetの攻撃回数は減少へと転じ、31%以上減少しました。

マイクロソフトがVBAマクロを無効にした [53] ことを受けて、EmotetのオペレーターはVBAマクロを悪用する手法を諦めました。Emotetは武器化したMicrosoft Officeファイル(91)やLNKファイル(9)を悪用する新しい攻撃手法に移行しています。いずれの場合でも、パスワードで保護されたZIPファイルがメールで配信されます。

LNKファイルを使用した大規模なキャンペーンは、5月18日に一度発生しました。このキャンペーンでは、主に日本とイタリアのユーザーが標的になりました。6月から7月中旬にかけてトレンドチャートで確認できる他の攻撃数の上昇はすべて、同じ地域を標的としており、武器化した文書やスプレッドシート(DOC)を含むマルスパムキャンペーンによるものでした。

ESETのテレメトリ(監視データ)によると、8月はEmotetのオペレーターにとって休暇の月だったと考えられます。2022年T2に初めてEmotetのオペレーターによって追加された機能は、Google Chrome CC スティラーモジュール [54] です。このモジュールは、ブラウザからクレジットカード情報を抽出し、コマンド&コントロールサーバーに送信します。また、数年前に利用されていたスプレッダーなど、初期のモジュールも再び悪用されるようになりました。



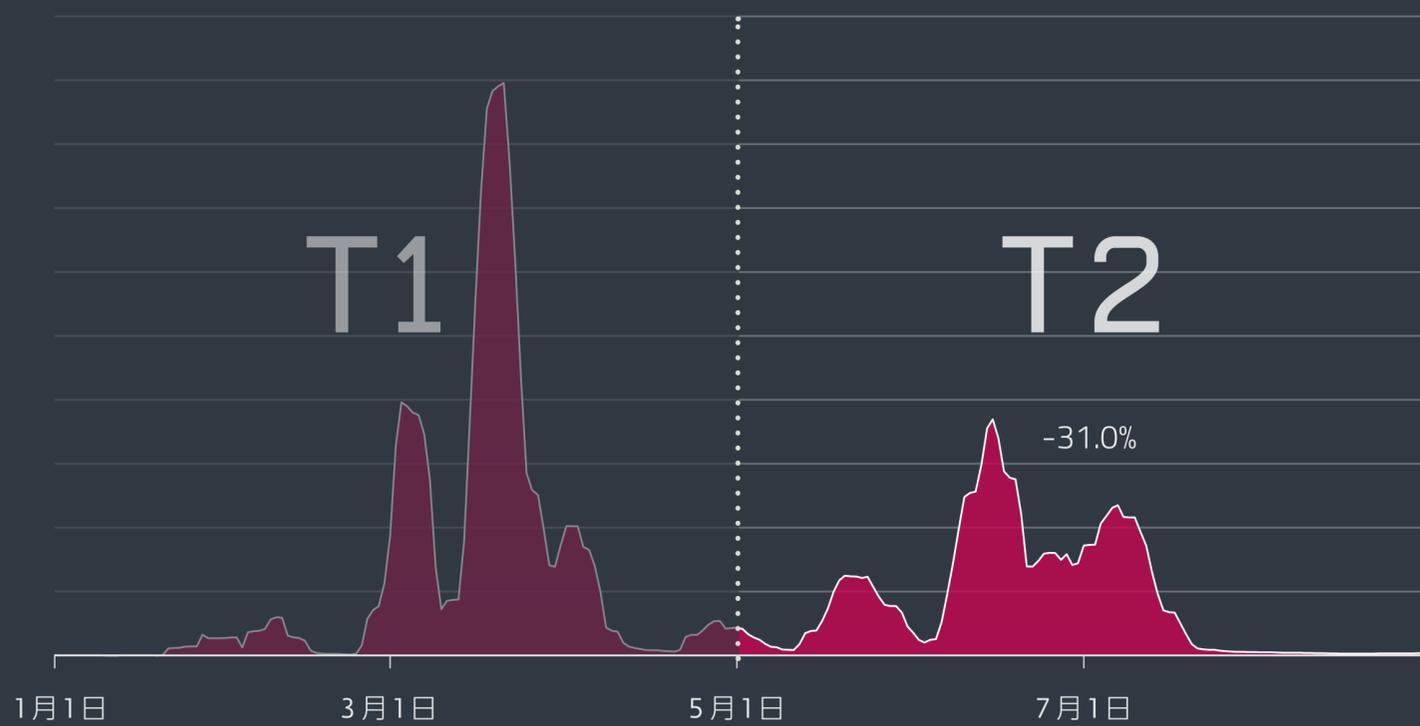
パスワードで保護されたZIPファイルを添付してマルウェアを拡散させるEmotetのマルスパムキャンペーンのメール

2022年T2の「ダウンローダー」カテゴリのトップ10では、引き続きEmotetが最も影響力のあるマルウェアになっています。Emotetの悪意のあるDOCファイルとLNKファイルは、「ダウンローダー」カテゴリ内の検出数のほぼ半分を占めています。このカテゴリ全体の検出数は16%減少しました。トップ10にランクインした注意が必要なマルウェアは、MSIL/TrojanDownloader.Agentです。検出数が21%増加しており、主にトルコとスペインのデバイスを攻撃しています。

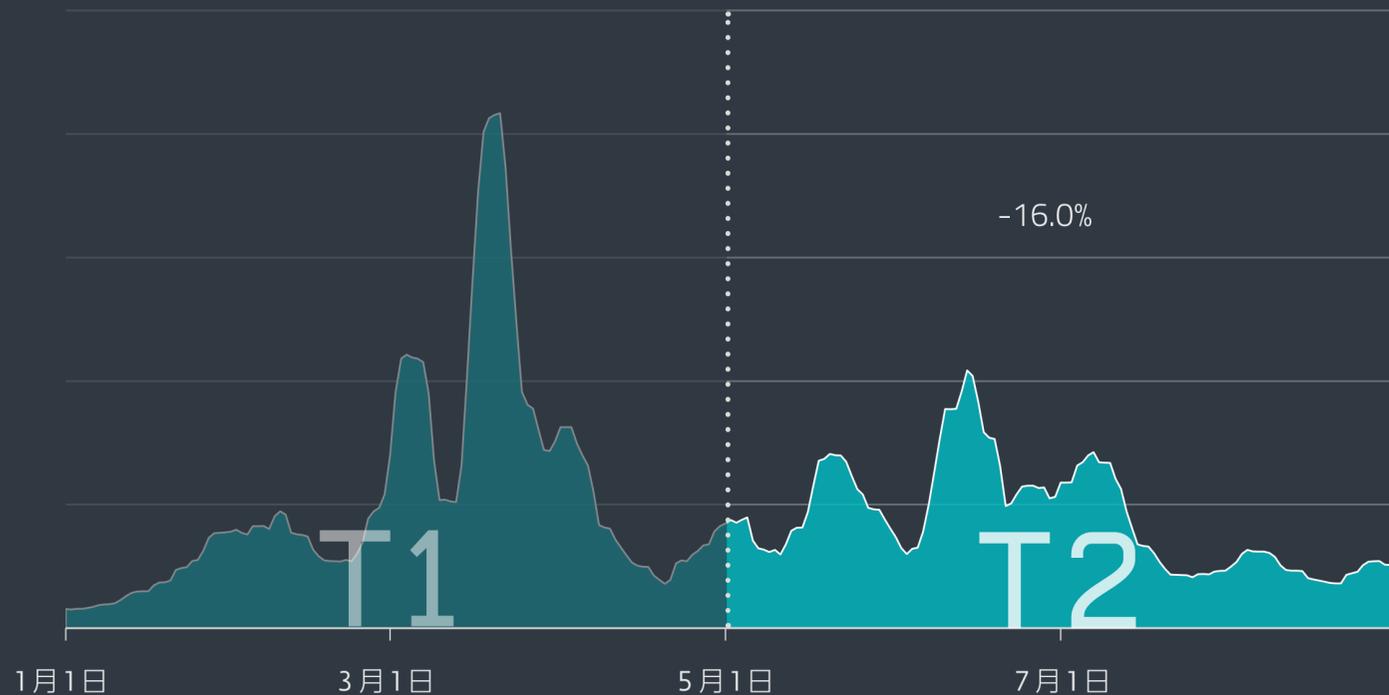
ESETのエキスパートの解説

6月には、Emotetのオペレーターは、2021年1月にテイクダウンされるまでラテラルムーブメント(ネットワーク内の水平移動)に使っていた古いスプレッダーモジュールを再び利用していることが確認されました。この主な目的は、ハードコードされたユーザー名とパスワードのリストを使用して、ブルートフォース攻撃によってネットワークにある他のデバイスにリモートからアクセスすることです。アクセスに成功すると、このスプレッダーは侵害したシステムにメインのEmotetバイナリをコピーし、サービスとして実行します。

ESETマルウェアリサーチャー、Zoltán Rusnák

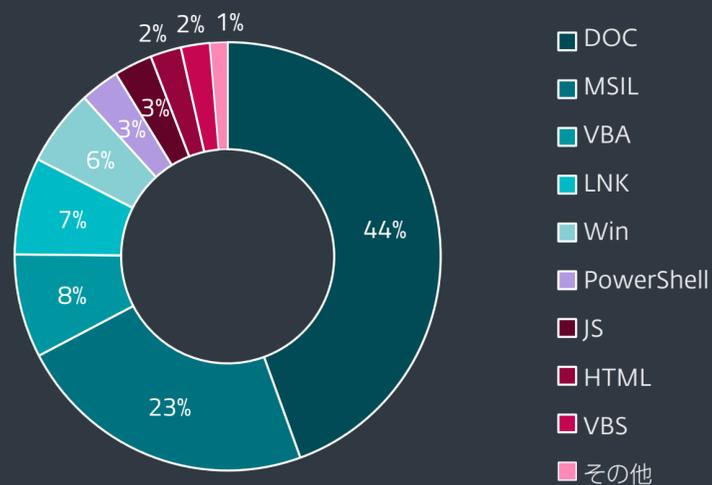


2022年T1～2022年T2のEmotetの検出傾向、7日移動平均線

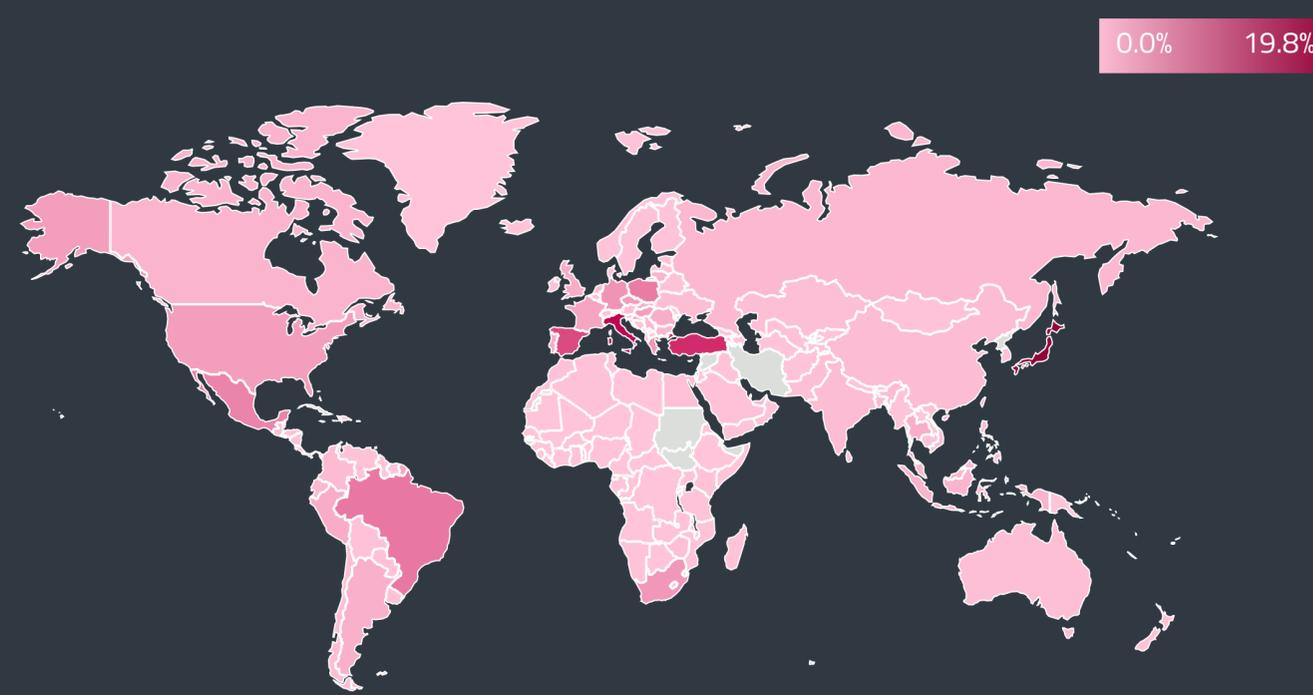


2022年T1～2022年T2のダウンローダーの検出傾向、7日移動平均線

MSILの亜種であるJDM、MVU、MRSは、EXEファイルとそれを実行するDLLツールの2つのバイナリをダウンロードする既知の手法を使用しています。標的となったシステムは、その後、Agent Tesla、Fareit、MSIL/Agent.CFQ トロイの木馬のいずれかに侵害されます。KXQとMFVの亜種は戦術を変えており、JPGまたはBMPファイルを偽装した暗号化されたDLLインジェクタをダウンロードします。このインジェクタが実行されると同じペイロードが配信されます。



2022年T2のダウンローダータイプ別の検出率



2022年T2におけるダウンローダー検出の世界的な分布

トップ10にランクインしたもう1つのダウンローダーは、攻撃を開始する手法としてVBAマクロを使用しない、PowerShell/TrojanDownlader.Agentです。その亜種であるFSWとFSVは、T2にこのファミリーでそれぞれ5番目に多く検出されており、武器化されたWindowsのコンパイルされたHTMLヘルプファイル(拡張子「.chm」)を拡散するキャンペーンで使用されています。

CHMファイルを実行すると、通常のWindowsヘルプウィンドウが開きますが、バックグラウンドでは秘密裏にHTMLコードが実行されます。このコードは、2つのバイナリが含まれるPowerShellスクリプトをダウンロードします。このスクリプトはローダーになっており、実行中のプロセスに2番目のバイナリと最終的なペイロードMSIL/Spy.AgentTesla.Eを注入します。

セキュリティを侵害する方法としてVBAマクロを使用することが難しくなっていることから、VBAマクロを諦める傾向が2022年T1に確認されていますが、Emotetとこのヘルプファイルを使用するキャンペーンではこの傾向が反映されています。新型コロナウイルスの感染拡大が始まってから、VBAマクロはEmotet、Trickbot、Qbotをなどの多くのマルウェアファミリーで最も多く使用されてきた攻撃手法でした。しかし、2022年の初めには、VBAを使用するダウンローダーは減少し始め、武器化されたOfficeファイル(DOC)やMSILの検出数の方が多くなっています。T2では、VBAが3位、LNKプラットフォームが僅差で4位になっています。

この要因の1つは、2022年2月にマイクロソフトが「インターネットからダウンロードした文書内のVBAマクロはデフォルトで無効化する」と発表したことです。2022年T2には、無効化のロールバックや、無効化についての再アナウンスなど混乱もありましたが、サイバー犯罪者は、LNKファイルやCHMファイルなど、標的を侵害する新しい方法を試しており、VBAマクロはすでに積極的に利用されなくなってきたと考えられます。

CRYPTOCURRENCY THREATS

Cryptostealers were on the rise while cryptocurrency exchange rates plunged.

T2 2022 brought a steep decline in cryptocurrency exchange rates, including the price of bitcoin dipping below USD 20,000 for the first time since late 2020. It seems that, for now, cryptocurrencies, NFTs, and other blockchain-related ventures have lost much of their shine. Looking at the Cryptocurrency threats trend chart, this is true for cybercriminals to a degree, with the T2 detection numbers continuing the decrease started in T1, this time going down by 18.9%.

However, the threat posed by cryptocurrency-related malicious activities was far from gone, as recent headlines were rife with stories of various criminal feats, from NFTs stolen in a [Discord phishing scam](#) [55] to an [exploit](#) [56] allowing hackers to steal bitcoin from ATMs. Law enforcement is also staying vigilant: the US Securities and Exchange Commission (SEC) [announced](#) [57] in May that it plans to increase the size of its cybersecurity unit to protect investors in cryptocurrency markets.

In T2 2022, the Cryptominers subcategory continued its decline from T1, going down by a further 20.7%. Cryptominers still experienced a strong detection peak, which occurred on June 11 and was caused by the AH variant of the MSIL/CoinMiner potentially unwanted application (PUA).

An interesting development in the coinminer threat landscape was the emergence of a new piece of malware based on the ESET-discovered [KryptoCibule](#) [58]. First documented by researchers at [Symantec](#) [59], who named it ClipMiner, this new coinminer, with the ability to scan clipboard content

for wallet addresses, has made its operators at least USD 1.7 million. ESET tracks ClipMiner as two detections, MSIL/Agent_AGen.UG, and MSIL/Agent_AGen.UL. Our telemetry shows that both of them were on an upward trend in T2 2022.

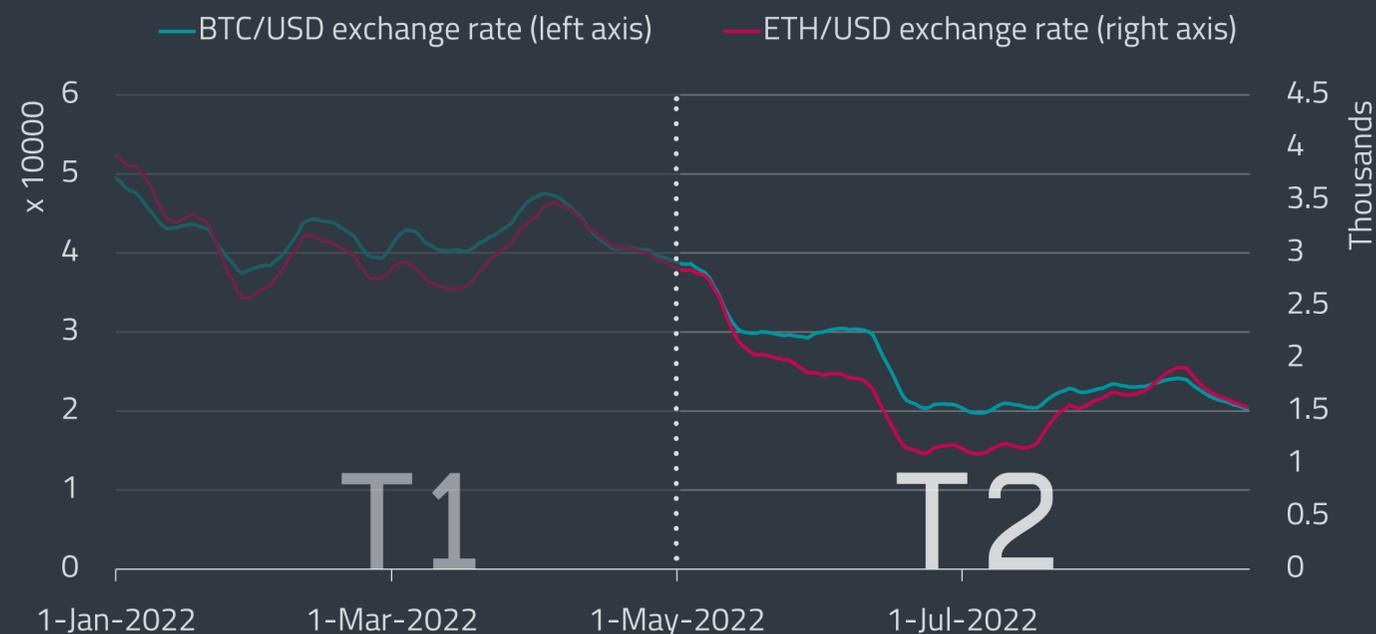
The top three coinminer detections – as usual – continued to be occupied by the same families. Despite a significant decrease in numbers between T1 and T2 2022 (32.8%), the Win/CoinMiner PUA was first with 41.7%. The JS/CoinMiner PUA with 13.8% declined by 7.6%, the smallest drop among the top three. This allowed it to claim second place from its long-time holder, the Win/CoinMiner trojan, which had 12% of Cryptominer detections in T2 after its numbers decreased by 22.9% compared to T1.

Even though PUAs boasted the two most-detected cryptominers, their overall proportion shrunk slightly in the Trojan:PUA ratio, making it 33% (Trojans) to 67% (PUAs) this time, continuing the trend that started in T1. Similarly, the amount of in-browser detections increased relative to desktop detections: in T1, it was 13% to 87%, compared to T2's 17% to 83%.

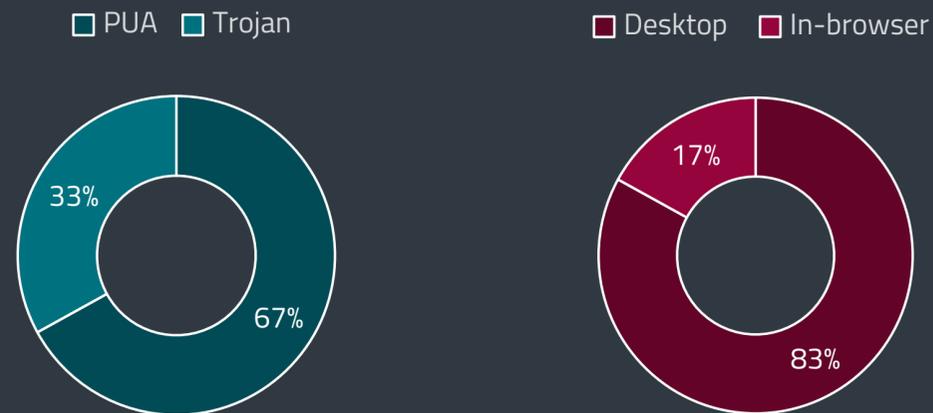
Related to the increase of in-browser detections, the number of cryptojacking domain visits grew by 16.4% in T2. If you want to avoid having your computer used against your will for mining, we advise you to steer clear of free streaming websites or torrent sites.



Cryptocurrency threat detection trend in T1 2022 – T2 2022, seven-day moving average



Bitcoin and Ethereum/USD exchange rates in T1 2022 – T2 2022, seven-day moving average



Trojan:PUA and desktop:in-browser ratio of cryptominer detections in T2 2022

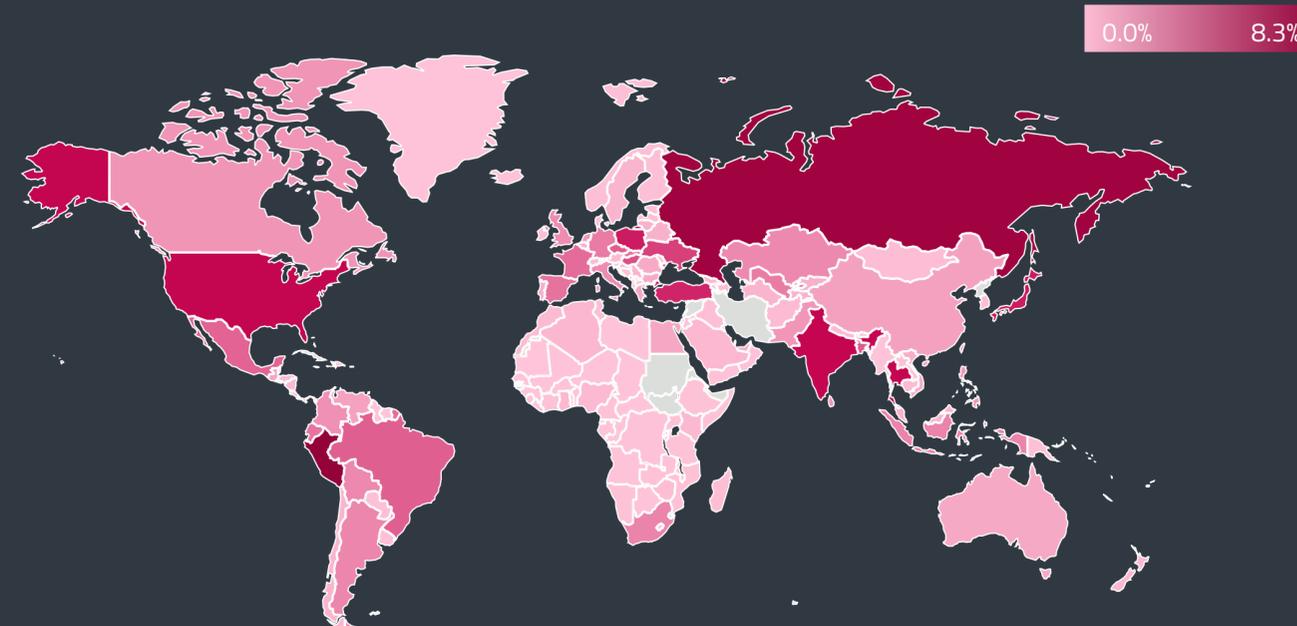
In a surprise twist, the Cryptostealers subcategory did not decline this time. Even more surprisingly, not only did they not decrease in number, they actually experienced rather significant growth of almost 50%. This can be almost single-handedly attributed to the meteoric rise of the PowerShell/PSW. CoinStealer trojan, a malware family that did not have many detections in the past, but managed to become the second most detected cryptostealer in T2 thanks to a new variant added to its arsenal, PowerShell/PSW.CoinStealer.D.

Threats belonging to this malware family search for installed cryptocurrency browser extensions such as Metamask, Binance, or Coinomi. They then exfiltrate this information for nefarious purposes, for example changing the target cryptocurrency addresses in memory to effectively transfer their ownership from the target to the cybercriminal.

We saw see two spikes in the Cryptostealers detection trend. The first, on June 13, was caused by Win/Spy.Agent, mainly registered in Peru. The second spike, which occurred on July 8, was due to PowerShell/PSW.CoinStealer, with the highest number of attempted attacks registered in India and the United States.

	T1 2022	T2 2022
1	webminepool[.]com	webminepool[.]com
2	dl-x[.]com	mainevnap[.]com
3	wypracowanie.edu[.]pl	dl-x[.]com
4	slovolam[.]sk	gsgazete[.]com
5	carrierecalciatori [.]it	mituus[.]com
6	arafifblues[.]com	slovolam[.]sk
7	kaizoku-ehime[.]jp	wypracowanie.edu[.]pl
8	mainevnap[.]com	monerominer[.]rocks
9	mituus[.]com	arafifblues[.]com
10	monerominer[.]rocks	geotimes[.]com.ge

Top 10 most visited cryptojacking domains in T1 2022 and T2 2022



Global distribution of Cryptocurrency threat detections in T2 2022

As in T1 2022, the Win/Spy.Agent trojan was the most-detected cryptostealer with 30.8%. However, the aforementioned heavy hitter of T2, PowerShell/PSW.CoinStealer, was close behind. Accounting for 27.9% of all cryptostealers, it beat the Win/PSW.Agent trojan, which ended up third and registered 20.7% of cryptostealer detections.

As opposed to the leading coinminers, all the families in the top three cryptostealers experienced growth in T2, paradoxically with Win/Spy.Agent growing the least out of the three, by 14.8%. Since PowerShell/PSW.CoinStealer was, according to our telemetry, mostly dormant in T1, it increased by more than a thousandfold in T2. Meanwhile, Win/PSW.Agent doubled its number of detections, going up by 102.1%.

ESET telemetry registered the highest number of cryptocurrency threat detections in Peru (8.3%), with Russia (7.2%) and the United States (4.3%) in second and third places, respectively.

EXPERT COMMENT

Soaring energy prices negatively influence cryptocurrency exchange rates and the willingness to trade or mine cryptocurrencies. Malware authors now increasingly find it more profitable to steal cryptocurrencies than to illicitly mine them. Additionally, free streaming websites and torrenting sites are capitalizing on the trend of releasing films straight to streaming platforms that started during the height of the pandemic, and in-browser coinminers are taking advantage of that. With the continuing energy crisis, we anticipate that the growth of cryptostealers accompanied by the rise of in-browser coinminers will continue.

Igor Kabina, ESET Senior Detection Engineer

WEB THREATS

Shipping-themed phishing lures skyrocketed while most web threats stagnated.

Web threats did not experience as extensive a decrease in T2 2022 as other monitored categories, but nevertheless started exhibiting a slight downward trend. Overall blocks decreased by 6% and the decline was somewhat more pronounced when it came to the number of unique URLs blocked, which went down by 10.3%. All of the web threat subcategories followed this trend too, the only exception being unique phishing URL detections – those increased by 28.3%.

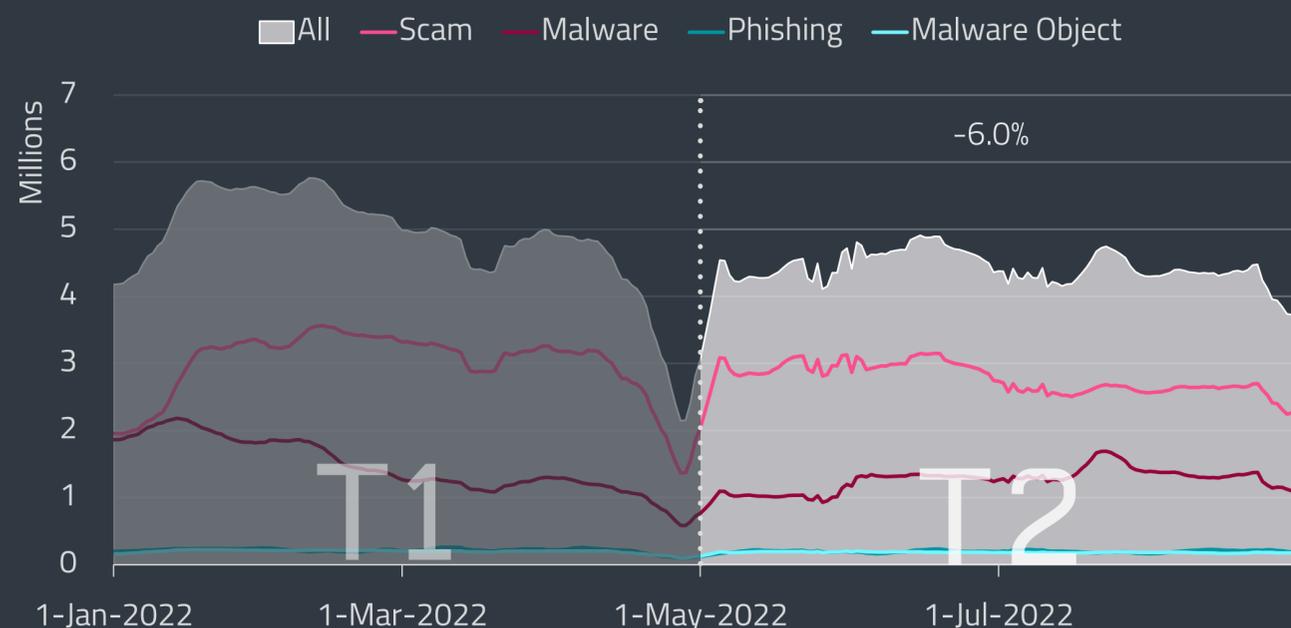
The number of unique phishing URLs that ESET products blocked reached almost 4.7 million in T2. On average, we blocked 38,000 of these a day. Interestingly, despite the significant uptick in unique URLs, the overall number of detected phishing websites remained relatively stable, only decreasing by 3.9%.

As in T1, of all of the Web threat subcategories, Malware blocks declined the most. The total number of malware-distributing website blocks went down by 9.8%, while the number of unique URLs our products blocked diminished by a quarter. On the other hand, the number of legitimate websites hosting malware, labeled Malware objects in the accompanying charts, stayed stable, with only a 3% decrease in both all blocks and unique blocks.

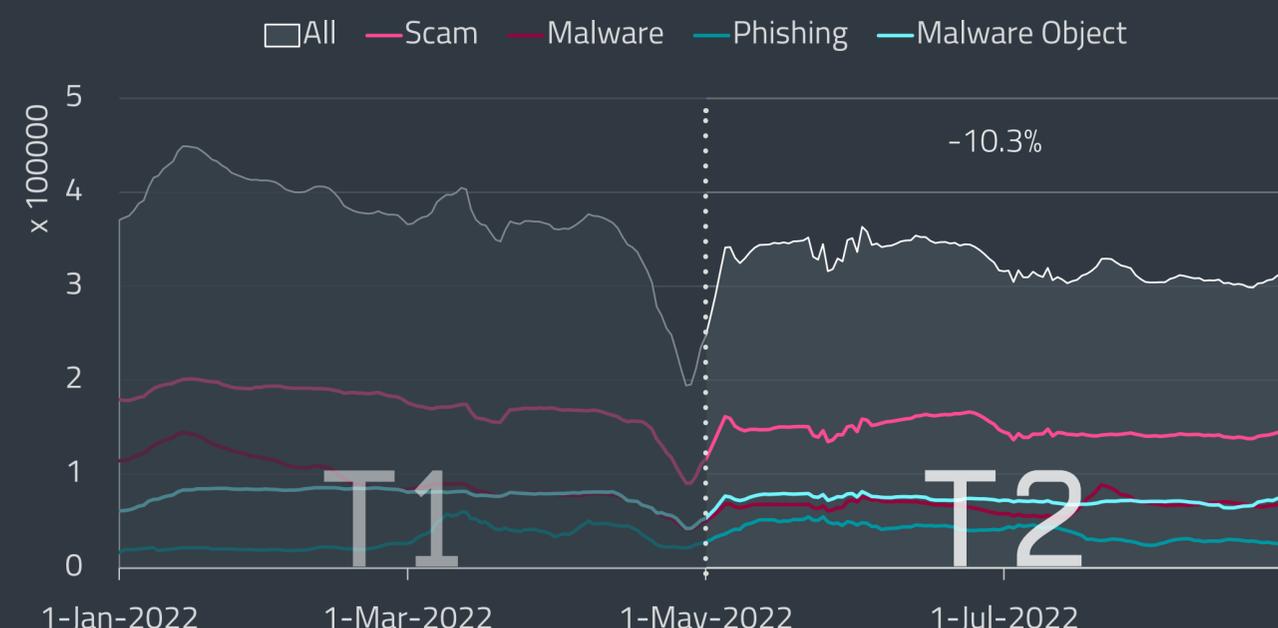
Scam site detections did not change drastically (4.5% decrease) and remained the most prevalent form of web threat, with over 340 million overall blocks and 18 million unique blocks. Their numbers

	Malware	Scam	Phishing
1	freychang[.]fun	survey-smiles[.]com	propu[.]sh
2	aj2396[.]online	s.sarafan[.]fun	mrproddisup[.]com
3	jecromaha[.]info	v.vfghe[.]com	foreign-movies.baby-supernode[.]xyz
4	www.hostingcloud[.]racing	mybetterck[.]com	thecred[.]info
5	iclickcdn[.]com	newrrb[.]bid	watchvideoplayer[.]com
6	webanalyser[.]org	bwukxn[.]com	www--bancosantafe--com-- ar.insuit[.]net
7	d1ywb8dvwodsnl.cloudfront[.]net	serch07[.]biz	tech4-you[.]com
8	vk-online[.]xyz	cellar.z5h64q92x9[.]net	tabledownstairsprovocative[.]com*
9	browworker1s[.]com	loft.z5h64q92x9[.]net	gtorra[.]pw
10	buikolered[.]com	hilarion-lar[.]com*	google-qa[.]net

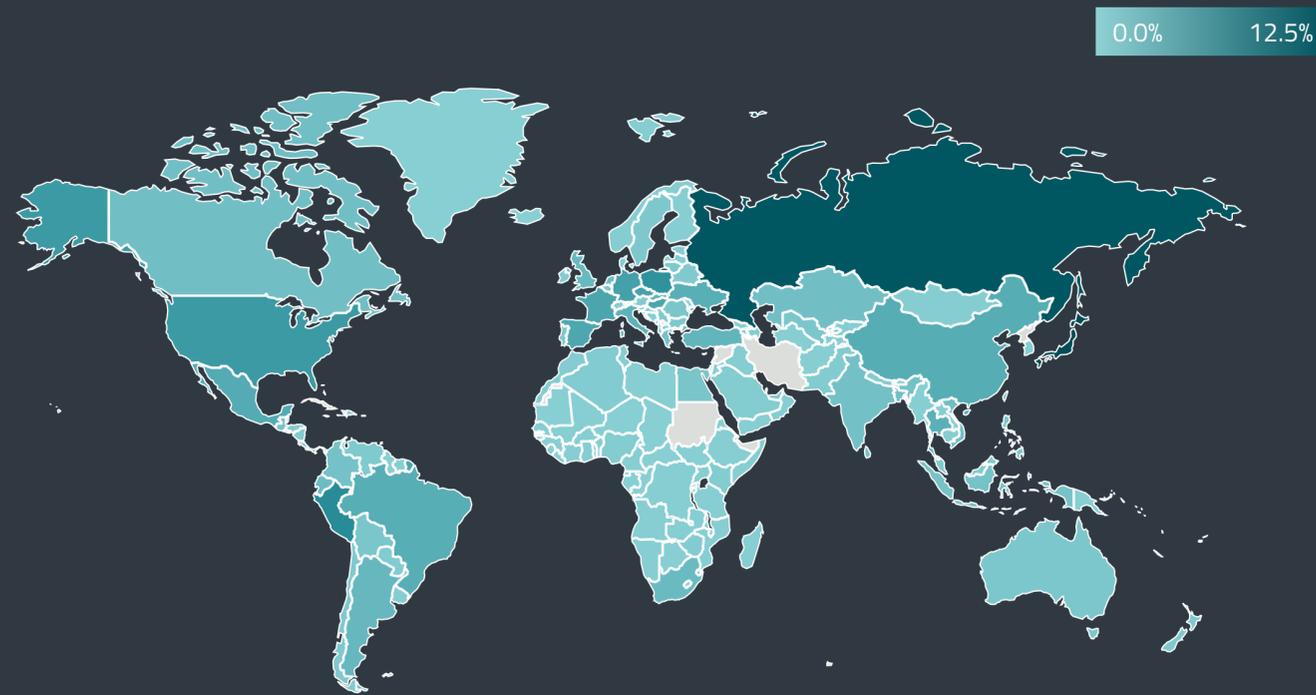
Top 10 blocked Malware, Scam and Phishing domains in T2 2022; domains first detected in this period are marked with *



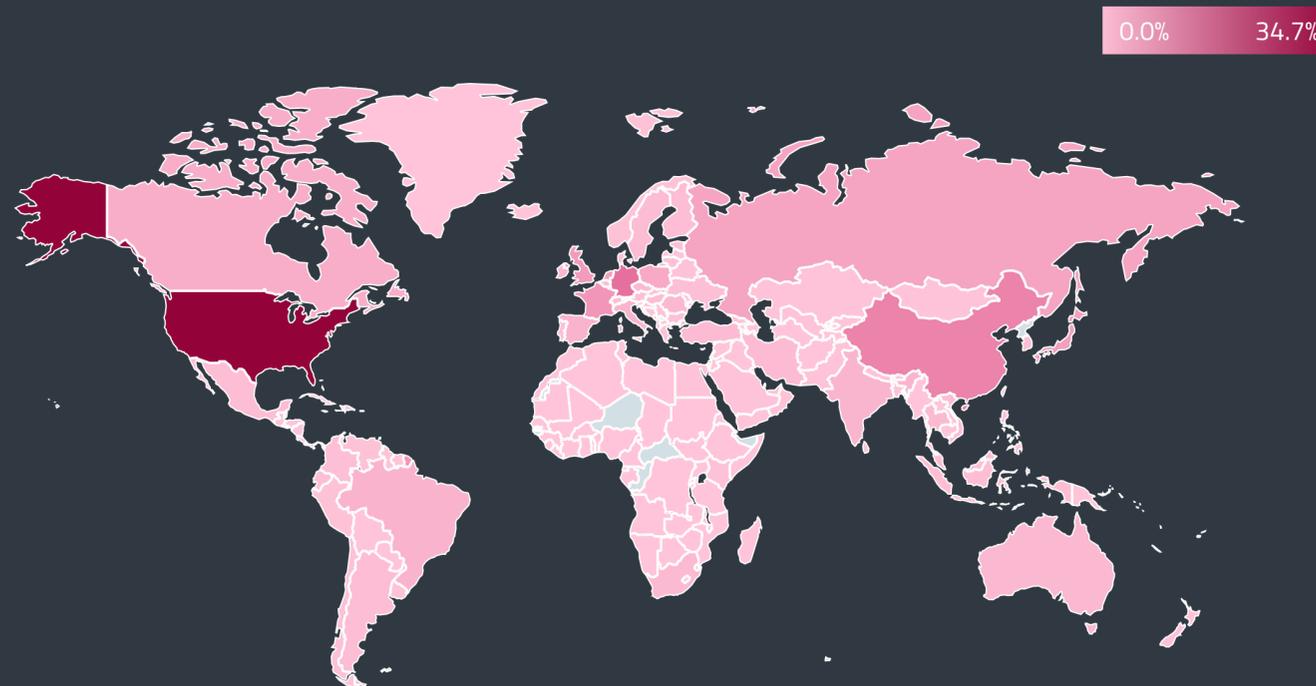
Web threat block trend in T1 2022 – T2 2022, seven-day moving average



Unique URL block trend in T1 2022 – T2 2022, seven-day moving average



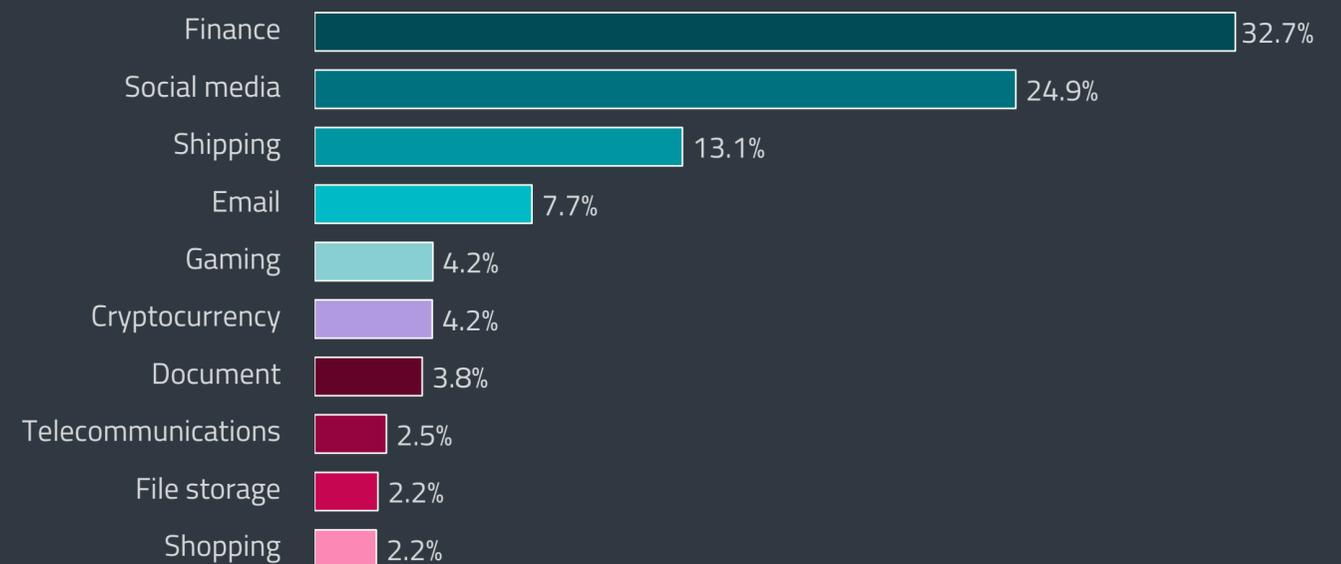
Global distribution of Web threat blocks in T2 2022



Global distribution of blocked domain hosting in T2 2022

peaked on May 25, when we registered 5 million scam website blocks, almost double the daily average amount. Unique scam URL blocks were down by 12.1%, with the largest number of unique blocked scam URLs on July 4, coming to almost 210,000.

Based on GeolIP tracking, the US remained the country hosting the largest proportion of detected Web threats, being the virtual home to more than a third of them (34.7%). Apart from that, the threats were slightly more spread out among other countries, where their shares did not reach double digits, with Germany in second place hosting 7.6% of web threats, followed by China with 5.9%. Conversely, the countries that found themselves on the receiving end of web threat attack attempts the most often were Japan (12.5%), Russia (10.6%), and Peru (4.4%).

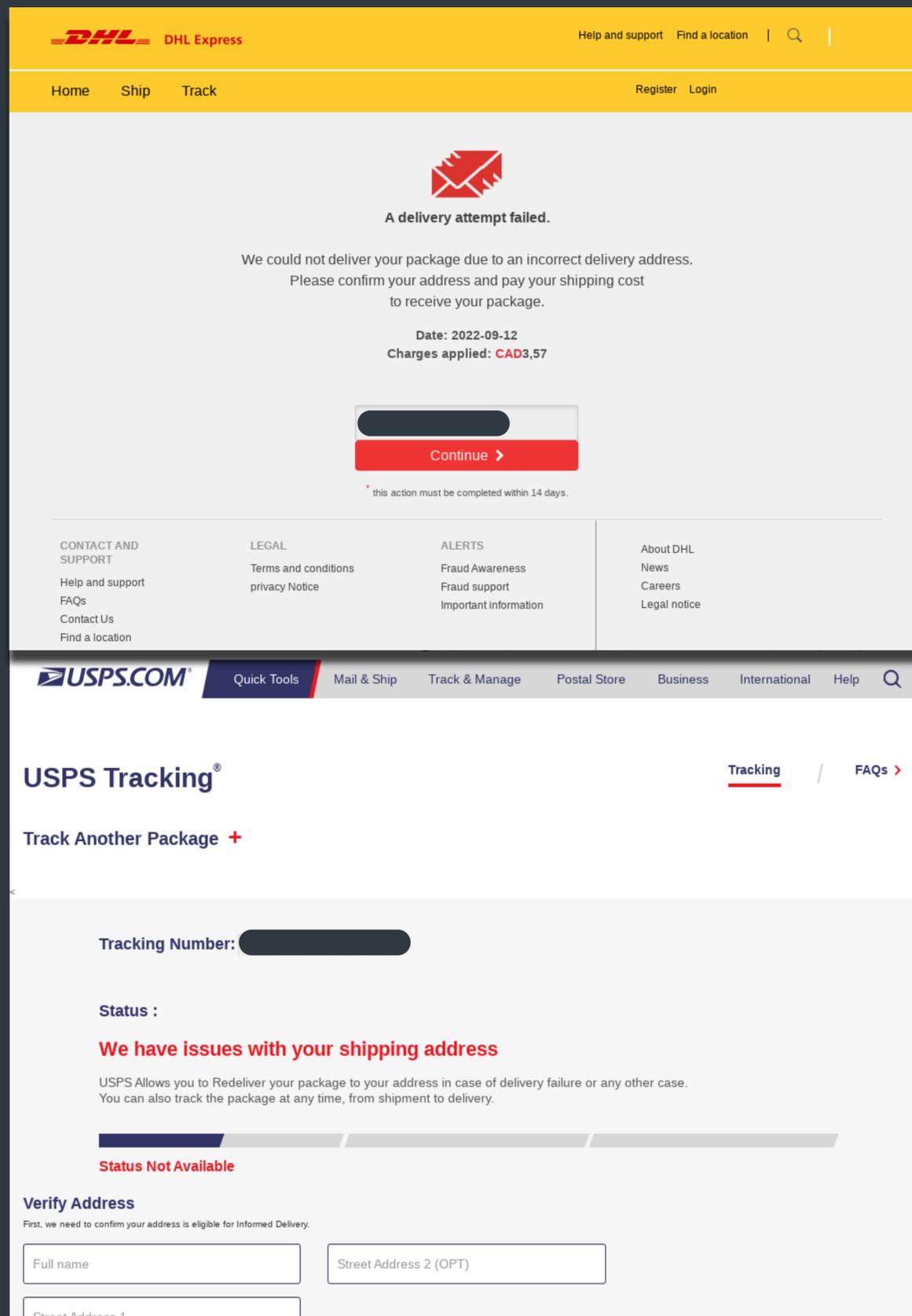


Top 10 phishing website categories in T2 2022 by number of unique URLs

ESET phishing feeds show that the Finance category remained the go-to sector when it comes to phishing websites, making up almost a third of the recorded unique phishing URLs in T2 2022¹. It was followed by the Social media category, which in turn took up one-fourth of detections. That comes as no surprise considering that, according to our data, Facebook was the most impersonated among companies and services. Starting in 2021 and culminating at the beginning of T2 2022, Facebook and Messenger were used as lures in a *large-scale phishing operation* [60] that generated its operators significant advertising revenue.

Of note is also the sixfold increase in detections that catapulted the Shipping category into third place among phishing categories, where it now resides with 13.1%. This category was mostly represented by fake DHL and USPS requests to verify shipping addresses.

¹ The statistic is based on phishing URLs that could be categorized.

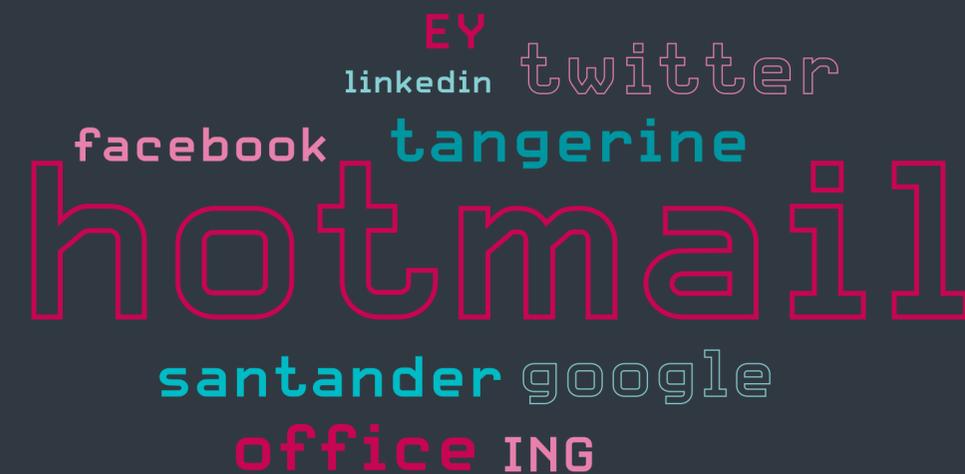


Phishing websites impersonating DHL and USPS and claiming issues with shipping addresses

Though cryptocurrency-themed lures accounted for basically the same percentage of phishing websites as in T1, their actual numbers almost doubled. This is an interesting development at a time when cryptocurrency exchange rates are plummeting. Notably, the increase in these websites is happening alongside the rising number of cryptostealers and in-browser coinminers caused by criminals turning to stealing cryptocurrencies instead of mining them (for more details, see the [Cryptocurrency threats](#) section).

After being reduced by almost half in T1, the number of homoglyph blocks remained practically the same in T2. Hotmail remained the most impersonated service, while T1's second-most targeted, Eastman Credit Union, disappeared from our telemetry completely in T2.

The list of the 10 most targeted services and domains featured two newcomers: the first was a domain that impersonated the Canadian internet-only bank Tangerine at tangerine[.]com – note the a changed into ą and i written as l; the other targeted the global finance group ING using the domain ingdirect[.]com, switching e to ę. Both of them were inaccessible at the time of writing.



Top 10 brands and domain names targeted with homoglyph attacks in T2 2022

EMAIL THREATS

Emotet's weaponized Office file attachments again doubled their proportion of detections. Outlook was the brand most abused by phishers in T2 2022.

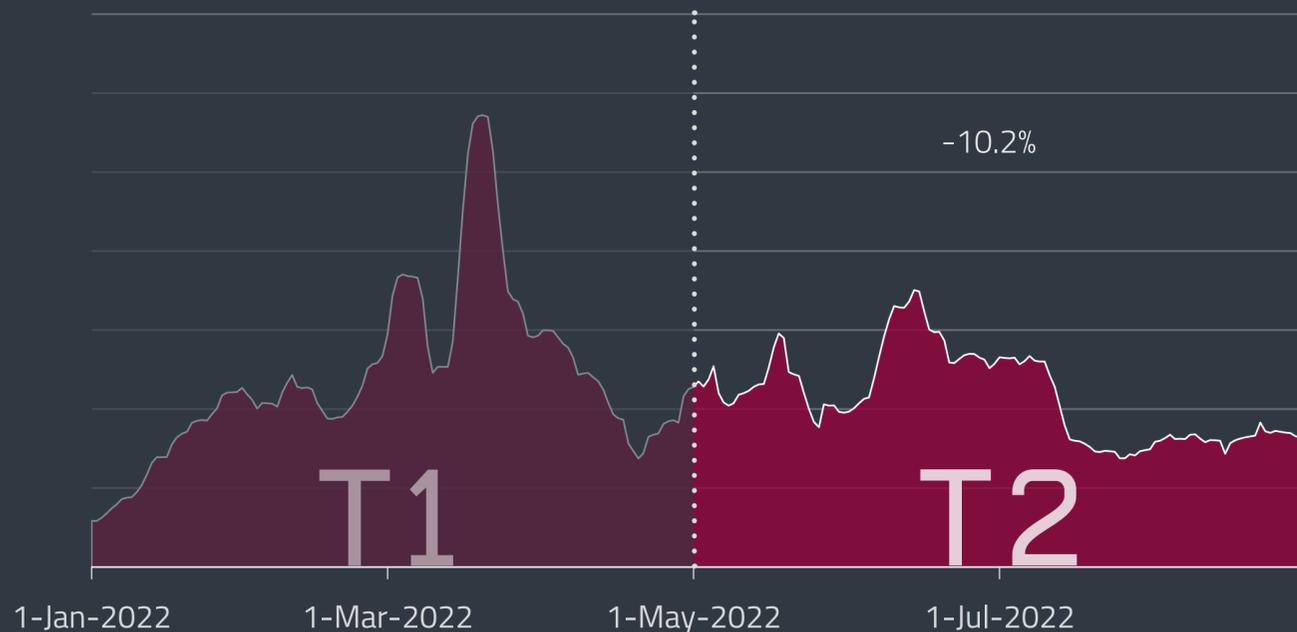
Email threats, which in T1 experienced their largest growth since the beginning of 2021, saw a 10% decline in T2 2022. The decrease was influenced by the lower number of Emotet malspam campaigns and adjustments in ESET's tracking of phishing emails.

Detection levels saw less fluctuation than in the first four months of 2022, with only a handful of smaller spikes in May and June, followed by a period of lower activity starting in mid-July and lasting throughout August.

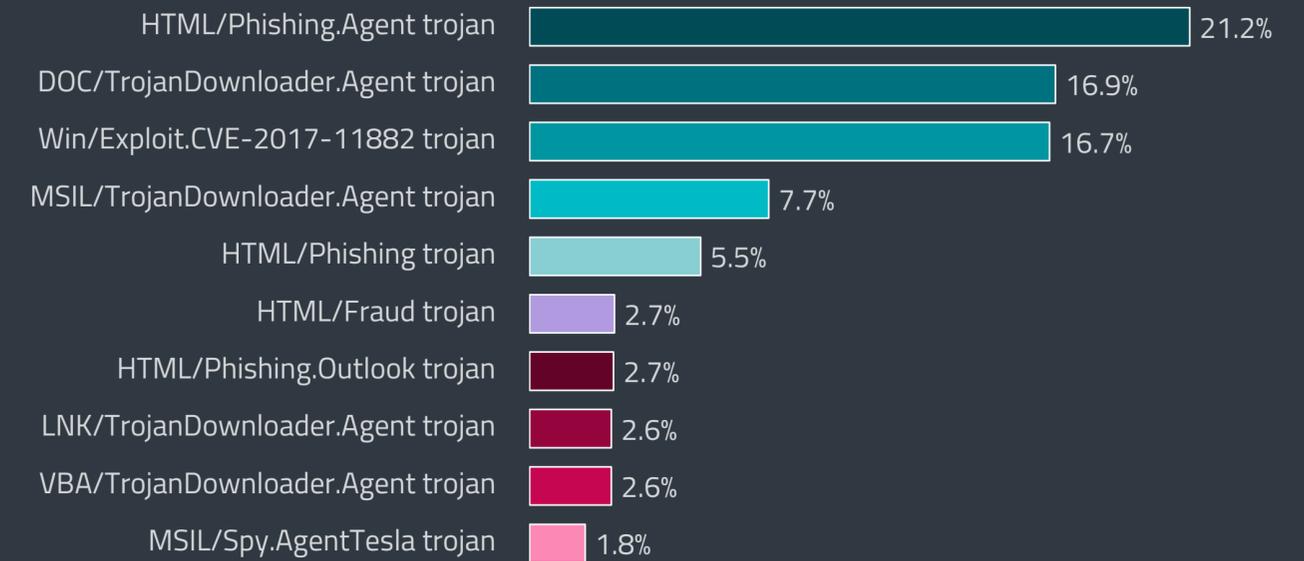
May 16 saw the first notable spike in ESET telemetry this period, with the BOR and F variants of Win/Exploit.CVE-2017-11882 as the main drivers. These variants were part of malspam campaigns distributing RTF downloaders, which in turn delivered MSIL/Spy.AgentTesla as their final payloads.

The recipients of these emails were typically lured into opening attachments that appeared to be DOC files containing a jumble of characters. To hide the malicious nature of the documents, attackers masked them as invoices or purchase lists.

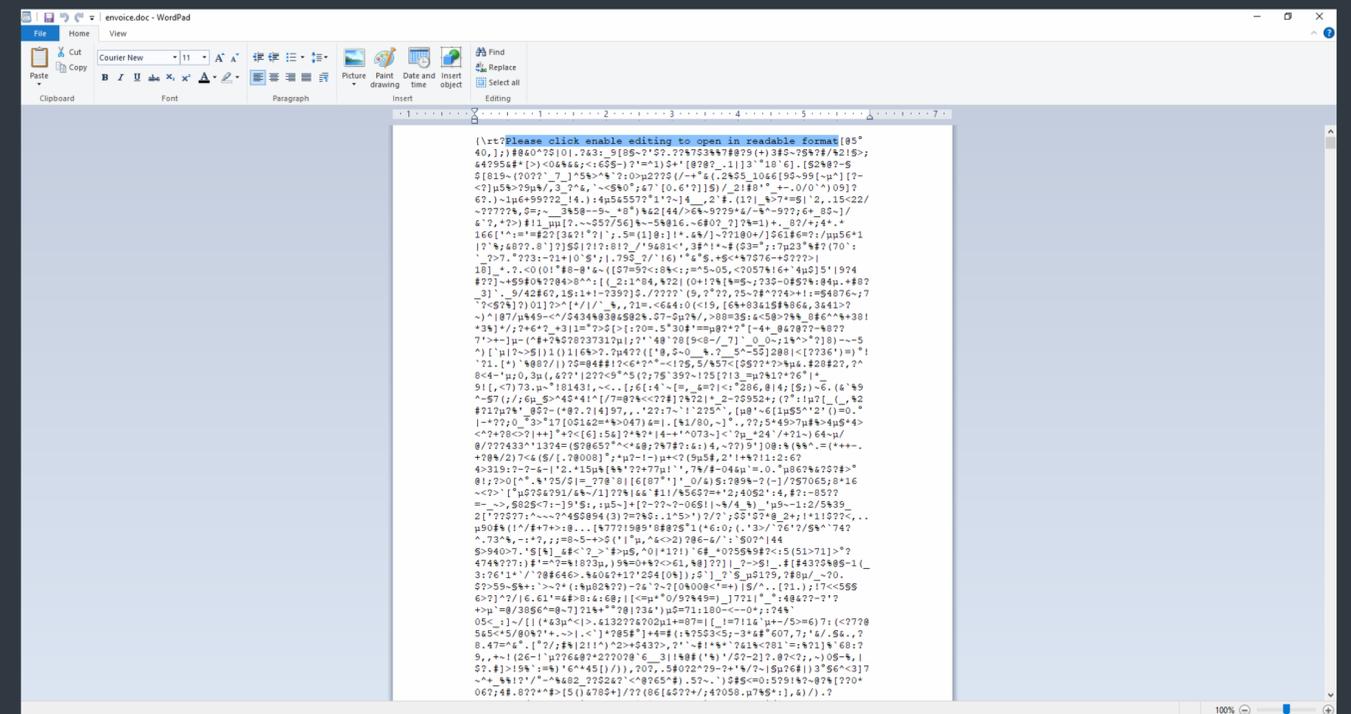
Another wave of the same campaign was seen on June 14, contributing to the largest T2 2022 uptick. However, it wasn't the only wave of malspam that wreaked havoc on that day. The Emotet botnet was flooding inboxes in Japan and Italy with messages carrying weaponized Office files – typically



Malicious email detection trend in T1 2022 – T2 2022, seven-day moving average



Top 10 threats detected in emails in T2 2022



Documents used in a malspam campaign that spread variants of MSIL/Spy.AgentTesla

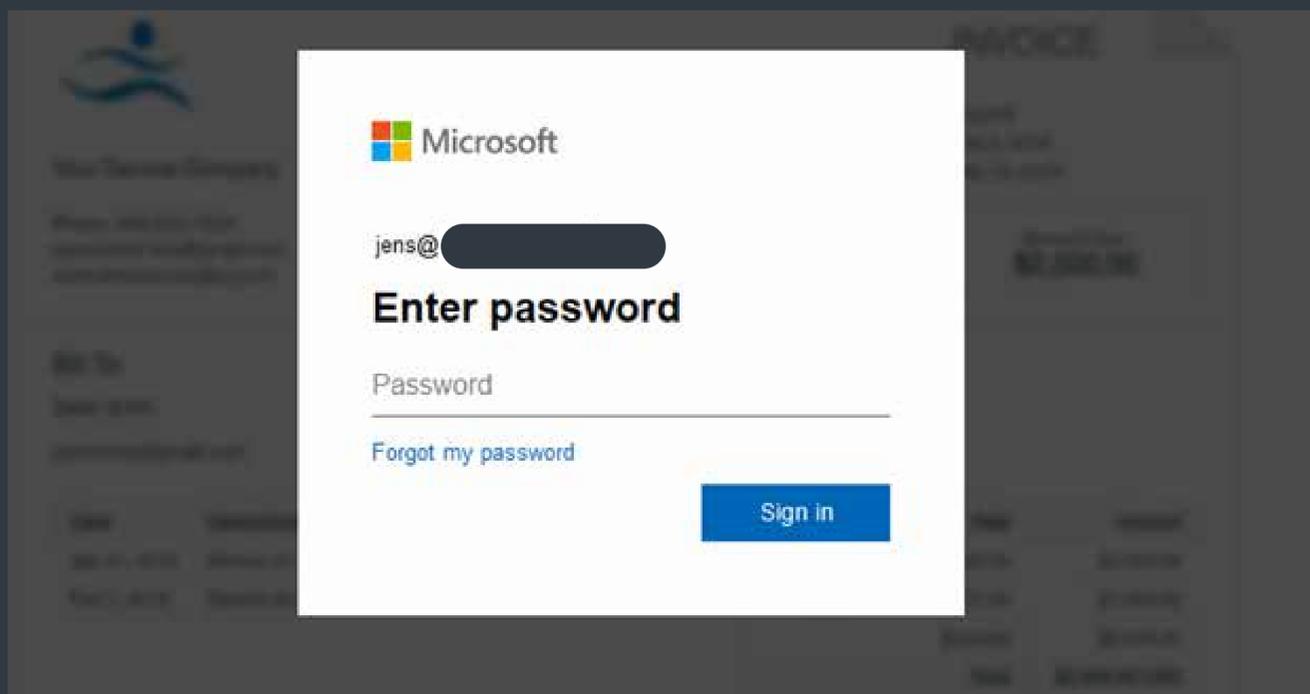
Microsoft Excel spreadsheets – triggering the DOC/TrojanDownloader.Agent.EAR and .DOV detections. The latter also contributed to spikes in the detection trend on June 22 and July 7.

Among the top 10 Email threats, HTML/Phishing.Agent kept its lead with 21%. Its overall numbers declined by 20% between T1 and T2, partially due to an adjustment in ESET telemetry that separated it from emails spreading fraudulent pharmaceutical offers.

The second most prevalent threat, DOC/TrojanDownloader.Agent triggered by Emotet campaigns, also saw a drop of 31%, diminishing its share in the T2 Email threats category to 17%. With this botnet shifting away from VBA macros, VBA/TrojanDownloader.Agent detections are slowly but surely sliding down the top 10, descending from the leading position to ninth place in just one year.

A noteworthy addition to the top 10 was HTML/Phishing.Outlook – a threat that tries to lure its victims to open an HTML file attached to an email, presenting them with a fake Outlook login page and attempting to steal their passwords. Its numbers were already growing in T1, and it further increased its share by 54% in T2, moving up from eleventh to seventh place. Countries that faced the biggest portion of these attacks were the United Kingdom and New Zealand.

While keeping similar detection levels as in T1, Microsoft became the number two among abused brands, being used to target victims in the United States and in the UK. HTML/Phishing.DHL emails, which were wildly popular during the 2020 and 2021 pandemic lockdowns, declined by 55% between T1 and T2 2022, descending to the third position among branded phishing threats.



Example of a fake login form displayed by HTML/Phishing.Outlook

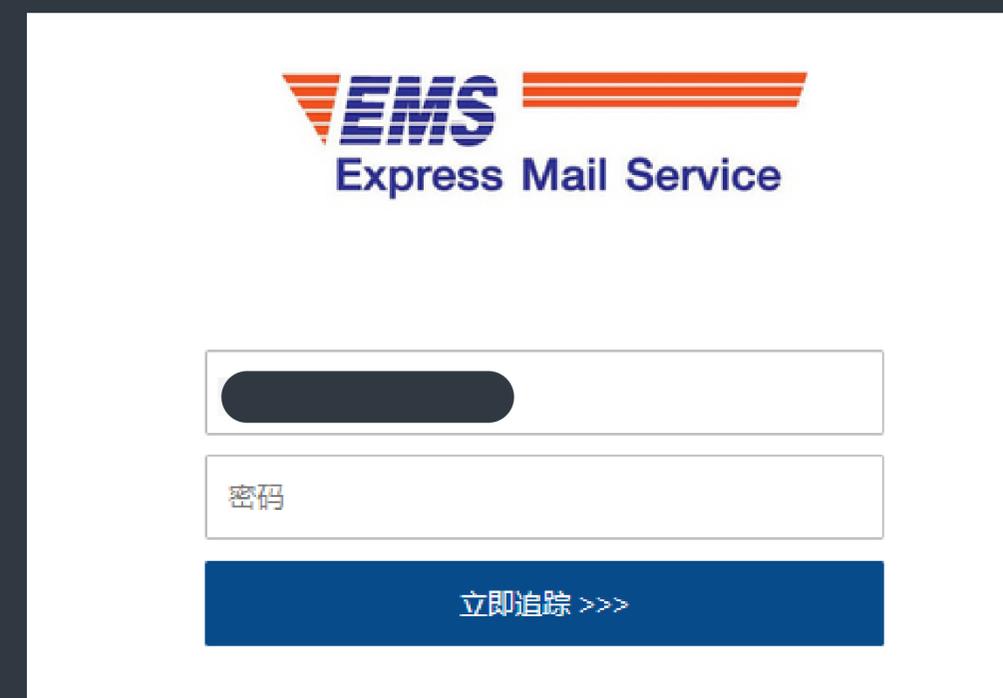
EXPERT COMMENT

The phishing forms found in HTML/Phishing.Outlook email attachments typically come pre-filled with email addresses, probably in an attempt to appear more trustworthy. This might make the targeted user more likely to insert the rest of the requested information, thus making the operation more effective for the phishers.

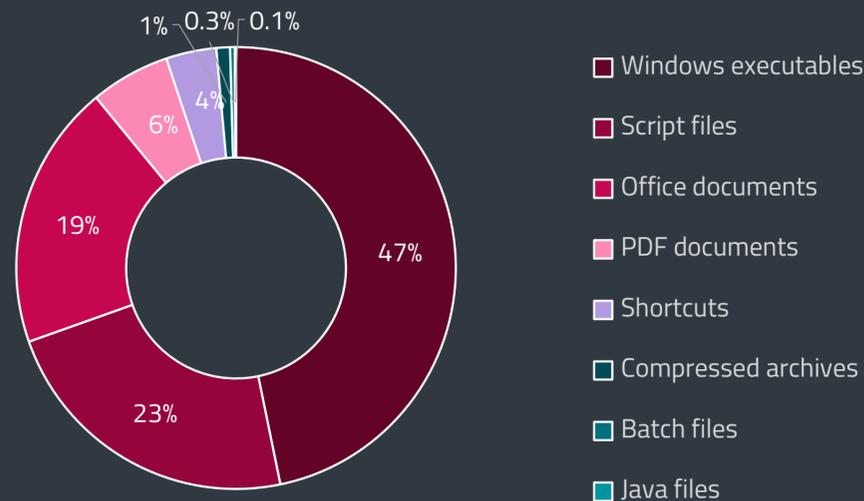
Jiří Kropáč, ESET Director of Threat Detection

The organization whose logo and name saw the biggest jump in abuse between T1 and T2 2022 was Express Mail Service (or EMS). Moving up from fourteenth place to sixth, its detections were 33 times more prevalent than in the previous four months, with most of its targets in the Asia-Pacific region.

Being generic in the subject line presumably pays off, considering that "Re:", "RE", and "Fwd:" were the highest-ranking subject lines reported by ESET telemetry in T2 2022. As for broader subject topics used, hoping to dupe victims into opening the email, the "payment" theme – including invoices, orders and purchases – outran its competition, being used in 46% of malicious emails. The "Bank message" theme was the second most prevalent, being the topic of a quarter (24.7%) of the encountered malevolent messages.



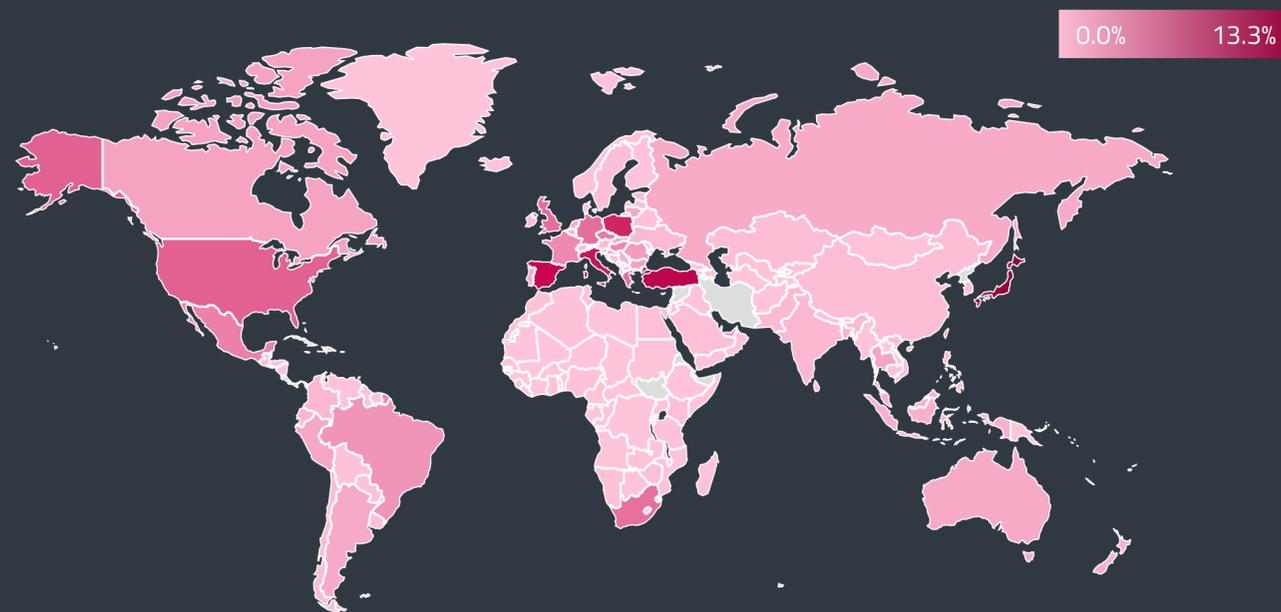
A phishing page posing as an EMS form and spread as an email attachment, detected as HTML/Phishing.EMS



Top malicious email attachment types² in T2 2022

As COVID-19 is becoming endemic, it apparently loses its appeal as a lure. Emails that used the disease in the subject line in T2 were only half as frequent as in T1 2022, reaching a 0.19% share – the lowest level since the beginning of 2021. Going in the opposite direction, “travel” topics were 70% more frequent in T2 than in T1, being the subject line in 1.4% of detected emails.

EU-BusinessRegister.pdf remained the most prevalent name of blocked attachments seen in T2, fueling the well-known subscription scam. Another popular filename among attached files – 198_Invoice_#15427.html – might sound generic, yet is presumably effective, as it triggers the already mentioned and booming HTML/Phishing.Outlook detection.



Global distribution of Email threat detections in T2 2022

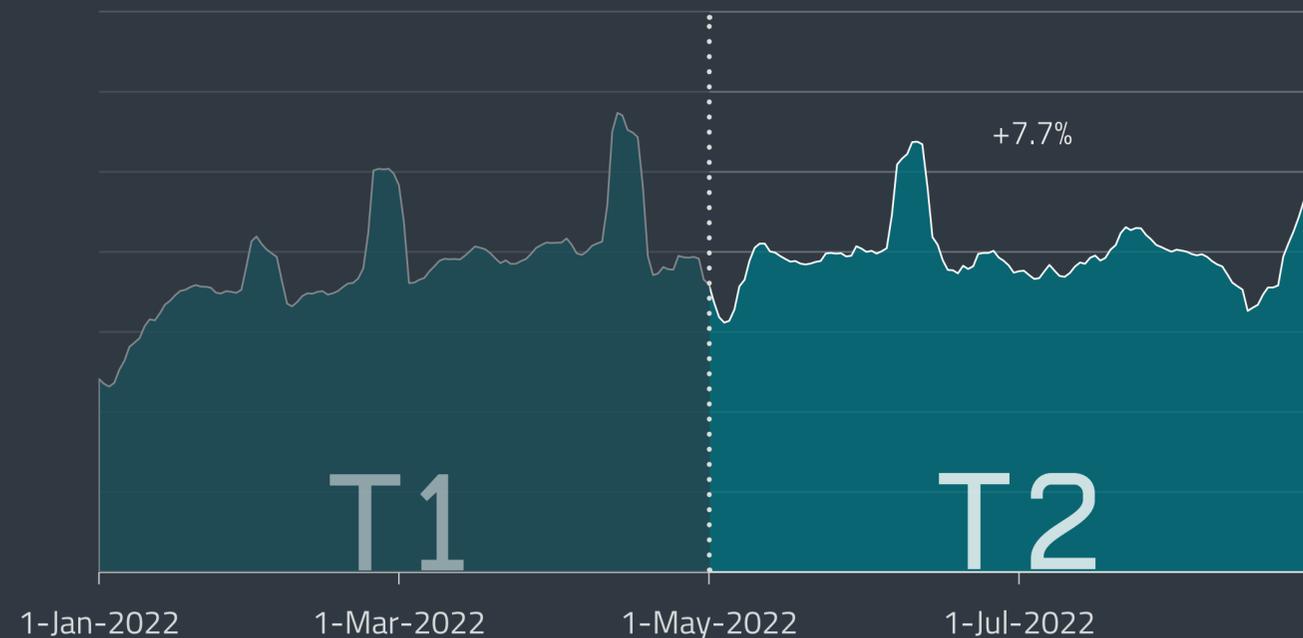
At 47%, Windows executables were the most prevalent malicious attachment type in T2 2022. Although losing eight percentage points relative to T1, this file format kept its distance from the 23% reached by the second-place contender, script files. As in T1 2022, compromised Office files almost doubled their share, going from 10% in T1 2022 to 19% in T2 2022. The reason for the uptick is identical to the previous four months, namely Emotet “promoting” Office files other than VBA-macro-containing ones to its main intrusion vector, instead of those with VBA macros.

Spam emails kept a steady upward pace between T1 and T2 2022, increasing by 8%. There were two short-lived spikes in ESET data: one around June 6, with numbers reaching approximately double the volume of a regular day, and a second one in the last days of August, probably driven by the end of the holiday season.

If the geographic distribution is considered, the top five countries remained the same, but some of them switched places. The United States remained the biggest source of spam, spewing out 20.5% of the global volume. The second most prolific spam producer was China with 14.6%, followed by Poland with 11%, France with 9.4%, and Japan with 8.8%.

Looking at the spam portion in all emails, China has the worst ratio, with 76% of sent messages falling into the unsolicited category. Singapore is second with 41.3% and Russia third with close to 30%.

When interpreting this data, it should be noted that ESET’s visibility into spam is limited due to email traffic commonly first being filtered at the level of internet email service provider, and elsewhere, before reaching ESET-protected endpoints.



Spam detection trend in T1 2022 – T2 2022, seven-day moving average

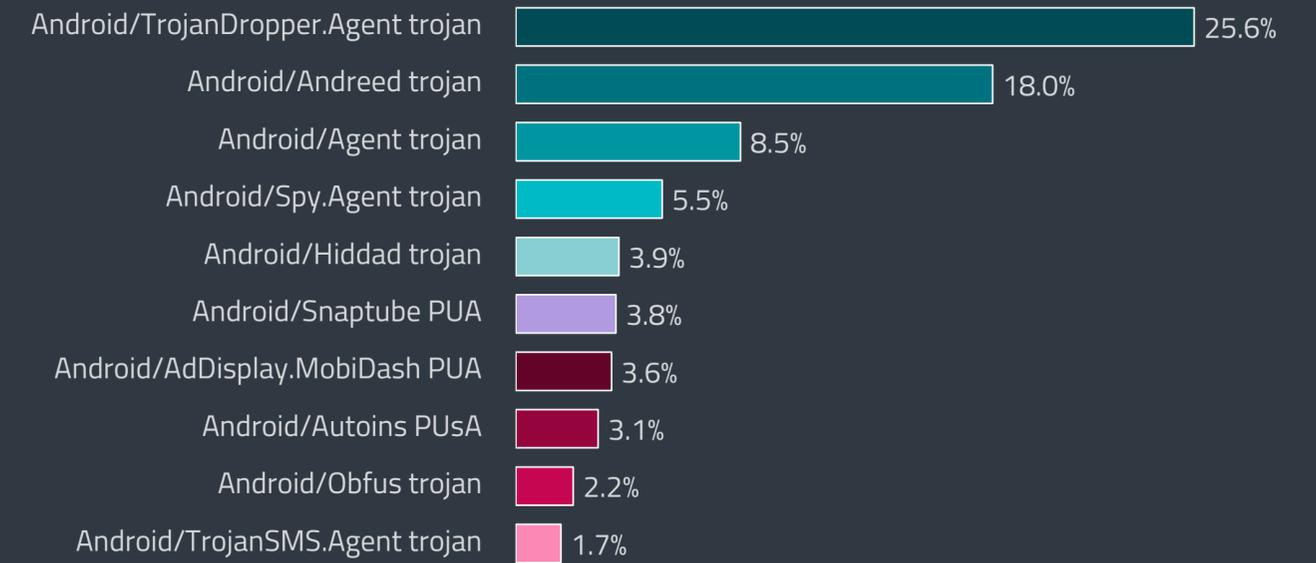
² The statistic is based on a selection of well-known extensions.

ANDROID

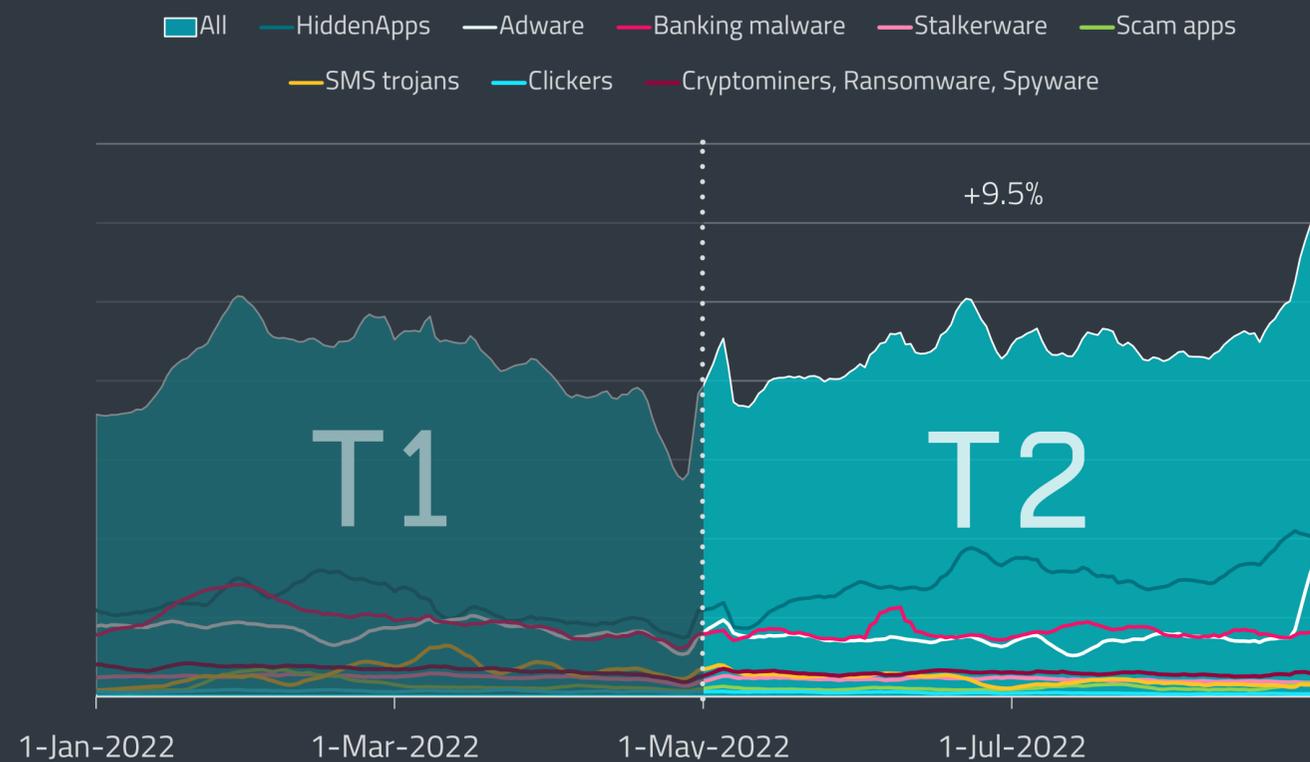
For over a year, Android detections have continued to grow – in T2 2022 by 9.5%. The most significant growth was seen in the Spyware category.

For 16 months now ESET telemetry has exposed continuous but leisurely growth of Android detections, most recently at 9.5% in T2 2022. The category that experienced the biggest growth was again Spyware (109%), represented by Android/Spy.Agent trojan, which is number three in the top 10 Android detection list. Compared to T1 2022, this threat has jumped four places from number seven. Malicious apps falling under this detection name have a wide range of spying capabilities including recording audio and video.

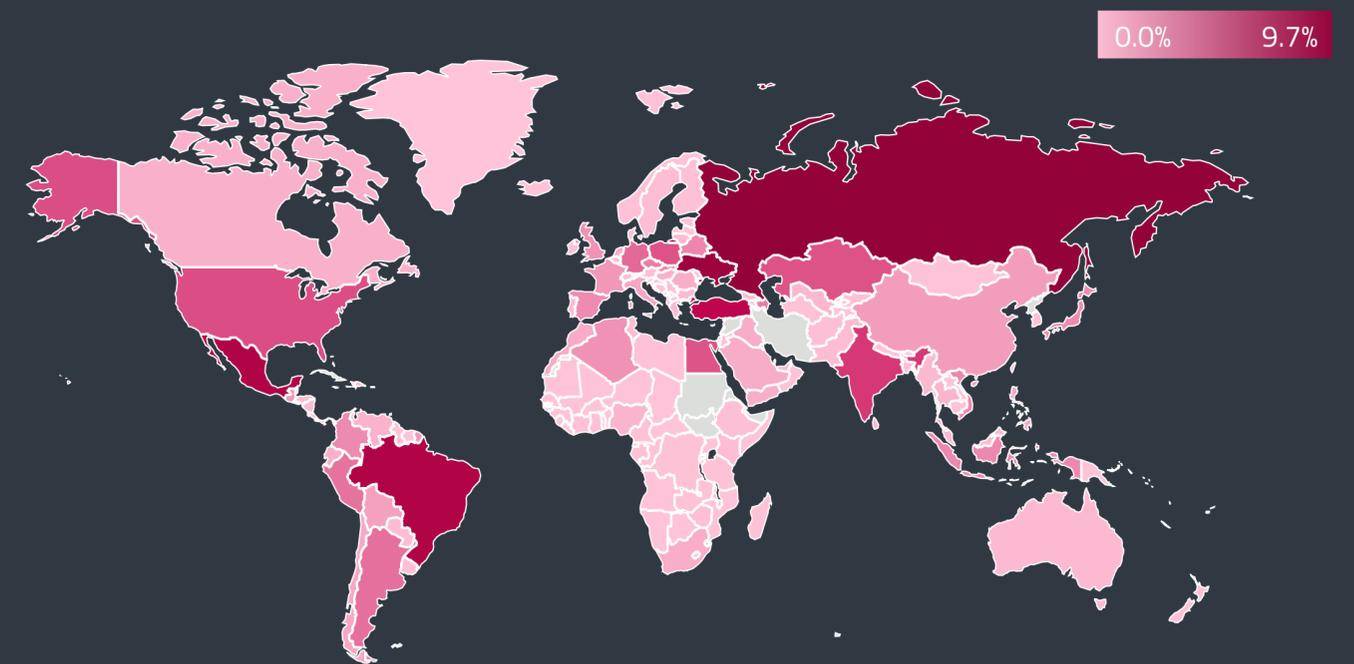
Behind a large portion of Android/Spy.Agent detections recognized in ESET telemetry is “GB WhatsApp” – a popular but cloned (and therefore unofficial) third-party version of WhatsApp with additional features. However, the cloned app is not available on Google Play; there are no security checks in place compared with the legitimate WhatsApp and versions available on various download websites are riddled with malware. WhatsApp is even *temporarily banning* [61] accounts that use such unsupported apps and if these accounts continue to use them, they are permanently banned from accessing WhatsApp. Most of these detections in T2 were seen in Egypt, Brazil, India, and Peru.



Top 10 Android detections in T2 2022 (% of Android detections)



Detection trends of selected Android detection categories in T1 2022 – T2 2022, seven-day moving average



Global distribution of Android detections in T2 2022

EXPERT COMMENT

Behind the growth of Spyware are mainly easy-to-access, off-the-shelf Android spyware kits available on various online forums. In many cases, amateur attackers can find working and reliable remote access trojans (RATs) online for free. In comparison, the successful deployment of other types of Android malware, such as banking malware, requires at least some level of technical skill.

Lukáš Štefanko, ESET Malware Researcher

Another Spyware variant, detected by ESET as Android/Spy.Facestealer trojan, was spotted on Google Play by [Trend Micro](#) [62]. Facestealer disguises itself as various useful applications and changes its code frequently, therefore it repeatedly manages to enter the digital marketplace. In its beginnings, the spyware would steal people's Facebook login credentials (hence the name); however, currently, it can also exfiltrate various other user credentials and even private keys to cryptocurrency wallets.

The [macOS and iOS](#) section mentions vulnerabilities in iOS that have been exploited by commercial surveillance companies. [Google's Threat Analysis Group](#) [63] revealed that it found commercial surveillance software developer Cytrox packaging exploits for several zero-day vulnerabilities, with one of them affecting Android. High-profile and carefully chosen victims are first served with the Alien trojan, which then loads the Predator spyware onto their Android devices to exfiltrate their data and spy on their activities. Google claims that Cytrox sold these zero-day attacks to various government-backed threat actors.

Even with this growth, Spyware didn't come close to reaching the detection numbers of HiddenApps – deceptive apps that hide their own icons, then stealthily display ads – or Adware. HiddenApps also experienced growth in T2 2022, increasing by 32.4%. In the top 10, this category is represented by Android/Hiddad in fifth place.

As is visible in the trend chart, Adware detections saw a steep increase towards the end of T2 2022, even though the category experienced a mild overall decline of 4.2%. In terms of functionality, Adware is similar to HiddenApps, but typically doesn't have the stealthy features made to avoid discovery on the affected device. Behind the growth of this category towards the end of T2 was Android/AdDisplay.Fyben PUA. This detection covers modded apps – reworked copies of original apps – that have malicious code injected into the `com.android.app.Activity` package, which is responsible for the display of unwanted ads. For obvious reasons, these apps are not available on Google Play.

Even though the official versions of these apps are available in official stores, some people still resort to downloading modded versions from unofficial download sites. One reason is that the desired app

is not compatible with the device that the person is currently using and modded apps are sometimes recompiled to work even on device models that the original does not support. Another reason is that the developer has not made the app available in certain regions. Due to sanctions following Russia's invasion of Ukraine, people in Russia and Belarus can [no longer download or update](#) [64] paid apps from Google Play. Sanctions also mean that developers from those countries can no longer place their paid apps on the platform.

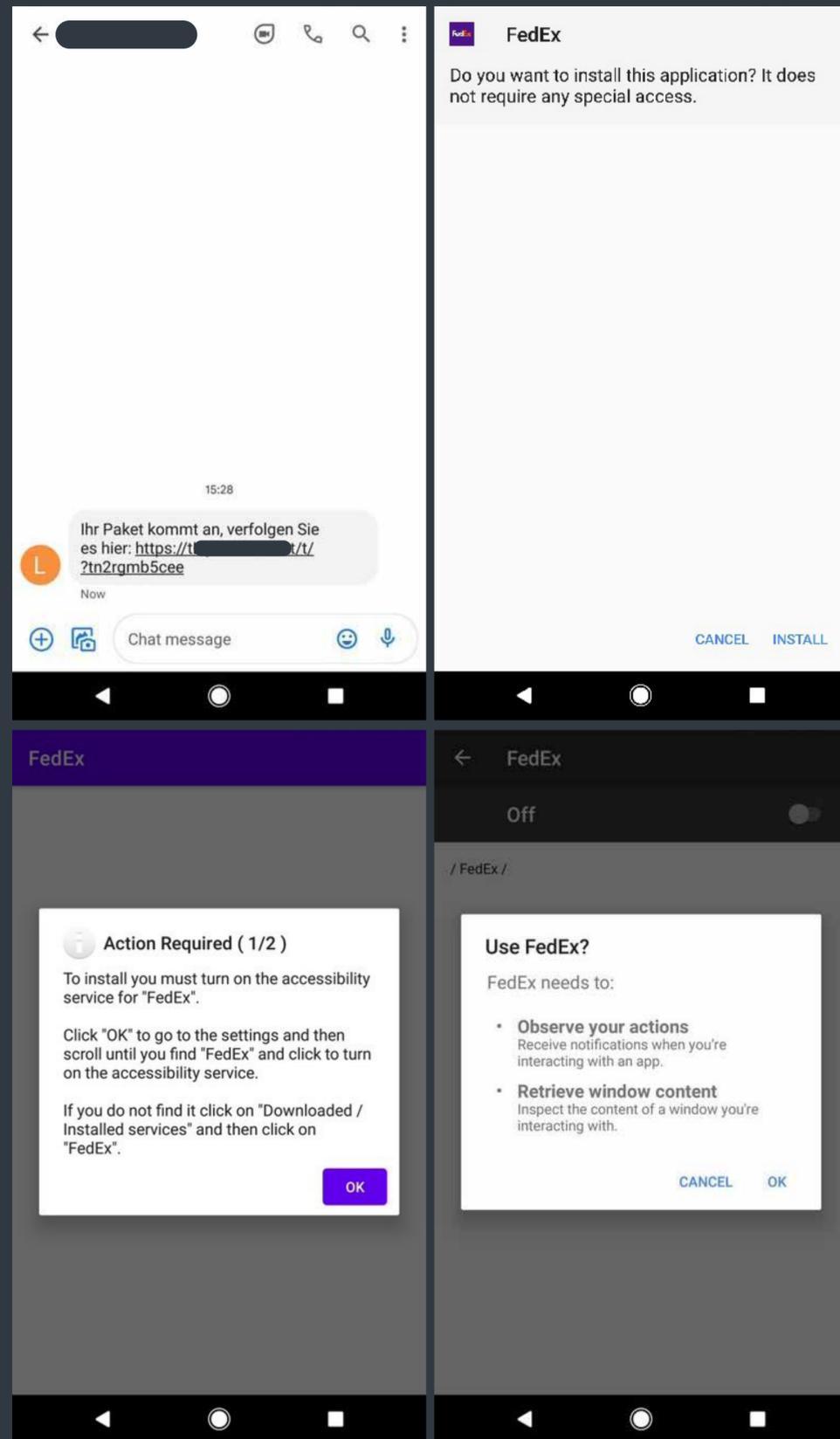
In Russia, this has led to the launch of NashStore (meaning Our Store), which offers apps for the owners of Android devices in Russia, Kazakhstan, Belarus, Kyrgyzstan, and Armenia. The above-mentioned reasons may explain why ESET telemetry saw most Android/AdDisplay.Fyben PUA detections in Ukraine, Mexico, Russia, Turkey, and Poland.

All of the other Android detection categories monitored by ESET experienced a decline in T2 2022 – Ransomware decreased by 8%, Stalkerware by 10%, Clickers by 30%, SMS Trojans by 32%, and Cryptominers by 48.5%.

Even banking malware saw a decrease of 17%; this category had experienced relatively steady and sometimes very strong growth in the past, with the exception of T3 2021. Ultimately, this decrease has put the T2 Android banking malware detections on a similar level as they were at the end of 2021. The global [law enforcement takedown](#) [65] of the notorious [FluBot Android banking malware](#) [66] is partially behind the decrease in detection numbers in this category. ESET detects this threat as several variants of the Android/TrojanDropper.Agent trojan.



Android Banking malware detection trend in T1 2022 – T2 2022, seven-day moving average

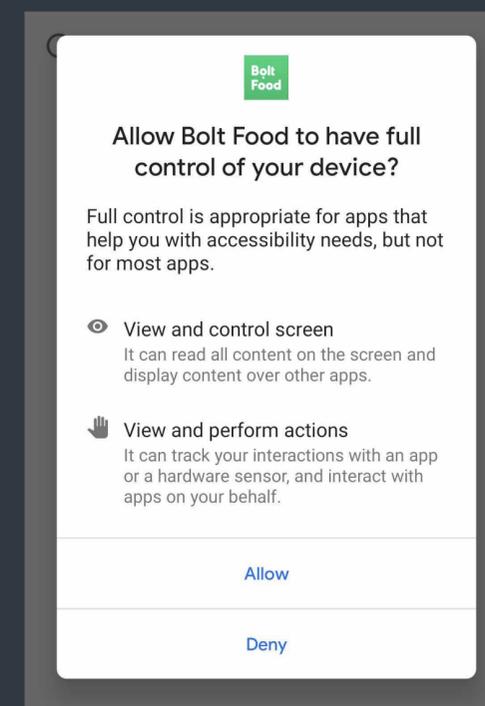


One of many FluBot examples detected by ESET: this one was spreading in Germany and impersonating the FedEx app

The FluBot banking malware had been wreaking havoc in many European countries and in the US, attacking the customers of various banks and aggressively spreading through SMS. Its infrastructure was successfully disrupted in May by the Dutch Police and the investigators are now trying to identify the individuals behind this Android threat. Even with this takedown, ESET still detects many unrelated Android banking malware variants that can exfiltrate online banking credentials and immediately access the victim's finances. Vigilance is therefore always necessary.

In Poland, *ESET researchers detected* [67] new Android banking malware called ERMAC 2.0; it impersonates the popular food delivery app Bolt Food. Since March 2022, the ERMAC 2.0 banking trojan has been available for rent on underground forums for USD 5,000 a month and its purpose is to steal victims' credentials for various financial and cryptocurrency apps. The list of targeted apps is received from the attacker's C&C server and is based on the apps installed on the device. ESET detects this threat as a variant of Android/TrojanDropper.Agent trojan, which has been number one on the top 10 Android detection list not only in T2 2022 but also during the last 12 months.

Cleafy [68] found newer versions of the SOVA (owl in Russian) Android banking malware with the functionality to intercept multifactor authentication codes. Additionally, this trojan served as a base for another Android banking trojan described by *F5 Labs* [69] that they named MaliBot. Both of these Android banking trojans are detected by ESET as different variants of Android/TrojanDropper.Agent. *Trend Micro* [70] also detected several apps on Google Play that, after installing, download additional banking malware onto the compromised Android device. As such, ESET detects these malicious apps as variants of Android/TrojanDownloader.Agent.



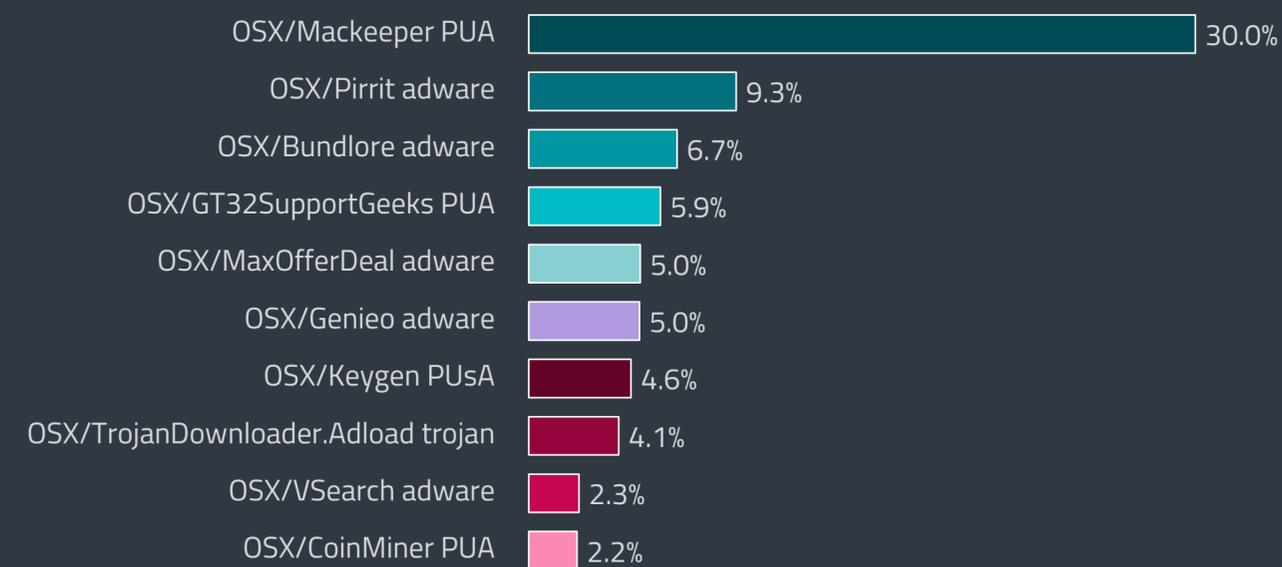
ERMAC 2.0 impersonating the popular food delivery app Bolt Food

macOS AND iOS

macOS detections continued to decline throughout T2 2022, with the Adware category losing one-fifth of its detection numbers.

In T2 2022, macOS detections saw a decline of 15.1%, with the Adware category experiencing the largest decrease in detection numbers (20.3%). This type of detection covers programs that display unsolicited ads, and is represented in the top 10 macOS detection list by OSX/Pirrit, OSX/Bundlore, OSX/MaxOfferDeal, OSX/Genieo, and OSX/VSearch. All of these adware families saw decreasing numbers of detections, with the exception of OSX/MaxOfferDeal – compared to T1 its detections increased by 30% in T2. OSX/MaxOfferDeal displays unwanted online ads and redirects users to websites that can be riddled with malicious links; ESET products detected it in T2 mainly in the United States and France.

Even though their numbers also declined (by 15.7%), Potentially Unwanted Applications (PUAs) continued to be the most widespread type of macOS detection. In T2 2022, PUAs accounted for 44% of all macOS detections and were represented in the top 10 by OSX/Mackeeper, which has the potential to mislead users into unnecessary purchases, OSX/GT32SupportGeeks, which is often presented as a macOS performance scanner reporting alleged issues, and OSX/Coinminer, which uses the system's resources to mine digital currency.

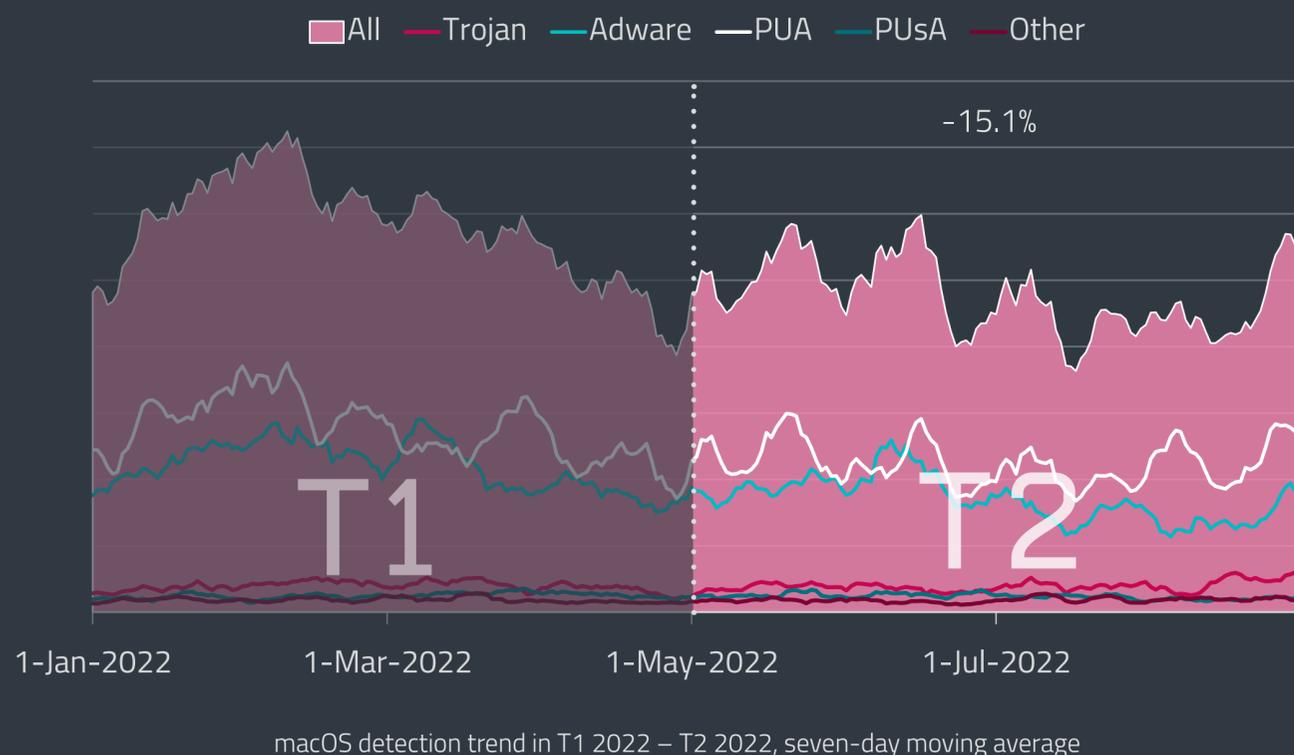


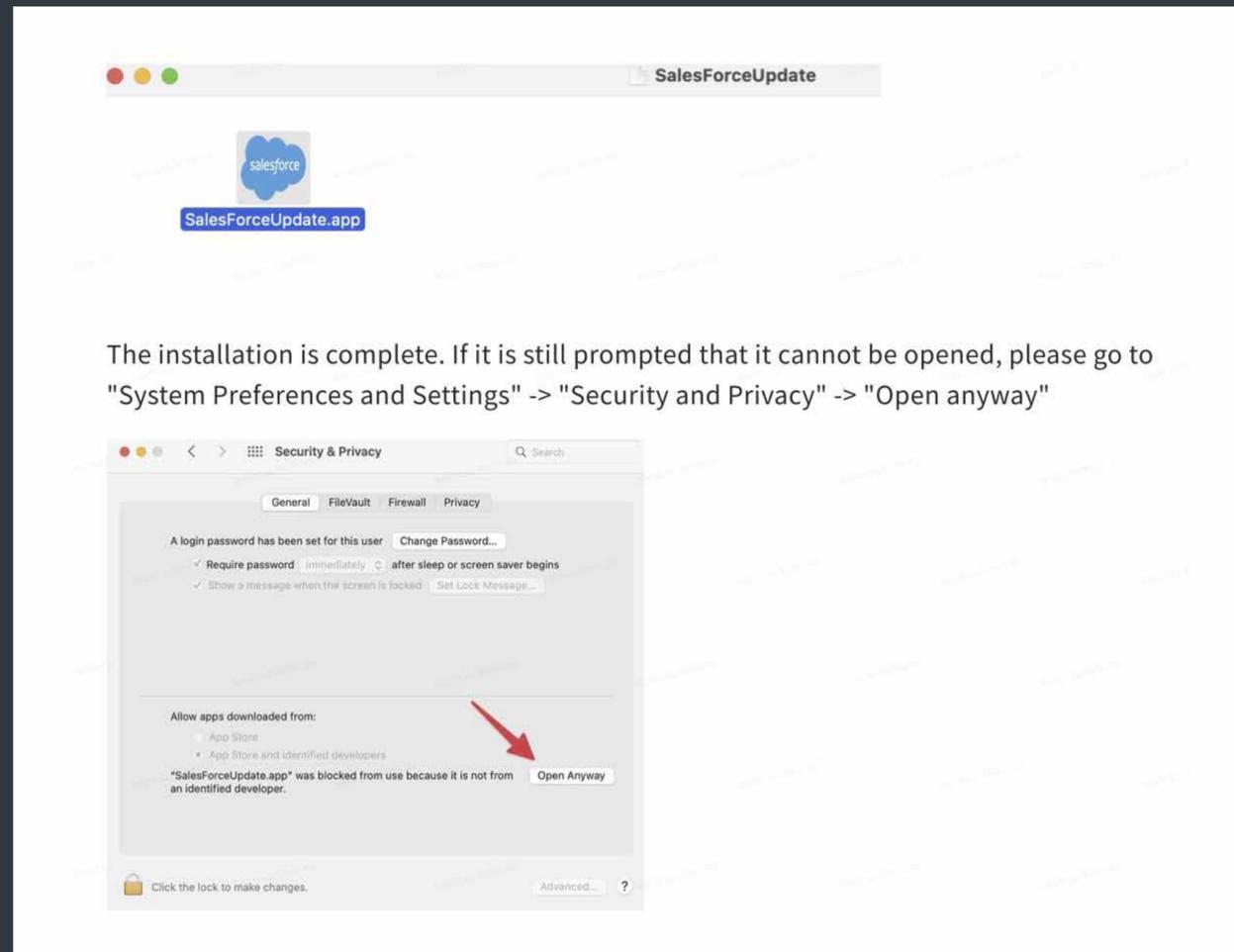
Top 10 macOS detections in T2 2022

Potentially Unsafe Applications (PUAs) also declined by just a smidge (-1.2%) and the only category that experienced a very minor increase in numbers was Trojans (2.6%), represented by OSX/TrojanDownloader.Adload, which is currently number eight on the top 10 macOS detection list.

In July, [ESET researchers](#) [14] warned about a new campaign using a fake update of the Salesforce customer relationship management (CRM) software. Its goal was to deploy the [Sliver](#) [71] malware to macOS and Windows systems. The macOS compromise chain is very similar to a COVID-19-themed campaign previously documented by [SentinelOne](#) [13]; however, this newer campaign didn't include the "covid" malware and only installed the Sliver implant, which has sufficient functionality to deploy additional malware if needed. The download page included a link to a PDF document that contains instructions on how to install the file – one of the instructions basically guides the victim into disabling macOS security features. ESET products detect this threat as variants of the aforementioned OSX/TrojanDownloader.Adload trojan.

ESET telemetry registered the most macOS detections in T2 2022 in the United States (23.8%), Japan (11%), France (7.8%), Germany (4.4), and the United Kingdom (3.9%). The macOS detection numbers in all of these countries saw decreasing numbers, with the United Kingdom experiencing the biggest drop among this group, by 38.5%.

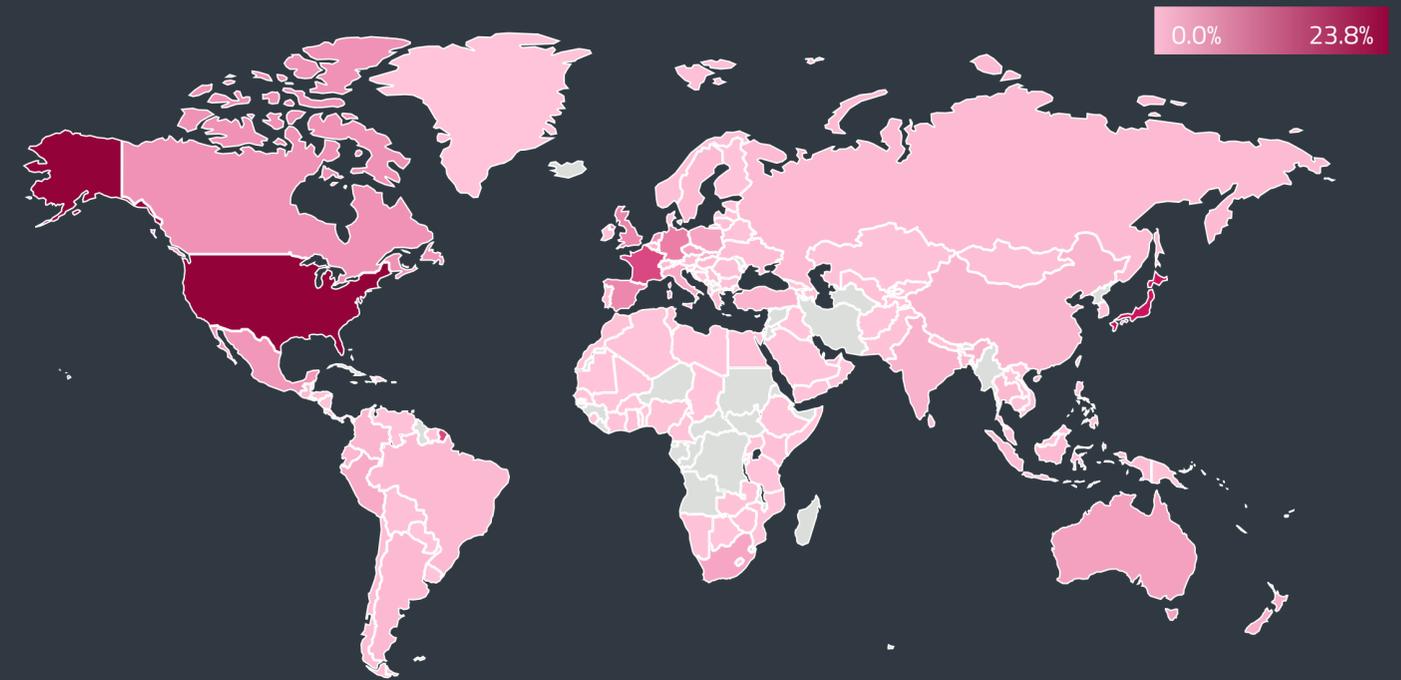




PDF document navigating the victim into disabling macOS security features

Even though the overall macOS detection numbers are decreasing, ESET researchers continue to discover new threats to the users of this platform being deployed by various APT groups. As described in the [Featured story](#), ESET researchers discovered a previously unknown macOS backdoor, which they dubbed [CloudMensis](#) [6], that spies on users of macOS systems and exclusively uses public cloud storage services to communicate back and forth with its operators. The limited distribution of OSX/CloudMensis.A suggested to the researchers that it is used as part of a targeted operation. Later on, this hypothesis was corroborated – ESET researchers were able to attribute CloudMensis to the ScarCruft APT group.

In previous issues, the ESET Threat Report has extensively covered the topic of Pegasus, the commercial phone hacking tool developed by the NSO Group. In T2 it [was revealed](#) [72] that the tool was used by at least five member states of the European Union. And to show that it is not the only commercial-grade spyware targeting high-profile individuals, Google's [Threat Analysis Group \(TAG\)](#) [73] informed the public about the iOS version of another commercial-grade spyware called Hermit, spying on users in Italy and Kazakhstan.



Global distribution of macOS detections in T2 2022

To address the security issues related to iOS spyware, such as Pegasus and Hermit, Apple included a new security feature in iOS 16, which was released in September 2022. The feature is called Lockdown Mode: it limits certain functions of the iPhone and some of its apps that can be vulnerable to an attack. For instance, it blocks attachments in messages (except for pictures), FaceTime calls if the iPhone has not called that contact before, incoming invitations, configuration profiles, and wired connections to a computer or an accessory. This function also blocks attempts to enroll the iPhone into mobile device management software. Lockdown Mode will also be part of macOS Ventura scheduled to be released in October. According to ESET researchers, protecting against the aforementioned CloudMensis malware may be one of the reasons some users would want to enable this additional feature on their Apple devices. Another new security feature of iOS 16 is that security updates no longer require a full iOS update and can be installed automatically: this option has to be enabled manually via Settings → General → Software Update.

Vulnerabilities tied to Pegasus are, however, not the only ones that Apple device owners should be concerned about. In August, Apple released patches for two new zero-day vulnerabilities ([CVE-2022-32893](#) [74] and [CVE-2022-32894](#) [75]) that [may have been actively exploited](#) [76], according to Apple. The first vulnerability was found in Apple's WebKit (HTML rendering software) and allows a malicious website to trick iPhones, iPads, and Macs into running unauthorized software. The second vulnerability then allows the attacker, who has already exploited the WebKit vulnerability, to gain control of the operating system kernel, which would allow the attacker to take over control of the whole device. An update is therefore highly advised.

IoT SECURITY

While zombie botnet Mozi started losing steam, other Mirai-based botnets used T2 2022 to expand while updating the list of vulnerabilities they exploit.

Is Mozi, the biggest zombie IoT botnet monitored by ESET research, finally dying? Our telemetry data suggests just that, as the number of bots dropped by 23%, falling from 500,000 compromised devices in T1 to 383,000 in T2. The number of attacks took the same downward path, plunging from 5.6 million in T1 to 4.3 million in T2, meaning an equal decline of 23%. Most of these attacks were aimed at machines in the US (30.4%).

As in the previous periods, the largest portion of the botnet was geolocated in China (53%) and India (35%). Of the approximately 94,000 targeted IPs, most were in Germany (17%), the United States (8%), and Japan (7%).

Most of these statistics confirm the assumption that the Mozi botnet is on autopilot, running without human supervision since its reputed author was *arrested* [77] in 2021. Subsequently, the distribution of both attacker IPs and target IPs as well as the share of individual countries have hardly changed. There was also no change in the list of vulnerabilities abused to spread Mozi malware and the share of attacks caused by each one of them.

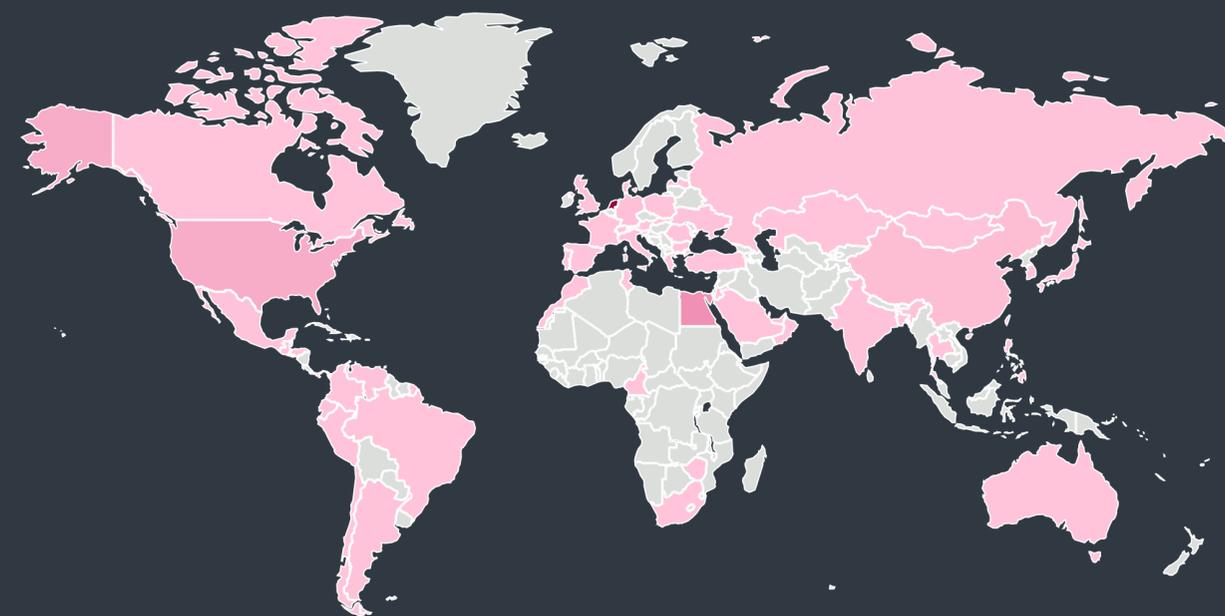
However, that's not the case for other botnets monitored by ESET researchers, with the ZHtrap botnet being a prime example. The number and distribution of its bots have changed dramatically between T1 and T2 2022.

While the number of ZHtrap attacks dropped from 106,000 to 58,000 – taking a 45% dip – the geolocations of its bots changed massively. Almost 77% of attacks caused by this botnet in T2 2022 came from the Netherlands, an increase of 48 percentage points compared to T1. The second largest ZHtrap bot activity was seen in Egypt, growing from nonexistent in T1 to a 10% share in T2 2022, pushing the United States down to the third place with 5% (-23 percentage points).

While the operators didn't seem interested in the US as the location of their bot farm, they moved most of their *payload* servers there, growing their share to 53% in T2 versus 9% in T1. In contrast, ZHtrap shut down a large part of its payload servers in the Netherlands, its share dropping from 41% in T1 to 16% in T2.

In stark contrast to Mozi, the list of vulnerabilities used to spread ZHtrap has also changed dynamically. In T1 2022, it was spreading almost exclusively (99.5%) via the old [CVE-2015-2051](#) [78] in D-Link routers. In T2, this weakness remained the number one choice but was used in "only" 80% of attacks,

0.0% 76.8%

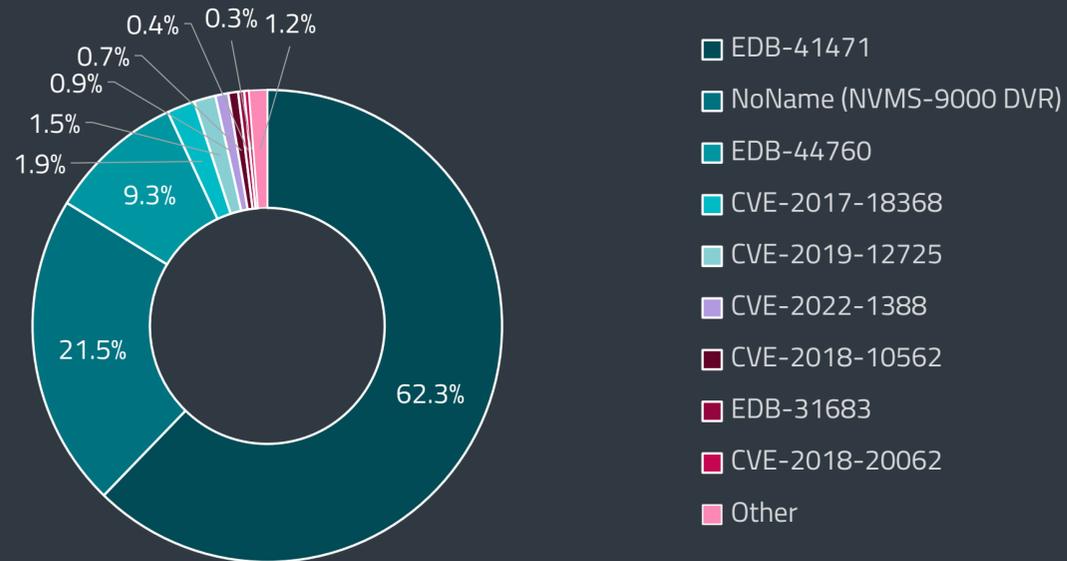


Global distribution of ZHtrap bot activity in T2 2022

followed by the [EDB-41471](#) [79] bug in MVPower DVR devices with 13%. Also, two recently reported flaws – one in Confluence servers ([CVE-2022-26134](#) [80]) and another in Zyxel devices ([CVE-2022-30525](#) [81]) – were at least tested by the operators as a distribution vector.

Of course, ZHtrap and Mozi aren't the only two botnets that used Mirai's leaked source code to build their own malware. Gafgyt, BotenaGo, Dofloo, and Tsunami are just a few of the most prominent names that ESET labels with one umbrella name – "Mirai-based botnets". This diverse group cumulatively accounted for 11.7 million attacks in T2 2022, a 61% increase compared to T1 2022.

What significantly influenced these figures was our recent addition of detection for attacks against a patched 2019 flaw in [NVMS-9000 Digital Video Recorders](#) [82]. Despite this vulnerability not having a CVE or EDB entry, it has become quite prevalent in T2 2022 and is now the second most "popular" attack vector, accounting for 21% of attempts caused by Mirai-based botnets.



Vulnerabilities most exploited by Mirai-based botnets in T2 2022

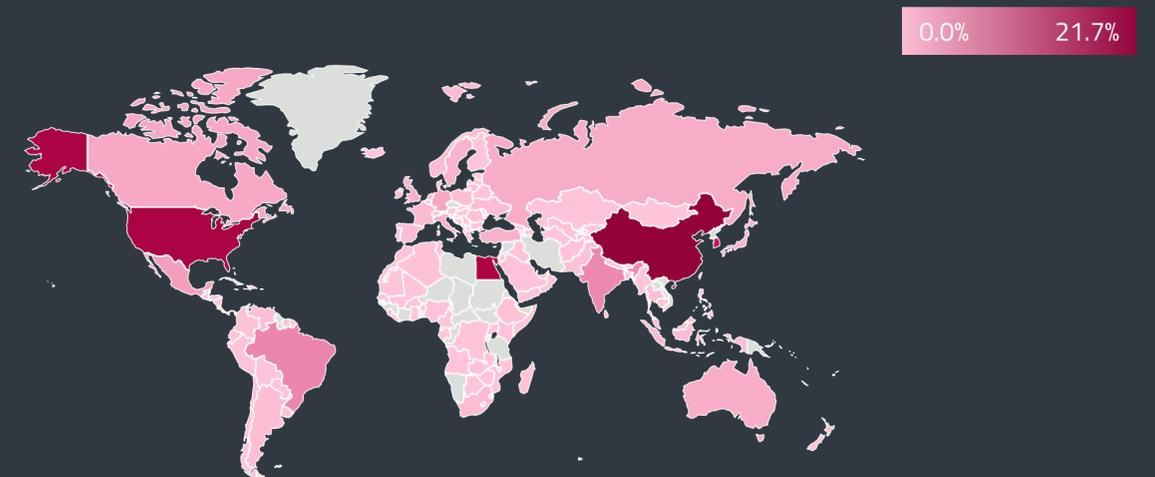
Another strong contributor to the same 11.7 million attacks was the vulnerability found in D-Link routers [EDB-44760](#) [83]. Between T1 and T2 2022, its detection numbers grew more than twenty-fold, making it the third most exploited flaw, with 9.3%. However, both previously mentioned vulnerabilities are still dwarfed by the [EDB-41471](#) [79] bug in MVPower DVR devices, which claimed a 62.3% share of the Mirai-based detection pie.

From a geographic point of view, the United States withstood 25% of attacks by the Mirai-based botnets – not counting Mozi and ZHtrap – followed by Germany with 7.1% and the United Kingdom with 6.6%. Considering only the targeted IP addresses, Germany (16%) led the pack, followed by the US (9%) and Japan (6%).

Regarding the infrastructure of Mirai-based botnets, 8% of their payload servers disappeared between T1 and T2 2022. Most of those remaining were detected in the US (38%), Netherlands (11%), and Germany (9%). As for bots, these were most prevalent in China (21%), the US (16%) and Egypt (15%).

Moving away from the botnets, the number of user-requested router scans in ESET security products fell by 17%, with the number of tested routers falling by 21%. Due to a smaller scan base, the number of devices that were using easy-to-guess passwords declined proportionately, dropping by 25%. The dip in the T2 data was probably caused by the Northern Hemisphere summer vacations and lower overall activity in July and August.

With IoT devices, even basic vulnerabilities can be a major issue, since patching them is seldom as straightforward as with computers, phones, and tablets. But when a critical CVSS 9.8 flaw hits the



Global distribution of Mirai-based attacks, bots and payload servers (from top to bottom) in T2 2022

market, threat actors don't wait long to start exploiting it. This was the case with [CVE 2022-1388](#) [84] found in F5 Big-IP network devices. It allowed an unauthenticated attacker to gain full control of victims' devices – and based on news stories there were a few occasions where it was even used to [wipe them](#) [85].

In T2 2022, ESET telemetry reported over 100,000 exploitation attempts targeting CVE 2022-1388 in F5 devices. If not blocked, the established connections would have been used to drop and run a Linux shell script that would then download a Mirai binary from a predefined list of URL links. Several Mirai-based botnets exploited this vulnerability to expand their bot network.

The last four months were rife with experiments that showed how vulnerable the IoT-powered world can become. Manufacturers including [Honda](#) [86], [Hyundai/Kia](#) [87], and [Tesla](#) [88] saw their products broken into by researchers, who not only gained access but started and even drove off in them.

In T2 2022, Forescout researchers also presented [proof-of-concept ransomware](#) [89] that can target IoT, IT, and operational technology (OT). Not exactly a new idea, as this type of threat has been [predicted for years](#) [90], but certainly one worth keeping in mind as more PoCs like this are being published.

In T1 2022, we mentioned the sabotage of Viasat's [KA-SAT satellite network](#) [91], which caused major disruptions to communications and forced the company to distribute 30,000 replacement modems. In T2, Ukraine, the European Union, and the Five Eyes nations all [attributed the incident to Russia](#) [92].

EXPERT COMMENT

According to expectations, the zombie-like Mozi botnet is slowly starting to lose steam, which opens up the field to other Mirai-based botnets. And as our data shows, these are becoming increasingly powerful and widespread, experimenting with vulnerabilities both old and new, including those from popular vendors. What this means for organizations and users is that patching is of the utmost importance, especially in developed countries, which are still the main targets of most IoT threats monitored by our systems.

Milan Fránik, ESET Malware Researcher

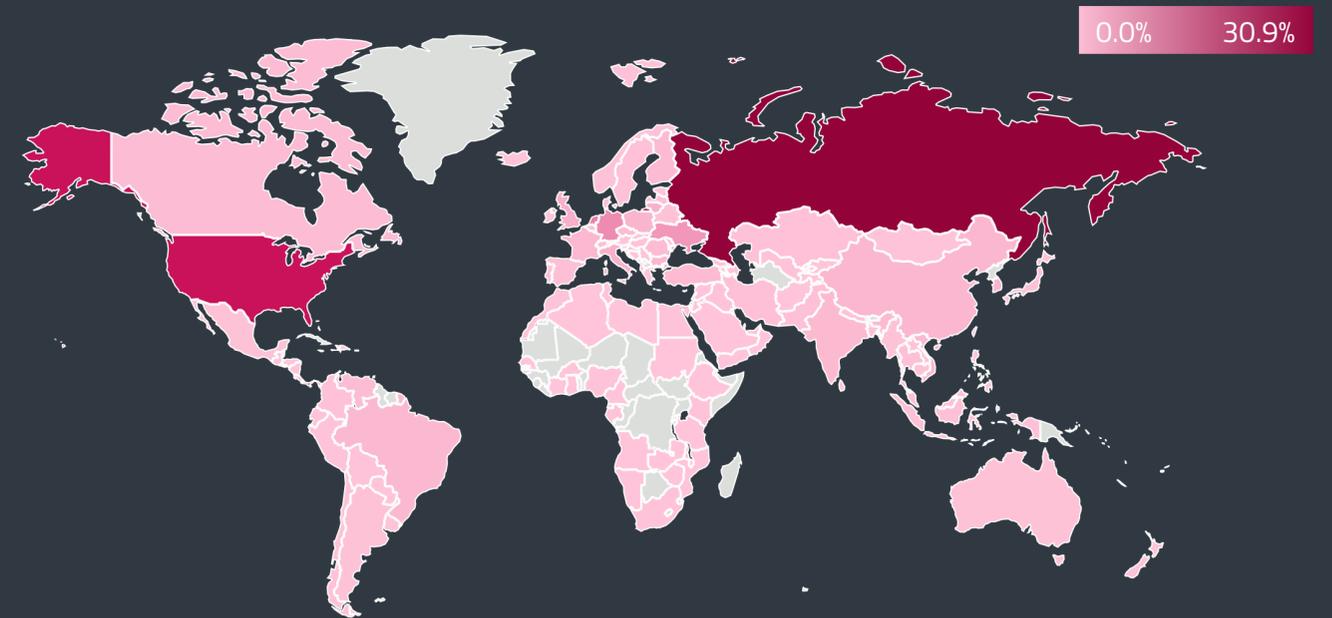
EXPLOITS

While attack attempts against RDP, SQL and SMB followed a downward spiral in T2 2022, new exploits like Log4Shell and Spring4Shell grew in popularity.

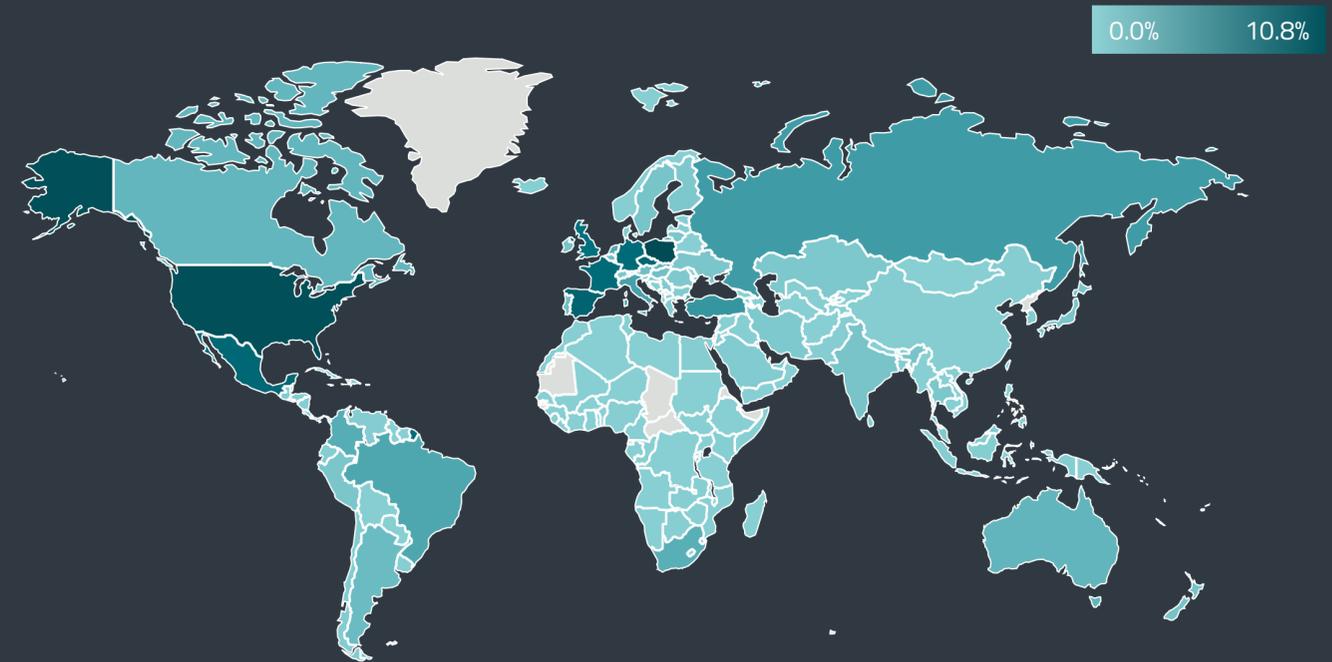
After an unprecedented drop in RDP password-guessing attacks in T1 2022, the detection trend did not recover and stayed down at levels not seen since 2020. The decrease between the two periods was still a whopping 89.4%, going from 123 billion detections to 13 billion; however, this difference was mostly caused by the high volumes of blocked attempts in the first days of January 2022. On an average day in T2 2022, 104 million RDP connection attempts were blocked compared to 1 billion in T1 2022.

The trend of unique clients reporting an RDP attack attempt declined at a much slower pace, going down by 22.8% between T1 and T2, stabilizing in May. The average number of unique clients facing an RDP attack attempt in May through August 2022 receded from 102,000 to 73,000 devices.

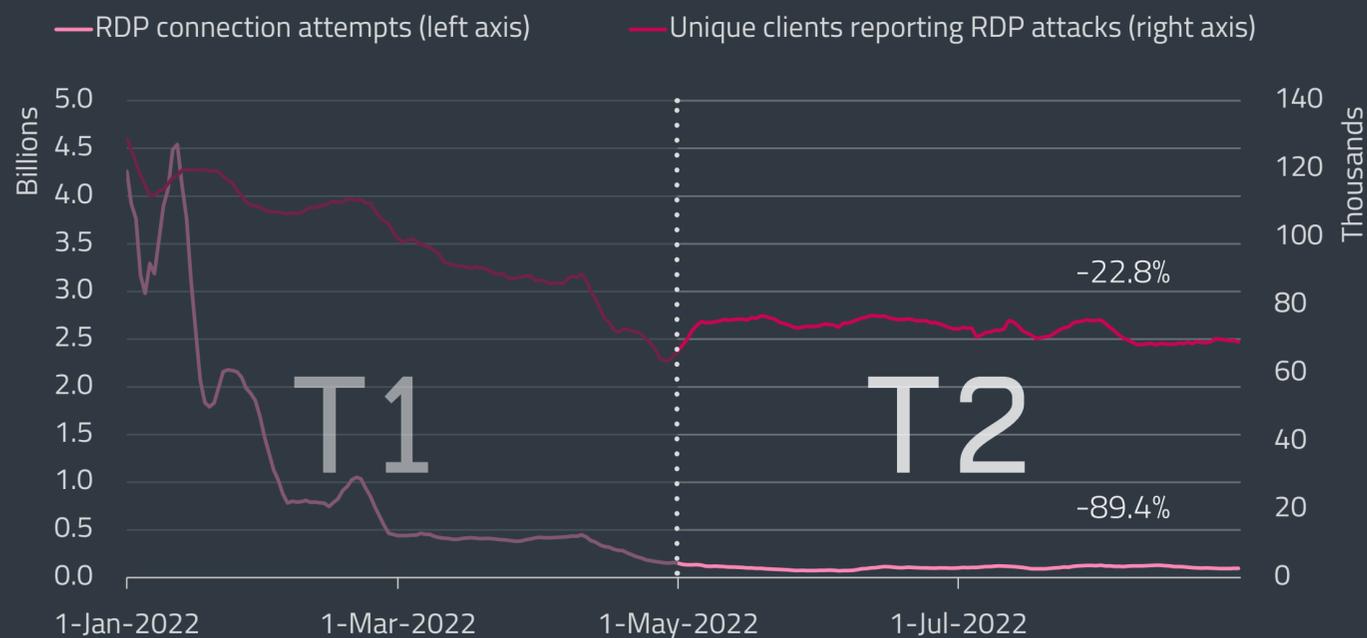
The reasons for the decline remain the same as in T1: less remote work, better countermeasures implemented by security and IT departments, and Russia's war with Ukraine, which seems to have impacted portions of the attacking infrastructure. Another factor that might cause further drops in RDP attacks is the *default protection* [93] in Windows 11 against brute-force attacks. However, its effects will probably become apparent only after more organizations have adopted the newest version of that operating system.



Global distribution of RDP password guessing attack attempt sources in T2 2022



Global distribution of RDP password guessing attack attempt targets in T2 2022



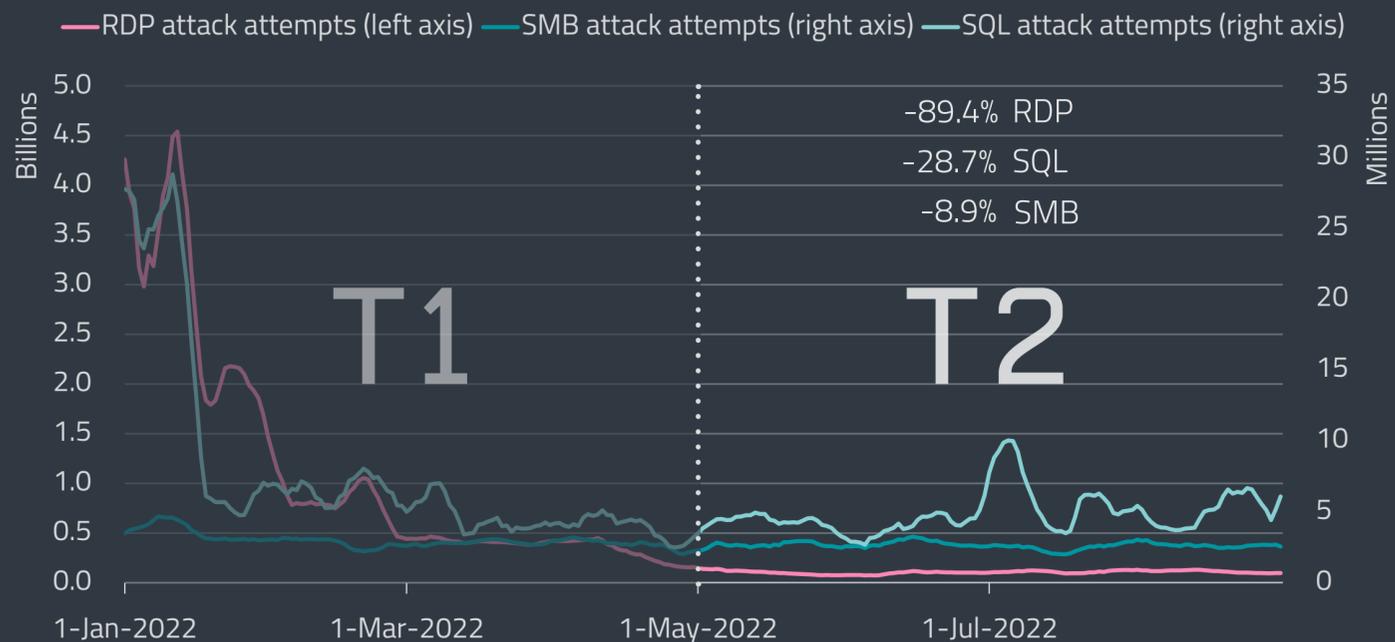
Trends of RDP connection attempts and number of unique clients in T1 2022 – T2 2022, seven-day moving average

From a geographical standpoint, most of the 13 billion blocked RDP attacks in T2 2022 were aimed at Poland (10.8%), the United States (10.2%), and Spain (7.3%). Keeping a distant lead, Russian IP addresses were responsible for the largest portion of the attacks (31%), followed by IPs in the US (14%) and Panama (8%). It is important to note that the use of VPNs and proxy services might influence these statistics.

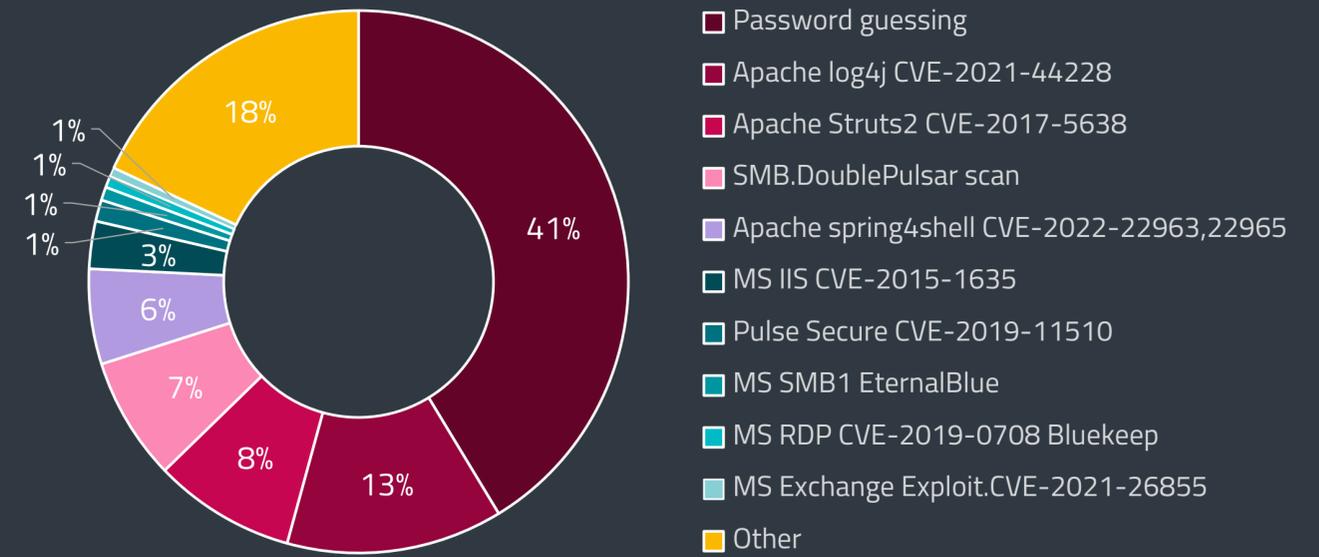
In comparison to RDP, attacks against public-facing SQL services only saw one sharp drop in January after which detection numbers found steady ground. Attack attempts declined from 859 million in T1 to 612 million in T2 2022, meaning a 29% reduction. The number of unique clients closed T2 2022 with a negligible 1.8% decline. On an average day in May through August 2022, SQL services had to withstand 4.9 million attack attempts.

Geographically, the country that saw the most attacks against SQL services in T2 was Turkey. Threat actors hit it especially hard on July 1 and July 20, causing peaks in our data that accounted for 65% and 61% of SQL attack detections on those days. The last uptick in SQL data occurred on August 31, with the United Kingdom facing 49% of SQL attacks on that day, followed by Austria with 19%.

In contrast with SQL and RDP, the trend of attacks targeting SMB services kept its balance. Blocked connection attempts went from 356 million in T1 to 324 million in T2 2022, accounting for a minor decline of only 9%. The number of unique clients reporting such incidents remained steady, losing only 0.7%. On an average day in T2 2022, ESET's brute-force attack protection blocked 2.6 million malicious SMB connection attempts.



Trends of RDP, SMB and SQL attack attempts per client in T1 2022 – T2 2022, seven-day moving average



External network intrusion vectors reported by unique clients in T2 2022

The country facing the biggest portion of the attacks aimed at SMB was Mexico with 35%, followed by France with 16% and the US with 9%.

Regarding the most prevalent network intrusion vectors in T2 2022, password guessing kept its lead with 41% of the detection pie – identical to its share in T1.

The second most favored vector was the critical Log4J vulnerability, with 13%, which became increasingly popular among threat actors. T2 2022 data showed a 14% growth in exploitation attempts correlating with news reports of [ransomware gangs](#) [94] and sophisticated groups such as [Mercury](#) [95] and [Lazarus](#) [96] abusing the vulnerability. Despite a patch being available, it seems Log4J isn't going away anytime soon – with CISA's Cyber Safety Review Board calling it [endemic](#) [97].

In T1 2022, another high-profile vulnerability called Spring4Shell came to light and started to gain traction. Despite having potentially less severe consequences than Log4J, it followed a similar trajectory, demonstrating the potential to become one of the top network attack vectors. After T2 2022, we can say that scenario did not materialize, at least not yet.

Spring4Shell remained fifth among the top 10 network intrusion vectors, but its share grew from 4% in T1 to 6% in T2 2022. Its overall detections in May through August also went up by 113%; however, the trendline showed a major drop of activity around May 20.

Last but not least, a new zero-day vulnerability surfaced in T2 2022. The now-patched [CVE-2022-30190](#) [98] – also known as Follina – affects Microsoft's Support Diagnostic Tool and enables an



Detection trend of Log4J exploitation attempts in T1 and T2 2022, seven-day moving average

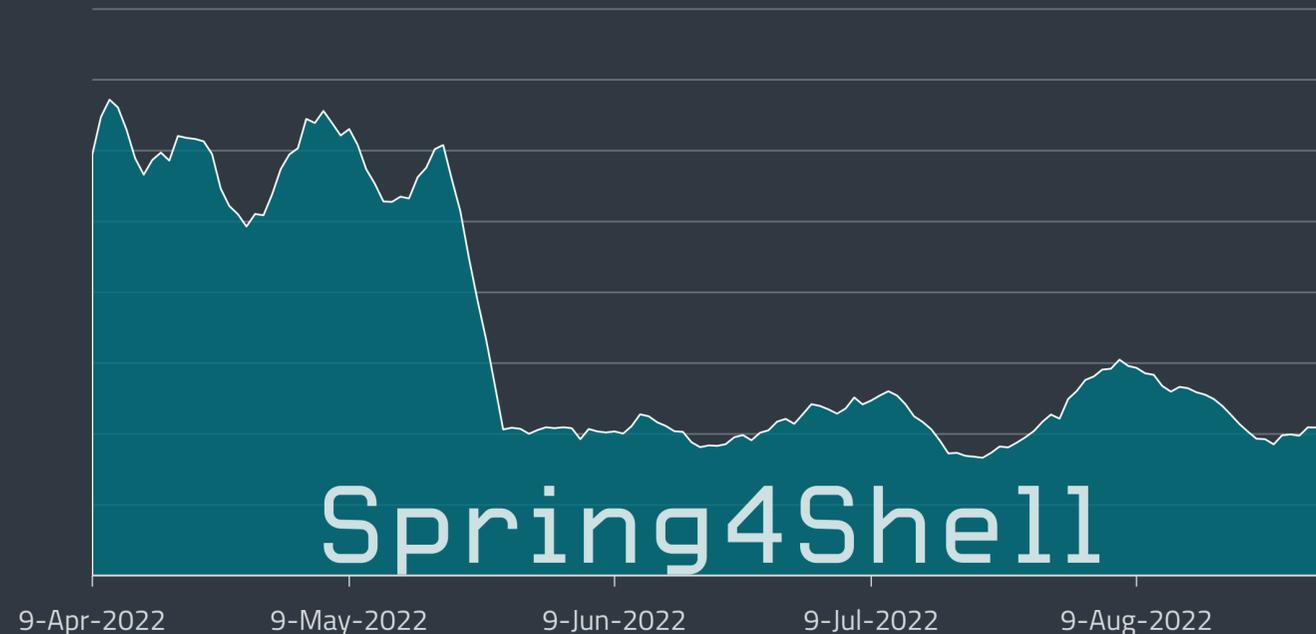
attacker to take control of a victim's device. The bug also made *headlines* [99] because it has been used by state-backed threat actors targeting EU and US organizations. CERT-UA even pointed its finger at *APT28* [100] as the possible culprit.

ESET telemetry reported hundreds of attempts to exploit Follina, demonstrated by several spikes in our detection data. The countries facing most of the attacks were Spain (20%), the US (7.5%) and the United Arab Emirates (7.3%).

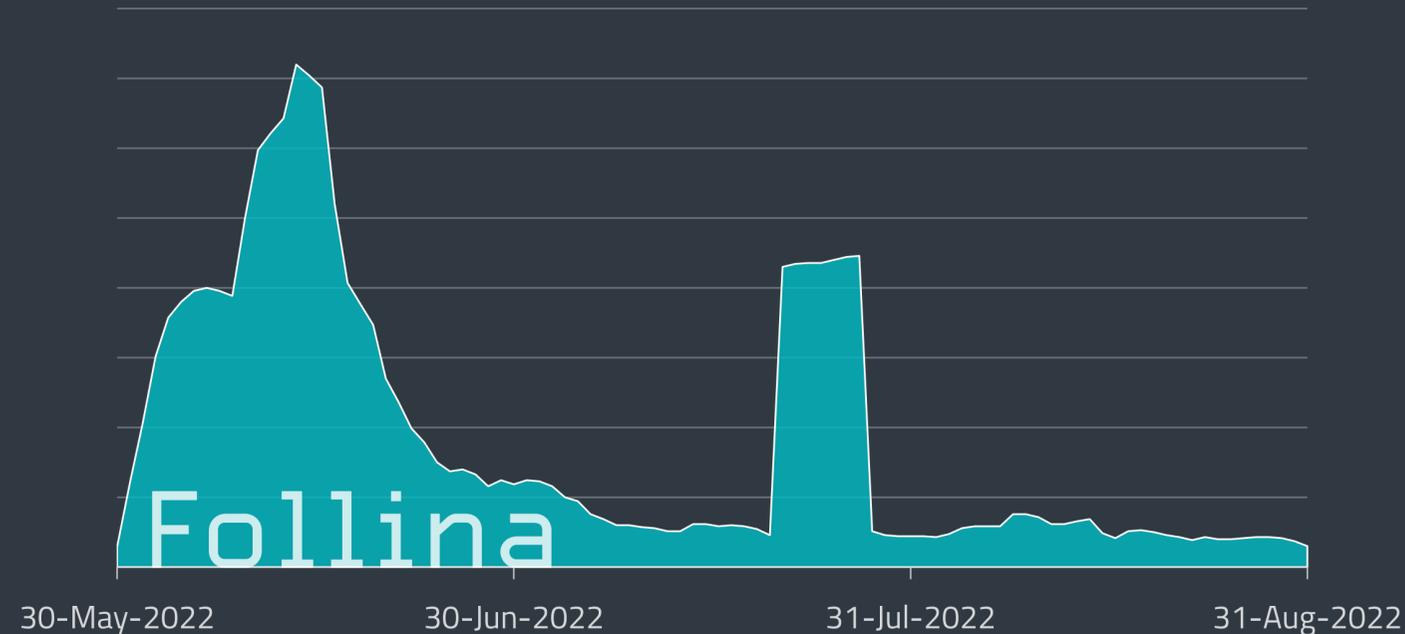
EXPERT COMMENT

A likely explanation for the sudden drop in Spring4Shell detections is that a group of threat actors tested the vulnerability as an intrusion vector and decided to drop it due to unsatisfactory performance. Another is that they decided to use a different attack avenue for the time being.

Ladislav Janko, ESET Senior Malware Researcher



Detection trend of Spring4Shell exploitation attempts in April through August 2022, seven-day moving average



Detection trend of attack attempts targeting the Follina vulnerability in T2 2022, seven-day moving average

ESET RESEARCH

CONTRIBUTIONS

Latest engagements and achievements
of ESET Research experts

UPCOMING PRESENTATIONS

AVAR 2022

Lazarus declares war on Windows system monitoring [101]

Since late 2021, Lazarus group malware authors have been improving new malware that is able to turn off as many Windows monitoring features as possible, effectively blinding most monitoring tools, security solutions, and event logging. In their presentation, ESET senior malware researcher Peter Kálnai and ESET malware analyst Matěj Havránek will focus on the most recent version of this malicious module, discovered in summer 2022 and containing newly added blinding features. They will demonstrate how these mechanisms operate and what changes the malware makes to the system once the module is executed. For developers of security products, the contents of this session should provide the impetus to reevaluate their implementations and to increase their solutions' self-protection.

Who's swimming in South Korean waters? Meet ScarCruft's Dolphin [101]

ScarCruft, also known as APT37 and Reaper, is an espionage group that has been operating since at least 2012 and primarily focuses on South Korea. Last year, ScarCruft conducted a watering-hole attack on a South Korean newspaper site. This attack was previously publicly described as having the BLUELIGHT backdoor as its final payload. However, as ESET malware researcher Filip Jurčacko will explain in his presentation, ESET Research discovered a second, more sophisticated backdoor called Dolphin that was deployed on selected compromised machines via BLUELIGHT. In his talk, Jurčacko will present a technical description of the Dolphin backdoor and its capabilities, provide useful information for threat hunters looking to track ScarCruft activity, and show the evolution of multiple Dolphin versions that ESET researchers observed after their initial discovery.

Behind the MirrorFace mask: LODEINFO malware interfering with Japanese elections [101]

In the weeks leading up to the Japanese House of Councillors election in July 2022, the APT group that ESET researchers track as MirrorFace launched a spearphishing campaign against Japanese political entities. Once the victims opened the malicious attachments, LODEINFO malware – in use since 2019 and exclusively against Japanese entities – was executed, opening the door for the threat actor to move to the next stage of the attack. In his presentation, ESET malware researcher Dominik Breitenbacher will introduce the audience to the MirrorFace APT group, a threat actor exclusively targeting Japanese entities with the LODEINFO malware, and will then provide a detailed description of the campaign against Japanese political entities. In the process, Breitenbacher will unearth MirrorFace tactics and procedures that haven't been published in detail before. The presentation will close by describing the evolution of the LODEINFO malware over the past few years.

[SparklingElf, recent supplies to SparklingGoblin's Linux malware arsenal, new ties to APT41](#) [101]

ESET researchers Thibaut Passilly and Vladislav Hřčka will present the discovery of a Linux variant of SideWalk, a modular Windows backdoor belonging to the SparklingGoblin APT group, that was originally named StageClient. The researchers also discovered that the backdoor exhibits a huge functionality overlap with the Specter IoT botnet malware, a modular Linux RAT, that creates an all but indisputable link between the malware authors, meaning that these tools come from the same threat actor. During their presentation, the ESET researchers will explain the connections between StageClient and Specter, introduce the SparklingGoblin APT group to the audience, and describe the code similarities between StageClient and SideWalk. Lastly, they will describe how the Linux userland rootkit, discovered alongside StageClient, injects itself into processes and hides its files and network connections to achieve stealthiness.

Ekoparty 2022

[Ukraine's past and present cyberwar](#) [102]

For the past eight years, Ukraine has been the target of enormous cyber-aggression by numerous APT groups. ESET principal malware researcher Robert Lipovsky will walk attendees through the most notable attacks, including those against the country's power grid with a special focus on the latest attempt: Industroyer2. This new version of the only malware specifically designed to trigger electricity blackouts was deployed in Ukraine amidst the ongoing Russian invasion. As in 2016 with the original Industroyer, the aim of this cyberattack was to cause a major power outage – but this time the attackers failed. Lipovsky will outline how the attack unfolded, why it was unsuccessful, and reverse engineer the samples, showing how the code evolved since the first version. The presentation will also focus on the evolution of disruptive wiper campaigns of the Sandworm APT group – from the infamous NotPetaya worm, through the HermeticWiper campaign that ESET discovered on February 23, 2022, only a few hours before the invasion, and on to CaddyWiper. It will also disclose how the attackers have recently been trolling ESET.

DELIVERED PRESENTATIONS

BSides Montreal

[Clustering malware activity: How we do attribution](#) [103]

In this presentation, ESET malware researcher Alexandre Côté Cyr explained how ESET Research does attribution using technical artifacts (such as code similarity), infrastructure, TTPs, and socio-political factors like victimology. Concrete examples from previous research were showcased to illustrate how these indicators can be used, or misused, to cluster activity. The relative merits and

reliability of these indicators were discussed, along with how they can be combined to arrive at a more accurate conclusion. Attendees were also presented with the pitfalls associated with each of them, with examples of how we can get it wrong. This part of the presentation also brought up other obstacles encountered when doing attribution, including the varying definitions of certain APT groups among various researchers, along with tool sharing and so-called “umbrella groups” that encapsulate multiple subgroups.

LABSCon

[Phosphorescent Connections and Shifting Oil Reserves: Overlap in Middle Eastern Threat Actors](#) [104]

In his presentation, ESET senior threat intelligence analyst Adam Burgher revealed insights into recent campaigns deployed by Middle Eastern threat actors OilRig, APT35 (aka Phosphorus), and Agrius. Attendees learned about a new OilRig campaign and the group's shift in C&C methodology; a sharp APT35 pivot from public vulnerability exploitation to a low-key custom backdoor campaign that is ongoing; and an Agrius wiper campaign called Fantasy Vacation that targets the diamond industry and has ties to APT35.

Black Hat USA 2022



[Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again](#) [105]

ESET senior malware researcher Anton Cherepanov and ESET principal researcher Robert Lipovsky provided technical details on Industroyer2, a new version of the only malware specifically designed to trigger electricity blackouts. Its latest observed variant was detected in Ukraine amidst the ongoing

war, aiming to cause a major electricity outage in a region with a population of more than two million, using components amplifying the impact. Joining the presentation was Deputy Director of Ukraine's State Service of Special Communications and Information Protection, Victor Zhora. This is the first time that a Ukrainian governmental representative has taken part in such a high-profile cybersecurity conference. The Industroyer2 attack was thwarted thanks to the swift response of Ukrainian defenders and CERT-UA. ESET Research provided the Ukrainian side with crucial analysis of this threat. In the presentation, the researchers showed data linking this attack to the notorious Sandworm APT group and discussed why and how the attack was mostly unsuccessful. On top of that, the attendees were provided with actionable advice for defenders, including log entries, EDR rules, and detection/hunting rules for Snort and YARA.

Virus Bulletin 2022

[Lazarus & BYOVD: Evil to the Windows core](#) [106]

In their session, ESET malware researcher Peter Kálnai and ESET malware analyst Matěj Havránek took a deep technical dive into a malicious component that was used in an attack by the Lazarus APT group in late 2021. Previously undocumented, this malware is a sophisticated user-mode module that uses the Bring Your Own Vulnerable Driver (BYOVD) technique, leveraging a vulnerability in a legitimate, signed Dell driver. After gaining write access to kernel memory, the module's global goal is to blind security solutions and monitoring tools. This is tactically realized via several distinct mechanisms that target important kernel functions, structures, and variables of Windows systems from versions 7.1 up to Windows Server 2022. Kálnai and Havránek explained these mechanisms by demonstrating how they operate and what changes they make to system monitoring once the user-mode module is executed. Our researchers also compared this Lazarus case to other APT groups abusing BYOVD, as it possesses a complex bundle of ways to disable monitoring interfaces not seen in the wild thus far.

[Creepy things that glow in the dark: a deep look at POLONIUM's undocumented tools](#) [107]

POLONIUM is a threat actor that was first publicly documented in June 2022 by Microsoft researchers. While public visibility of the group's activities is very limited, ESET telemetry shows that POLONIUM has in fact been active since at least September 2021, continuously developing new tools and improving its existing ones. The presentation explained and exposed various components of POLONIUM's toolset – the findings of ESET malware researcher Matias Porolli, presented by ESET principal researcher Robert Lipovsky, show that the group uses four previously undocumented backdoors, and several in-house-developed tools, including custom keyloggers and a tool to capture snapshots from the webcam. Lipovsky also shared insights about how the group operates, its victimology, network infrastructure, the tricks that POLONIUM operators use to try to evade detection, and how they abuse cloud storage services for command and control. The presentation concluded with a showcase of possible overlaps with other APT groups.

RSA Conference 2022

[ESpecter: Showing the Future of UEFI Threats](#) [108]

In recent years, it has become clear that UEFI threats are real and have been deployed in the wild. UEFI implants such as LoJax and MosaicRegressor have used the lowest level of persistence, SPI flash, but the actors behind the ESpecter bootkit think that compromising the bootloader is the way. This session by ESET head of threat research Jean-Ian Boutin and ESET malware researcher Martin Smolár described ESET's discovery of the aforementioned ESpecter – a previously undocumented real-world UEFI bootkit persisting on the EFI System Partition (ESP). This session raised awareness of UEFI threats affecting the ESP and provided guidance and resources for defenders to help secure their pre-OS environments. Boutin and Smolár's analysis of this previously unknown, real-world UEFI ESP bootkit helped attendees understand details of the techniques used by these threats. Although UEFI threats are very rare, ESET's discovery of ESpecter shows they are definitely not mere specters.

CODE BLUE 2022 REcon 2022 SecTor 2022

[Under the hood of Wslink's multilayered virtual machine](#) (CODE BLUE 2022) [109]

[Under the hood of Wslink's multilayered virtual machine](#) (REcon 2022) [110]

[Under the hood of Wslink's multilayered virtual machine](#) (SecTor 2022) [111]

Wslink is a unique loader, linked to the Lazarus group, that ESET researchers discovered and documented at the end of 2021. Most Wslink samples are packed and protected with an advanced virtual machine (VM) obfuscator; the samples contain no clear artifacts, such as specific section names, that easily link them to an already known and publicly described obfuscator. This VM additionally introduces several other obfuscation techniques such as insertion of junk code, encoding of virtual operands, duplication of virtual opcodes, opaque predicates, merging of virtual instructions, and a nested VM. In his presentation, ESET malware researcher Vladislav Hřčka analyzed the internals of the VM and described ESET Research's semiautomated approach to seeing through the obfuscation techniques in a reasonable time. The approach was demonstrated on a few chunks of bytecode from a protected sample and the results were compared against a subsequently discovered non-obfuscated sample to confirm the validity of the method.

MITRE ATT&CK CONTRIBUTIONS

ESET will be participating in the next round of [MITRE Engenuity ATT&CK](#) [112] evaluations that will focus on tactics, techniques, and procedures (TTPs) applied by the Turla APT group. Turla is a cyber-espionage group that has been active for more than 12 years. It has compromised many governments, especially diplomatic entities, all around the world, operating a large malware arsenal that ESET Research [has documented over the last few years](#) [113] [114] [115] [116] [117]. Besides our research, we also made several [contributions](#) [118] to the MITRE ATT&CK Enterprise Matrix related to the [Turla Group](#) [119].

ESET's research into APT groups like Turla has directly or indirectly helped many organizations and nation-states successfully thwart potential attacks by providing much-needed visibility into TTPs used by those very same groups for economic, espionage, geopolitical, or criminal purposes. ESET will again participate in both the Detection and the Protection evaluation rounds; results are to be expected during the second quarter of 2023.

OTHER CONTRIBUTIONS

ESET researchers discovered three buffer overflow vulnerabilities in the UEFI firmware of several Lenovo Notebook devices, affecting more than 70 various models, including several within the ThinkBook series. All of these vulnerabilities were reported to the manufacturer on February 18. Lenovo acknowledged them, and released a [security advisory](#) [11] on June 12 containing a list of affected devices and firmware update instructions.

[CVE-2022-1890](#) [120]

UEFI BIOS images of several Lenovo laptop models contained a buffer overflow vulnerability leading to arbitrary code execution while processing the `System` NVRAM variable inside the ReadyBootDxe driver.

[CVE-2022-1891](#) [121]

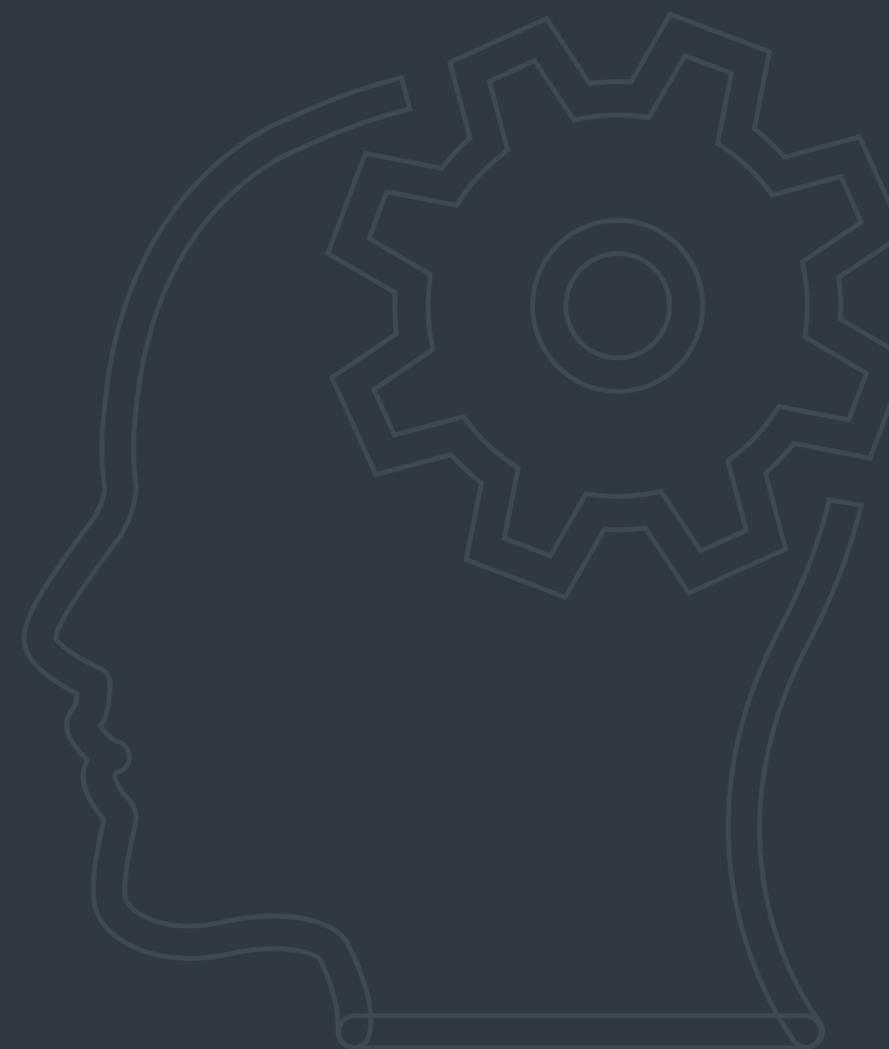
UEFI BIOS images of several Lenovo laptop models contained a buffer overflow vulnerability leading to arbitrary code execution while processing the `System` NVRAM variable inside the SystemLoadDefaultDxe driver.

[CVE-2022-1892](#) [122]

UEFI BIOS images of several Lenovo laptop models contained a buffer overflow vulnerability leading to arbitrary code execution while processing the `OilSetup` NVRAM variable inside the SystemBootManagerDxe driver.

The vulnerabilities can be exploited to achieve arbitrary code execution in the early phases of the platform boot, possibly allowing the attackers to hijack the OS execution flow and disable some important security features. These vulnerabilities were caused by insufficient validation of the `DataSize` parameter passed to the UEFI Runtime Services function `GetVariable`. An attacker could create a specially crafted NVRAM variable, causing buffer overflow of the data buffer in the second `GetVariable` call.

It's a typical UEFI "double `GetVariable`" vulnerability that can be identified in the firmware code by the IDA plugin `efiXplorer`. However, the vulnerabilities we found [were not covered](#) [123] by this plugin at the time of discovery. To help fellow researchers discover similar vulnerabilities and improve overall real-world UEFI firmware security, we submitted our improvements to the [efiXplorer repository](#) [124].



CREDITS

Team

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

Aryeh Goretsky
Branislav Ondrášek
Bruce P. Burrell
Hana Matušková
Nick FitzGerald
Ondrej Kubovič
Zuzana Pardubská

Foreword

Roman Kováč, Chief Research Officer

Contributors

Dušan Lacika
Igor Kabina
Ján Šugarek
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Étienne M.Léveillé
Martin Červeň
Michal Malík
Milan Fránik
Miroslav Baláž
Miroslav Legéň
Patrik Sučanský
Peter Kálnai
Radim Raszka
Robert Kapp
Vladimír Šimčák
Zuzana Legáthová
Zoltán Rusnák

ABOUT THE DATA IN THIS REPORT

The threat statistics and trends presented in this report are based on global telemetry data from ESET. Unless explicitly stated otherwise, the data includes detections regardless of the targeted platform.

Further, the data excludes detections of *potentially unwanted applications* [125], *potentially unsafe applications* [126] and *adware* [127], except where noted in the more detailed, platform-specific sections and in the Cryptocurrency threats section.

This data was processed with the honest intention to mitigate all known biases, in an effort to maximize the value of the information provided.

Most of the charts in this report show detection trends rather than provide absolute numbers. This is because the data can be prone to various misinterpretations, especially when directly compared to other telemetry data. However, absolute values or orders of magnitude are provided where deemed beneficial.



REFERENCES

- [1] <https://www.pcloud.com/>
- [2] <https://office.hancom.com/>
- [3] <https://nvd.nist.gov/vuln/detail/CVE-2020-9934>
- [4] <https://medium.com/@mattshockl/cve-2020-9934-bypassing-the-os-x-transparency-consent-and-control-tcc-framework-for-4e14806f1de8>
- [5] <https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/>
- [6] <https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/>
- [7] <https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html>
- [8] <https://malpedia.caad.fkie.fraunhofer.de/actor/apt37>
- [9] <https://attack.mitre.org/groups/G0067/>
- [10] <https://twitter.com/ESETresearch/status/1575103839115804672>
- [11] https://support.lenovo.com/us/en/product_security/len-91369
- [12] <https://twitter.com/ESETresearch/status/1547166334651334657>
- [13] <https://www.sentinelone.com/blog/from-the-front-lines-new-macos-covid-malware-masquerades-as-apple-wears-face-of-apt/>
- [14] <https://twitter.com/ESETresearch/status/1547943014860894210>
- [15] <https://twitter.com/ESETresearch/status/1527531726905409536>
- [16] <https://www.welivesecurity.com/2022/05/20/sandworm-ukraine-new-version-arguepatch-malware-loader/>
- [17] <https://twitter.com/ESETresearch/status/1524731829139476480>
- [18] <https://twitter.com/ESETresearch/status/1526183746524876802>
- [19] <https://twitter.com/ESETresearch/status/1521735320852643840>
- [20] <https://twitter.com/h2jazi/status/1555205042331947011>
- [21] <https://twitter.com/ESETresearch/status/1559553324998955010>
- [22] <https://nvd.nist.gov/vuln/detail/CVE-2017-11882>
- [23] https://en.wikipedia.org/wiki/Advance-fee_scam
- [24] <https://asec.ahnlab.com/en/34793/>
- [25] <https://www.recordedfuture.com/amid-rising-magecart-attacks-online-ordering-platforms>
- [26] <https://www.bleepingcomputer.com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/>
- [27] <https://twitter.com/vxunderground/status/1561262483448512513>
- [28] <https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/>
- [29] <https://www.microsoft.com/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/>
- [30] <https://thehackernews.com/2022/07/new-rust-based-ransomware-family.html>
- [31] <https://www.lpalmieri.com/posts/error-handling-rust/>
- [32] <https://www.bleepingcomputer.com/news/security/ransomware-hacking-groups-move-from-cobalt-strike-to-brute-ratel/>
- [33] <https://www.bleepingcomputer.com/news/security/automotive-supplier-breached-by-3-ransomware-gangs-in-2-weeks/>
- [34] <https://www.bleepingcomputer.com/news/security/fbi-zeppelin-ransomware-may-encrypt-devices-multiple-times-in-attacks/>
- [35] <https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022>
- [36] <https://rusi.org/explore-our-research/publications/commentary/ransomware-now-threatens-global-south>
- [37] <https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/>
- [38] <https://www.phmsa.dot.gov/news/phmsa-issues-proposed-civil-penalty-nearly-1-million-colonial-pipeline-company-control-room>

- [39] <https://www.cisa.gov/uscert/ncas/alerts/aa22-187a>
- [40] <https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/>
- [41] <https://www.qnap.com/en/security-advisory/QSA-22-21>
- [42] <https://www.bleepingcomputer.com/news/security/new-redeemer-ransomware-version-promoted-on-hacker-forums/>
- [43] <https://blogs.blackberry.com/en/2022/05/yashma-ransomware-tracing-the-chaos-family-tree>
- [44] <https://www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/>
- [45] <https://www.bleepingcomputer.com/news/security/foxconn-confirms-ransomware-attack-disrupted-production-in-mexico/>
- [46] <https://www.darkreading.com/attacks-breaches/costa-rica-declares-state-of-emergency-under-sustained-conti-cyberattacks>
- [47] <https://www.bleepingcomputer.com/news/security/building-materials-giant-knauf-hit-by-black-basta-ransomware-gang/>
- [48] <https://www.bleepingcomputer.com/news/security/lockbit-claims-ransomware-attack-on-security-giant-entrust-leaks-data/>
- [49] <https://thehackernews.com/2022/05/us-charges-venezuelan-doctor-for-using.html>
- [50] <https://www.bleepingcomputer.com/news/security/astralocker-ransomware-shuts-down-and-releases-decryptors/>
- [51] <https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-astralocker-yashma-ransomware-victims/>
- [52] <https://www.europol.europa.eu/media-press/newsroom/news/hit-ransomware-no-more-ransom-now-offers-136-free-tools-to-rescue-your-files>
- [53] <https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/bc-p/3566717/highlight/true#M4281>
- [54] <https://thehackernews.com/2022/06/new-emotet-variant-stealing-users.html>
- [55] <https://www.bleepingcomputer.com/news/security/bored-ape-yacht-club-otherside-nfts-stolen-in-discord-server-hack/>
- [56] <https://thehackernews.com/2022/08/hackers-stole-crypto-from-bitcoin-atms.html>
- [57] <https://www.sec.gov/news/press-release/2022-78>
- [58] <https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/>
- [59] <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clipminer-bitcoin-mining-hijacking>
- [60] <https://www.bleepingcomputer.com/news/security/massive-facebook-messenger-phishing-operation-generates-millions/>
- [61] https://faq.whatsapp.com/824303528016260/?locale=en_US
- [62] https://www.trendmicro.com/en_us/research/22/e/fake-mobile-apps-steal-facebook-credentials-crypto-related-keys.html
- [63] <https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/>
- [64] <https://support.google.com/googleplay/android-developer/answer/11950272?hl=en>
- [65] <https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones?>
- [66] <https://www.welivesecurity.com/2021/05/17/take-action-now-flubot-malware-may-be-on-its-way/>
- [67] <https://twitter.com/ESETresearch/status/1526897310231322630>
- [68] <https://www.cleafy.com/cleafy-labs/sova-malware-is-back-and-is-evolving-rapidly>
- [69] <https://www.f5.com/labs/articles/threat-intelligence/f5-labs-investigates-malibot>
- [70] https://www.trendmicro.com/en_us/research/22/g/examining-new-dawdropper-banking-dropper-and-daas-on-the-dark-we.html
- [71] <https://github.com/BishopFox/sliver>
- [72] <https://www.politico.eu/article/pegasus-use-5-eu-countries-nso-group-admit/>
- [73] <https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/>
- [74] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32893>
- [75] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32894>

- [76] <https://www.theguardian.com/technology/2022/aug/18/apple-security-flaw-hack-iphone-ipad-macs>
- [77] <https://twitter.com/360Netlab/status/1420390398825058313>
- [78] <https://nvd.nist.gov/vuln/detail/CVE-2015-2051>
- [79] <https://www.exploit-db.com/exploits/41471>
- [80] <https://nvd.nist.gov/vuln/detail/CVE-2022-26134>
- [81] <https://nvd.nist.gov/vuln/detail/CVE-2022-30525>
- [82] <https://isc.sans.edu/diary/Scanning+Activity+for+NVMS-9000+Digital+Video+Recorder/25434>
- [83] <https://www.exploit-db.com/exploits/44760>
- [84] <https://nvd.nist.gov/vuln/detail/CVE-2022-1388>
- [85] <https://www.bleepingcomputer.com/news/security/critical-f5-big-ip-vulnerability-exploited-to-wipe-devices/>
- [86] <https://www.thedrive.com/tech/i-tried-the-honda-keyfob-hack-on-my-own-car-it-totally-worked>
- [87] <https://www.thedrive.com/news/how-thieves-are-stealing-hyundais-and-kias-with-just-a-usb-cable>
- [88] <https://arstechnica.com/information-technology/2022/06/hackers-out-to-steal-a-tesla-can-create-their-very-own-personal-key/>
- [89] <https://thehackernews.com/2022/06/researchers-demonstrate-ransomware-for.html>
- [90] <https://www.welivesecurity.com/2017/01/25/rot-ransomware-things/>
- [91] <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>
- [92] <https://thehackernews.com/2022/05/eu-blames-russia-for-cyberattack-on-ka.html>
- [93] <https://thehackernews.com/2022/07/microsoft-adds-default-protection.html>
- [94] <https://thehackernews.com/2022/05/avoslocker-ransomware-variant-using-new.html>
- [95] <https://www.microsoft.com/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations/>
- [96] <https://www.bleepingcomputer.com/news/security/lazarus-hackers-target-vmware-servers-with-log4shell-exploits/>
- [97] https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf
- [98] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190>
- [99] <https://www.wired.com/story/microsoft-follina-vulnerability-windows-office-365/>
- [100] <https://cert.gov.ua/article/341128>
- [101] <https://aavar.org/cybersecurity-conference/index.php/agenda/>
- [102] https://www.ekoparty.org/en_US/
- [103] <https://bsidesmtl.ca/bsides-montreal-2022-september-10-2022/program-2022/>
- [104] <https://www.labscon.io/speakers/adam-burgher/>
- [105] <https://www.blackhat.com/us-22/briefings/schedule/#industroyer-sandworms-cyberwarfare-targets-ukraines-power-grid-again-27832>
- [106] <https://www.virusbulletin.com/conference/vb2022/abstracts/lazarus-byovd-evil-windows-core/>
- [107] <https://www.virusbulletin.com/conference/vb2022/abstracts/creepy-things-glow-dark-deep-look-poloniums-undocumented-tools/>
- [108] <https://www.rsaconference.com/library/presentation/usa/2022/especter%20first%20real-world%20uefi%20bootkit%20persisting%20on%20esp>
- [109] https://codeblue.jp/2022/en/talks/?content=talks_21
- [110] <https://cfp.recon.cx/2022/talk/7EQPJX/>
- [111] <https://sector.ca/sessions/under-the-hood-of-wslinks-multilayered-virtual-machine/>
- [112] <https://attackervals.mitre-engenuity.org/enterprise/turla/>
- [113] <https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf>
- [114] https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf
- [115] <https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf>
- [116] <https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/>
- [117] <https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/>
- [118] <https://attack.mitre.org/software/S0126/>

[119] <https://attack.mitre.org/groups/G0010/>

[120] <https://github.com/eset/vulnerability-disclosures/commit/b7db546f7b58dc88509898d77bfdc8959b929eb0#diff-1b088545db98018b1b6c3909d4e879c0033325f4c3762a4afcb55a819c5cddb8>

[121] <https://github.com/eset/vulnerability-disclosures/commit/b7db546f7b58dc88509898d77bfdc8959b929eb0#diff-da115c7f06d6e27f4d388104dc64d82b1a101d13ed7339cdd3c5e94fd7d3056d>

[122] <https://github.com/eset/vulnerability-disclosures/commit/b7db546f7b58dc88509898d77bfdc8959b929eb0#diff-c0af4b8268b4ec4c292409326bfcf5e982993cf5275bcf0d2aa85ef18876a551>

[123] <https://i.blackhat.com/eu-20/Wednesday/eu-20-Labunets-efiXplorer-Hunting-For-UEFI-Firmware-Vulnerabilities-At-Scale-With-Automated-Static-Analysis.pdf>

[124] <https://github.com/binarly-io/efiXplorer/commit/6bccee7b6817c8af6a737c24c25e88435a85a3f0>

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

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

[127] <https://help.eset.com/glossary/en-US/adware.html>

About ESET

For more than 30 years, *ESET*[®] has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on [LinkedIn](#), [Facebook](#), and [Twitter](#).



© 2022 ESET, spol. s r.o. - All rights reserved.

Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o.
All other names and brands are registered trademarks of their respective companies.

WeLiveSecurity.com

 [@ESETresearch](#)

 [ESET GitHub](#)