脅威レポート

2022 年第 1 三半期

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ESET®
Digital Security
Progress. Protected.

目次

（以降のセクションは英語での提供となります）

序文

2022年T1（第1三半期）のESET脅威レポートをご覧いただきありがとうございます。

2年以上にわたって新型コロナウイルスのパンデミックに耐えた私たちに訪れたのは、戦争という新たな試練でした。いくつもの紛争が世界各地で起きていますが、今回のロシアとウクライナの戦争は、ESETにとって全く異なる意味を持っています。ESETの本社といくつかのオフィスがあるスロバキア東部の国境のすぐそばで、ウクライナの人々は核兵器を所有する敵の目の前で、正当な理由なきこの戦争から自分の生活と主権を守るために闘っています。本書の中でも説明しますが、ウクライナは陸上、海上および航空で防衛しているだけでなく、サイバー空間の攻撃に対しても抵抗しています。

ESETの今回の*特集記事*では、現在も続いているこの戦争に関連するさまざまなサイバー攻撃についてのESETの研究者の分析や、影響を緩和するための取り組みについて説明します。本書の中では、高電圧変電所を標的し悪名をはせたIndustroyerマルウェアの再来についても説明しています。

ロシアによる侵攻が始まる少し前に、RDP攻撃が2回急減しましたが、その内の1つがESETのテレメトリ（監視データ）に記録されています。ESET脅威レポートの「*エクスプロイト*」セクションで説明していますが、RDP攻撃は2年間にわたって増加の一途をたどっていましたが、この急減はロシアとウクライナとの戦争に関連している可能性があります。しかし、この期間に減少したにもかかわらず、2022年T1に検出されたRDP攻撃の約60%はロシアが発生源でした。この戦争は別の影響も及ぼしています。ESETのテレメトリでは、これまでランサムウェアの脅威はロシアにある標的を避ける傾向が見られていましたが、この期間はロシアが最大の標的となりました。ESETの研究者は、ウクライナへの敬意を示す「Slava Ukraini!（ウクライナに栄光を）」というメッセージで画面をロックするランサムウェアの亜種も検出しています。

当然のように、この戦争に便乗するスパムやフィッシングの脅威も多く発生しています。2月24日の侵攻直後から、詐欺師たちは、架空の慈善団体や募金活動を餌にして、ウクライナを支援しようとする人々を標的に攻撃しています。同日には、スパムの検出件数が大幅に増加したことが確認されています。主にスパムメールを使用して拡散する悪名高いマルウェアEmotetは、昨年テイクダウンされた後に復活を遂げており、ESETのテレメトリでも再び検出数が増加しています。Emotetのオペレーターは矢継ぎ早にスパムキャンペーンを展開しており、Emotetの検出数は100倍以上増加しました。

ESETのテレメトリでは、ロシアとウクライナとの戦争とは関係のない脅威も多く観測されています。これらの脅威の詳細は、本レポートの「*統計と傾向*」のセクションを参照してください。この数ヶ月間には、今後注意が必要な研究結果も多く公開されています。ESETの研究者は、カーネルドライバの脆弱性の悪用、広範囲に影響を及ぼすUEFIの脆弱性、AndroidおよびiOSデバイスを標的とする仮想通貨マルウェア、Mustang Panda、Donot Team、Winnti Group、TA410のAPTグループによるキャンペーンなどを特定しています。

ESETの研究者は、Industroyer2、エアギャップネットワークのセキュリティ侵害、InvisiMole、OilRig、MuddyWater、FreshFeline、TA410のAPTグループが実行しているキャンペーンを詳細に分析した結果を、S4x22、CARO Workshop、Botconf、NorthSecカンファレンスで発表しています。これらのカンファレンスにおける発表内容の概要は、本レポートの最後のセクションで参照できます。今後数ヶ月間に開催されるRSA、REcon、Virus Bulletin、その他多くのカンファレンスにおけるESETの講演に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

ウクライナに対するサイバー攻撃

ESET のリサーチ部門は、ウクライナで展開されているいくつもの新しいワイパー型マルウェアによる攻撃を発見しました。また、復活した悪名をはせる Industroyer を分析し、これらのすべての攻撃と現在進行中の戦争との関連性を説明しています。

APT グループの活動

Donot Team

ESET のリサーチ部門は、南アジアを主な標的にサイバースパイ活動を展開している Donot Team（別名 APT-C-35 および SectorE02）が最近実行したキャンペーンを分析しました。

Mustang Panda

ESET のリサーチ部門は、Mustang Panda APT グループによるサイバースパイキャンペーンが進行していることを特定しました。このキャンペーンでは、過去に検出・文書化されていない Korplug の亜種である Hodur を使用されています。

Winnti Group

ESET のリサーチ部門は、Winnti Group が使用している PipeMon の新たな亜種を発見しました。

TA410

ESET のリサーチ部門は、APT10 とのつながりが指摘されており、サイバースパイ活動を統括している TA410 グループの詳細な情報を公開しました。

統計と傾向

カテゴリ	2021 年 T3/ 2022 年 T1	2022 年 T1 の重要ポイント
脅威全体の検出数	+20.1% ↑	Emotet のキャンペーンにより、全体的な脅威活動が増加
情報窃取型マルウェア	+12.0% ↑	JS/Spy.Banker（別名：Magecart）が拡大
ランサムウェア	-4.3% ↓	ロシアがランサムウェアの標的となるケースが増大
ダウンローダー	+121.5% ↑	Emotet が大規模なスパムキャンペーンを開始
暗号通貨の脅威	-29.3% ↓	暗号通貨に関する脅威活動全般が減少
Web に関する脅威	-1.8% →	3 月にフィッシング URL の件数が急増
電子メールに関する脅威	+36.8% ↑	Emotet、悪意のある文書をメールに添付して大量に配信
Android に関する脅威	+8.0% ↑	Android のスパイウェアが蔓延
macOS の脅威	-14.9% ↓	監視対象の全脅威カテゴリで減少
RDP 攻撃	-40.8% ↓	RDP 攻撃は 2020 年以来の減少を記録

特集記事

ウクライナにおけるサイバー攻撃

ESET リサーチ部門

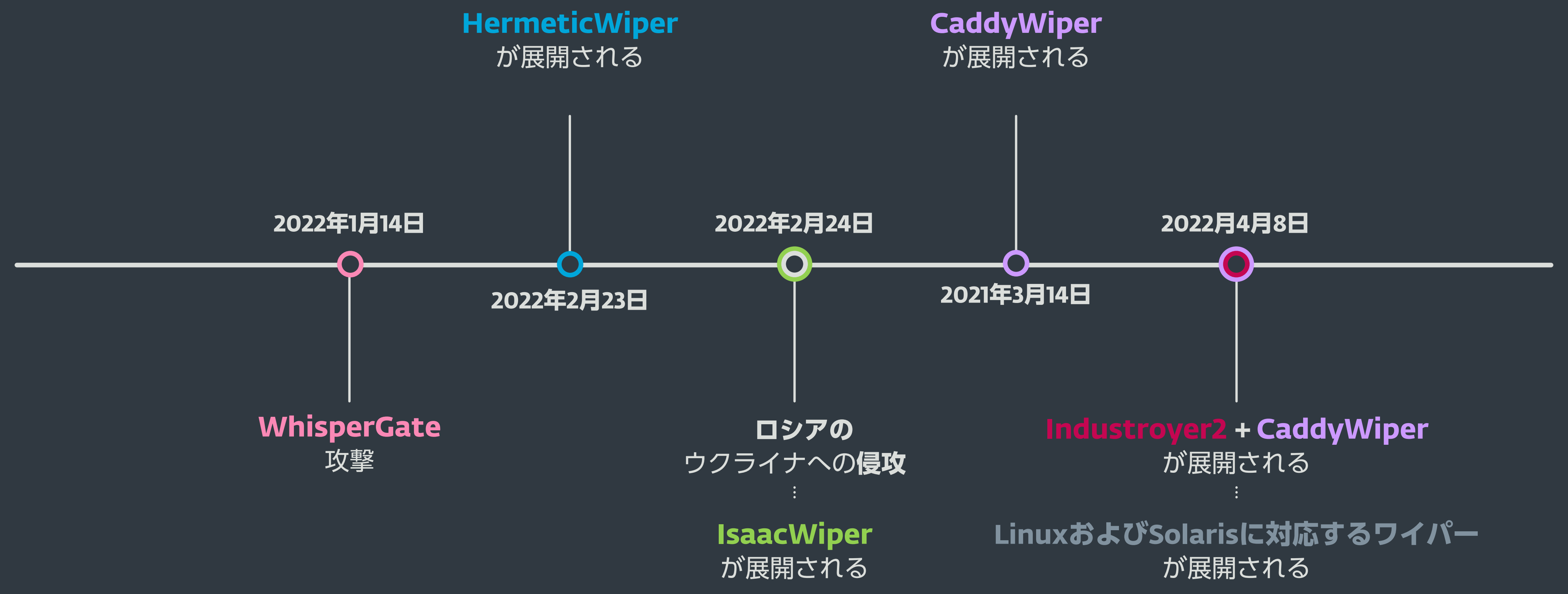
ESET の研究者は、複数の新しいワイパー型マルウェアによる攻撃がウクライナで展開されていることを発見しました。また、復活した悪名をはせる Industroyer を分析し、これらのすべての攻撃と現在進行中の戦争との関連性を説明しています。

ロシアがウクライナに侵攻する前夜、ESET の研究者はウクライナで新しいデータワイパー型マルウェアが展開されているのを発見し、同国の少なくとも 5 つの組織の数百台のマシンにインストールされていることを確認しました。分散型サービス拒否（DDoS）攻撃が一斉に行われ、いくつかの重要なウクライナの Web サイトがオフラインにされてから、わずか数時間後にはこれらのマルウェアが展開されました。このデータワイパー型マルウェアは、現地時間 2 月 23 日 17 時の直前（協定世界時 15 時前）に初めて発見されました。ESET の研究者は深夜までマルウェアを解析し、翌朝、世界のメディアが速報で取り上げてくれることを期待しながら、調査結果を *Twitter* [1] で公開しました。

ESET の研究者は、この調査結果から影響を受けたこれらの組織はこのワイパーが展開されるかなり前の段階から攻撃されていたことを確信しています。

- 攻撃者は、Hermetica Digital Ltd. という会社に 2021 年 4 月 13 日に発行された正規のコードサイニング証明書を使用していました。ESET がこのマルウェアを *HermeticWiper* [2] と名付けた理由もそこにあります。この名前は、*EESET のリサーチ部門のツイート* [3] への返信で提案されたものです。
- 初期の侵入方法は、標的組織によって異なっていましたが、少なくとも 1 つのケースではグループポリシーオブジェクト（GPO）を使用して HermeticWiper を展開していたことから、攻撃者はその標的組織の Active Directory サーバーの 1 つに事前にアクセスできていたと考えられます。
- タイムスタンプから 2021 年 12 月 28 日にコンパイルされたことがわかります。

HermeticWiper は、セキュリティを侵害したシステムのいくつかの場所（マスターブートレコードやマスターファイルテーブルなど）をランダムバイトで



ロシアのウクライナ侵攻時に ESET の研究者が検知した攻撃のタイムライン

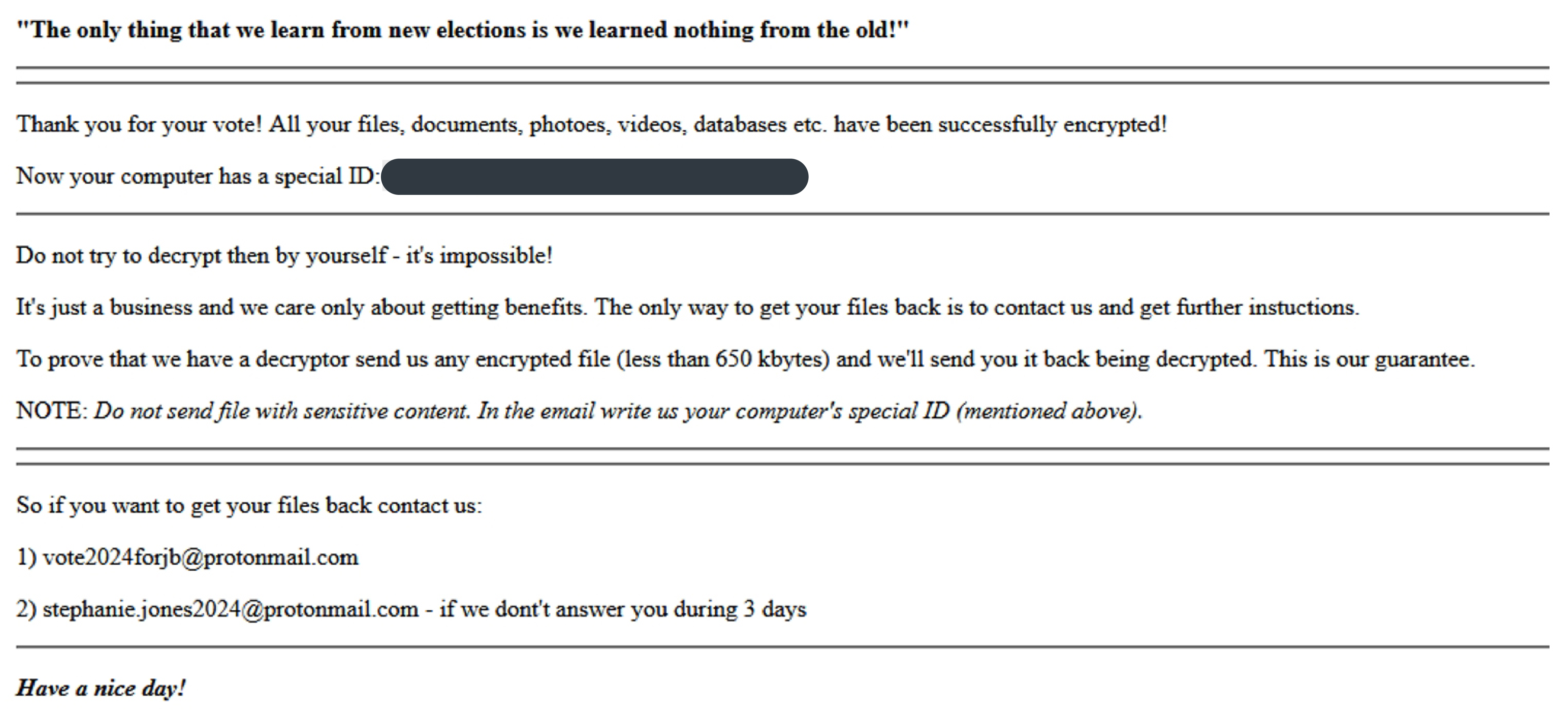
上書きします。「マイドキュメント」や「ドキュメント」フォルダにあるシンボリックリンクやサイズの大きなファイルもランダムバイトで上書きされます。また、Windows、Program Files、Program Files(x86)、PerfLogs、Boot、System Volume Information、およびAppDataフォルダにあるフォルダおよびファイルも再帰的に消去します。このワイパーは、自分のファイルをランダムバイトで上書きして、ディスクから自身も消去します。これは、インシデントの解析を防止するフォレンジック対策と考えられます。マシンは再起動されますが、ほとんどのファイルが消去されているため、起動に失敗します。ESETの研究者は、バックアップがない場合、攻撃を受けたマシンを復旧できないと考えています。

偽装ランサムウェアを使用する Hermeticキャンペーン

同じコード署名証明書で署名されている他の検体をESETが調査したところ、新しいマルウェアファミリーを特定し、*HermeticWizard* [4]と命名しました。これはワームであり、2022年2月23日14:52:49（協定世界時）に、ウクライナのあるシステムに展開されました。HermeticWizardは、最初にローカルネットワークにある他のマシンを探そうとします。ローカルIPアドレスを収集した後に、これらのIPアドレス（ローカルIPアドレスの場合のみ）に接続し、アクセス可能かどうかを確認します。アクセス可能なマシンを発見すると、スプレッダモジュールをドロップします。最終的には、HermeticWiperをドロップして実行します。拡散の仕組みは全体的に初歩的なものであり、この攻撃を急いで展開したことがうかがえます。

ESETの研究者は、HermeticWiperキャンペーンと同時に、Go言語で記述されたランサムウェアHermeticRansomがウクライナで使用されていることも発見しました。HermeticRansomは、2022年2月24日（UTC）の早朝にAVASTのツイート[5]で初めて報告されました。ESETのテレメトリを見ると、HermeticWiperと比較してその展開は小規模でした。このランサムウェアは、HermeticWiperと同時に展開されています。このワイパーの挙動を隠ぺいするためにHermeticRansomが展開されていた可能性があります。通常のランサムウェアとは異なり、HermeticRansomは金銭を得ることを目的としていなかったことから、ESETの研究者はHermeticRansomを「偽装ランサムウェア」だと見ています。

ある事例では、HermeticWiperと同様に、HermeticRansomがGPOから展開されていました。攻撃者は、バイデン米国大統領とホワイトハウスに関するいくつかのメッセージをバイナリに残していました。ファイルが暗号化されるときに被害を受けたユーザーに表示される身代金のメッセージに、「新しい選挙から学べる唯一のことは、古い選挙から何一つ学ばなかったことだ」と表示されます。



"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID:[redacted]

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote2024forjb@protonmail.com

2) stephanie.jones2024@protonmail.com - if we don't answer you during 3 days

Have a nice day!

格言を記した身代金メモ

IsaacWiper

2022年2月24日、ESETの研究者は、ウクライナ政府のネットワークでさらに別の新しいワイパーを検出し、IsaacWiperと名付けました。IsaacWiperは、HermeticWiperの攻撃の影響を受けていない組織で検出されています。HermeticWiperとIsaacWiperのコードには類似性がなく、IsaacWiperのコードは、比較的洗練されていません。タイムラインを考慮すると、両者が関連している可能性もありますが、ESETの研究者は関連性を強く示唆する証拠を見つけていません。PEコンパイルのタイムスタンプ(2021年10月19日)が改ざんされていなければ、IsaacWiperは数ヶ月前の作戦で使用されていた可能性があります。

IsaacWiperは、物理ドライブを最初に列挙し、メルセンヌ・ツイスタ擬似乱数生成器（PRNG）を使用して各ディスクの最初の0x10000バイトを消去します。次に、論理ドライブを列挙し、各ディスクにあるすべてのファイルを、同じくメルセンヌ・ツイスタPRNGで生成したランダムバイトで再帰的に消去します。単一のスレッドで再帰的にファイルを消去していることから、大きなディスクを消去する場合には長い時間が必要となっています。2022年2月25日に、攻撃者はデバッグログ機能を実装したIsaacWiperの新バージョンをドロップしました。攻撃者がターゲットマシンの一部を消去できなかったために何が起こっているかを特定するためにログメッセージを追加した可能性があります。

CaddyWiper

2021年3月14日、ESETの研究者は、ウクライナの組織への攻撃に別の破壊的なデータワイパーが使用されていることを発見しました。このワイパーは、限られた組織の数十台のシステムで検出されています。ESETが命名した*CaddyWiper* [6]は、HermeticWiperやIsaacWiperのコードと大きな類似性は見られません。しかし、HermeticWiperと同様に、CaddyWiperを操るサイバー攻撃者は、ワイパーを展開する前に標的にネットワークにすでに侵入していたこと示唆する証拠が存在します。

もう1つの偽装ランサムウェアである*NotPetya* [7]とは対照的に、これらのワイパーは、標的の組織を限定しながら展開されています。ESETの研究者は、前回のアウトブレイクとは異なり、このワイパーを使用したキャンペーンは、特定の組織のセキュリティ侵害への対応能力を低下させることを目的としていると考えています。ESETのリサーチ部門は、被害を受けた金融、メディア、政府機関を特定しました。ESETは調査結果から、CaddyWiperとHermeticWiperは悪名高いSandwormグループによる攻撃であると判断しています。

このロシアとウクライナの戦争の直前にも、ウクライナはさまざまなサイバー攻撃を受けていました。先に述べた *DDoS* [8] の前に実行された *Viasat 攻撃* [9] は、この企業の衛星インターネット網を標的としており、ウクライナのホームモデムに影響を与えました。ウクライナ当局によると、この戦争の直前に、この攻撃によって通信に重大な障害が発生しています。

1 月には、ウクライナのさまざまな政府機関の Web サイトが改ざんされ、「恐れよ、そして最悪の事態に備えよ」という警告メッセージが表示される事態が発生しました。その直後に、Microsoft Threat Intelligence Center は、ウクライナの組織を標的とする破壊的なマルウェア *WhisperGate* [10] についての*ブログ* [11] を公開しました。ESET の研究者は、関連する情報を調査した結果、この改ざんと WhisperGate 攻撃は関連していると考えています。

Industroyer 再び

さらに過去に目を向けると、2016 年 12 月 23 日にウクライナは電力網への攻撃に特化したマルウェア攻撃を史上初めて受けています。ESET の研究者は、Sandworm が展開したこのマルウェアを発見し *Industroyer* [12] と命名しました。Industroyer は、Stuxnet に次いで高度な設計になっており、キエフ北部の変電所を狙ったものでした。ESET の研究者は、5 年以上にわたって、これほど精巧な Industroyer がその後展開されていないことに疑問に感じていました。

今年 4 月に、ESET はウクライナ政府のコンピュータ緊急対応チームである *CERT-UA* [13] と協力し、同国のエネルギー企業を標的としたサイバーインシデントへの対応を行い、この最重要のインフラストラクチャを修復し保護しました。ESET と CERT-UA との連携により、攻撃による破壊活動を防止できただけでなく、新たな Industroyer の亜種を発見しました。CERT-UA と共同でこの亜種を *Industroyer2* [14] と命名しました。

Sandworm の攻撃者は、今回、ウクライナの高電圧変電所に Industroyer2 を展開しようとしていました。Sandworm は、Industroyer2 の他に、CaddyWiper、ORCSHRED、SOLOSHRED、AWFULSHRED などの破壊的なマルウェアも使用しています。ESET の研究者は、攻撃者がこのエネルギー企業に侵入した方法や、IT ネットワークから産業用制御システム（ICS）のネットワークに移動した方法を特定していません。この攻撃が成功していれば、200 万人が停電の影響を受けていた可能性があったと、ウクライナのエネルギー省副大臣である *Farid Safarov 氏* [15] は述べています。

Linux と Solaris を攻撃する破壊的なマルウェア

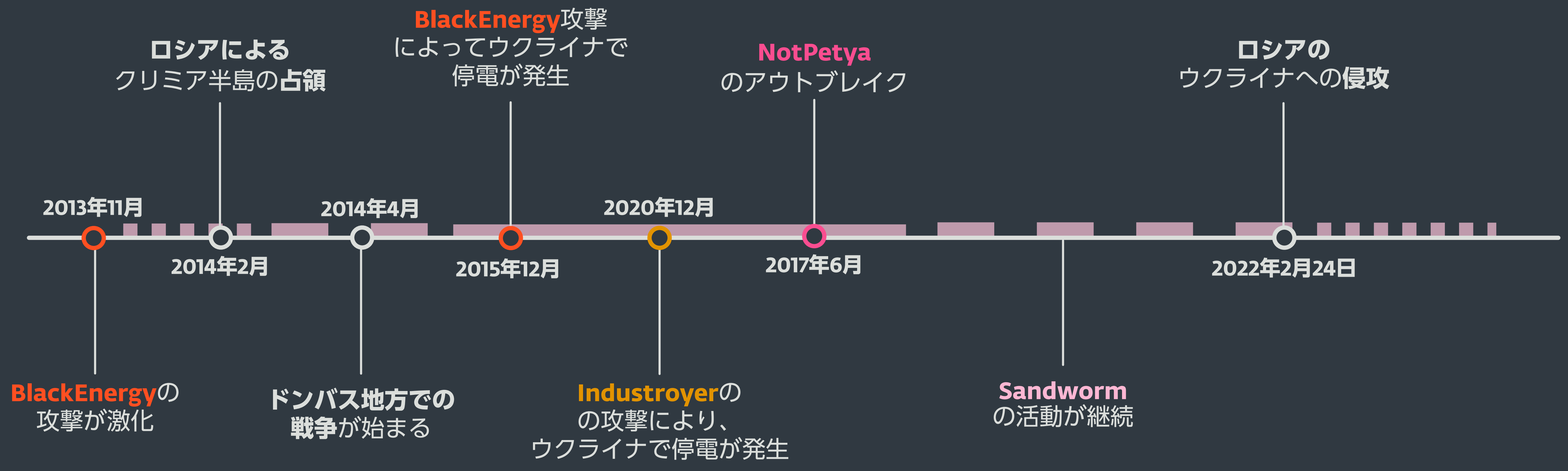
Industroyer2 は、その PE タイムスタンプから 2022 年 3 月 23 日にコンパイルされています。また、スケジュールタスクを使用して、2022 年 4 月 8 日 16 時 10 分 00 秒（UTC）に展開されるよう設定されていました。これは、攻撃者が 2 週間以上前から攻撃を画策していたことを示唆しています。攻撃者は、Industroyer2 と連携させて、破壊的なマルウェア CaddyWiper の新バージョンを ICS ネットワークに展開しています。

Windows 用のマルウェアに加え、Linux や Solaris を攻撃する破壊的なマルウェアが展開しています。これらのオペレーティングシステムを攻撃するワイパーは過去にはほとんど見られなかったものです。ESET の研究者は、この攻撃は復旧プロセスを遅らせ、エネルギー企業のオペレーターが ICS コンソールの操作を早期に再開できないようにする妨害工作だと考えています。また、Industroyer2 が実行されたマシンにもワイパーが展開されていますが、これは攻撃の痕跡を消し去るためだと考えられます。

ESET による支援

ESET は、人道支援 [16] に加えて、欧州および世界の多くの団体にセキュリティの調査結果と知見を提供しており、ロシアとウクライナとの戦争に起因するサイバー脅威に対応し、問題を解決し、その影響を緩和するように支援しています。この記事では、その成果の一部を紹介しています。

しかし、この戦争に関連するサイバー攻撃は、政府機関だけでなく、ウクライナの企業や一般市民にも向けられていることを知る必要があります。たとえば、*フィッシング* [17] の*多くのテーマ* [18] に見られるように、ウクライナの惨状に便乗する攻撃を ESET は検出しています。



ESET の研究者が検出して分析した、今回の戦争よりかなり以前にウクライナを標的とした過去に注目された大規模な攻撃

過去の大規模なサイバー攻撃

ウクライナはここ数年、激しいサイバー攻撃にさらされてきました。*ESETの研究者*[19]が*長年にわたって*[4]独占的に追跡してきたウクライナを主な標的としている国家主導型の代表的なAPTグループについて以下に説明します。

Sandworm

2013年末から2014年初めにかけて、ESETのテレメトリでSandwormがBlackEnergyマルウェアを使用してウクライナへの*攻撃を激化*[20]していることが確認されています。これらの攻撃は、ロシアがクリミア半島を占領し、その後ドンバス戦争が起こる少し前の時期に発生しています。2015年12月には、Sandwormは*ウクライナの電力網を攻撃*[21]しました。これはサイバー攻撃による史上初の停電を引き起こし、約23万人のウクライナの家庭が影響を受けました。1年後、Sandwormは*Industroyerを展開しました*[12]。その後、Sandwormは活動を分割しています。*GreyEnergyクラスタ*[22]はエネルギー業界への攻撃を続けており、*TeleBotsクラスタ*[23]はウクライナの金融業界を中心に攻撃を実行しています。これらの攻撃には、2017年の破壊的な*NotPetyaのアウトブレイク*[7]も含まれます。NotPetyaは、これまでのサイバー犯罪の歴史の中で、金銭的に最も壊滅的な被害をもたらしたサイバー攻撃です。

Sednit

Sednitは、ウクライナに対して攻撃しているほか、NATO諸国も標的にしています。2018年にESETの調査と分析でSednitの高度な技術力が明らかになっています。ESETの調査で、Sednitは*LoJaxを展開し*[24]、侵害したシステムに常駐する極めて回復力の高い手法を確立することに成功しています。LoJaxは実環境で初めて発見されたUEFIルートキットです。

Gamaredon

Gamaredonは2013年から活動しており、近年はウクライナに対する攻撃を活発に行っているAPTグループです。*Gamaredon*[25]は、大規模な攻撃やブルートフォース攻撃を展開し、常に新たなマルウェアの開発を続けています。通常は、スピアフィッシングキャンペーンによって標的の組織に侵入しており、サイバースパイを主な目的にしています。Gamaredonグループのいくつかの標的は、数年にわたってInvisiMoleグループに引き継がれていることをESETの研究者が確認しています。

InvisiMole

InvisiMoleは2013年から活動しています。*InvisiMoleの攻撃手法*[26]は、Gamaredonとは全く対照的であり、極めて秘密裏に実行されており、ウクライナと東欧での諜報活動に重点を置いています。InvisiMoleのオペレーターは、政府機関、軍関係者、外交機関に対して高度な標的型サイバースパイ攻撃を仕掛けています。

Turla

Turlaは、スパイ活動を実行しているAPTグループであり、*複雑なマルウェア*[27]を駆使していることが知られています。少なくとも、米軍のシステムへの侵入に成功した2008年から活動を開始していると考えられています。また、欧州や中東の多くの政府機関に対する大規模な攻撃にも関与しており、政府機関や軍事組織を主な標的としています。

Buhtrap

このグループは、ロシアとウクライナの金融機関や企業を標的にしていることが判明しています。2015年の後半以降、ESETの研究者はAPTグループの標的のプロファイルが変化していることを*確認しています*[28]。金銭的な利益を単に求めていたグループから進化しており、これらのAPTグループが使用するツールセットは、サイバースパイのためのマルウェアへと拡張されています。

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

エクスプロイト

署名されたカーネルドライバ — Windows のコア部分に存在する不備

ESET の研究者は、カーネルドライバに存在する脆弱性について詳細に調査した結果を発表しました。これらの脆弱性は、ゲームのチート行為対策を回避するために一般的に利用されていますが、複数の APT グループや汎用マルウェアでも悪用されています。

カーネルは Windows OS の中核となるコンポーネントです。カーネルドライバはソフトウェアレイヤーを構成しており、ハードウェア固有の機能やハードウェアから独立した機能を提供します。Windows の新しいバージョンでは、悪意のある署名のないドライバを直接読み込むことはできなくなりましたが、脆弱性のある正規のドライバを悪用して、悪意のあるコードをカーネルに読み込むことが可能です。この手法は、BYOVD（脆弱なドライバの持ち込み：Bring Your Own Vulnerable Driver）とも呼ばれます。

BYOVD は、APT グループの Slingshot や InvisiMole グループなど、さまざまな APT グループによって採用されている手法です。さらに、ESET が発見した *LoJax* [29] は世界で初めて発見された UEFI ルートキットであり、RWEverything ドライバを悪用して UEFI モジュールにアクセスします。

また、ESET の研究者が新たなカーネルドライバの脆弱性を発見し、この脆弱性の影響を受けるベンダーに通知しています。ベンダーは発見された問題の修正に積極的に取り組んでいます。発見された脆弱性の詳細なリストと有効な緩和策については、ESET のブログを参照してください。

WeLiveSecurity のブログ [30]

Android

Android マルウェアを使用した、偽のオンラインショップでの銀行の認証情報の窃取

ESET の研究者は、マレーシアの 8 つの銀行の顧客を標的とした悪意のある 3 つの Android アプリケーションを分析しました。スマートフォンを使用してショッピングするユーザーが増えるほど、サイバー犯罪者が利益を得る機会も増大します。このキャンペーンは現在も進行中であり、サイバー犯罪者は、正規のサービスを偽装した Web サイトを使用して、銀行の認証情報を盗み出しています。これらの Web サイトでは、なりすましのために、ユーザーがアクセスするサービスと似たドメイン名が使用されています。

ユーザーを騙して悪意のあるアプリをダウンロードさせるため、偽装サイトは直接買い物をするためのオプションは提供していません。代わりに、Google Play からアプリをダウンロードするためのボタンが設置されていますが、実際にはサイバー犯罪者が管理しているサーバーへと誘導されます。

被害者がこれらのアプリで注文すると、いくつかの支払い方法が提示されますが、実際には口座振込しか選択できません。口座振込を選ぶと、マレーシアで利用されている支払い方法である FPX の偽の支払いページに誘導され、8 つの銀行から 1 行を選択するように指示されます。銀行の認証情報を入力してしまうと、攻撃者に送信されます。また、この偽のオンラインショップアプリケーションは、二要素認証コードが含まれている場合、ユーザーが受信したすべての SMS メッセージをサイバー犯罪者に転送します。

今回のキャンペーンはマレーシアを対象としていますが、将来的には他の国の銀行にも展開される恐れがあります。現在は、攻撃者は銀行の認証情報を狙っていますが、将来的にはクレジットカード情報を窃盗する可能性もあります。

WeLiveSecurity のブログ [31]

Android および iOS

Android および iOS デバイスの暗号資産ウォレットを偽装したマルウェア

ESET のリサーチ部門は、人気の高い暗号通貨ウォレットを装い、トロイの木馬化として動作する Android および iOS アプリを配布する巧妙なスキームを発見しました。これらの悪意のあるアプリは、Coinbase、imToken、MetaMask、Trust Wallet、Bitpie、TokenPocket、または OneKey になりすまし、ユーザーの秘密のシードフレーズを盗み出していました。

攻撃者は、オリジナルと同じ機能を提供するようにこれらのアプリを模倣しており、検出が困難な場所に悪意のあるコードを挿入しています。このサイバー犯罪者は正規のアプリを詳細に分析しており、シードフレーズが生成されるか、またはユーザーによってインポートされるコードの場所を見つけています。

ESET は、これらのアプリが何十もの Telegram グループで宣伝されているのを発見しました。これは悪意のあるアプリの作成者が販売パートナーを拡大するために宣伝していたと考えられます。2021 年 10 月から、これらの Telegram グループが少なくとも 56 の Facebook グループで共有され、宣伝されていることがわかりました。また、2021 年 11 月に中国の 2 つの正規の Web サイトでこれらの悪意のあるウォレットを配布されていたことも ESET は発見しています。懸念されるのは、アプリのソースコードが流出しており、ネットで公開されているため、この悪意のあるアプリが今後さらに拡散する恐れがあることです。

これらの悪意のあるアプリは、インストールされるオペレーティングシステムによって動作が異なります。正規版のアプリが Android にインストールされている場合、別の証明書で署名されているため、偽造したアプリで上書きすることはできません。そのため、正規のウォレットアプリケーションをインストールしていない暗号通貨の新規ユーザーのみを標的としています。しかし、iOS の場合にはバンドル ID が同一ではないため、ユーザーは正規のアプリと不正なアプリの両方をインストールできます。

トロイの木馬として動作するこれらのアプリは、App Store からは直接入手できませんが、一部のアプリは Google Play から入手可能でした。*Google App Defense Alliance パートナー* [32] である ESET のリクエストに基づき、Google は 2022 年 1 月に公式ストアで発見された 13 個の悪意のあるアプリケーションを削除しています。

WeLiveSecurity のブログ [33]

ダウンローダー

ESET、Zloader のグローバルな解体作戦に参加

ESET のリサーチ部門は、マイクロソフトのデジタル犯罪対策部門（Digital Crimes Unit、DCU）、Lumen の Black Lotus Labs、Palo Alto Networks の Unit 42 などのパートナーと協力し、Zloader ボットネットの解体作戦を実施しました。ESET はこのプロジェクトの一員として、技術分析、統計情報、既知のコマンド＆コントロールサーバーのドメイン名と IP アドレスを提供しました。

Zloader は、猛威を振るった銀行を標的とするトロイの木馬「Zeus」から大きな影響を受けている数多くのバンキングトロイの 1 つであり、ランサムウェアなどの他のマルウェアを配信するソースとして進化しています。

今回の共同解体作戦は、3 つのボットネットを対象に実施されました。これらのボットネットは、それぞれ異なるバージョンの Zloader を使用していました。ESET は、これらのボットネットのオペレーターが最近使用していた 65 のドメインを特定し、この作戦に貢献しました。

他の汎用マルウェアと同様に、Zloader は地下フォーラムで広告および販売されています。Zloader を購入すると、アフィリエイト（マルウェアを購入したサイバー犯罪者）には、管理パネルを使用してサーバーを立ち上げ、ボットの構築を開始するために必要なあらゆる機能が提供されます。アフィリエイトは自らボットを拡散させて、ボットネットを維持します。

このマルウェアは現在も比較的容易に入手することが可能であるため、既存のボットネットに対する今回の解体作戦の後も、ESET は新たな活動について監視していきます。

WeLiveSecurity のブログ [34]

Wslink のマルチレイヤー仮想マシンの内部

ESET の研究者は、サーバーとして動作し、仮想マシンベースの難読化ツールが特徴である、これまで検出および文書化されていなかったローダー Wslink について調査し、その詳細を公開しました。Wslink の実行主体をこれまでに把握しているサイバー攻撃者と関連付けることができるコード、機能、操作の類似点は見つかっていません。

Wslink の検体は仮想化されており、既知の仮想化環境の難読化ツールと容易に関連付けることができる明確な痕跡（アーティファクト）はありませんが、プログラムのコードの解析を支援する半自動化されたソリューションを ESET は開発しました。

この仮想マシンは、さまざまな難読化手法を取り入れていましたが、ESET はこれらの難読化の手法を打ち破って、悪意のあるコードの一部を公開できました。Wslink について解説した ESET のホワイトペーパーには、通常の仮想マシンの内部構造の概要と、Wslink で使用されている難読化手法を見破るために必要なさまざまなステップの詳細情報が記載されています。また、ホワイトペーパーの最後のセクションでは、この問題を分析できるように ESET が開発したコードの一部についても紹介しています。

WeLiveSecurity のブログ [35]

ホワイトペーパー [36]

UEFI の脅威

崩れた安全神話：Lenovo のホーム用ノートパソコンに、深刻な UEFI の脆弱性を発見

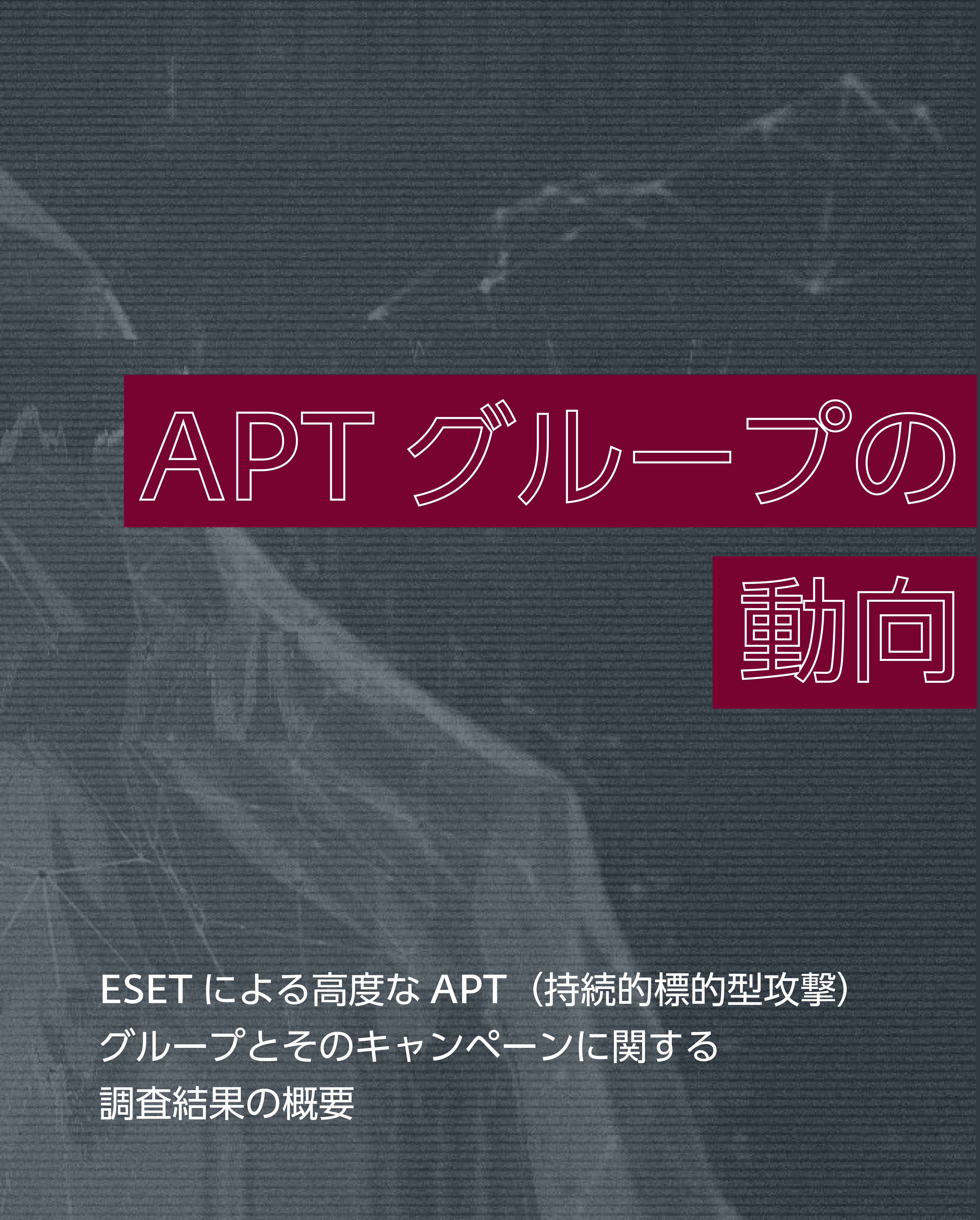
ESET の研究者は、Lenovo のコンシューマー向けノートパソコンの各モデルに影響を与える 3 つの脆弱性を発見し、分析しました。これらの脆弱性の最初の 2 つである *CVE-2021-3971* [37] と *CVE-2021-3972* [38] は、本来 Lenovo のコンシューマー向けノートパソコンの製造工程でのみ使用されている UEFI ファームウェアドライバに影響します。残念ながら、これらのドライバは正しく無効化されない状態で製品のファームウェアイメージに誤って含まれていました。これらの脆弱性が攻撃されると、UEFI のルートキットである LoJax や ESET が最近検出した UEFI マルウェア *ESPecter* [39] などの SPI フラッシュや ESP が埋め込まれて、影響を受けるデバイスに展開され実行される可能性があります。

また、上記の脆弱性が存在するドライバを調査していたところ、SW SMI ハンドラ関数内部で SMM メモリが破壊される第 3 の脆弱性（*CVE-2021-3970* [40]）が見つかりました。この脆弱性により、任意のデータを SMRAM から読み取ったり、SMRAM に書き込んだりすることが可能となり、SMM の権限で悪意のあるコードが実行され、SPI フラッシュにマルウェアが展開される可能性があります。

ESET は、これらの脆弱性を 2021 年 10 月 11 日に Lenovo に報告しました。百種類以上のコンシューマー向けノートパソコンのモデルがこれらの脆弱性の影響を受けます。影響を受けるデバイスの詳細なリストは、*Lenovo のアドバイザリ* [41] に掲載されています。

UEFI への攻撃は、ブートプロセスの早期の段階で実行されるため、セキュリティ機能のほぼすべての対策を回避でき、極めてステルス性が高く危険です。昨年、ESET が発見したこの脆弱性など広範に影響する UEFI ファームウェアの脆弱性が数多く特定されました。これは、UEFI の脅威を展開することが実際にはそれほど難しくないことを示しています。

WeLiveSecurity のブログ [42]



APT グループの動向

ESET による高度な APT（持続的標的型攻撃）
グループとそのキャンペーンに関する
調査結果の概要

Donot Team

標的を限定し執拗に攻撃

ESET のリサーチ部門は、Donot Team グループ（別名、APT-C-35 および SectorE02）が最近実施したキャンペーンを分析しました。2020 年 9 月から 2021 年 10 月にかけて Donot Team の活動を監視したところ、主に南アジアの少数の標的を中心にサイバースパイ活動を実施していました。アムネスティ・インターナショナルが公開した最近の報告書では、このグループが使用しているマルウェアとインドのサイバーセキュリティ企業との関連性が指摘されています。これらのサイバー攻撃者は非常に執拗であり、2～4 カ月ごとに同じ企業を標的としてスピアフィッシングメールを継続して送信しています。

ESET は、Donot Team の特徴である yty マルウェアフレームワークから派生している Windows 用のマルウェアを利用したいくつかのキャンペーンを追跡しました。このキャンペーンの主な目的は、データを収集して外部に送信することです。このフレームワークは、最終的に最小限の機能を実装したバックドアをダウンロードする一連のダウンローダーから構成されており、この APT グループが所有しているツールセットの別のコンポーネントをダウンロードし実行するために使用されます。ESET の研究者は、このマルウェアフレームワークの 2 つのバージョンである Gedit と DarkMusical を分析しました。

DarkMusical は、一連のダウンローダーの最初のコンポーネントを展開し、スケジュールタスクによって常駐化するマクロが埋め込まれた PowerPoint 文書を添付したスピアフィッシングメールから配信されています。Gedit はスピアフィッシングメールによって拡散していますが、今回は悪意のある RTF 文書が添付されています。この RTF 文書は、*CVE-2017-11882* [43] を攻撃し、この文書から 2 つの DLL ファイルをドロップし、そのうちの 1 つを実行します。他のコンポーネントは、さまざまな段階でセキュリティが侵害されたコンピュータにダウンロードされます。

WeLiveSecurity のブログ [44]

攻撃者が特定されていないキャンペーン

新しい macOS マルウェア DazzleSpy をアジアで展開する水飲み場型攻撃

ESET の研究者は、香港で民主主義を支持し擁護するしているラジオ局「D100」の Web サイトが改ざんされていることを発見しました。このサイトにアクセスしたユーザーの Mac には、サイバースパイマルウェアをインストールするための Safari エクスプロイトがダウンロードされます。この Web サイトは新しい macOS マルウェアを配信しており、ESET はこのマルウェアを DazzleSpy と命名しました。

この攻撃者はブラウザでコードを実行するために、1,000 行以上のコードが書かれたエクスプロイトを使用していました。コードの一部の記述から、iPhone Xs 以降のデバイスを含め、iOS でこの脆弱性が攻撃された可能性があります。

DazzleSpy はサイバースパイに使用されています。おそらく香港の政治的活動や民主化運動を推進している個人が標的になっていたと考えられます。このマルウェアは、侵入したコンピュータに関する情報の収集、特定のファイルの検索、「デスクトップ」、「ダウンロード」、「ドキュメント」フォルダにあるファイルのスキャン、指定されたシェルコマンドの実行、リモート画面のセッションの開始または終了、ディスクへのファイルの任意のファイルの書き込みを実行できます。

このキャンペーンで使用されていたエクスプロイトは複雑で高度であることから、この作戦の背後にいる組織は高度な技術力を有していると考えられます。このキャンペーンは、*2020 年に実施されたキャンペーン* [45] といくつかの類似点があります。2020 年のキャンペーンでは、香港の市民向けの Web サイトで iframe インジェクションが使用され、WebKit エクスプロイトが展開されています。このときにも、同じ方法で LightSpy iOS マルウェアが配信されています。この 2 つのキャンペーンが同じグループによって実行されたものかどうかは、現時点では確認できていません。

WeLiveSecurity のブログ [46]

Mustang Panda

Mustang Panda が使用する Hodur マルウェア：古い手法を使用する新しい Korplug の亜種

ESET の研究者は、Mustang Panda APT グループによる進行中のサイバースパイキャンペーンを発見しました。このキャンペーンでは、過去に検出・文書化されていない Korplug の亜種が使用されています。*Unit 42* [47] が過去に報告した THOR の亜種と似ていることから、ESET はこのマルウェアを Hodur と命名しました。Hodur（ヘズ）は北欧神話の登場人物であり、ロキに欺かれて異母兄のバルドルを殺した人物です。ESET は、このキャンペーンが Mustang Panda によって実行されたと確信しています。Mustang Panda は、主に東アジアや東南アジアの政府機関や NGO を標的としているサイバースパイグループです。

今回のキャンペーンでは、ロシアによるウクライナへの侵攻など、欧州で起きている最新のニュースをフィッシングのテーマにしています。フィッシングで利用されているその他のテーマとして、新型コロナウイルスによる渡航制限に関する更新情報、ギリシャ支援計画の承認、欧州議会と理事会の規則などが使用されており、この APT グループが時事問題に迅速に取り入れていることを示しています。

Mustang Panda は、精巧で独自のローダーや Korplug の亜種を開発していることが知られており、今回のキャンペーンで使用された検体にも、その高い技術力が反映されています。このキャンペーンの特徴は、展開プロセスのあらゆる段階で、コントロールフローが難読化され、分析を妨害する技術が多用されていることです。

WeLiveSecurity のブログ [18]

Winnti Group

PipeMon の新たな亜種が見つかる

ESET の研究者は、Oreans 社の Code Virtualizer を使用して仮想化され、システムの専用のプリントプロセッサディレクトリの外部にあるプリントプロセッサとして常駐化する、Winnti Group が使用している新しい PipeMon の亜種を発見しました。ESET が、PipeMon バックドアについて最初に検出して文書化したのは *2020 年* [48] でした。このバックドアは、韓国と台湾に拠点を置く複数のビデオゲーム会社に対して使用されていました。

マイクロソフトのドキュメントでは、プリントプロセッサの DLL はシステムのプリントプロセッサのディレクトリに配置されなければならないと明記されていますが、これらの DLL はシステムドライブの任意の場所に配置でき、単にファイル名だけでなく、DLL を指すレジストリの相対パスを使用することが可能です。こうすることで、攻撃者は悪意のある DLL をプリントプロセッサとして常駐させ、プリントプロセッサ専用のディレクトリに配置することなく、監視の目をかいくぐることができます。

Twitter thread [49]

TA410

TA410 の傘下のサイバースパイ活動の TTP とその活動内容

ESET のリサーチ部門は、APT10 とのつながりが指摘されておりサイバースパイを統括している TA410 の詳細な情報を公開しました。この組織は、主に米国に拠点を置く公益事業部門の組織や、中東やアフリカの外交機関を標的としていたことも確認されています。

TA410 は、ESET が発見したスパイ活動のためのバックドアである FlowCloud の新バージョンなど、異なるツールセットを使用している 3 つのチームから構成されていると考えられます。これらのチームは、それぞれ FlowingFrog、LookingFrog、JollyFrog と呼ばれており、TTP、標的、ネットワークインフラが共通しています。これらのサブグループはある程度独立して活動していますが、収集するインテリジェンスの要件、スピアフィッシングキャンペーンを実行する初期アクセス担当のチーム、ネットワークインフラを展開するチームなどを共有している可能性があります。

TA410 の標的の多くは外交や教育分野における大規模な組織ですが、ESET は、軍事産業分野、日本の製造企業、インドの鉱業会社、イスラエルの慈善団体でも被害を受けていることを確認しています。

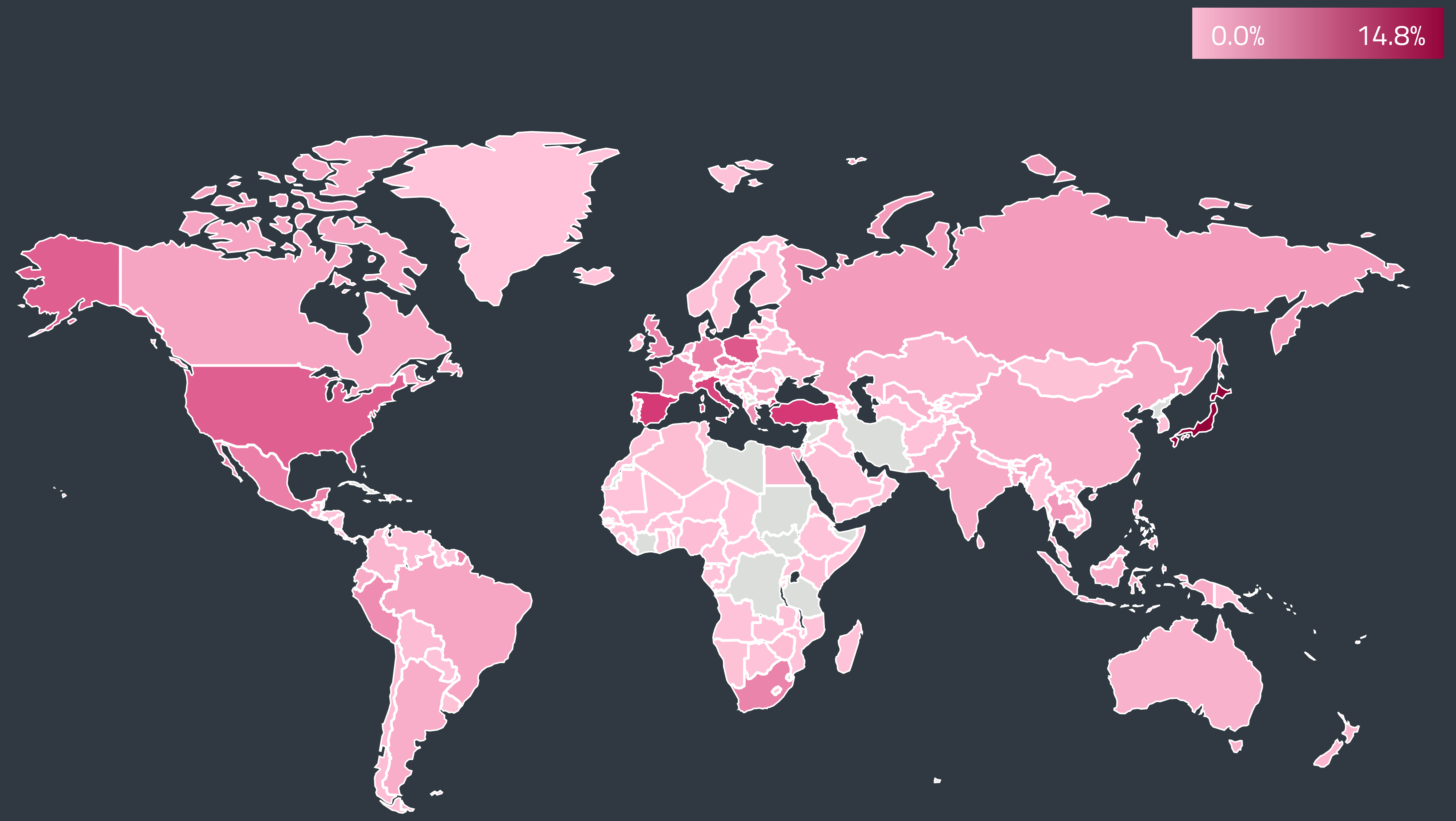
FlowingFrog チームが使用している FlowCloud の新バージョンは、複雑でモジュール化された C++ RAT であり、注意が必要ないくつもの機能を備えています。クリップボードイベントを監視してクリップボードのコンテンツを窃取する、ファイルシステムイベントを監視して新規ファイルや変更ファイルを収集する、接続されたカメラデバイスを制御して侵害したコンピュータの周囲を録画する、さらには接続されたマイクロフォンを制御して一定音量以上のサウンドレベルを検出すると録音を開始するなど、さまざまな機能を実装しています。最後の録音機能は、通常の会話の最大音量とされる 65 デシベル以上で作動する仕組みになっています。

WeLiveSecurity のブログ [50]

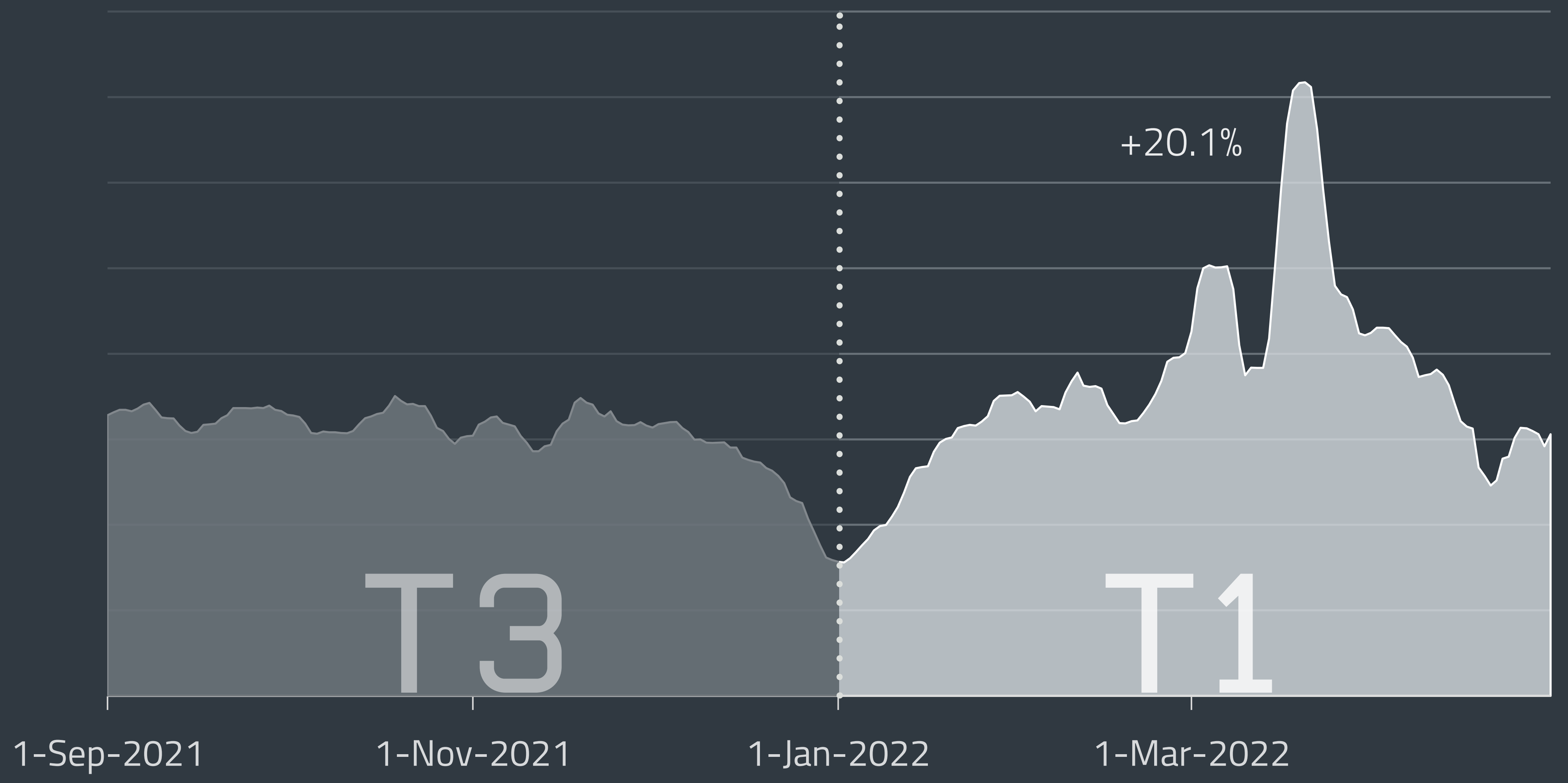
レポート全文は*こちらより英語版原文*を参照いただけます。

STATISTICS & TRENDS

The threat landscape in T1 2022
as seen by ESET telemetry



Global distribution of malware detections in T1 2022



Overall threat detection trend in T3 2021 – T1 2022, seven-day moving average

THREAT LANDSCAPE OVERVIEW

A summary of the threat landscape developments in T1 2022.

After being generally stable for some time now, the number of threat detections rose by 20.1% in T1 2022. There were two notable spikes, on March 2 and 15, caused by the DOC/TrojanDownloader.Agent trojan. Both the higher overall threat detection numbers and the spikes were caused by the dramatic return of Emotet.

It comes as no surprise, then, that the *Downloaders* category was dominated by the recent Emotet campaign. Even if the comparison is made based on the malware's relatively low numbers in T3, its astronomical, over a hundredfold, increase still boggles the mind. Talk about coming back with a vengeance!

Emotet's campaign also influenced the *Email threats* category, which grew by 37% as a result. Additionally, the campaign led to an 829% jump in the incidence of DOC/TrojanDownloader.Agent, which climbed to the second place in the Email threats top 10 list.

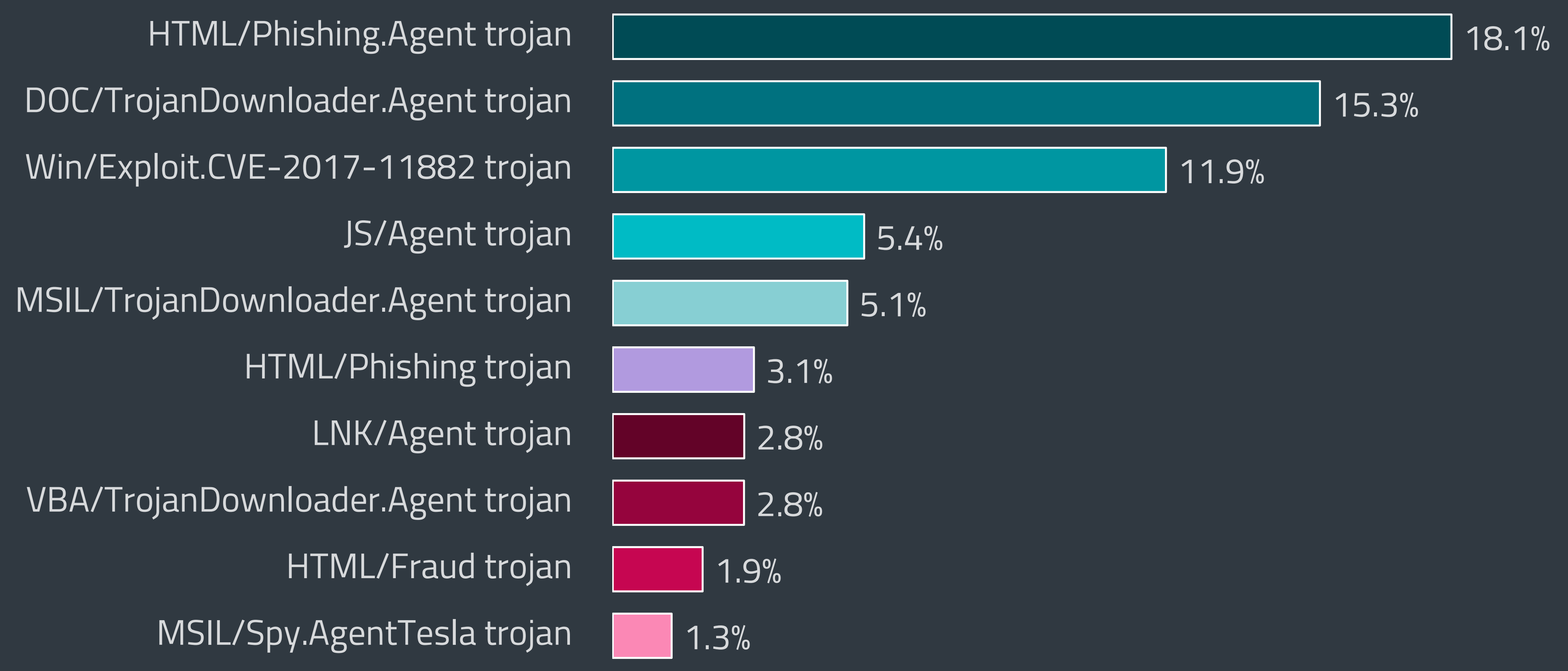
Over in the *Exploits* section, the number of RDP attacks, the usual source of the big scary numbers for the Threat Report, dropped by 43% after experiencing non-stop growth since the beginning of 2020.

As usual, the *Ransomware* threat landscape was far from boring, with Sodinokibi core members being arrested, the Conti gang suffering major internal information leaks, and Russia becoming the number one ransomware target in T1, according to our telemetry.

macOS threats saw declines in all of their subcategories, with the overall decrease being 14.9%. Almost half of the monitored threats were categorized as potentially unwanted applications (PUAs). A slight rise in detections marked the *Android* category, which went up by 8%. However, two of its subcategories, Android SMS trojans and Android Spyware, grew dramatically, the former by 145% and the latter by 170%.

When it came to *Cryptocurrency threats*, T1 2022 was marked by several high-profile cryptocurrency platform hacks, which made cybercriminals a lot of money, even while the overall number of detections in this category decreased by 29.3%.

The *IoT* category data shows that years after the online publication of the Mirai source code, botnets using the code are still very common, attacking hundreds of thousands of devices. While the rate at which the notorious Mozi botnet is spreading slowed down by 11%, ZHTrap managed to increase the number of its attacks by 9%.



Top 10 malware detections in T1 2022 (% of malware detections)

Regarding *Web threats*, our telemetry registered a 29% increase in phishing URLs caused by a spike in new URLs in March. As cybercrooks are always ready to make a profit out of human misery, there was also a surge in phishing and scam websites exploiting interest in and concerns about the Russia-Ukraine war.

Finally, after a pause in T3 2021, *Infostealers* were growing again. They increased by 12%, with the highest subcategory growth (74.5%) being demonstrated by Banking malware. Most of this growth was due to JS/Spy.Banker, which went up by 177.7% and made for 77.6% of Banking malware.

The Emotet surge also affected the overall top ten malware detections: while it did not succeed in dethroning the HTML/Phishing.Agent trojan, which constituted 18.1% of all detections, DOC/TrojanDownloader.Agent jumped from being the ninth most detected malware family to the second with 15.2%. Compared to T3 2021, its numbers rose by 758.4%.

MSIL/TrojanDownloader.Agent, which drops malware such as Agent Tesla and Fareit, also grew significantly in T1, and this 117.9% growth landed it in fifth place instead of T3's eighth. The rest of the top ten malware detections mostly shuffled down a position or two, but the list itself did not lose any of the previous top 10 families, nor were there any newcomers.

TOP 10 MALWARE DETECTIONS

→ HTML/Phishing.Agent trojan

HTML/Phishing.Agent is a detection name for malicious HTML code often used in a phishing email's attachment. Attackers tend to use it instead of other file types, since executable attachments are usually automatically blocked or more likely to raise suspicion. When such an attachment is opened, a phishing site is opened in the web browser, posing as e.g., an official banking, payment service or social networking website. The website requests credentials or other sensitive information, which are then sent to the attacker.

↗ DOC/TrojanDownloader.Agent trojan

This classification represents malicious Microsoft Word documents that download further malware from the internet. The documents are often disguised as invoices, forms, legal documents, or other seemingly important information. They may rely on malicious macros, embedded Packager (and other) objects, or even serve as decoy documents to distract the recipient while malware is downloaded in the background.

↘ Win/Exploit.CVE-2017-11882 trojan

This detection name stands for specially crafted documents exploiting the *CVE-2017-11882* [51] vulnerability found in Microsoft Equation Editor, a component of Microsoft Office. The exploit is publicly available and usually used as the first stage of compromise. When the user opens the malicious document, the exploit is triggered and its shellcode executed. Additional malware is then downloaded onto the computer to perform arbitrary malicious actions.

↘ JS/Agent trojan

This detection name covers various malicious JavaScript files. These are often obfuscated to avoid static detections. They are typically placed onto compromised but otherwise legitimate websites, with the aim of achieving drive-by compromise of visitors.

↗ MSIL/TrojanDownloader.Agent trojan

MSIL/TrojanDownloader.Agent is a detection name for malicious software written for the Windows platform, and that uses the .NET Framework; this malware tries to download other malware using various methods. It usually contains either a URL or a list of URLs leading to the final payload. This malware often acts as the first layer of a much more complex package, taking care of the installation part on the victimized system.

↘ HTML/Phishing trojan

HTML/Phishing trojan represents generic malware detections that are collected based on scanning malicious URLs in emails and email attachments. If an email or its attachment contains a blacklisted URL, it triggers an HTML/Phishing.Gen detection.

↘ LNK/Agent trojan

LNK/Agent is a detection name for malware utilizing Windows LNK shortcut files to execute other files on the system. Shortcut files have been popular among attackers, as they are typically considered benign and less likely to raise suspicion. LNK/Agent files don't contain any payload and are usually parts of other, more complex malware. They are often used to achieve persistence of the main malicious files on the system or as a part of the compromise vector.

↘ VBA/TrojanDownloader.Agent trojan

VBA/TrojanDownloader.Agent is a detection typically covering maliciously crafted Microsoft Office files that try to manipulate users into enabling the execution of macros. Upon execution, the enclosed malicious macro typically downloads and executes additional malware. The malicious documents are usually sent as email attachments, disguised as important information relevant to the recipient.

↘ HTML/Fraud trojan

HTML/Fraud detections cover various types of fraudulent, HTML-based content, distributed with the aim of gaining money or other profit from the victim's involvement. This includes scam websites, as well as HMTL-based emails and email attachments. In such an email, recipients may be tricked into believing they have won a lottery prize and are then requested to provide personal details. Another common case is the so-called *advance fee scam* [52], such as the notorious Nigerian Prince scam also known as "419 scam".

→ MSIL/Spy.AgentTesla trojan

MSIL/Spy.AgentTesla is a .NET-based spyware-as-a-service trojan available on underground forums. It gets data and commands from remote hosts and serves to acquire sensitive information, log keystrokes, and gain control over the camera or the microphone of the victim.

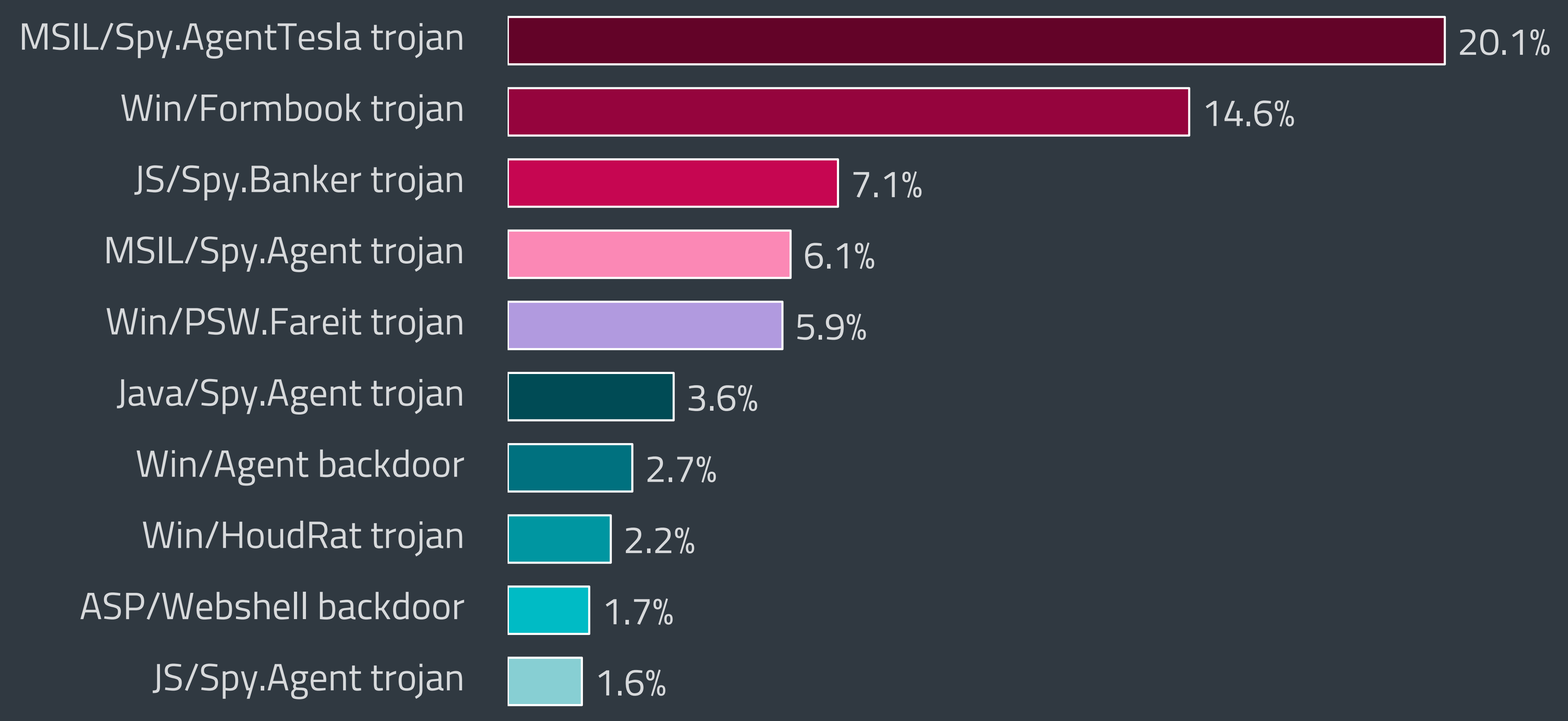
INFOSTEALERS

TrickBot bows out while JS/Spy.Banker dominates the banking malware threat landscape.

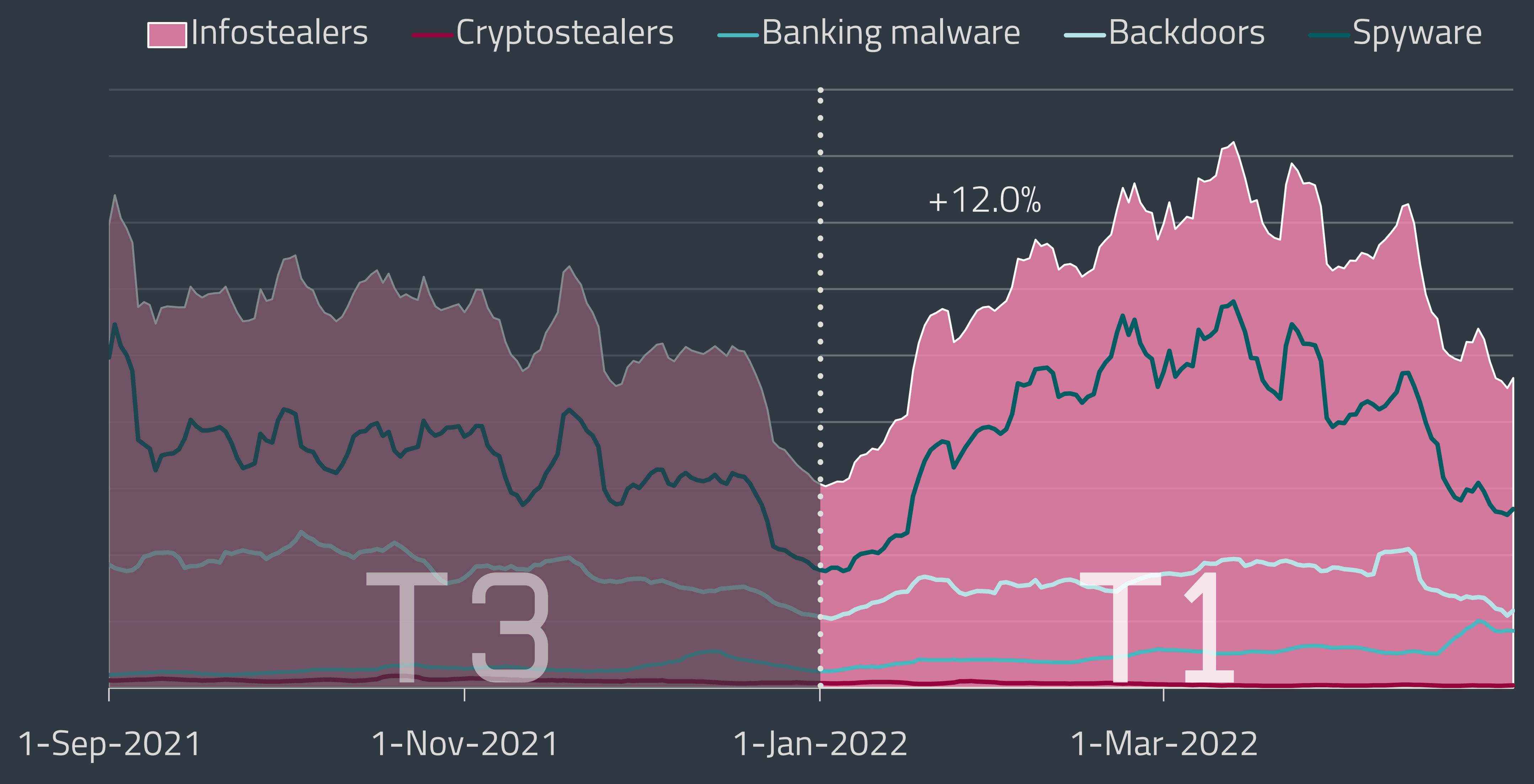
After a brief pause in T3 2021, the category of Infostealers resumed its growth in T1 2022, going up by almost 12%. As usual, the driving force behind most of the detections was spyware, which also accounted for the most significant spike on March 22, 2022, courtesy of MSIL/Spy.AgentTesla. Spyware and Banking malware increased in number of detections, Backdoors decreased, and Cryptostealers declined steeply in trend and numbers both.

In T1 2022, Spyware grew by 18.2% and made for 64.4% of all Infostealer detections, further cementing its status as the largest Infostealer subcategory. It was aided by the relative affordability of spyware-as-a-service malware on underground forums. A typical example of this business model, the MSIL/Spy.AgentTesla trojan, or simply Agent Tesla, was again the most prominent spyware according to ESET telemetry data, growing by 243.6% between T3 2021 and T1 2022. In T1, it was being spread by *malicious PowerPoint documents* [53] in phishing campaigns. Additionally, ESET registered its distribution in another phishing campaign alongside the Win/Agent backdoor near the end of April.

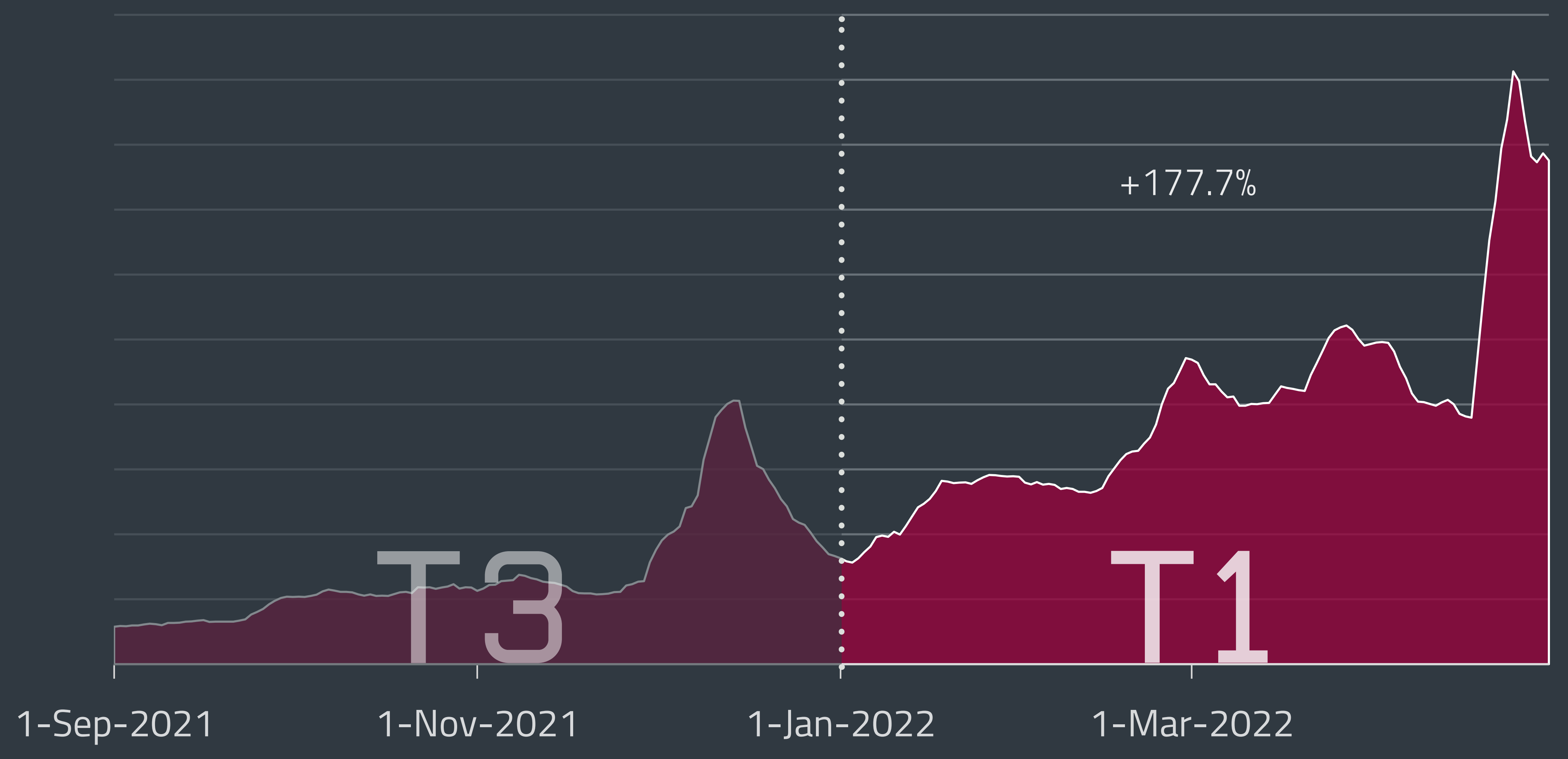
Top 10 Infostealer detections were also led by spyware, which took up the first two spots in the list. Agent Tesla had the highest numbers, with 19.3% of all Infostealer detections and 29% of Spyware



Top 10 infostealer families in T1 2022 (% of Infostealer detections)



Infostealer detection trend in T3 2021 – T1 2022, seven-day moving average

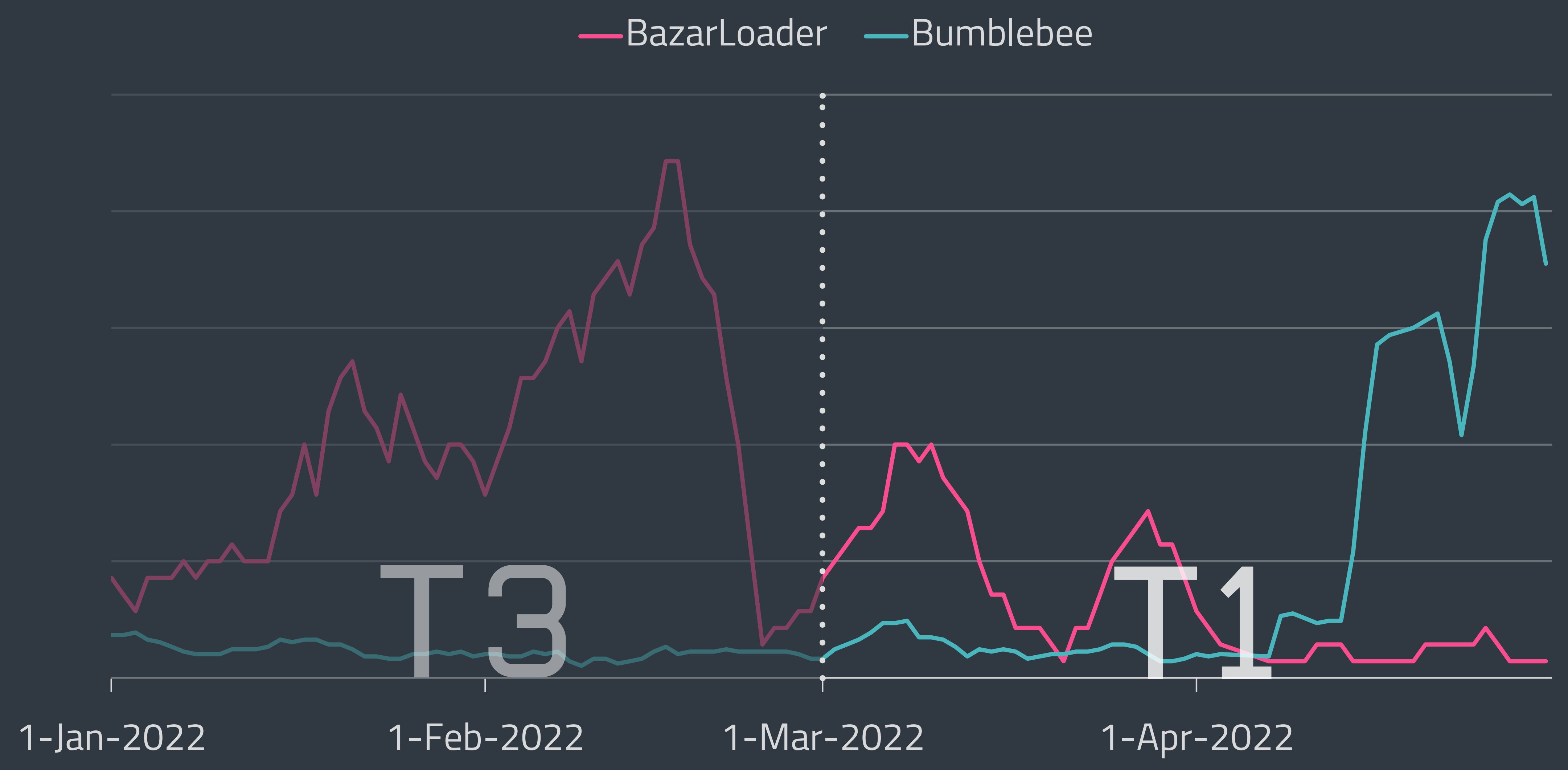


JS/Spy.Banker detection trend in T3 2021 – T1 2022, seven-day moving average detections. It was followed by Win/Formbook trojan, which accounted for 14% of Infostealers and 21.1% of Spyware. The MSIL/Spy.Agent trojan placed fourth in the overall ranking with 5.8% and was the third most detected spyware with 8.8%.

While the top ranks in the list have traditionally been taken by spyware and backdoors, this time around a banking malware family rose to third spot. The JS/Spy.Banker trojan represented 6.8% of Infostealers. This malware family, also known as Magecart, injects JavaScript skimmer code into websites in order to harvest credit card information. Between T3 2021 and T1 2022, it grew by 177.7% and became more or less synonymous with the Banking malware subcategory, accounting for 77.6% of Banking malware detections. The next most detected malware in the subcategory, the MSIL/ClipBanker trojan, was left with mere peanuts compared to JS/Spy.Banker, having decreased by 59.4% and constituting only 4.5% of Banking malware.

This subcategory grew by 75% in T1 2022 and accounted for 8.5% of all Infostealer detections. It experienced a major spike on April 19, which was caused by the aforementioned JS/Spy.Banker, with Thailand as the most affected country.

TrickBot, banking malware turned multipurpose attack tool targeting enterprises, and one of the mainstays of the threat landscape, *ended its operations* [54] in February. It was speculated that the gang behind TrickBot, which has close ties to the Conti ransomware group, decided to switch its focus to BazarLoader instead. While TrickBot was very successful and even managed to come back from the disruption efforts in 2020, there were no significant updates to its core afterward.



BazarLoader and Bumblebee detection trends in T3 2021 – T1 2022, seven-day moving average

BazarLoader, another tool in the TrickBot creators' arsenal, uses more advanced techniques, and is harder to track and analyze. Interestingly, it is possible that even BazarLoader has been replaced, as *reports* [55] started emerging that a new loader named Bumblebee has been spreading since March. Bumblebee is being used by the same threat actors that would previously use BazarLoader. It remains to be seen which one of these loaders will win out in the end, or if they both stay in circulation.

EXPERT COMMENT

Since the beginning of the year 2021, BazarLoader has been in continuous development, the pace of which has ramped up considerably in the first three months of 2022, when we saw progress in its anti-analysis techniques. The malware now sports an improved API call obfuscation technique, which combines three hashes instead of one, and added code flow obfuscation.

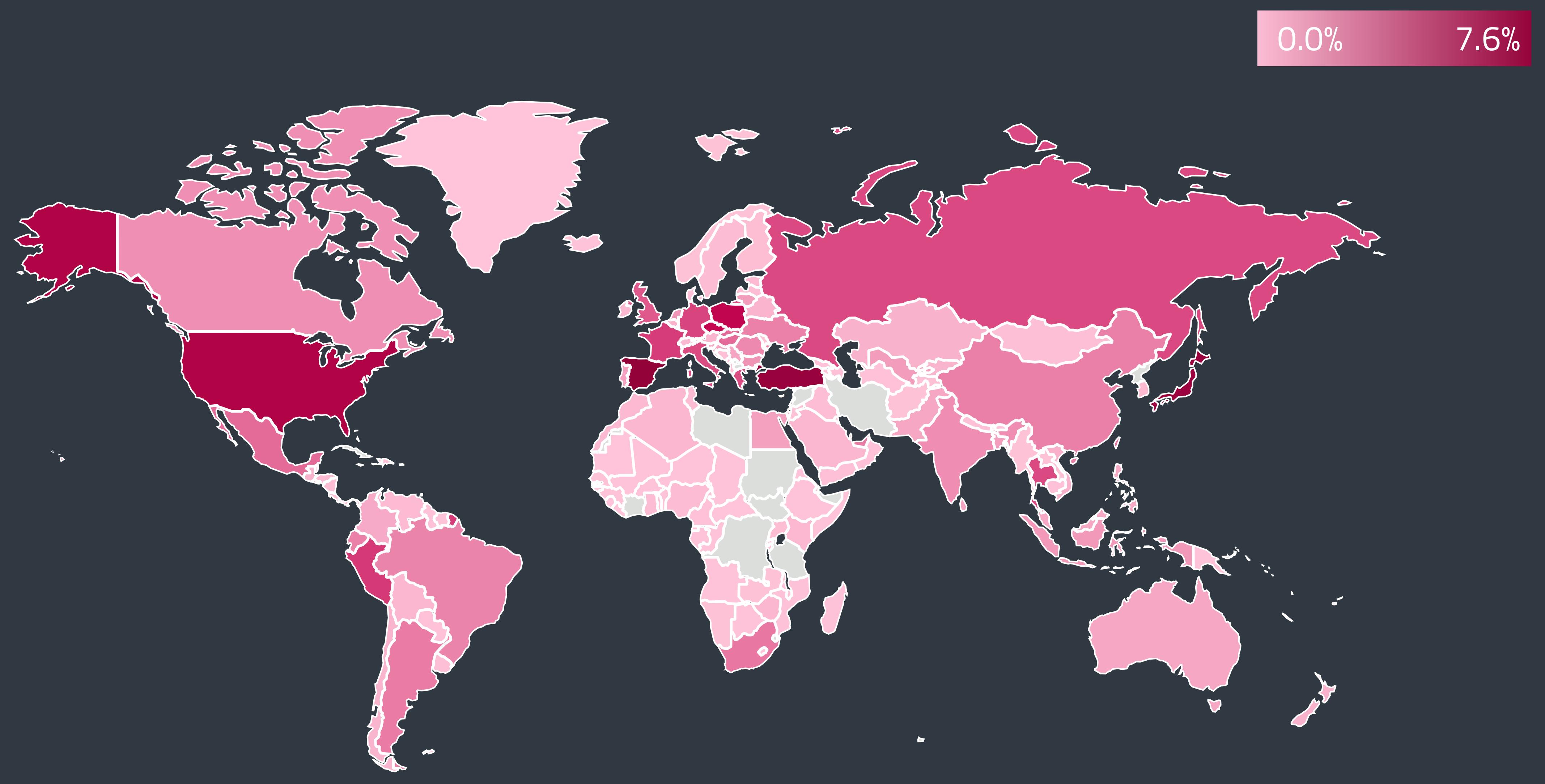
I find our latest research pointing towards Bumblebee replacing BazarLoader quite surprising. From an analyst's point of view, BazarLoader is actively being worked on and has become sophisticated malware that is hard to track and analyze. These factors do not indicate that it is a tool that should be discarded, so I believe that we will meet BazarLoader again.

Compared to that, Bumblebee in its current state is not obfuscated whatsoever at its core and partially uses open-source code. It is likely that Bumblebee will undergo more development in the near future.

Jakub Tomanek, ESET Malware Analyst

Most Latin American banking trojans did not stray far from their ordinary patterns, stealing bank credentials and targeting mostly Mexico and Brazil with the occasional foray into Spain. However, it looks like one of the members of this malware cluster is trying to expand its horizons considerably: *Grandoreiro* [56] added *over 900 new targets* [57] to its portfolio, among them cryptocurrency exchanges and NFT games. This LATAM banking trojan can currently be considered the most active of the group.

It seems that while Grandoreiro started encroaching onto cryptostealers' turf, cryptostealers themselves were not very active. Their detection numbers dropped by 51.6% in T1 2022, continuing their downward trend that ought to make all cryptocurrency owners quite happy. This subcategory experienced one notable spike on January 25 caused by the Win/PSW.Delf trojan, whose attack attempts were registered mostly in Japan and Hong Kong at the time.



Global distribution of Infostealer detections in T1 2022

The usually strong subcategory of Backdoors declined in detections, now for the second period in a row. Despite their 11.1% decrease, they still constituted the second-largest portion of Infostealer detections – 25.5% of which were categorized as backdoors.

They were also represented in the top 10 Infostealer detections list, coming in sixth, eighth, and tenth overall. The first among them was the PHP/Webshell backdoor (15.6% of Backdoors, 4.1% of Infostealers), followed by the Win/Agent backdoor (9.7% of Backdoors, 2.6% of Infostealers), and ASP/Webshell backdoor (6.4% of Backdoors, 1.7% of Infostealers). There was one significant backdoor spike, on April 7, caused by the Win/Agent backdoor and its TJS variant, with over three-fourths of its attack attempts registered in Spain. Win/Agent.TJS is the same variant that ESET products caught spreading through emails along with Agent Tesla at the end of April.

Another variant of this backdoor, more precisely Win/Agent.NE aka the G3ll3rt Grind3lwald RAT, was being distributed in a *new campaign* [58] discovered by ESET researchers at the beginning of the year. While our telemetry did not show that many hits at the time, some criminal gangs such as Zloader were taking an active interest in this malware. After its activity surges in January and February, G3ll3rt Grind3lwald's numbers gradually dropped.

In T1, Infostealers were most prevalent in Spain, which saw 7.6% of all attack attempts, then Turkey with 7.1%, and Japan third, registering 6.9%.

RANSOMWARE

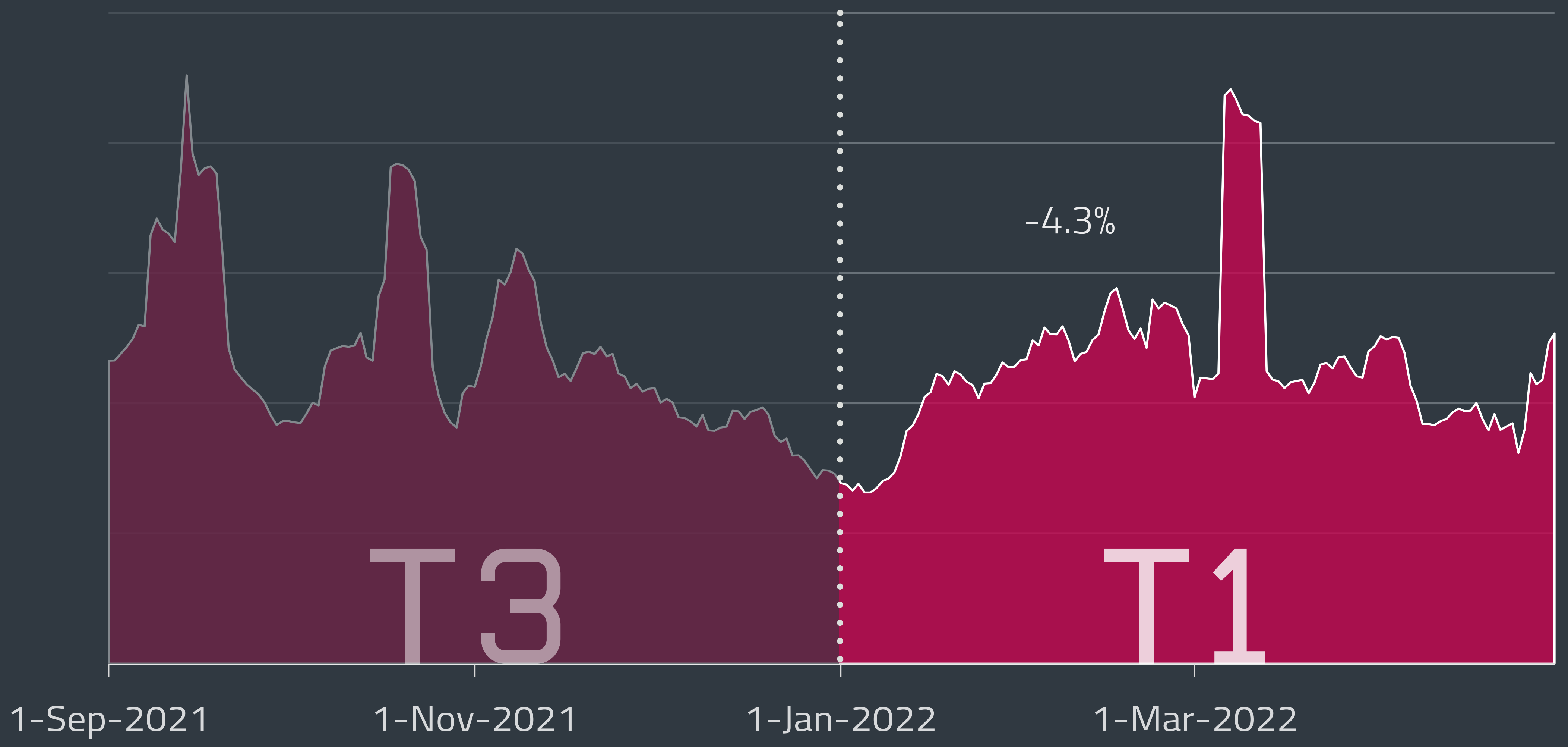
War in Ukraine sparks an increase in ideology-motivated ransomware attacks with ransomware increasingly targeting Russia.

T1 2022 started with big news. In January, the Russian Federal Security Service (FSB) raided 25 addresses and arrested 14 alleged core members of the infamous *Sodinokibi/REvil* [59] ransomware gang. The operation was sparked by the US authorities reporting on the leader of the group. During the raids, agents seized crypto- and fiat currencies worth over $6 million, 20 luxury cars, and hardware used to run the malicious operation.

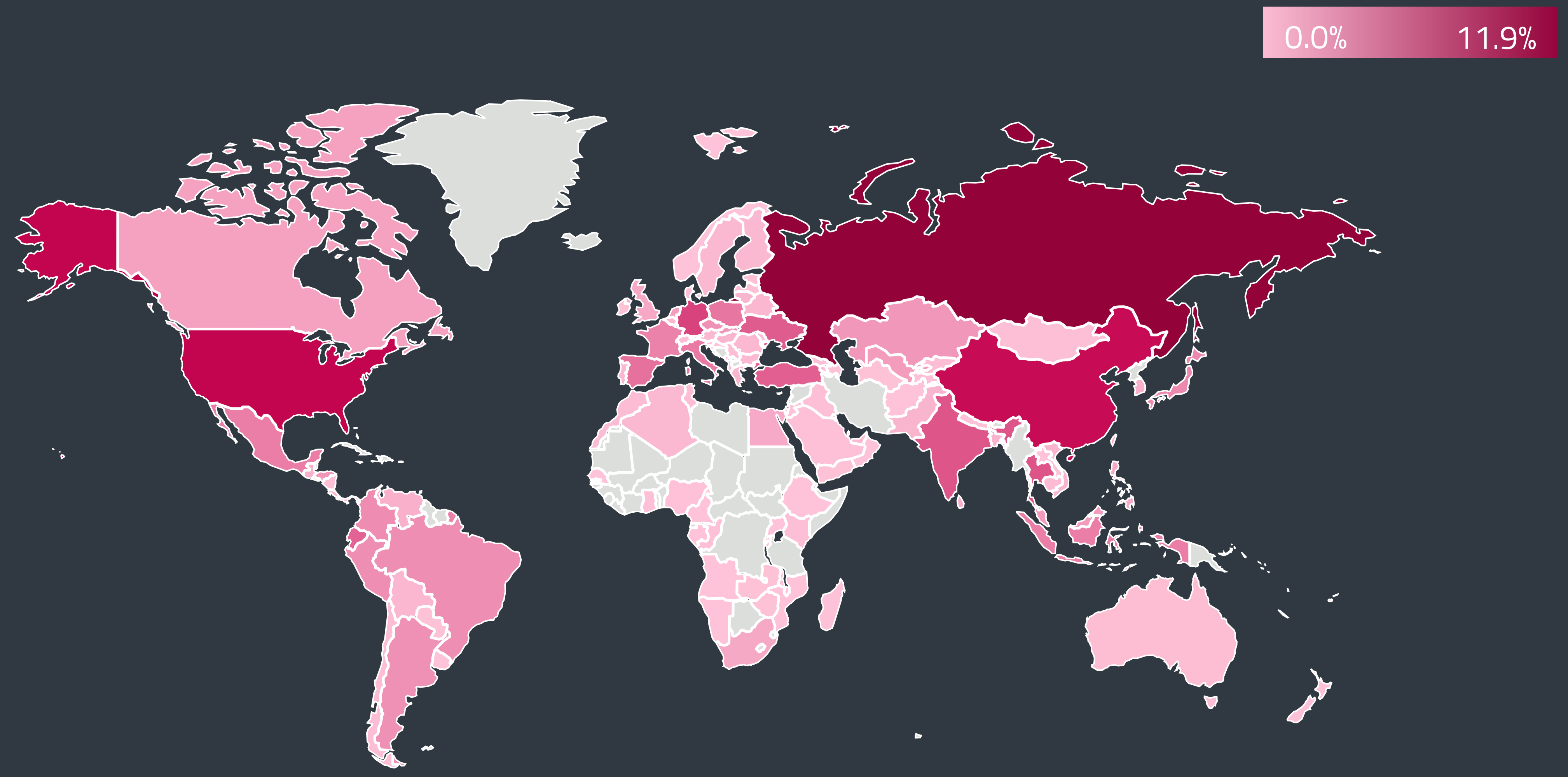
However, the arrests didn't have a lasting effect as *Sodinokibi's TOR leak site* [60] came alive only a few weeks later and started listing new victims. After analyzing the samples from the attacks, researchers confirmed these were *new Sodinokibi instances* [61], compiled from the original source code. This suggests that one of the former core members – with access to the gang's resources – is still free and running the operation.

But law enforcement activity around Sodinokibi was soon to be overshadowed by much grimmer events. The Russian invasion of Ukraine had numerous influences on the Ransomware category. Apart from the *HermeticRansom* [4] attacks on several high-profile Ukrainian organizations, the ransomware detection trend continued its slow downward pace, dropping by 4% compared to T3 2021.

Looking at the upticks in the chart, the first dent was caused by the Conti gang attacking systems in Honduras, accounting for 53% of the daily detections. The second spike, on March 6, was even larger and was caused by MSIL/Filecoder.ACB attacking a network of a single large organization in Russia, attempting to encrypt its data from within the environment.



Ransomware detection trend in T3 2021 – T1 2022, seven-day moving average

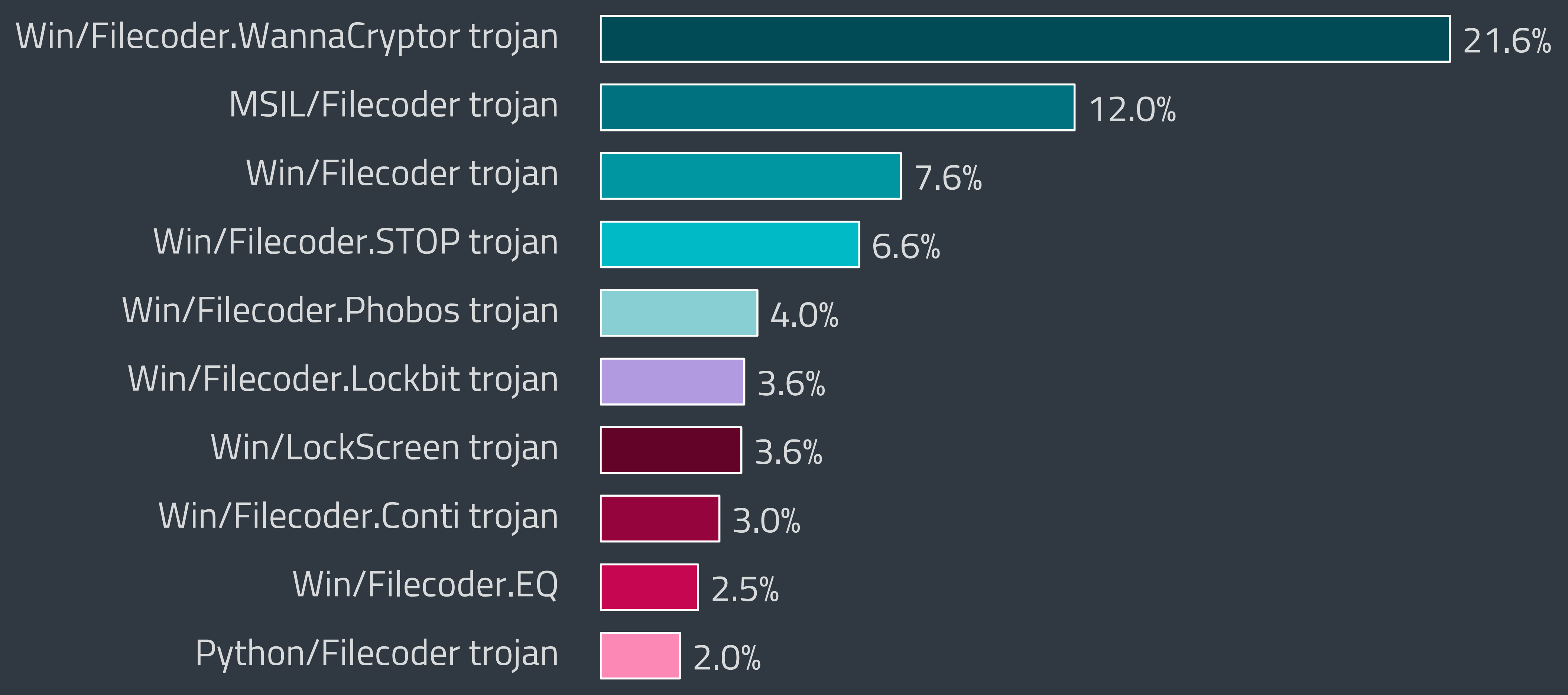


Global distribution of Ransomware detections in T1 2022

This incident points to a potential shift in the ransomware scene. Before the invasion, Russia and some of the Commonwealth of Independent States (CIS) were excluded from many ransomware target lists. This was probably due to criminals residing in those countries or fearing Russia's retribution. T1 2022 hints at a possible change, as Russia faced the highest proportion of detections (12%) in the Ransomware category. Although not unheard of, Russia has never had to eat so much of its own dog food.

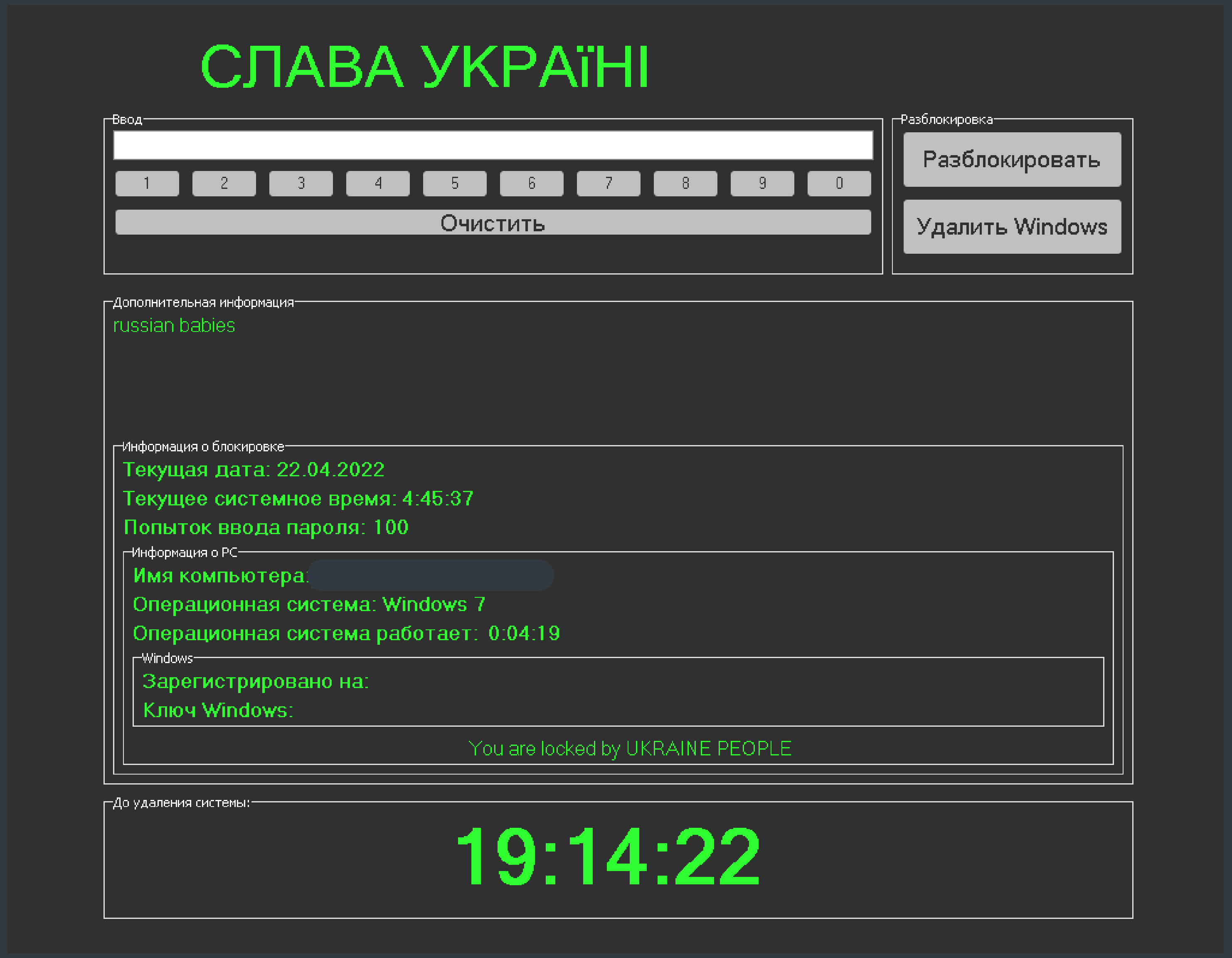
A series of incidents against high-profile Russian targets seems to support this interpretation. One group that started attacking victims such as Russian space agency Roscosmos and the state-owned Russian TV and radio was *NB65* [62]. In a reaction to the massacre in Bucha, Ukraine, NB65 used the leaked source code of Conti ransomware to breach its targets and leak their sensitive info online.

A second actor that misused the topic of the war was *OldGremlin* [63]. This group reportedly used well-crafted spearphishing emails and custom backdoors to breach Russian banks, industrial enterprises, medical organizations, and software developers.



Top 10 ransomware families in T1 2022 (% of Ransomware detections)

An interesting data point that stood out in T1 2022 was the increased number of screen-locking ransomware incidents, which jumped to the seventh most frequent ransomware detection. Close to 40% of these attacks were aimed at Russia and 11% at Ukraine. The Win/LockScreen.AWI variant targeting Russia even displayed the title "Slava Ukraini" (in uppercase Ukrainian Cyrillic) or "Glory to Ukraine" – a national salute used by the Ukrainians.



russian babies

Текущая дата: 22.04.2022
Текущее системное время: 4:45:37
Попыток ввода пароля: 100

Имя компьютера: [redacted]
Операционная система: Windows 7
Операционная система работает: 0:04:19

Зарегистрировано на:
Ключ Windows:

You are locked by UKRAINE PEOPLE

19:14:22

Win/LockScreen.AWI variant targeting Russian victims using the title "Glory to Ukraine"

Another major ransomware story connected to the war in Ukraine is the already mentioned Conti data leak. The material was published by a Ukrainian computer *researcher* [64], who became irritated by the gang's *pledge* [65] to support Russia in its aggressive war efforts. In turn, he started a *Twitter account* [66] leaking the group's data, including source code for several of their malware families and years of *sensitive internal communication* [67] that contained hints at a possible link to the Russian government. Other actors such as *LockBit* [68] tried to avoid similar fallout and published statements in multiple languages saying they will stay impartial.

For a bit of good news, T1 2022 saw a large number of free decryptors released. The list includes some of the most notorious names such as *Maze, Egregor, Sekhmet* [69] and *Diavol* [70], but also less known strains such as *TargetCompany* [71], and *Yanlouwang* [72]. Regarding the war in Ukraine, a free decryptor has been published for victims of *HermeticRansom* [73], described in our *Featured story*. South Korean researchers also detailed vulnerabilities in the *Hive ransomware* [74] encryption algorithm and showed how to exploit them to recover affected data.

The beginning of 2022 was also the period when some of the ransomware actors heard their sentences. An Estonian man will spend the next *66 months in jail* [75] and pay $36 million in restitution due to his ties to 13 attacks, causing cumulative losses of more than $50 million. A Canadian NetWalker affiliate was *sentenced to 80 months* [76] for his involvement in attacks hitting 17 victims.

Despite some of the actors ending up arrested, there still seem to be enough greedy criminals who want to have a part of those large payouts and join the ransomware scene with their gangs. *NightSky* [77] was one of the first and most visible ones that popped up in T1 2022, targeting corporate networks and *exploiting Log4J* [78]. On top of eCh0raix, NAS devices are under attack from new ransomware called *DeadBolt* [79]. Another newcomer, White Rabbit, seems to be a side-project of the FIN8 hacking group.

But not all ransomware gangs are focused on corporations and big payouts. A new RaaS called *Sugar ransomware* [80] seems rather interested in regular users and small businesses, demanding significantly smaller ransoms than the competition. Also new in T1 2022 were *Black Basta* [81] and *Onyx* [82] ransomware, the latter mostly destroying data instead of just encrypting it.

EXPERT COMMENT

Since the Russian invasion of Ukraine, we have observed an increased number of amateurish ransomware and wipers. Their authors often pledge support for one side or the other and make the attacks an act of personal vendetta. What's interesting is that the pro-Ukrainian variants outnumber the pro-Russian ones by a small margin. We expect attacks supporting a particular side to continue in the upcoming months and even escalate as ideology and war propaganda are becoming the central driving forces for their spread.

Igor Kabina, ESET Senior Detection Engineer

DOWNLOADERS

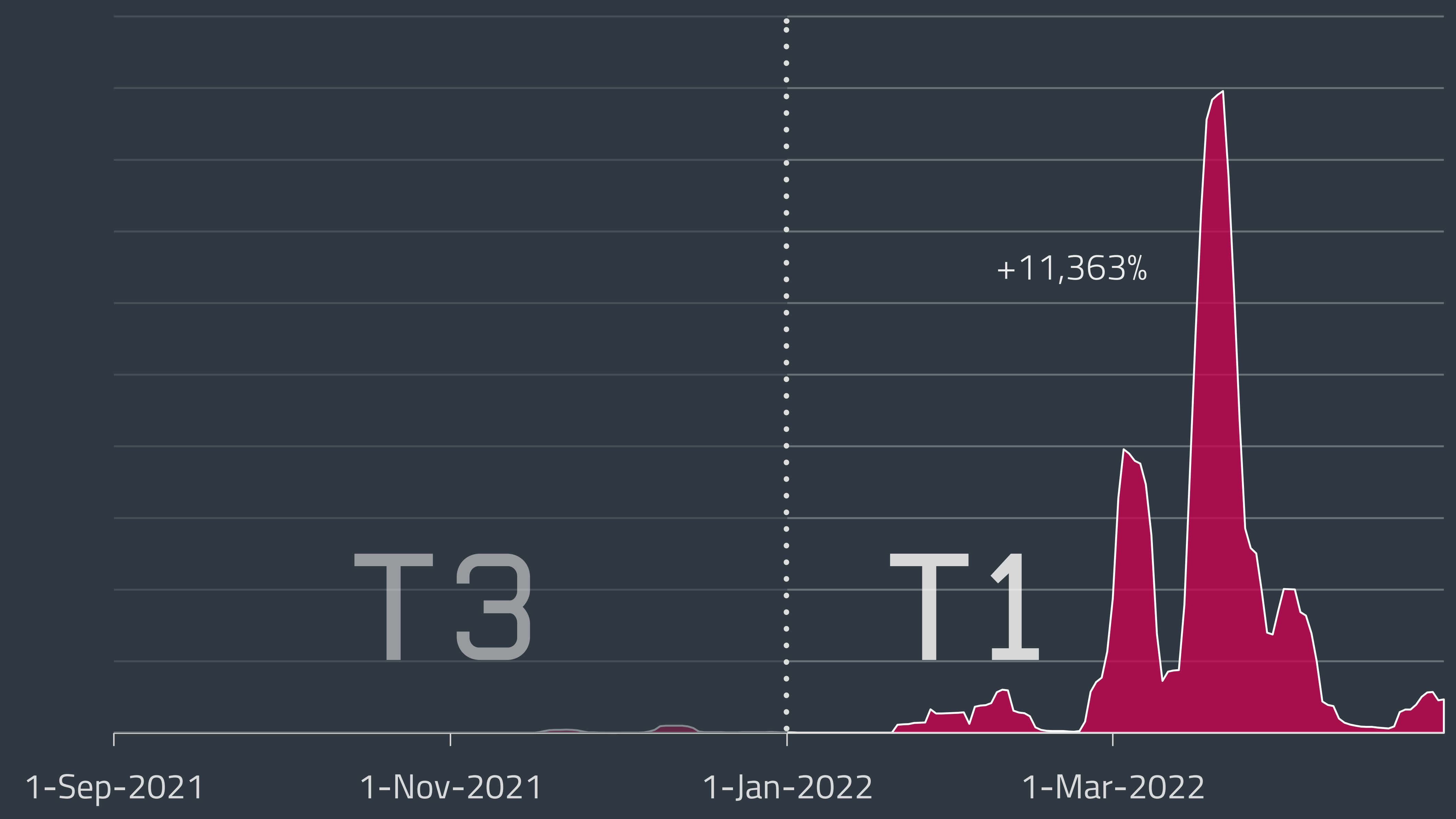
Emotet shifts to a higher gear and adds new distribution method, Zloader faces a takedown attempt.

In T3 2021, we detailed the resurrection of Emotet, improvements to its binary and modules, and adjustments to its technique mostly aiming at the switch to Cobalt Strike beacon as its payload. While that list might seem extensive, T1 2022 shows it was only a preparatory stage for what was yet to come.

In March and April 2022, Emotet operators shifted into a higher gear, their botnet spewing spam campaign after spam campaign, using malicious Word documents (DOC/TrojanDownloader.Agent) as attachments. Comparing that with the relatively small initial campaigns seen after its return in T3 2021, Emotet's detections in T1 2022 shot up more than a hundredfold (growth of over 11,000%).

The first larg uptick occurred on March 2, aiming very directly at Japan (67% of detections). On March 16, it was followed by the largest spike since Emotet's resurrection, hitting mostly victims in Japan (50%), Italy (16%), and Mexico (4%). There was also one smaller aftershock on March 21 with similar targets.

As *announced* [83] in February, Microsoft disabled downloaded Visual Basic for Applications (VBA) macros by default. This *effectively cut* [84] one of the most popular distribution avenues used by Emotet, Trickbot, Qbot, Dridex, and many others.



Emotet detection trend in T3 2021 – T1 2022, seven-day moving average

Emotet operators tried to adapt to the new reality by experimenting with other compromise vectors on smaller samples of victims. One such test *campaign* [85] was documented by ESET researchers between April 26 and May 2, where botnet operators replaced the typical Office document attachment with malicious LNK files (LNK/TrojanDownloader.Agent.AMQ). One of the frequently seen filenames was `form.lnk` and tried to lure victims from Japan (28%), Italy (16%), and Mexico (11%) to download and run the Emotet binary.

A different technique was documented by *Proofpoint* [86] in Emotet's campaign between April 4 and April 19. Operators used salary- and bonus-related bait, leading to a ZIP archive stored on OneDrive, which upon unpacking, contained Microsoft Excel Add-in (XLL) files. If executed, these files dropped and ran the main Emotet binary.

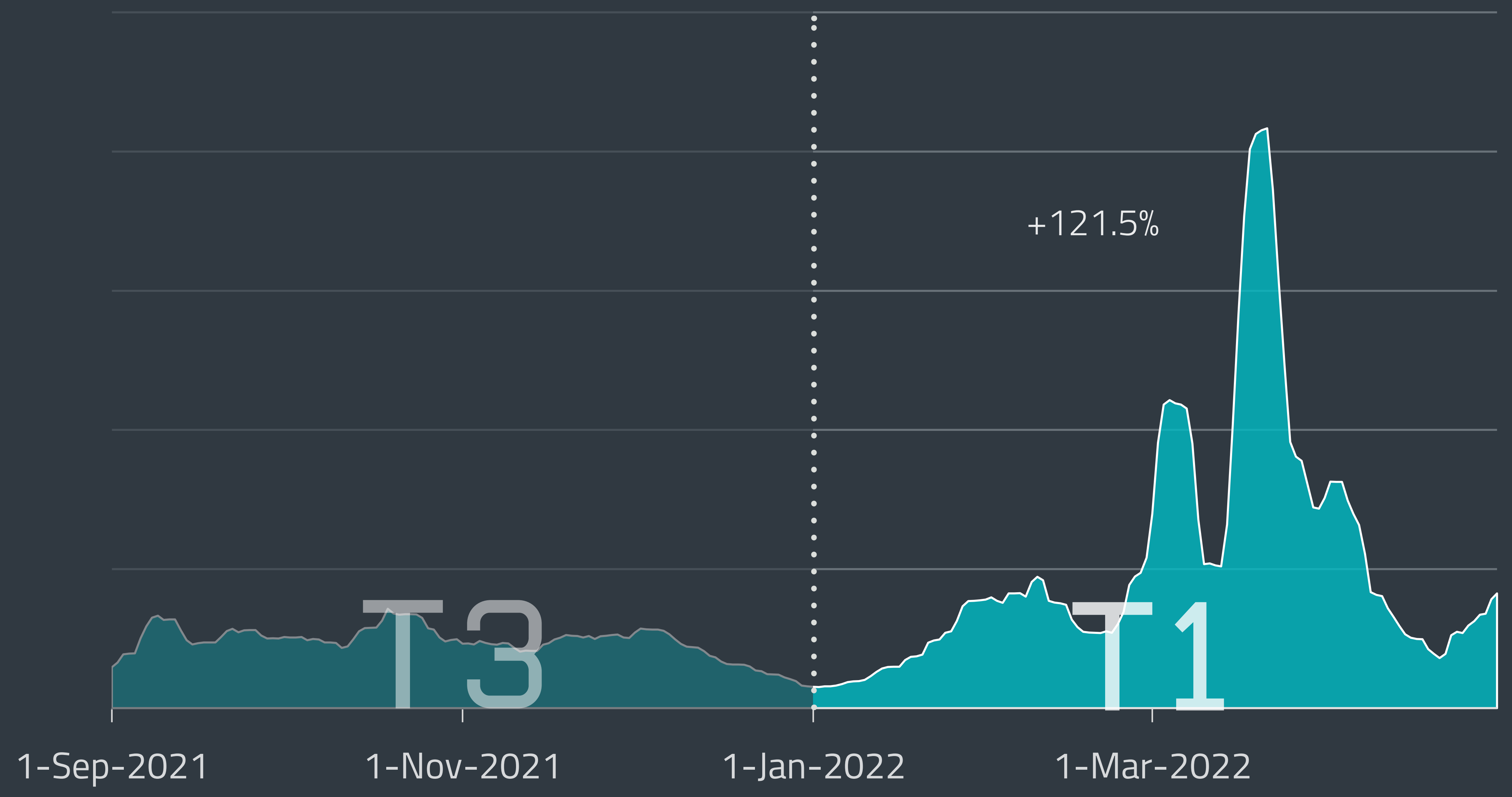
EXPERT COMMENT

The size of Emotet's latest LNK and XLL campaigns was significantly smaller than those distributed via compromised DOC files seen in March. This suggests that the operators are only using a fraction of the botnet's potential while testing new distribution vectors that could replace the now disabled-by-default VBA macros. As soon as one of the tested approaches yields satisfactory results, we can expect Emotet to shift back into high gear.

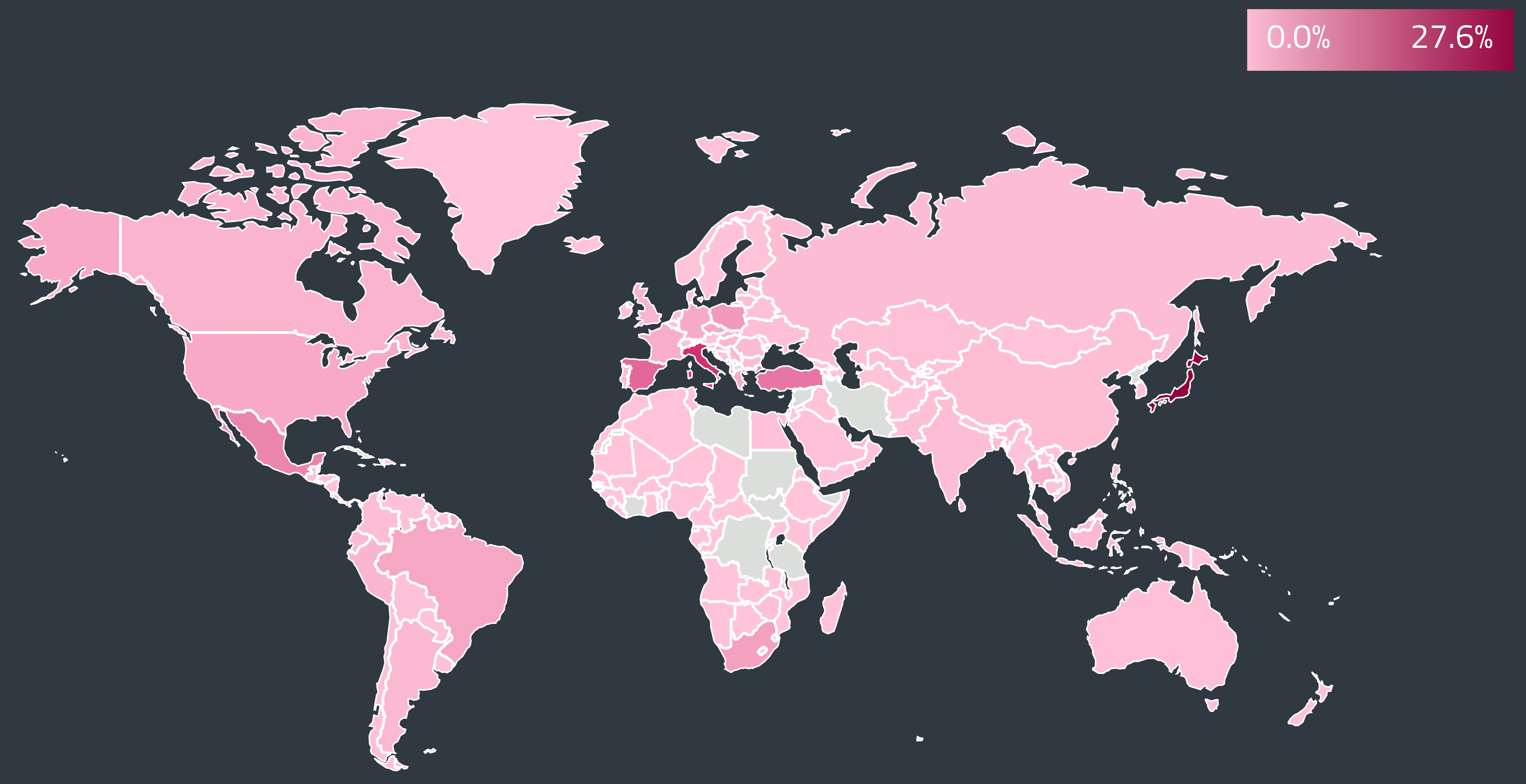
Dušan Lacika, Senior Detection Engineer

Looking at the Downloader category in general, the detection trend was mostly influenced by upticks of the Emotet botnet, significantly contributing to the 121% growth of the whole category between T3 2021 and T1 2022.

However, there was one other threat supporting those numbers – MSIL/TrojanDownloader.Agent. This downloader family increased its activity by 118% compared to T3 2021 and ended up second in the top 10 with 18%. Four out of its top five variants (MSIL/TrojanDownloader.Agent.JBZ, .IYB, .IUU, .JEG) were downloading two binaries: a payload in the form of an EXE file, and a DLL tool used to execute it. The final payloads were downloaded from the Discord platform and included Agent Tesla, Fareit, and MSIL/Agent.CFQ trojan.

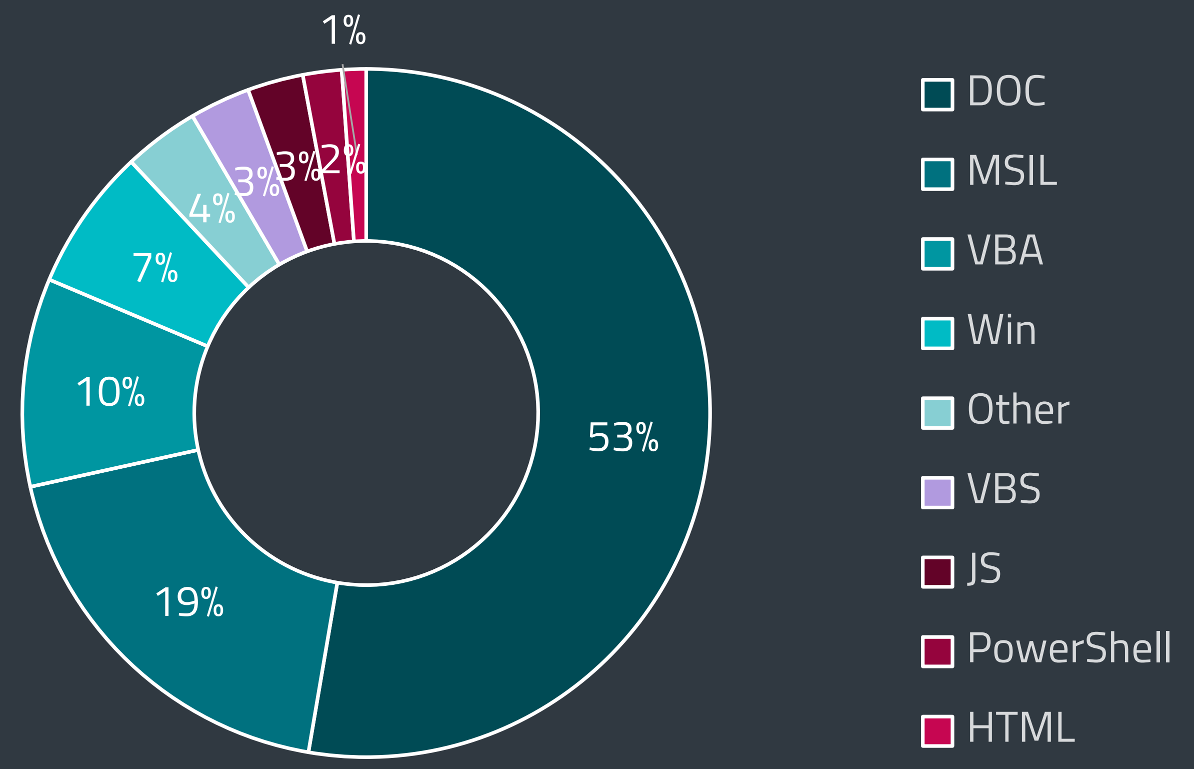


Downloader detection trend in T3 2021 – T1 2022, seven-day moving average



Global distribution of Downloader detections in T1 2022

T1 2022 is the first period since ESET started publishing Threat Reports in which the VBA platform lost its lead, landing only in third place with 10%. Due to Microsoft disabling macros by default, we expect to see a continuous decline of VBAs in the future as attackers will replace this vector with new, more effective ones. The highest share of the DOC platform is primarily caused by the massive Emotet campaigns in March, using weaponized Word documents.



Downloader detections per detection type in T1 2022

T1 2022 also brought a takedown attempt. A coalition of vendors led by Microsoft's Digital Crimes Unit made a move against Zloader – a former banking trojan that evolved into a distribution channel for other malware strains. The disruption effort took aim at three specific botnets tied to the malware family. ESET Research contributed to the operation by providing technical analysis and threat intelligence. For a more detailed account of the Zloader takedown, read the *News from the Lab* section or our *blogpost* [34].

A new loader named *Verblecon* [87] was spotted for the first time in T1 2022 by Symantec's Threat Hunter team. According to their findings, it is complex, powerful and polymorphic malware that uses anti-analysis mechanisms to avoid the watchful eye of security solutions and researchers. ESET detects the threat as Java/Agent.OR.

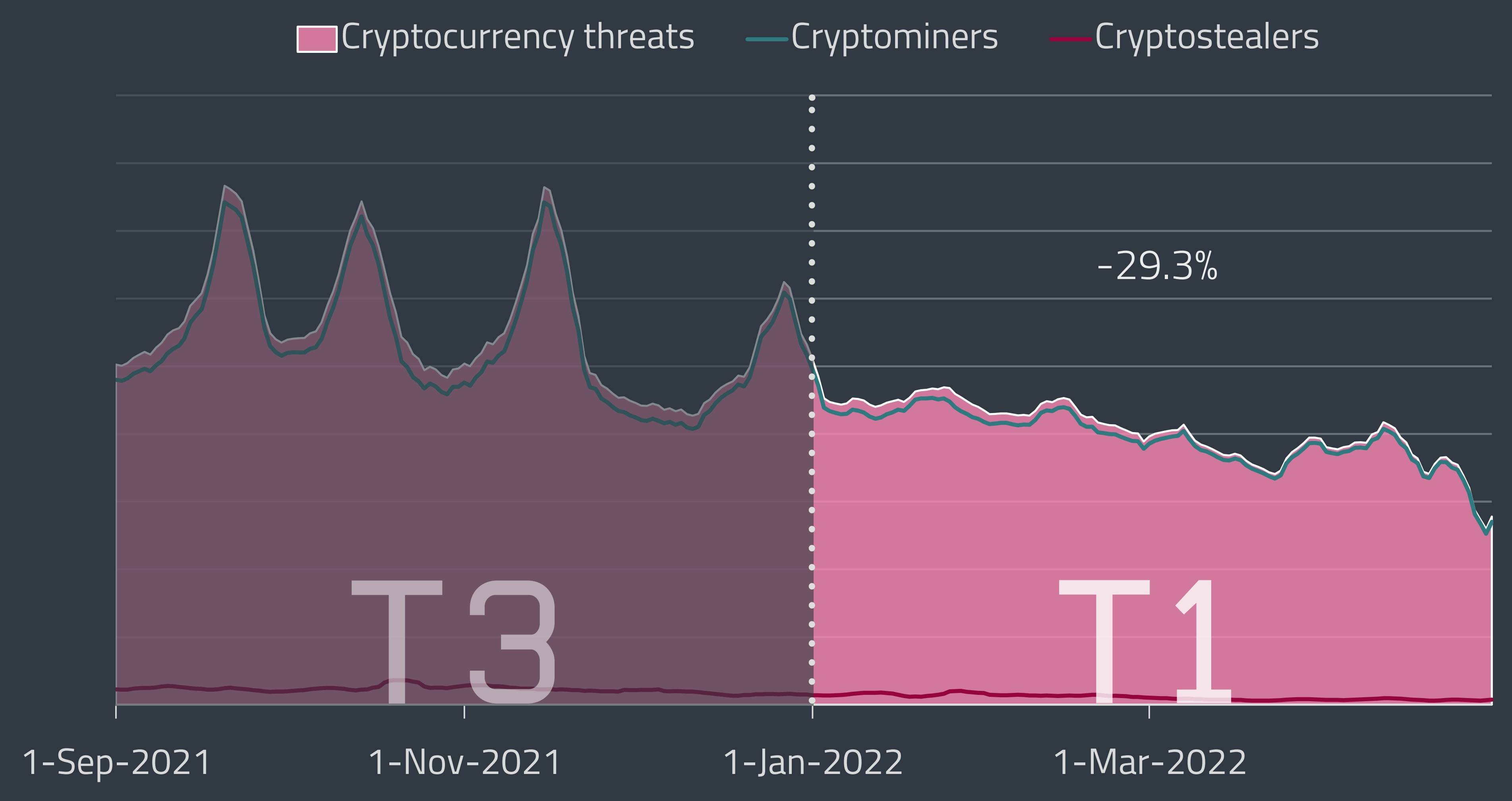
CRYPTOCURRENCY THREATS

Cryptocurrency platforms hacked for significant profit even as cryptocurrency threat detections decline.

T1 2022 was not the best period for cryptocurrencies. Even though their exchange rates did not by any means crash, the most prominent cryptocoins were having a hard time reaching their previous highs. The price of bitcoin hovered around USD 40,000 throughout T1, and Ethereum only managed to breach USD 3,500 at the start of the year and then for a few days in April. Faring even worse than the currencies themselves, the number of Cryptocurrency threat detections decreased by 29.3% in T1 2022.

As stated numerous times in our Threat Reports, the number of cryptocurrency threats correlates with cryptocurrency exchange rates to a certain extent. It could safely be said that the period from January to April was not very generous to these alternate forms of payment and investment. The stagnation in cryptocurrency values can be *attributed to* [88] the general turmoil in the market, caused mostly by Russia waging war on Ukraine, along with the anticipation of monetary regulations in the US.

However, even though the number of cryptocurrency threats went down, they remain as dangerous as ever. The beginning of the year saw several high-profile cryptocurrency platform hacks: cryptocurrency exchange Crypto.com users lost more than *USD 30 million* [89] in mostly Ethereum and bitcoin after malicious actors bypassed the site's two-factor authentication; the cross-chain cryptocurrency platform Wormhole was hacked for *USD 326 million* [90] when cybercrooks exploited a vulnerability in their network; and finally, the NFT marketplace OpenSea was once again targeted by hackers, who managed to steal about *USD 1.7 million* [91] worth of digital tokens in a phishing attack.



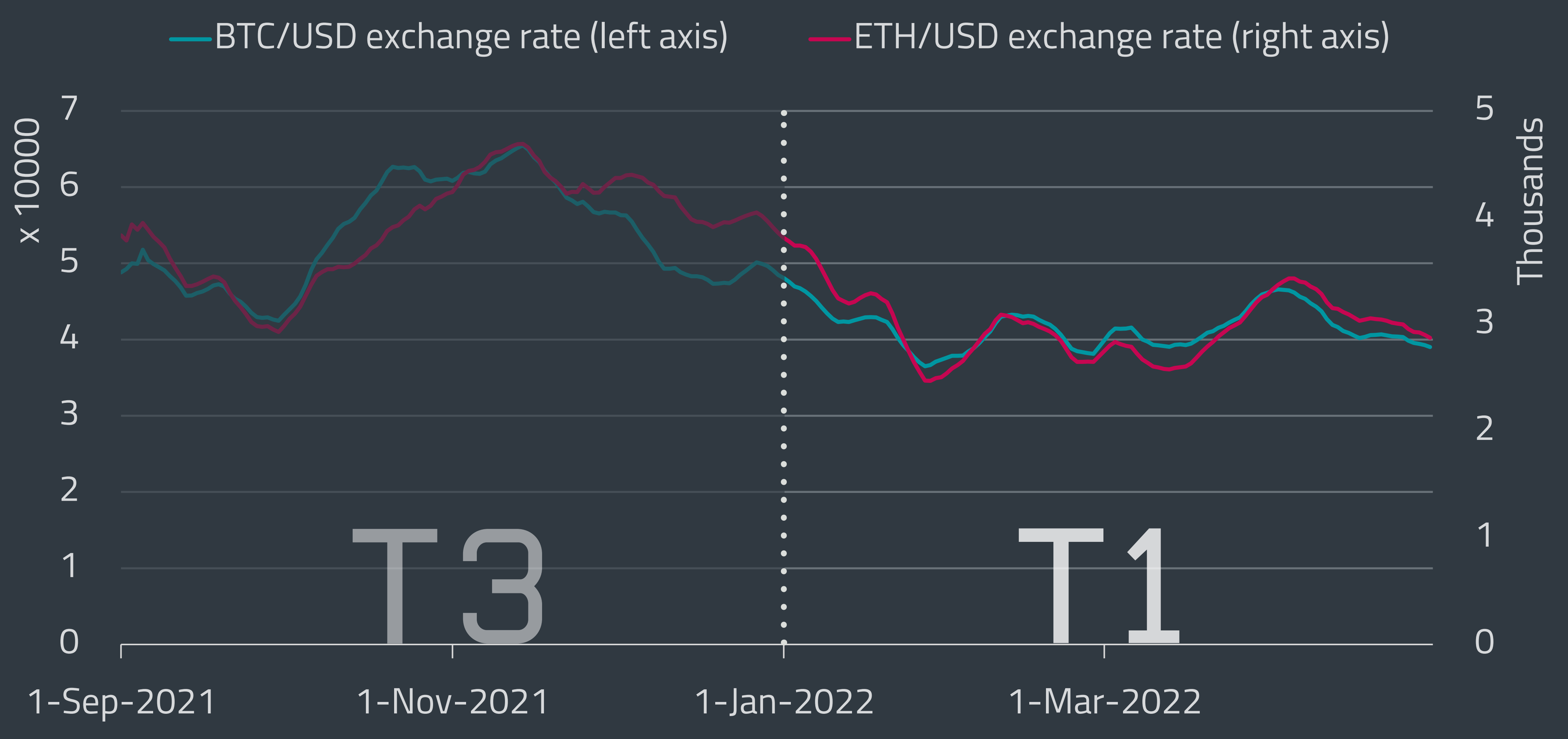
Cryptocurrency threat detection trend in T3 2021 – T1 2022, seven-day moving average

EXPERT COMMENT

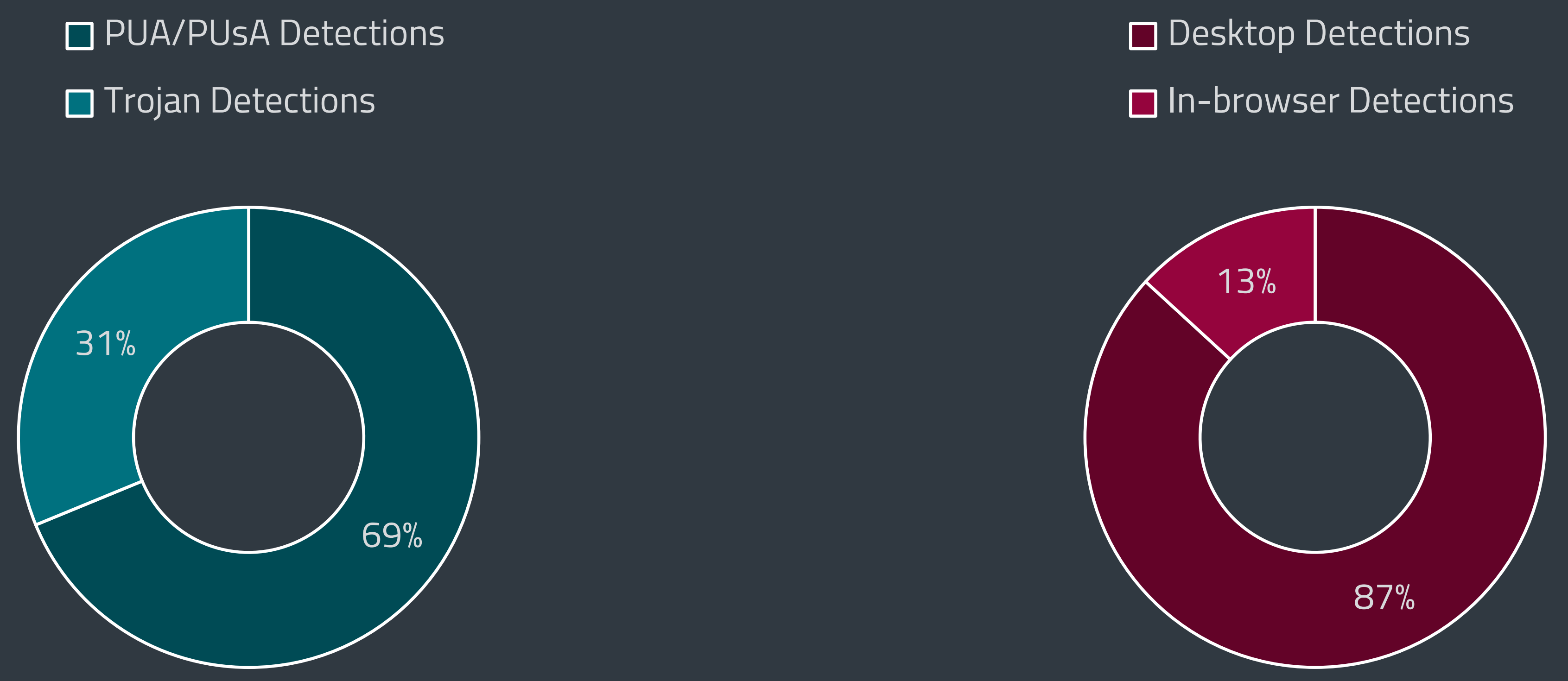
The war in Ukraine, strict sanctions on Russian cryptomining companies, and the increased targeting of cryptocurrency platforms in cyberattacks have all lessened the motivation of malicious actors to create and spread cryptocurrency-related malware. On the other hand, cryptocurrency exchange rates grew thanks to the Central African Republic adopting bitcoin as an official currency. Because of the current situation, it is quite difficult to predict how the threat landscape will develop, but we can expect a rise in large-scale targeted attacks, similar to what is happening with ransomware.

Igor Kabina, ESET Senior Detection Engineer

Coinminers, usually the more active of the cryptocurrency threat subcategories, decreased by 28.4% between T3 2021 and T1 2022. There were no major jumps in their activity up until April, which saw two smaller spikes in the numbers of the potentially unwanted application (PUA) Win/CoinMiner. The first was on April 11 when a surge of the AGen.D variant was registered in France, and the second was on April 20, led by the TA and SF variants, both mainly seen in Japan.



Bitcoin and Ethereum/USD exchange rates in T3 2021 – T1 2022, seven-day moving average



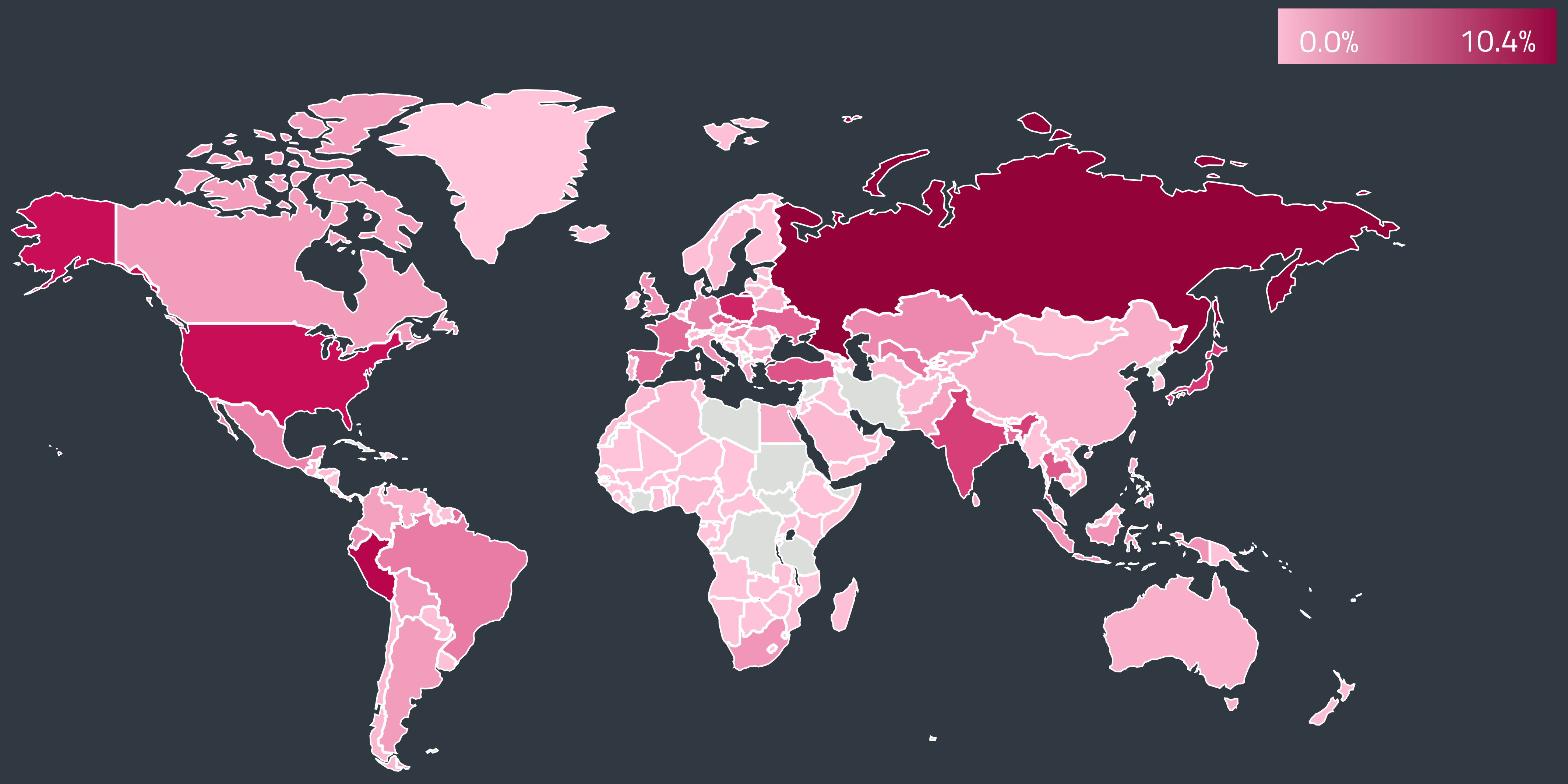
Trojan:PUA and desktop:in-browser ratio of cryptominer detections in T1 2022

The three most detected coinminers in T1 were Win/CoinMiner PUA, Win/CoinMiner trojan and JS/CoinMiner PUA. Win/CoinMiner PUA constituted almost half of all coinminer detections with 49.2%, even while its numbers went down by 41.5% when compared to the previous period. Win/CoinMiner trojan had a 12.4% share of detections and also decreased in number by 16.4%. JS/CoinMiner PUA was close behind with 11.8% and suffered the smallest decline out of the top three, which was 9.6%. Despite the falling numbers, the top three players have managed to keep the same positions as in T3 and indeed the overall 2021 statistics.

In the last report we mentioned that an interesting trend regarding PUA-vs.-Trojan and Desktop-vs.-In-browser ratios had emerged over 2021, namely that PUA and Desktop detections were steadily growing each period. This time around, however, both Trojans and In-browser detections managed to regain some lost ground. In T3 2021, the ratio of PUA to Trojan detections was 74% to 26%, while in T1 2022 it was 69% to 31%. As for the Desktop:In-browser ratio, it was 90% to 10% in T3 and 87% to 13% in T1.

	T3 2021	T1 2022
1	dl-x[.]com	webminepool[.]com
2	wypracowanie.edu[.]pl	dl-x[.]com
3	monerominer[.]rocks	wypracowanie.edu[.]pl
4	carrierecalciatori[.]it	slovolam[.]sk
5	instagrammi[.]ru	carrierecalciatori [.]it
6	newsoholic[.]com	arafifblues[.]com
7	mituus[.]com	kaizoku-ehime[.]jp
8	idaakulubu[.]com	mainevnap[.]com
9	cumpleañosdefamosos[.]com	mituus[.]com
10	slovolam[.]sk	monerominer[.]rocks

Top 10 most visited cryptojacking domains in T3 2021 and T1 2022



Global distribution of Cryptocurrency threat detections in T1 2022

The increased percentage of In-browser coinminers should serve as a reminder to be wary of free streaming websites and sites with adult content, as some of them can hijack the user's computer to mine for cryptocurrencies. You can find the list of the top 10 most visited cryptojacking domains in T3 2021 and T1 2022 on the left-hand side of the page.

Coinminers were seen mainly in Russia, where ESET registered 10.6% of their detections, then Peru with 6.4%, and the United States, which saw 5% of all their attack attempts.

Cryptostealers' decline was even sharper than that of coniminers – the subcategory went down by 51.6%. There was one spike in their detections: on January 25, the OSF variant of Win/PSW Delf trojan had its peak, with the most attack attempts seen in Turkey, Japan, and Hong Kong.

Compared to T3 2021, the top three cryptostealers stayed the same, even if they shuffled their positions a bit. The Win/Spy.Agent trojan was the most detected cryptostealer, accounting for 37.4% of cryptostealer detections. The Win/PSW.Delf trojan had the second-highest share of detections at 24.3%, followed by MSIL/ClipBanker with 19.5%. As with coinminers, all three most-detected cryptostealers were on a downward trend in T1. MSIL/ClipBanker suffered the worst decline out of the three and dropped by almost 70%.

Based on our telemetry, cryptostealer attacks were pretty spread out all over the world. Still, somebody had to be the one that faced the most cryptostealer attack attempts, and in T1 2022 it was Peru with 6.9%. The next in line was Turkey with 4.9% and the third-place holder was Spain and its 4.5%.

The country statistics of all cryptocurrency threat detections had the same three countries on top as in the coinminer list: Russia with 10.4%, Peru with 6.4%, and the US with 4.9%.

WEB THREATS

The number of phishing URLs shoots up; scammers exploit interest in the Russia-Ukraine war.

The first four months of 2022 saw a stable level of overall web threats blocked, with only a negligible decline of 1.8%. In regard to the number of unique URLs blocked, there was a 14.9% decline in T1 2022. On average, ESET telemetry recorded 4.8 million daily web threat blocks and 370 thousand harmful URLs daily.

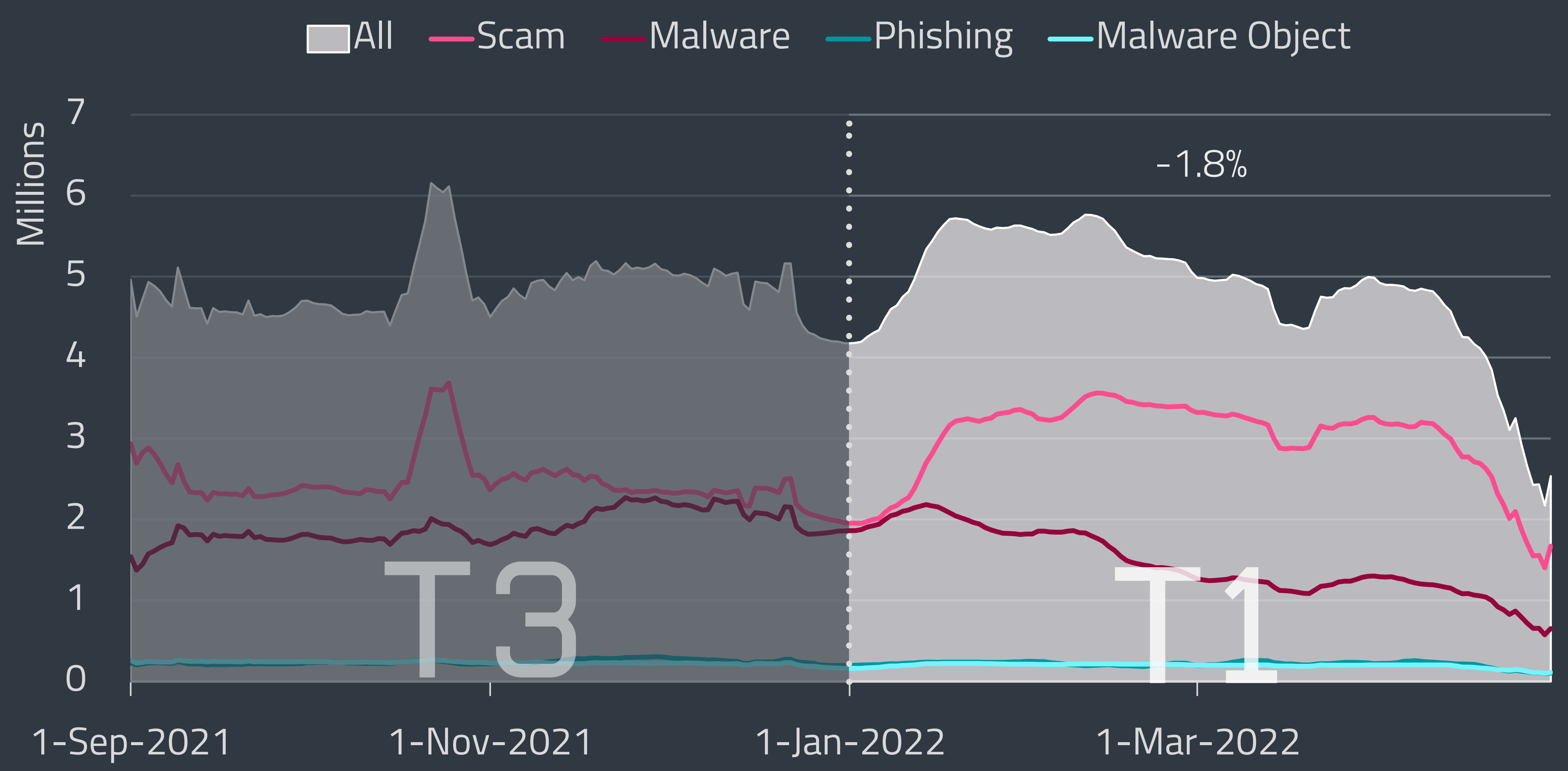
Malware-distributing websites, represented by the Malware category, saw the steepest decline in both total blocks and the number of URLs seen, declining by 26% and 23%, respectively. In the Phishing category, the number of URLs blocked increased by almost 30%. Interestingly, this didn't result in a growth in total phishing blocks, and these even saw a decline of 13.2%.

The number of blocked phishing URLs started increasing sharply in March and the levels stayed way beyond the T1 and preceding T3 average for the rest of the period. The peak detection level, reached on March 7, was three times higher than the daily T1 average, with 82,000 unique URLs blocked.

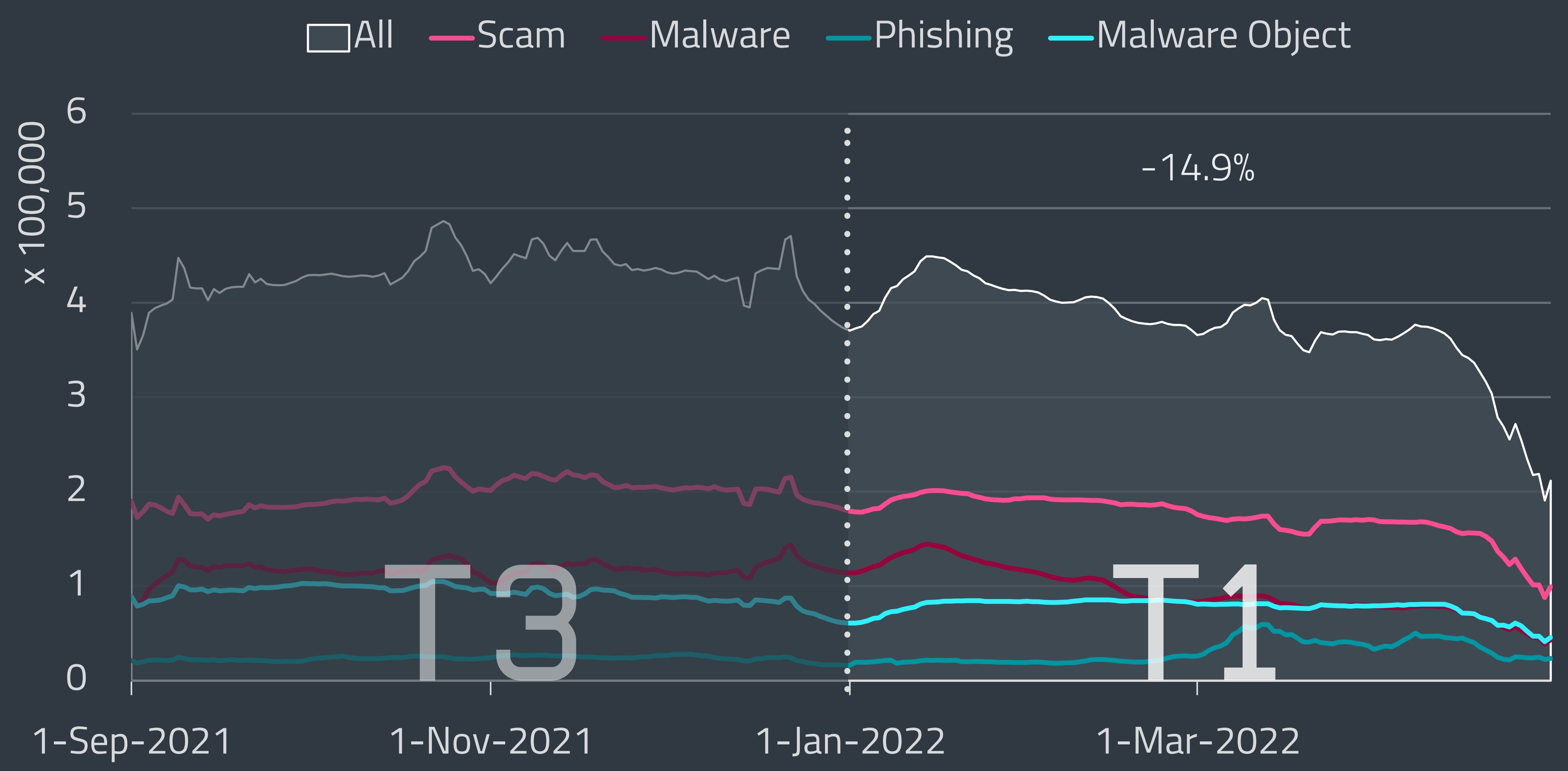
The opposite was true for websites categorized as Scam, which had approximately 20% more total blocks, but this increase wasn't reflected in the number of URLs seen. Scam blocks started increasing in the second half of January, remained at the raised levels until mid-April, and then dropped to T1's minimum.

	Malware	Scam	Phishing
1	pdloader[.]com	survey-smiles[.]com	propu[.]sh
2	iclickcdn[.]com	newrrb[.]bid	mrproddisup[.]com
3	demotzincky[.]casa	v.vfghe[.]com	tech4-you[.]com
4	aj2396[.]online	bwukxn[.]com	www--bancosantafe--com--ar.insuit[.]net
5	plehimselves[.]info	cellar.z5h64q92x9[.]net	thecred[.]info
6	jecromaha[.]info	loft.z5h64q92x9[.]net	foreign-movies.baby-supernode[.]xyz
7	vk-online[.]xyz	prirodnolijecite[.]com	watchvideoplayer[.]com
8	www.hostingcloud[.]racing	sentrynew.sdh.com[.]ua	update.updtbrwsr[.]com
9	d.ftte[.]fun*	glotorrents[.]pw	medvitro[.]info
10	buikolered[.]com	serch07[.]biz	gelturla[.]com

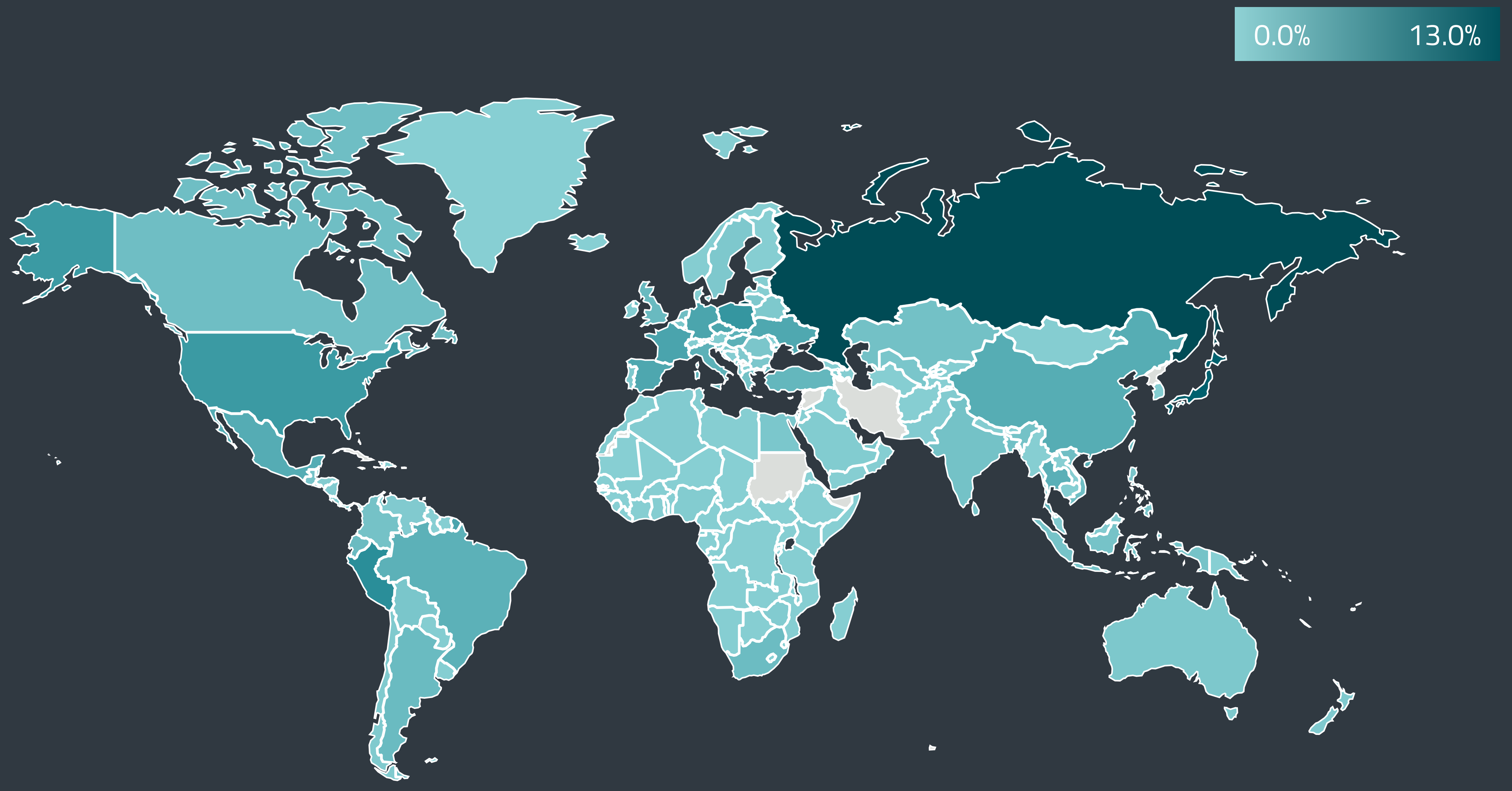
Top 10 blocked Malware, Scam and Phishing domains in T1 2022; domains first detected in this period are marked with *



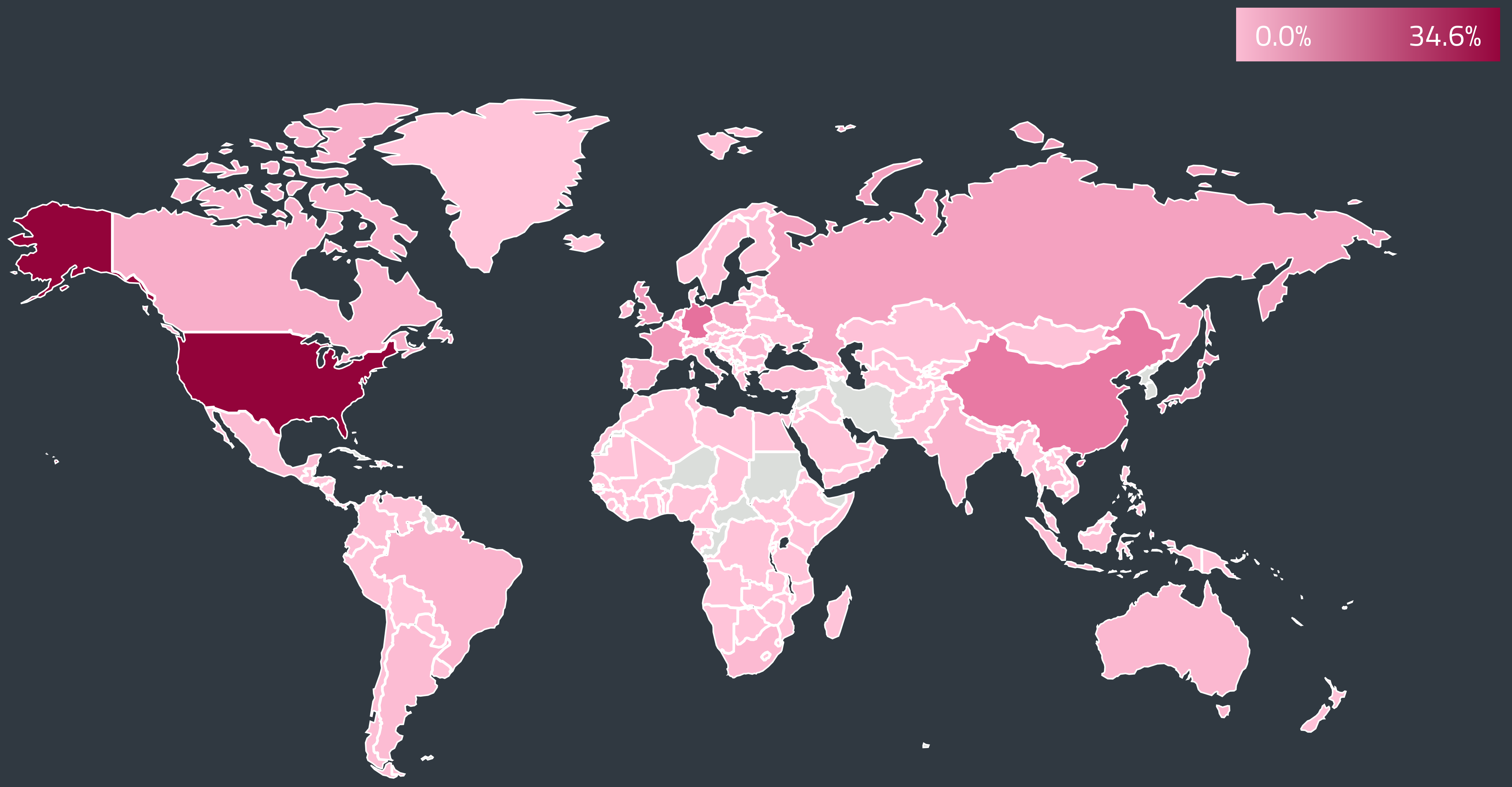
Web threat block trend in T3 2021 – T1 2022, seven-day moving average



Unique URL block trend in T3 2021 – T1 2022, seven-day moving average



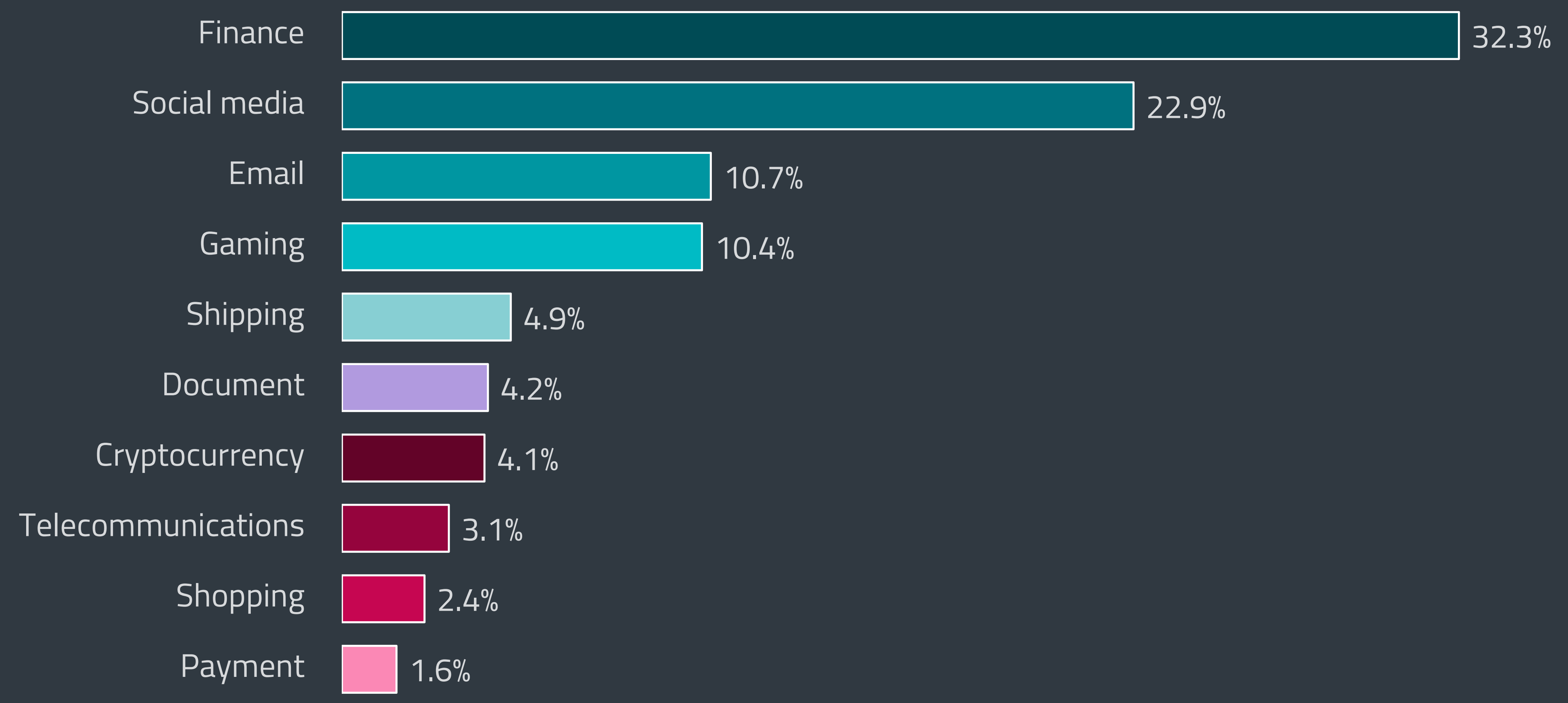
Global distribution of Web threat blocks in T1 2022



Global distribution of blocked domain hosting in T1 2022

The Russian invasion of Ukraine brought on an influx of phishing and scam campaigns attempting to take advantage of people trying to support Ukraine during the war. Most commonly, the campaigns used fictitious charities and fundraisers as lures. The first fraudulent domains exploiting the war started cropping up almost immediately after the start of the invasion, as documented by ESET Research on *Twitter* [92].

Overall, the number of harmful websites blocked in T1 2022 was greatest in Russia (13.0% of all website blocks), followed by Japan (9.1%), Peru (4.4%), Poland (3.9%), and the United States (3.6%). As for the source countries of the web threats – determined by the GeoIP of the blocked domains – more than a third of the blocked domains were hosted in the US (34.2%), followed by a wide margin by Germany (7.4%), China (6.6%), France (3.9%), and Japan (3.5%).

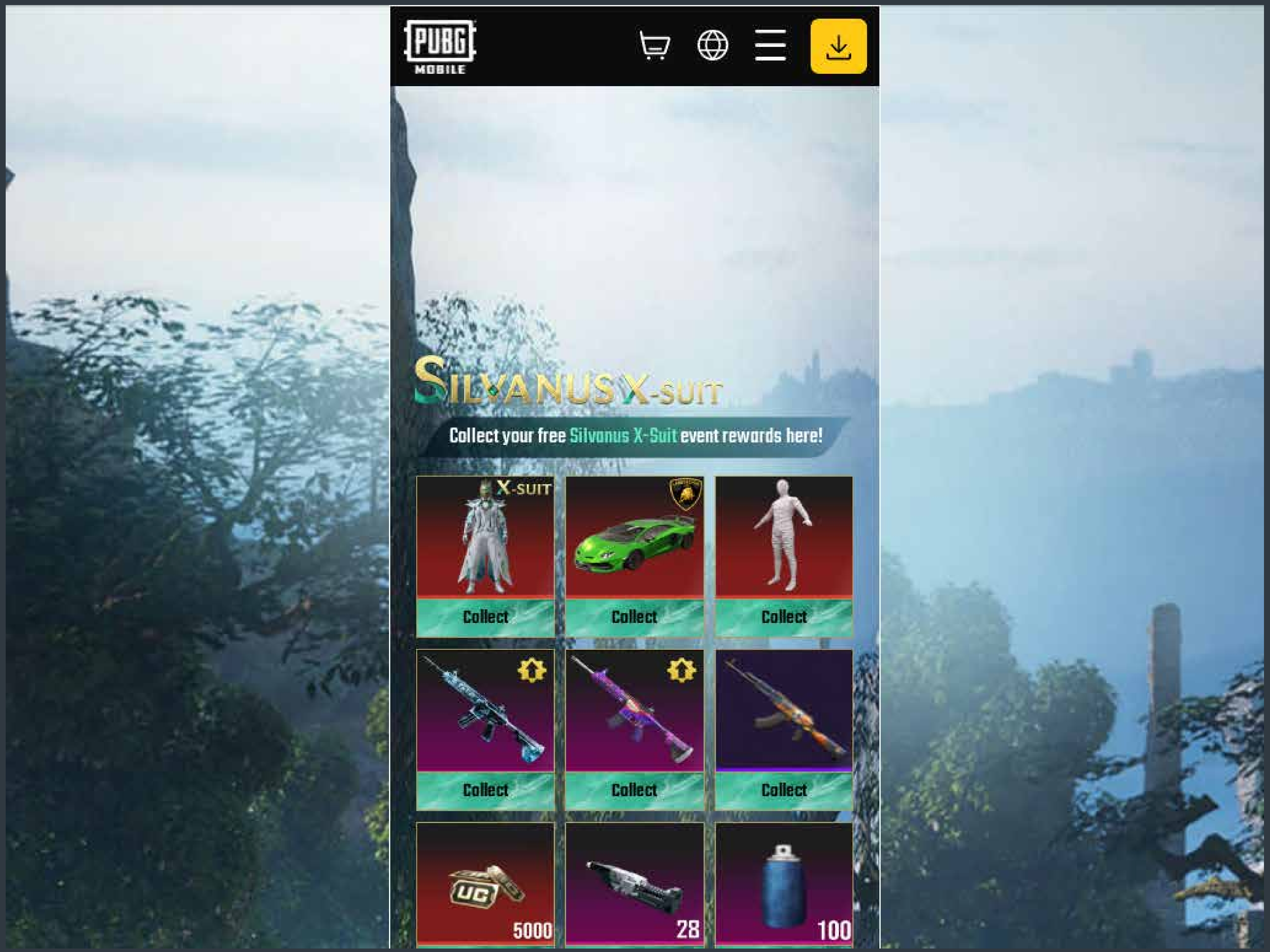


Top 10 phishing website categories in T1 2022 by number of unique URLs

Based on ESET phishing feeds, approximately a third of the phishing URLs detected in T1 2022[1] impersonated financial organizations, much as in T3 2021. Social-media-themed phishing lures, mainly represented by fake Facebook and WhatsApp login pages, came in second with 23% of URLs seen.

After booming in T3 2021, the Shopping and Cryptocurrency categories were both on the decline in T1 2022. Online-shopping-themed phishing, represented mostly by websites impersonating Amazon, was significantly reduced in the number of URLs in circulation, decreasing by 73.6% and dropping from third to ninth place. Phishing websites impersonating cryptocurrency platforms retreated from fourth to sixth place, declining by 45% in the number of unique URLs detected.

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



Example of a phishing website (pubgmystical[.]com) impersonating a marketplace for the PUBG MOBILE game

On the other hand, phishing websites masquerading as email services and gaming platforms were on the rise this period, the former increasing by 54% and the latter by a remarkable 291% in numbers of URLs seen. In the Gaming category, websites impersonating marketplaces for various online games were widespread.

Although not placing in the top 10 categories, there was a notable 126% increase in travel-themed phishing URLs. These were almost exclusively represented by Airbnb copycats, often residing on deceptive domains, with “airbnb” used as a subdomain on what is actually an unrelated domain (e.g., airbnb.com[.]ee).

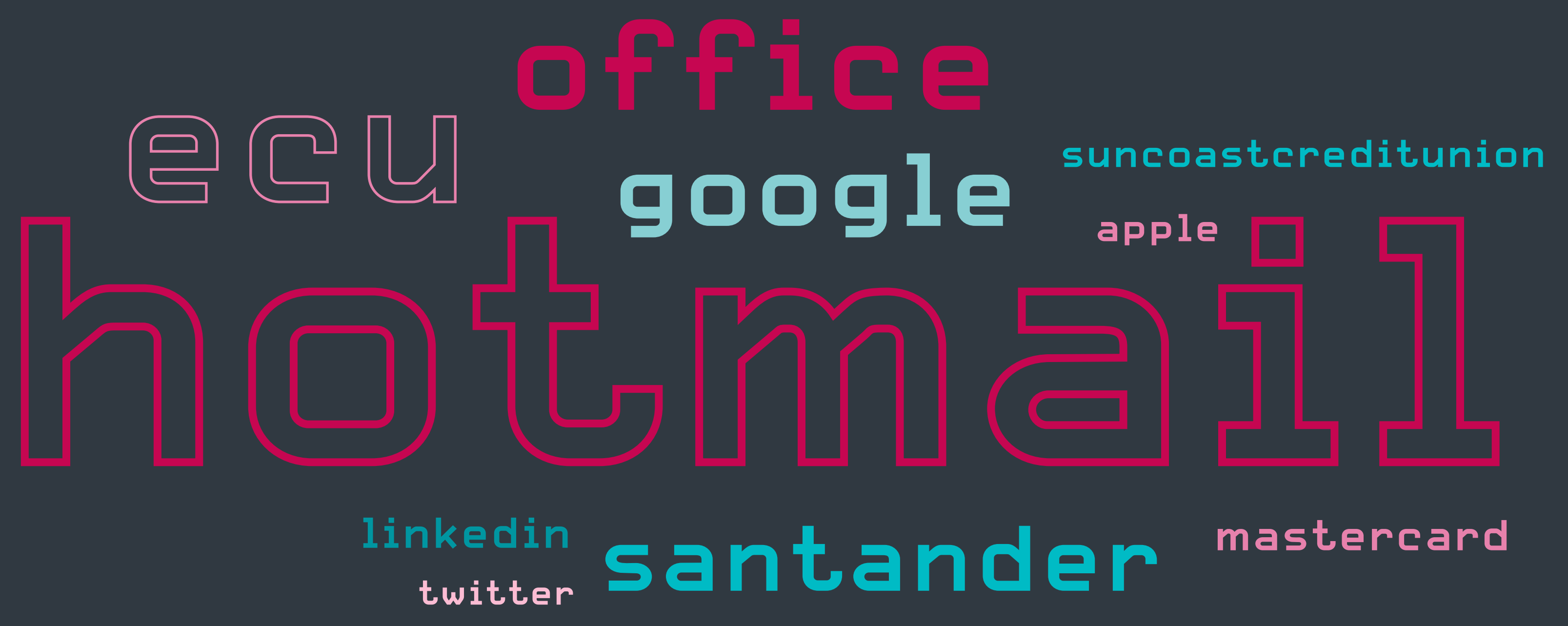
A similar trend of rising travel-themed lures was also noted in *Email threats*, presumably the result of lifting pandemic restrictions.

In the area of homoglyph attacks, the top 10 targets saw a bit of reshuffling, with eight of the targets being newcomers to the top 10 and about a half of the underlying fraudulent domains first appearing only in T1 2022.

On the other hand, several of the previously prevalent homoglyph domains completely disappeared from the scene in T1, and the overall number of blocks recorded was almost halved compared to T3 2021. Interestingly, fake cryptocurrency-themed websites, which previously led the charts along with those impersonating banks and social media, were not among the top detected homoglyph domains during this period.

The second most prevalent impostor domain, new in T1, “ecц[.]online” (ц instead of u), likely attempted to impersonate the website of Eastman Credit Union. At the time of writing, the fraudulent domain was no longer operational.

Other homoglyph domains first seen in T1, albeit with only a handful of blocks, impersonated Mastercard (mastercaṛd[.]com – ṛ instead of r), Suncoast Credit Union (suncoastcreditunlọn[.]com – l instead of i and ọ instead of o), LinkedIn (lınkedin[.]com – ı instead of i) and Twitter (twịtter[.]com - ị instead of i).



Top 10 brands and domain names targeted with homoglyph attacks in T1 2022

EMAIL THREATS

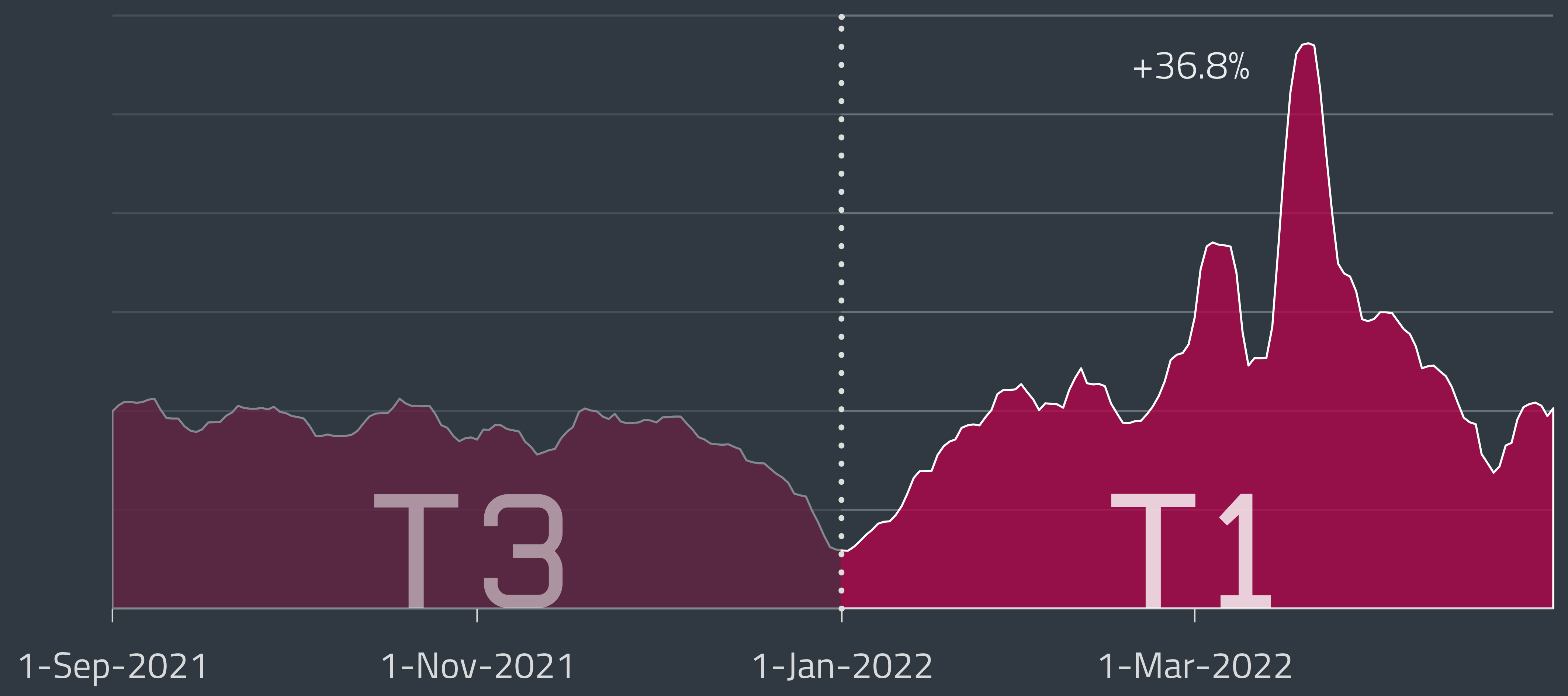
Email threats spike as Emotet's malicious documents flood back to users' inboxes.

Email threats grew by 37% in T1 2022 – the largest increase observed in this category since 2020. Threat activity rose continually throughout January and February, peaked in mid-March – daily email threat detections more than tripled the T1 average – and declined throughout April.

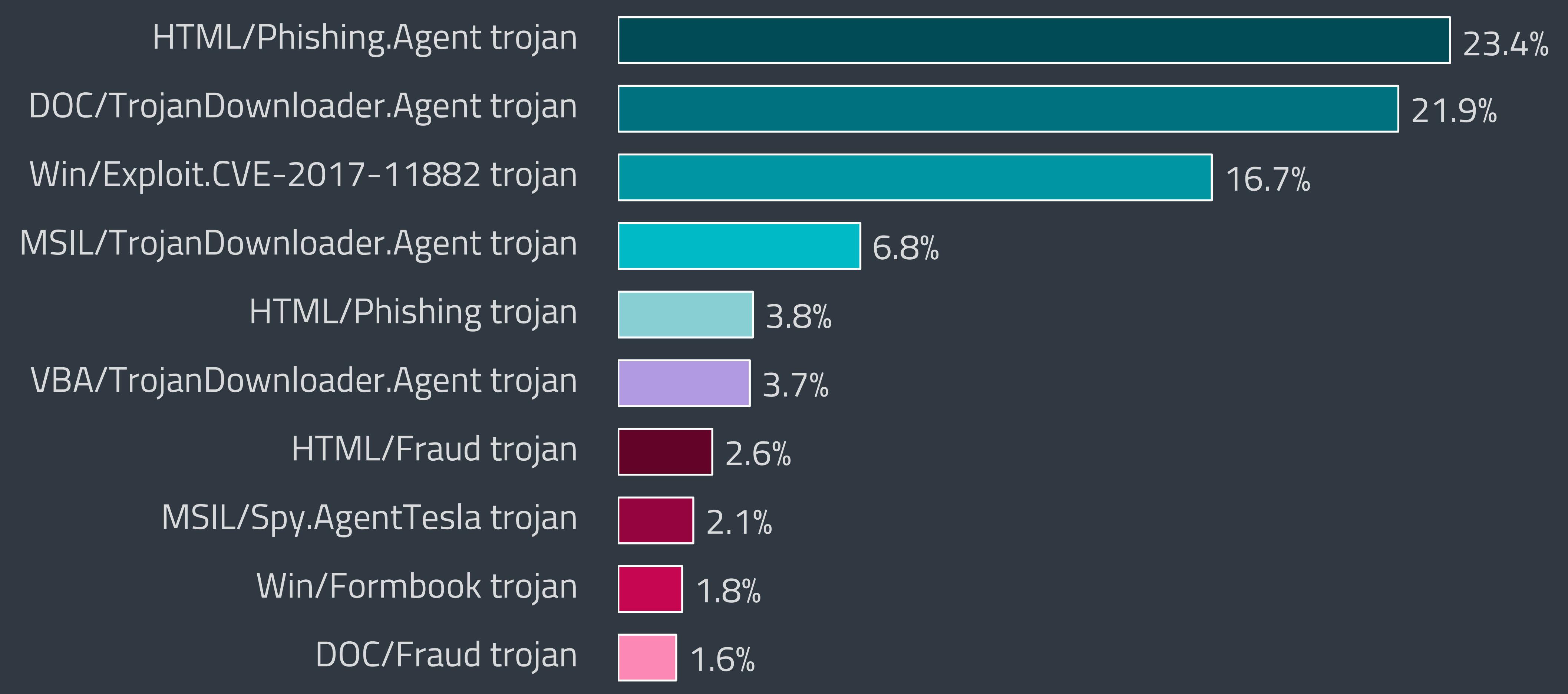
The March peak was driven by mass-scale email campaigns of the notorious Emotet, relying on malicious Microsoft Word documents, detected as variants of DOC/TrojanDownloader.Agent. The incidence of DOC/TrojanDownloader.Agent in email inboxes sprung up by a whopping 829% compared to T3 2021, making it the second most prevalent email threat of the T1 period.

DOC/TrojanDownloader.Agent detections were dominated by its DPV and DWJ variants, which built the majority of the mid-March spike. Japan was the country most affected by these Emotet campaigns, followed by Italy and Spain. These three countries were also in the lead in terms of overall email threat detections.

As discussed in the *Downloaders* section, this campaign preceded Microsoft's move to block macros from the internet, by default in Office programs. Toward the end of T1, just when the change was set to roll out, ESET researchers noticed Emotet operators shifting their tactics and switching to malicious LNK email attachments – although operating on a much smaller scale than with their infamous document-based campaigns.



Malicious email detection trend in T3 2021 – T1 2022, seven-day moving average



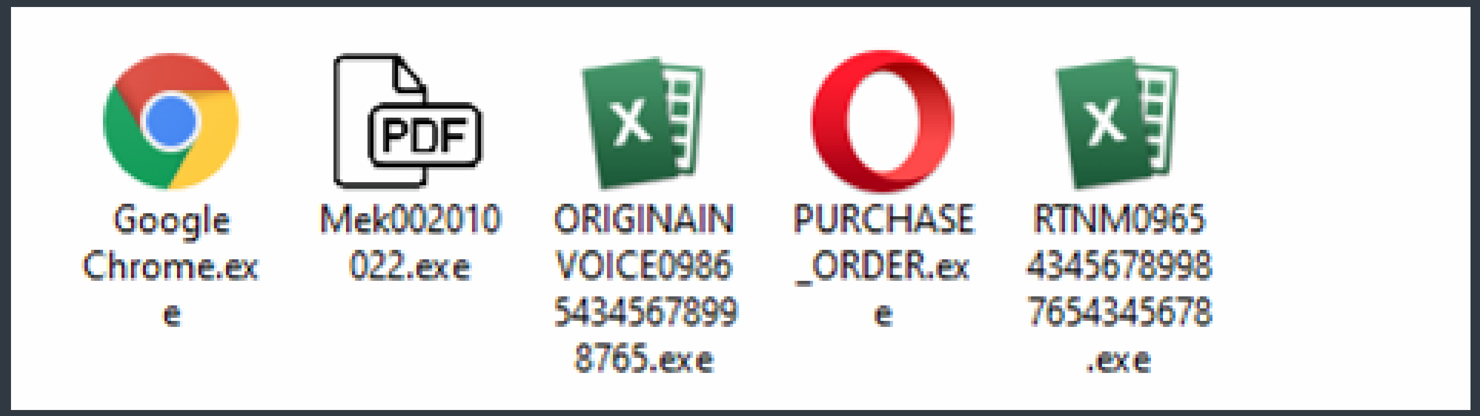
Top 10 threats detected in emails in T1 2022

EXPERT COMMENT

The Emotet email campaigns seen in T1 2022 brought on an unpleasant flashback to the botnet's prolific pre-takedown era in 2020. With macros now blocked by Microsoft, however, the March wave may well have been the last onslaught of malicious documents delivered by Emotet that we'll see – but unfortunately, it's only a question of the time until cybercriminals find another distribution avenue with similar potential.

Jiří Kropáč, ESET Director of Threat Detection

Another threat seeing substantial growth in T1 was MSIL/TrojanDownloader.Agent, marking a 130% increase from T3. Most often seen in email inboxes was MSIL/TrojanDownloader.Agent.KJO, a trojan used to download further malware from the communication platform Discord. It is distributed via Discord messages and email, in EXE attachments often using icons mimicking Excel or HTML files.

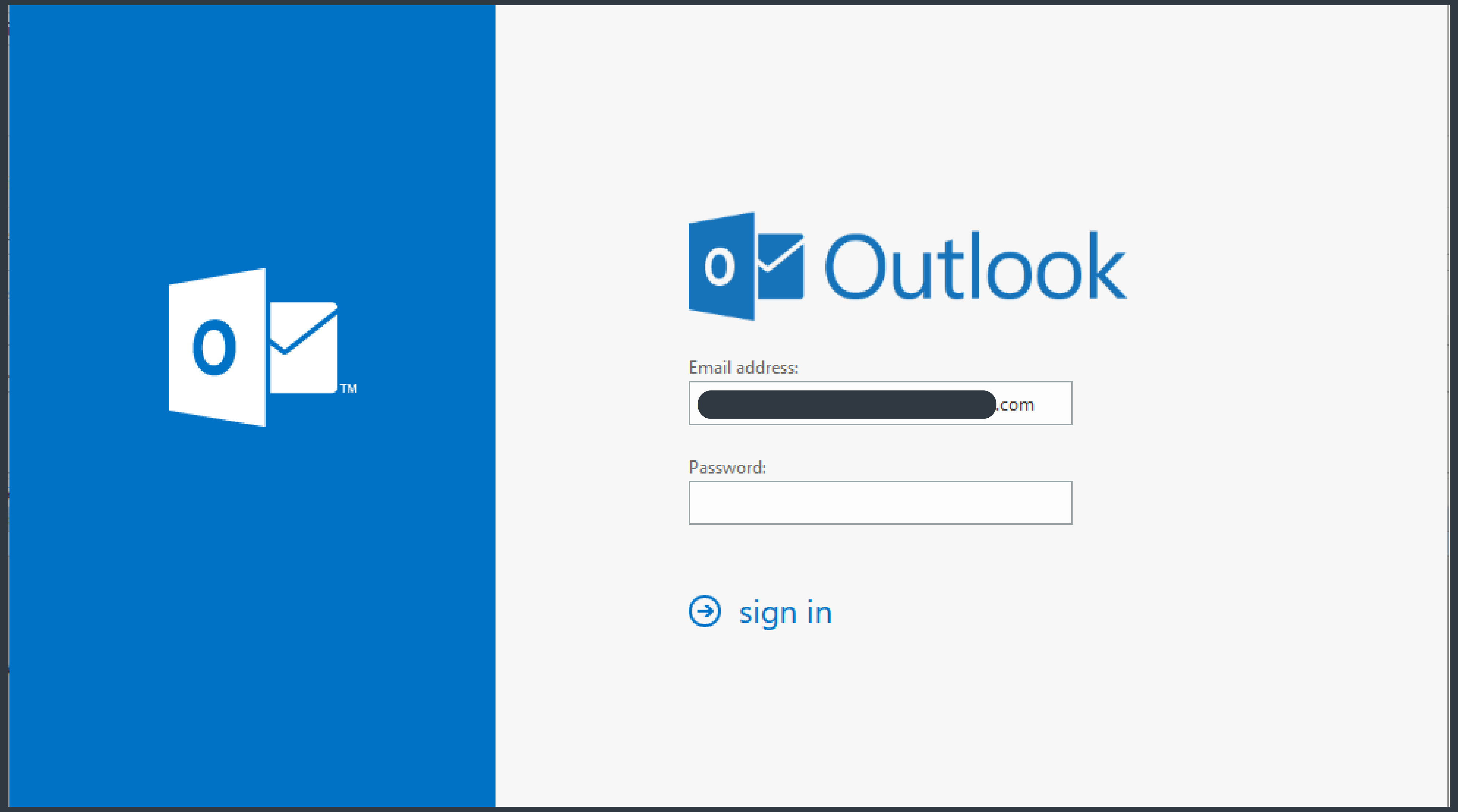

Google Chrome.exe
Mek002010022.exe
ORIGINAINVOICE09865434567899 8765.exe
PURCHASE_ORDER.exe
RTNM0965434567899 87654345678.exe

Examples of MSIL/TrojanDownloader.Agent email attachments

The downloaded malware is typically a high-profile infostealer, such as Agent Tesla or QBot. ESET telemetry shows a large but short-lived MSIL/TrojanDownloader.Agent.KJO email campaign in February, with highest detection numbers in Turkey, Japan, and Spain.

Outlook, DHL, and Microsoft were brands most commonly seen impersonated in phishing emails in T1 2022. Emails purporting to include an Outlook login page were detected in large waves in February and April, overtaking the previously leading DHL-themed lures in the overall number of detections. In fact, these emails, detected as HTML/Phishing.Outlook, just failed to make it into the top 10, placing eleventh with 1.5% of all Email threat detections caught in T1.

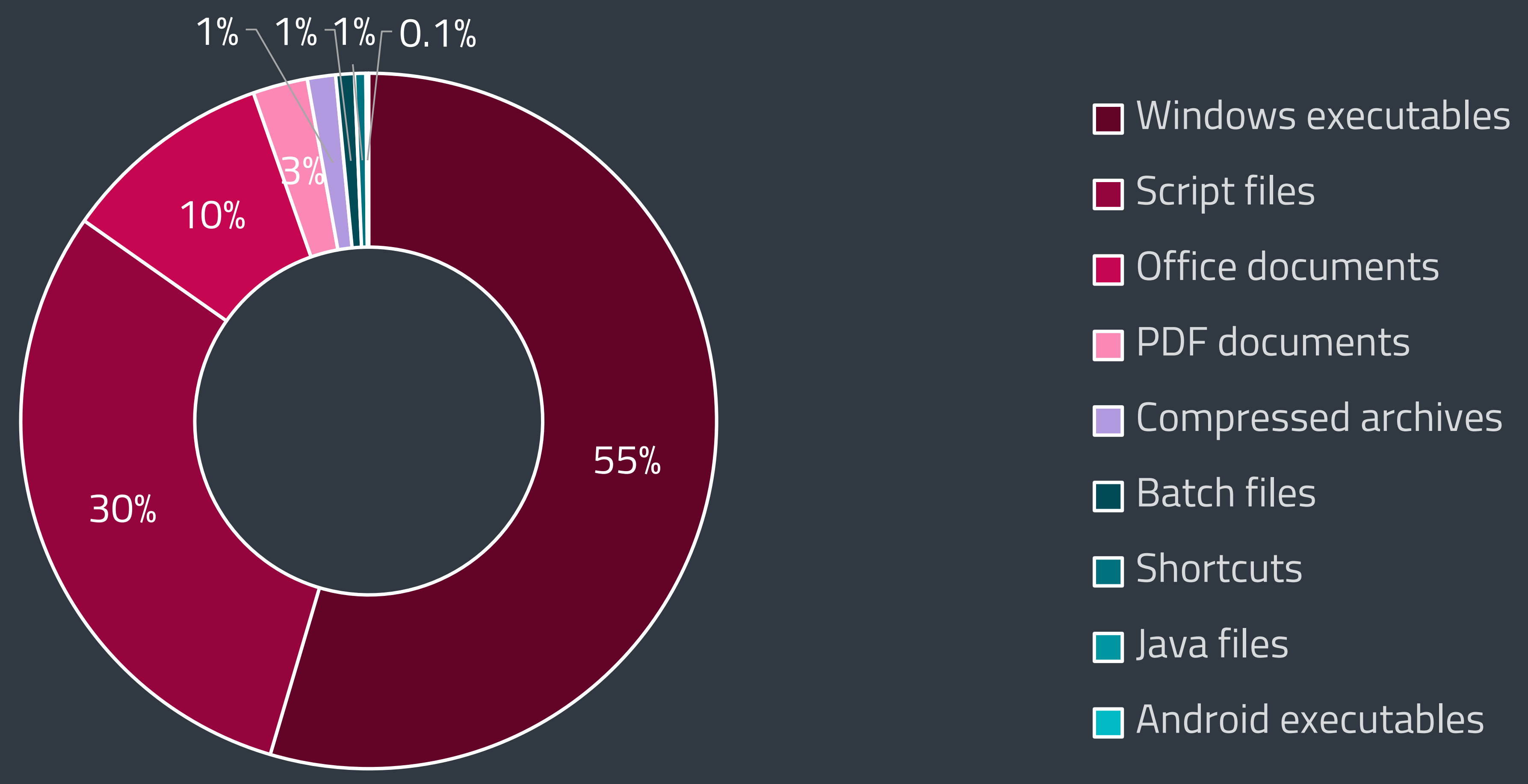
According to ESET telemetry, HTML/Phishing.Outlook was most commonly detected in the UK, followed by New Zealand and the US However, pre-filled email addresses in the phishing forms suggest the phishing might have been targeted against extractive industries in Kazakhstan and Africa.



Email address: [redacted].com

Password:

Phishing form impersonating Outlook, detected as HTML/Phishing.Outlook



Top malicious email attachment types[2] in T1 2022

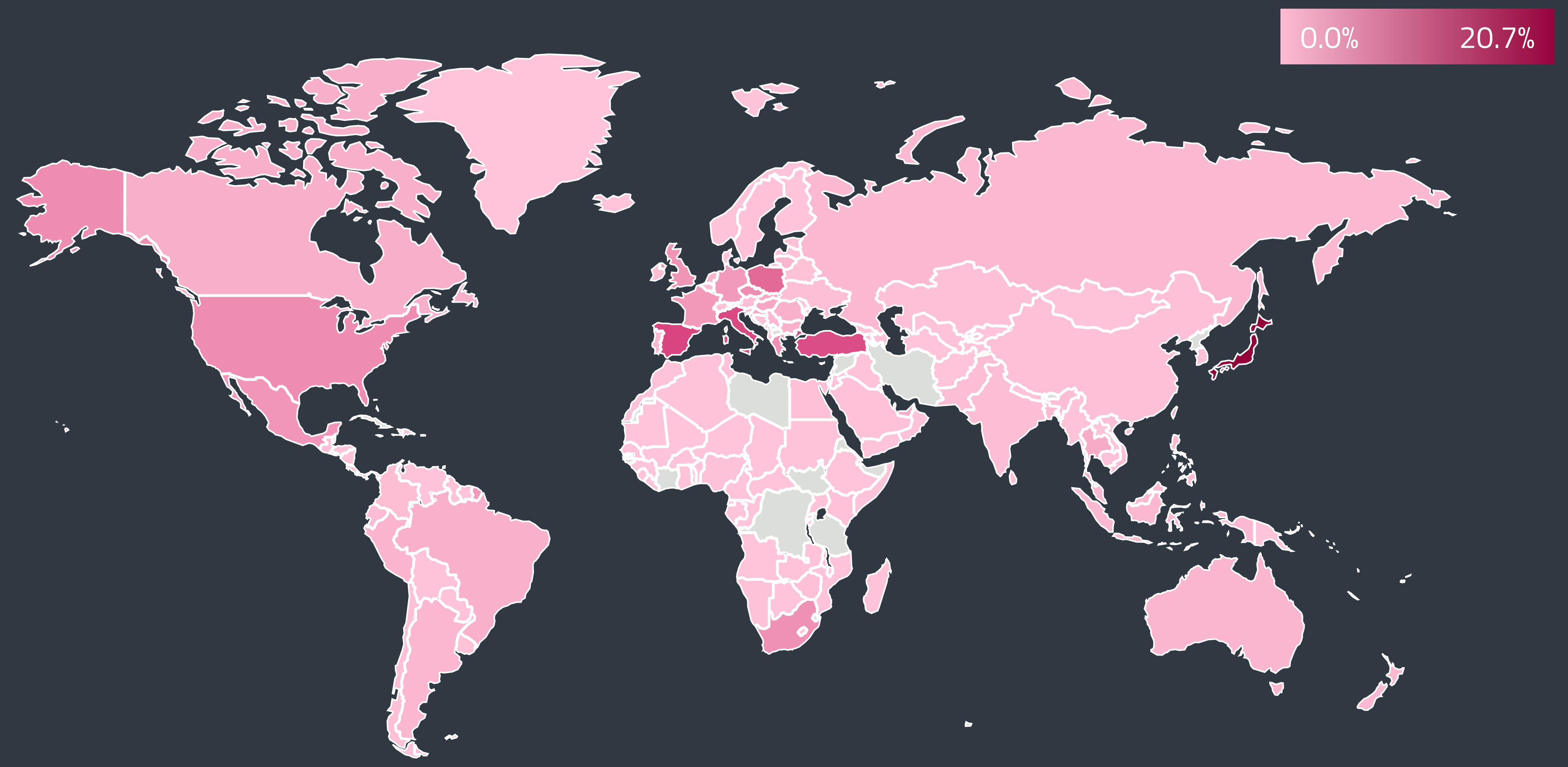
On the other hand, previously active phishing campaigns posing as the document-signing service DocuSign subsided in T1 2022, their detections declining by 75% compared to T3 2021.

Looking into the subject lines of the malicious emails detected in T1, the most common subject line was "EU Business Register 2022/2023", updated messaging of a long-circulating, widespread scam detected as PDF/Fraud. Through these emails, scammers attempt to trick recipients into paying a large fee for their inclusion into a purported database of European business subjects.

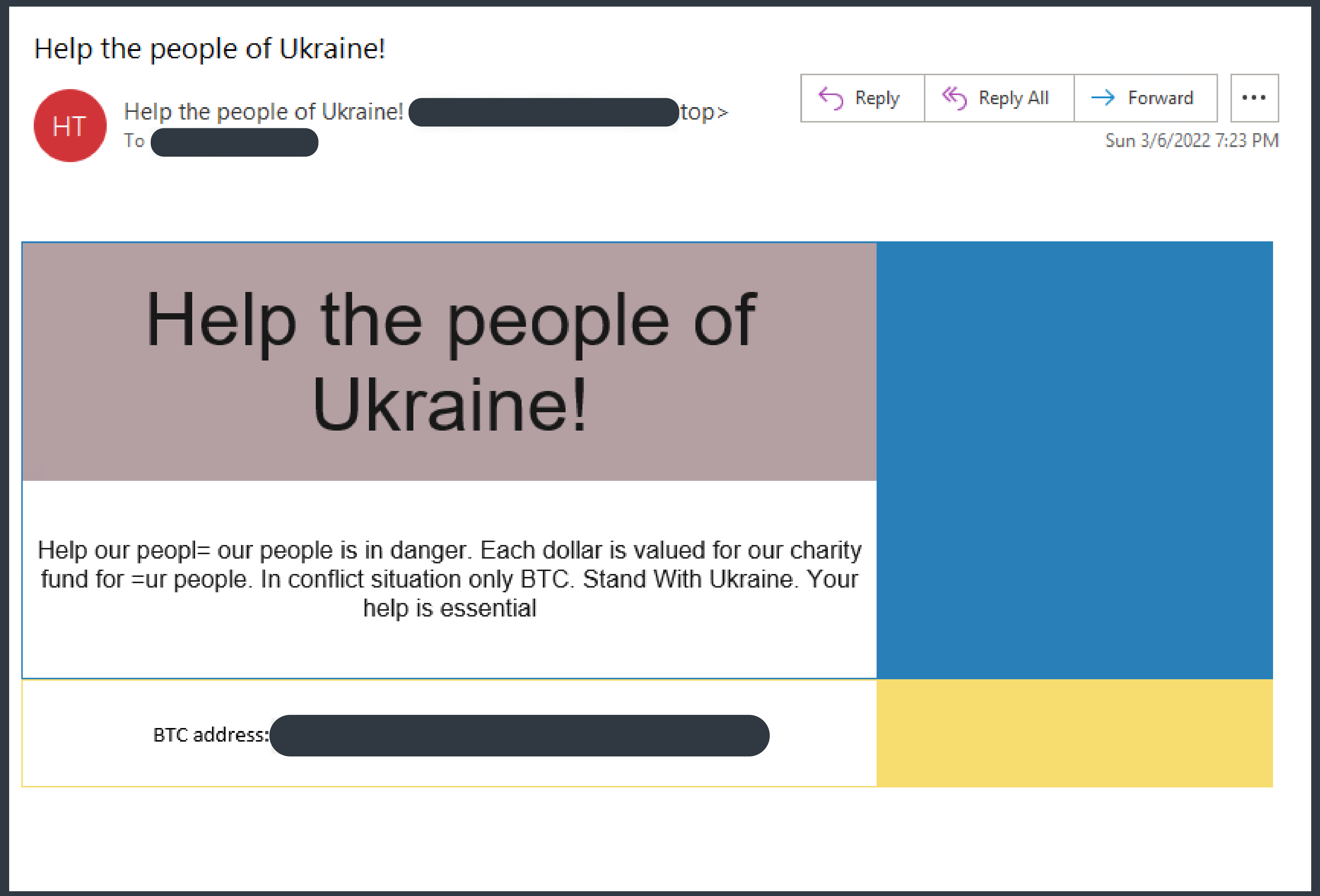
Beyond the usual topics of malicious email subjects (such as payments, orders, and deliveries), which remained largely unchanged, there was a notable increase in malicious travel-themed emails in T1. These increased more than sevenfold compared to T3 2021, but still represented less than 1% of all identified malicious email messages.

As for the file types of malicious attachments detected in emails, executables remained the leading format, followed by script files and Office documents. While the share of executables was reduced in T1, script files and Office documents grew more prevalent. Office files doubled their share this period as a result of the aforementioned Emotet activity – but this trend is expected to be reversed in the following periods.

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



Global distribution of Email threat detections in T1 2022


Help the people of Ukraine!

Help the people of Ukraine! [redacted]top>
To [redacted]

Sun 3/6/2022 7:23 PM

Help the people of Ukraine!

Help our peopl= our people is in danger. Each dollar is valued for our charity fund for =ur people. In conflict situation only BTC. Stand With Ukraine. Your help is essential

BTC address: [redacted]

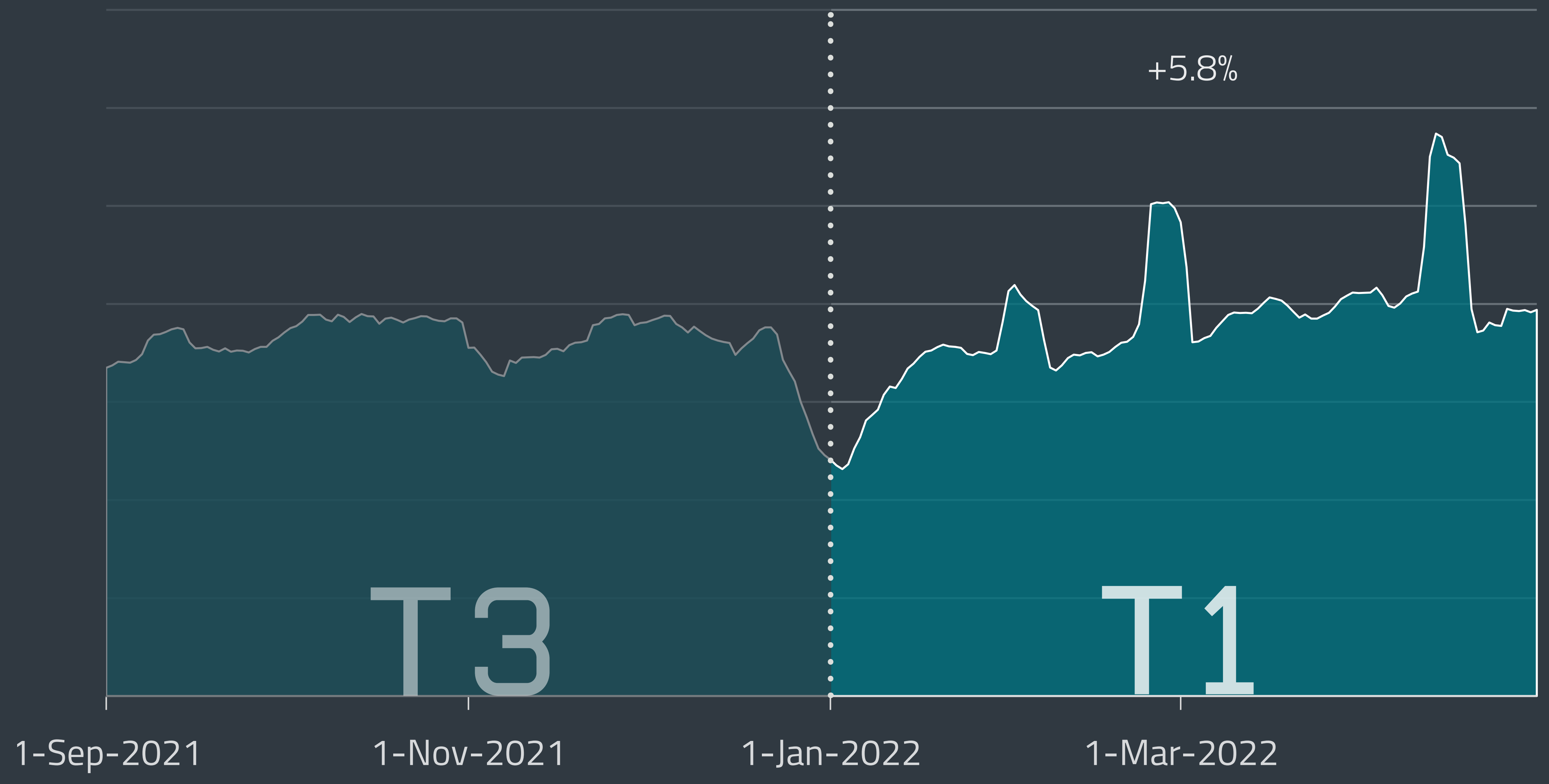
Example of a spam email exploiting the war in Ukraine

Spam detections increased by 5.8% in T1, mostly due to two large spikes, the first on February 24 and the second on April 12. ESET telemetry recorded an overall increase in email messages scanned around these dates, but while the total numbers of emails scanned increased up only to 37% against the T1 average, spam levels jumped between two- and threefold. Other than these upticks, spam levels remained fairly steady over this period.

The February 24 spike coincides with the beginning of Russia's invasion of Ukraine. As noted in the *Web threats* section, scammers didn't shy away from exploiting the war and immediately started taking advantage of people trying to support Ukraine, using fictitious charities and fundraisers as lures.

Looking at the geographic distribution of spam sources according to ESET telemetry, 16% of spam emails detected in T1 originated from the United States, followed by China (13.2%), Japan (9.9%), Poland (6.5%), and France (5.7%) – the same top five countries as in the previous period. The share of spam in all emails sent was highest in China (66%), followed by Singapore, South Korea, Russia ,and Argentina, where between 23% and 34% of emails sent constituted spam.

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 T3 2021 – T1 2022, seven-day moving average

ANDROID THREATS

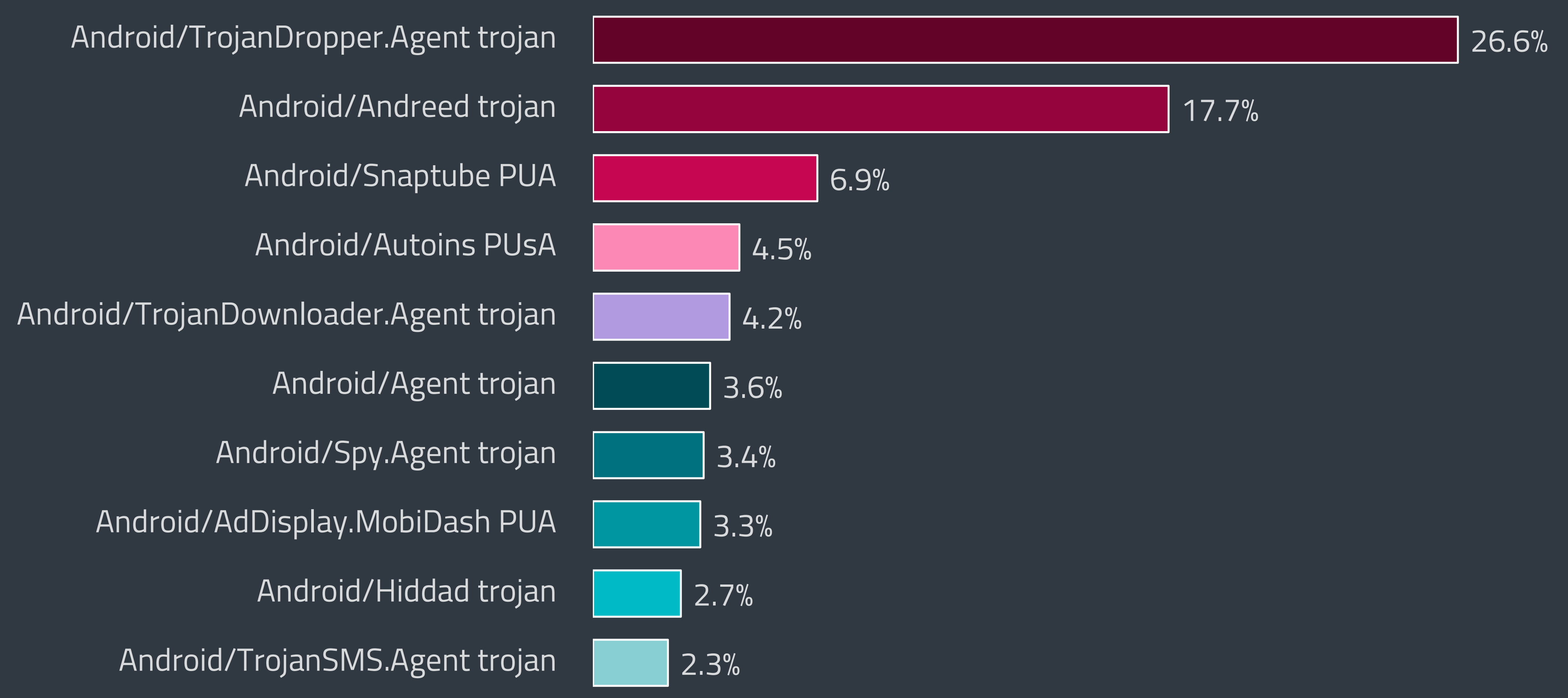
Android threat detections grew slightly in T1 2022; HiddenApps continued to be the most prevalent type of Android threat while Spyware experienced significant growth.

Compared to the last four months of 2021, Android detections saw a slight growth of 8% in T1 2022; however not all Android threat categories experienced increased numbers of detections.

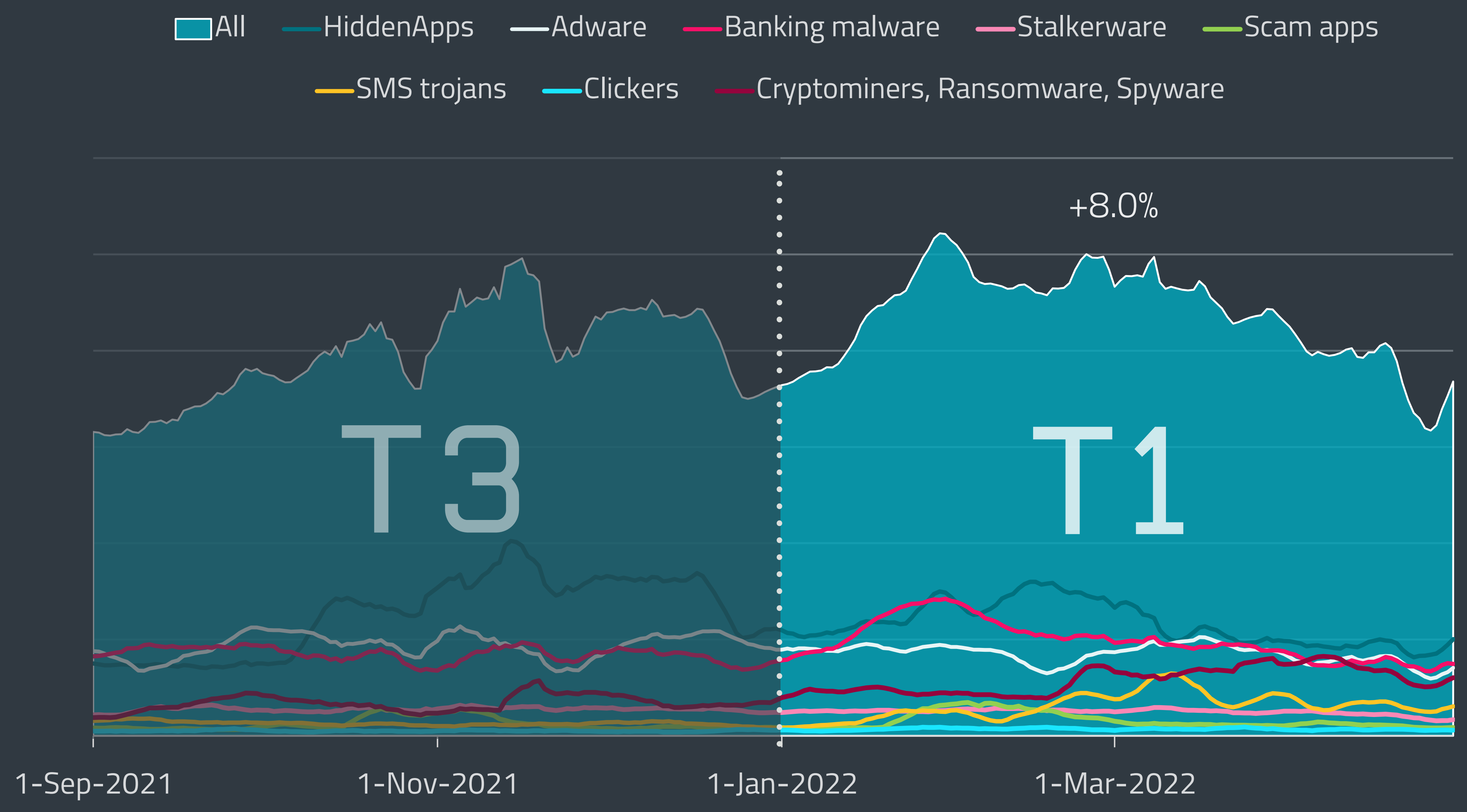
HiddenApps, deceptive apps that hide their own icons, continued to be the most prevalent type of Android threat according to ESET telemetry; although their detections decreased by 10.2% in T1.

Another Android category that experienced a decrease in detection numbers is Adware (-11%), continuing the trend started in T3 2021. Stalkerware detections also dropped compared to T3 2021, by 11.7%. ESET monitors this threat category separately and not as a part of Spyware, even though Stalkerware is a type of consumer-grade spyware.

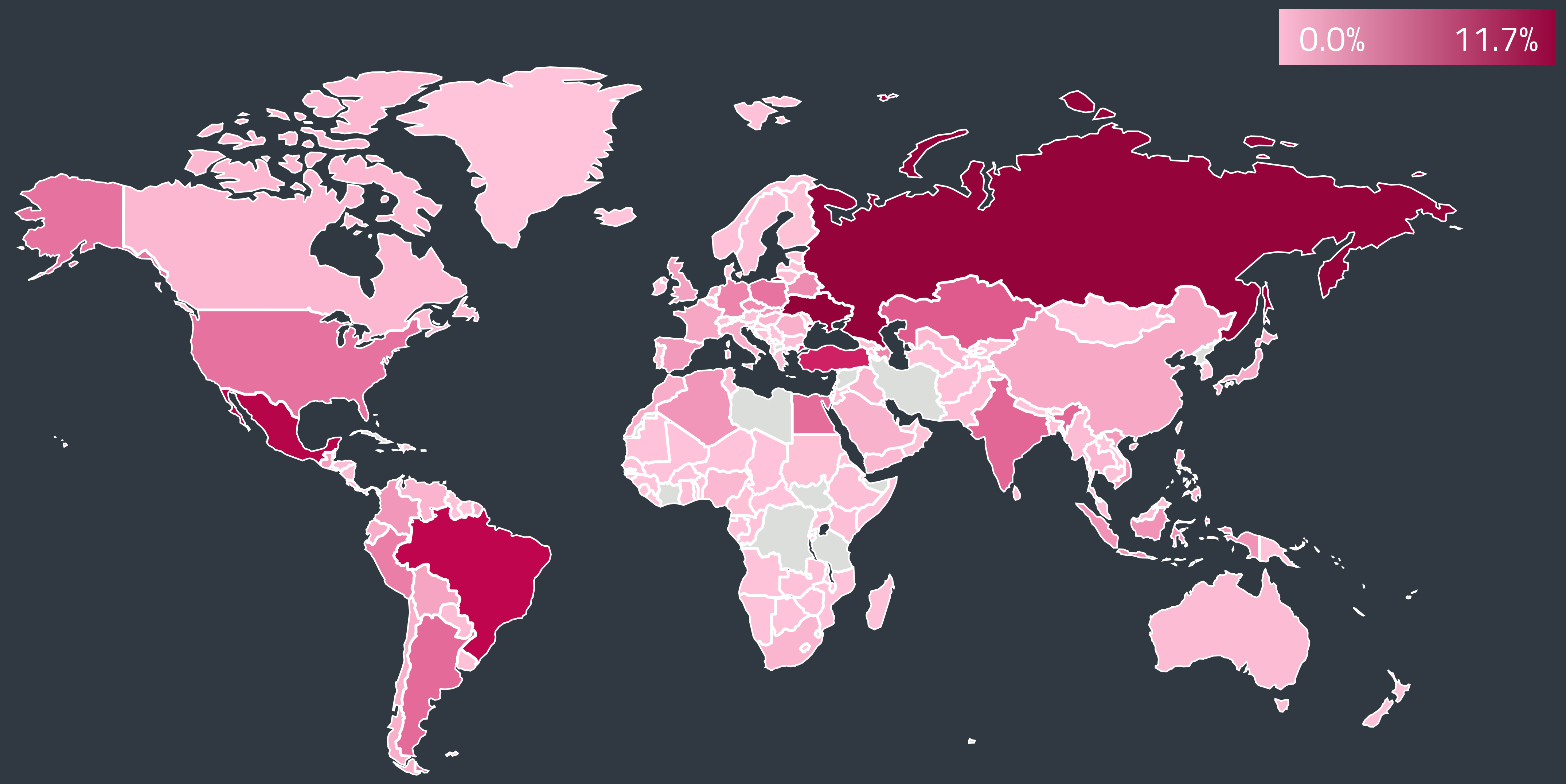
It is important to repeat the findings of ESET Research's *in-depth analysis of stalkerware* [93], because an investigation by TechCrunch revealed that some of the stalkerware apps identified in ESET's previous analysis are in fact controlled by one operator that is, *according to TechCrunch* [94], a



Top 10 Android threat detections in T1 2022 (% of Android threat detections)



Detection trends of selected Android threat categories in T3 2021 – T1 2022, seven-day moving average



Global distribution of Android threat detections in T1 2022

Vietnam-based company called 1Byte. Just as ESET Research showed, these stalkerware apps tend to be riddled with vulnerabilities, exposing not only the victim but also the buyer of these apps.

Android Ransomware also saw a significant fall in detections in T1 2022 (-49.3%). This drop can be explained by the high volatility of cryptocurrencies that are usually used as ransom payments, which means it is difficult to make any predictions about any threats using cryptocurrencies.

The category that saw the biggest growth was Spyware (170.2%). This type of threat can access a variety of smartphone functions, such as audio and video recordings, and the huge rise in its detections means that the attackers can find various ways to monetize personal or even company data accessible through an Android device. Researchers from *Lab52* [95] identified spyware that establishes complete control over the device and its contents if permissions of the malicious app are accepted by the user. ESET detects this threat as "a variant of Android/Spy.Agent trojan", which is number seven in the top 10 Android threat detection list.

Researchers Joel Reardon and Serge Egelman at *AppCensus* [96] discovered several apps available on Google Play that contained malicious code to harvest phone numbers, email addresses and location data. Some of them had been downloaded more than 10-million times before Google took them down. However, they later appeared again in the store, albeit without the software development kit (SDK) responsible for the data collection. The researchers connected these apps with a Panama-based company which is, according to the *Wall Street Journal* [97] (paywall), linked to a US defense contractor that provides cyberintelligence services.

Further, other spyware, installed thanks to a new distribution vector by more than 100,000 users, was described by *Pradeo* [98]. The Facestealer spyware was available on the Google Play store as a cartoon photo tool and used social engineering to steal Facebook credentials. Google later removed the malicious app from its store.

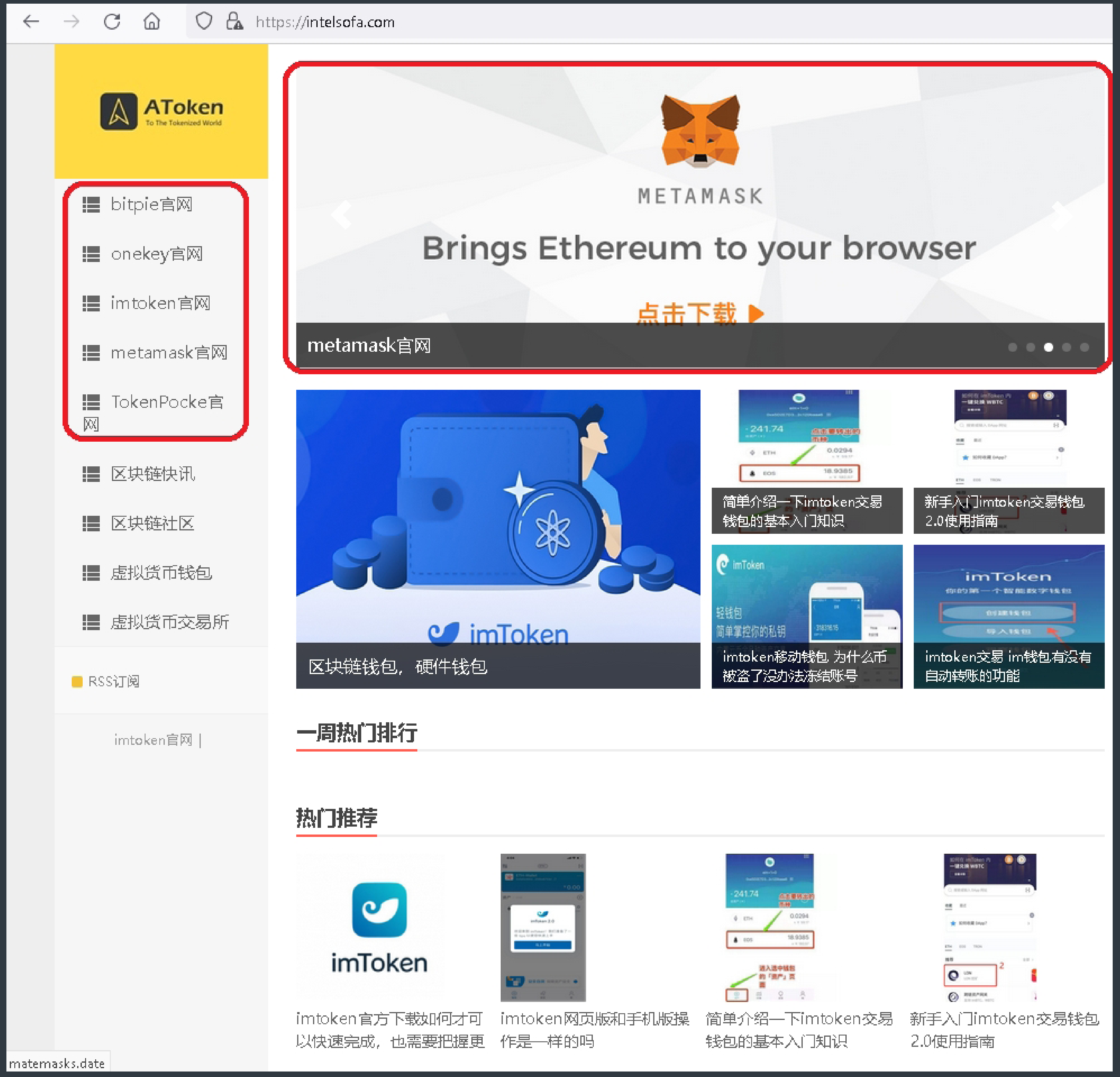
EXPERT COMMENT

Spyware does not directly steal money from its victims; instead, it steals as much sensitive data from the affected mobile device as possible. The attacker then aggregates a package with data from a large number of victims and sells it on the black market either to the highest bidder, or basically to anyone. The victims might then never know when their data will be abused and in many cases, they might be surprised years later and not be able to connect their personal identity theft to any action that might have led to this. Therefore, most people affected by this recent rise in spyware detections will not yet know they have become victims.

Lukáš Štefanko, ESET Malware Researcher

Other Android categories that experienced a significant rise in detections were Scam Apps (27.7%), Clickers (31.6%) presenting a form of ad fraud, and SMS trojans (145.20%). This threat, which is most visible on the mobile monthly bill of affected users, is represented in the top 10 Android threat list by Android/TrojanSMS.Agent.

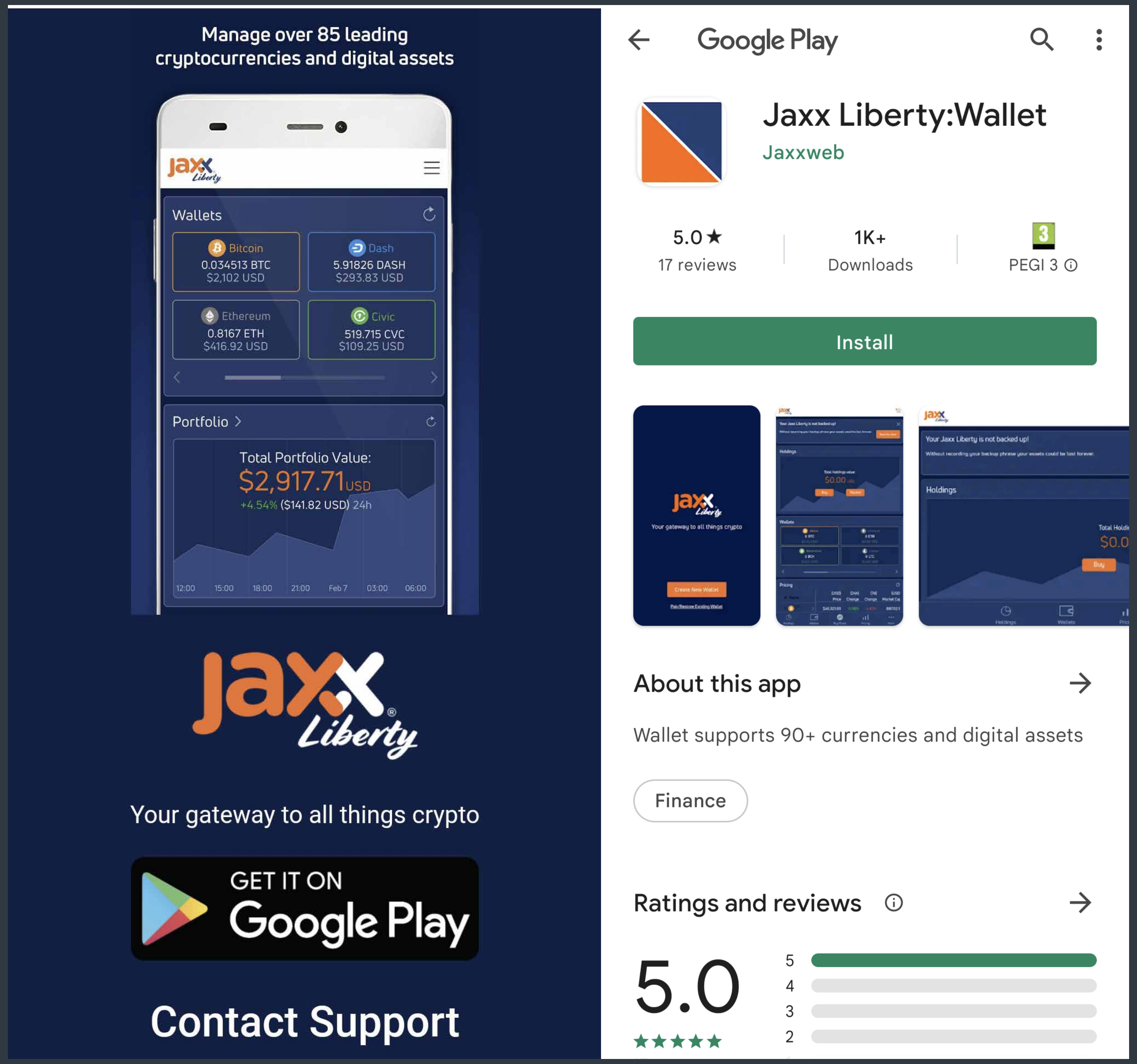
Detections of Android Cryptominers increased twofold in T1 2022, however, their overall numbers on the Android platform are too low to judge whether this growth is of any significance. As ESET researchers have pointed out many times in the past, crypto-threats are dependent on sometimes highly volatile currencies and when bitcoin appeared to be slowly regaining its value after several bad months, *ESET researchers uncovered* [33] a sophisticated scheme that distributes trojanized Android and iOS apps posing as popular cryptocurrency wallets.


https://intelsofa.com
AToken
To The Tokenized World
bitpie官网
onekey官网
imtoken官网
metamask官网
TokenPocke官网
区块链快讯
区块链社区
虚拟货币钱包
虚拟货币交易所
RSS订阅
imtoken官网 |
METAMASK
Brings Ethereum to your browser
点击下载
metamask官网
imToken
区块链钱包，硬件钱包
简单介绍一下imtoken交易钱包的基本入门知识
新手入门imtoken交易钱包2.0使用指南
imtoken移动钱包 为什么币被盗了没办法冻结账号
imtoken交易 im钱包有没有自动转账的功能
一周热门排行
热门推荐
imToken
imtoken官方下载如何才可以快速完成，也需要把握更
imtoken网页版和手机版操作是一样的吗
简单介绍一下imtoken交易钱包的基本入门知识
新手入门imtoken交易钱包2.0使用指南
matemasks.date

Page containing advertisement for fake wallets

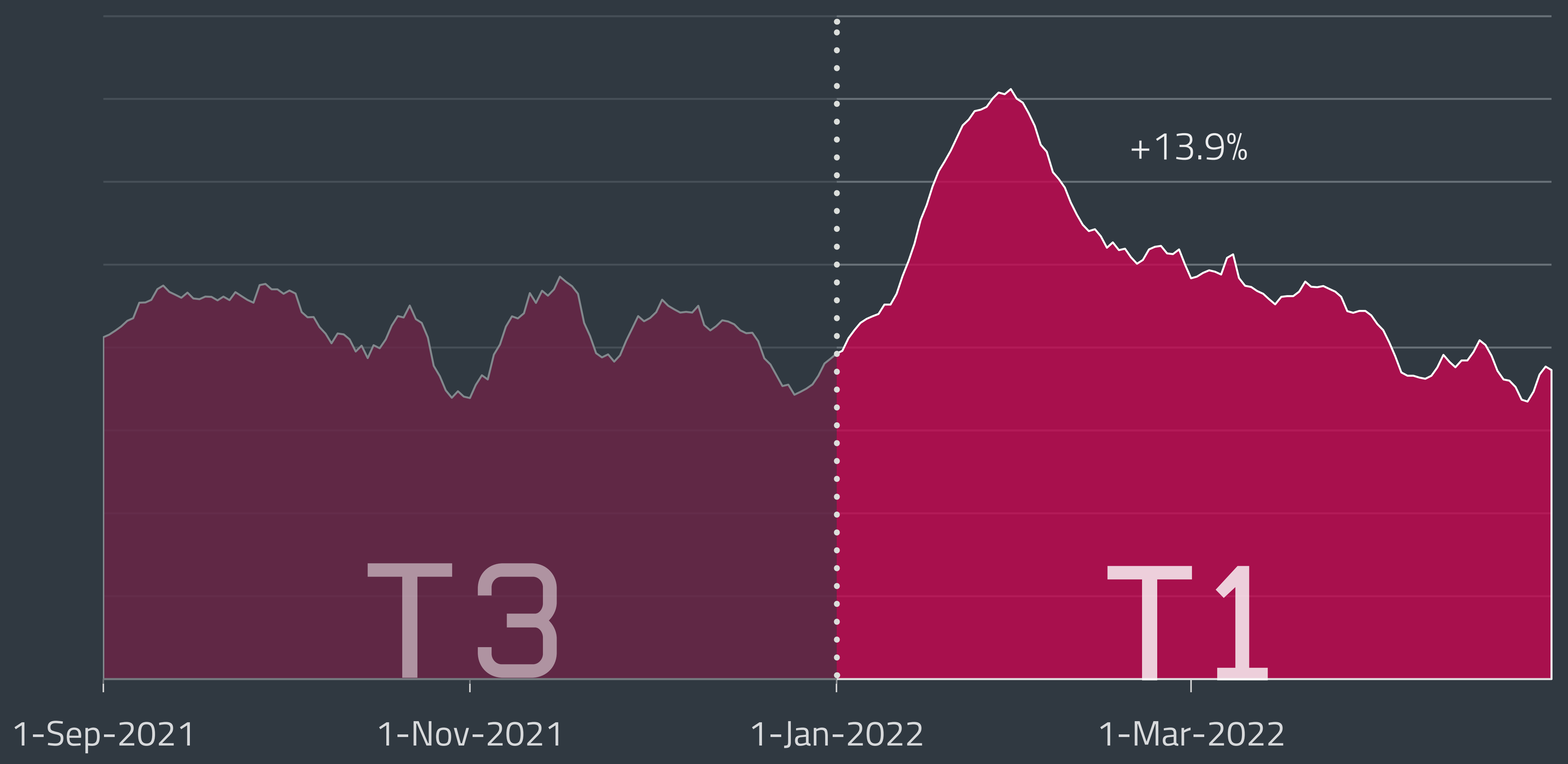
These malicious apps are able to steal victims' secret seed phrases by impersonating Coinbase, imToken, MetaMask, Trust Wallet, Bitpie, TokenPocket, or OneKey. This is a sophisticated attack vector since the malware author carried out an in-depth analysis of the legitimate applications misused in this scheme, enabling the insertion of their own malicious code into places where it would be hard to detect while also making sure that such crafted apps had the same functionality as the originals. All of the dozens of trojanized cryptocurrency wallet apps detected by ESET were distributed through websites mimicking legitimate services. To make things worse, their source code was leaked online, which means it might attract other attackers.

ESET researchers also found malicious applications impersonating the legitimate Jaxx Liberty Wallet app in the Google Play store. One of the apps used a fake website mimicking Jaxx Liberty as a distribution vector. As the threat actor behind this malicious app managed to place it in the official Google Play store, the fake website redirected the user to download its mobile version from the Google Play store and didn't have to use a third-party app store as an intermediary. Google removed 13 of these apps from its store in January 2022.



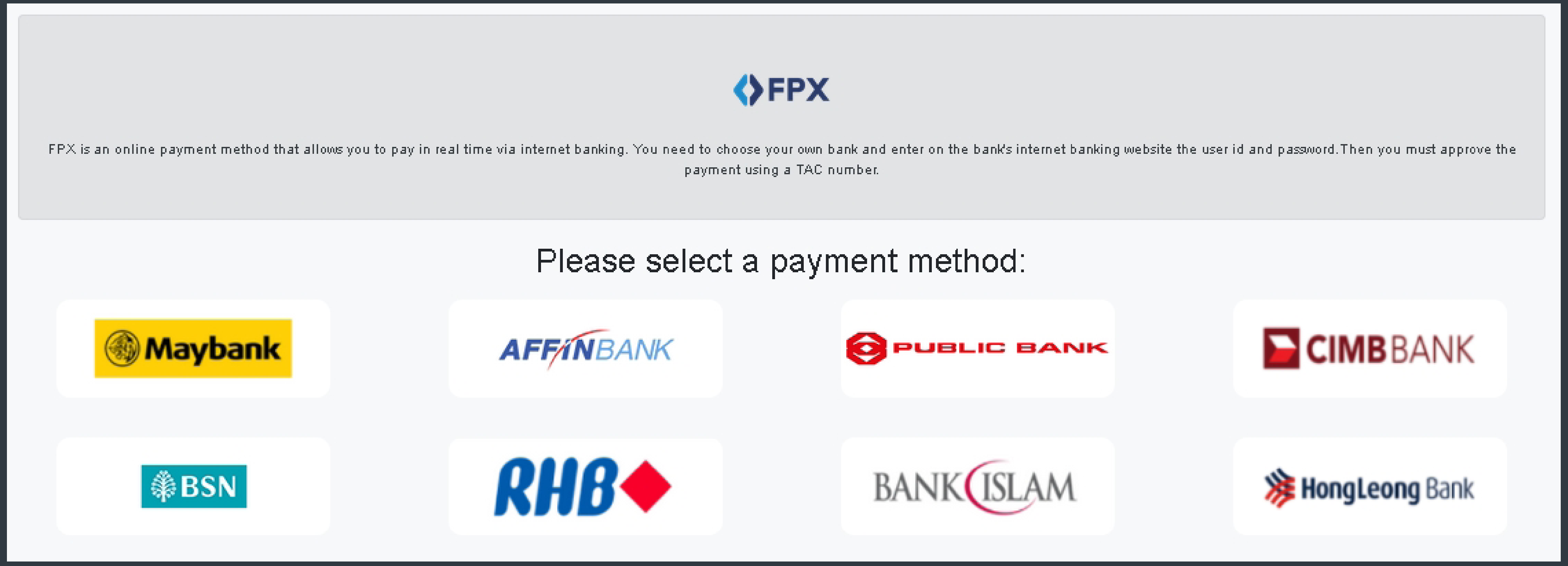
Wallet supports 90+ currencies and digital assets

Fake website redirects the user to install the fake app from Google Play



Android Banking malware detection trend in T3 2021 – T1 2022, seven-day moving average

Android Banking malware grew by 13.9% in T1 2022, after experiencing a decline in T3 2021. In the Android top 10, it was represented by Android/TrojanDropper.Agent. One of the Android banking malware cases that ESET researchers analyzed in T1 was a campaign targeting the customers of *eight Malaysian banks* [31]. The malware is distributed via copycat websites of legitimate services with the majority being cleaning services available in Malaysia.



FPX is an online payment method that allows you to pay in real time via internet banking. You need to choose your own bank and enter on the bank's internet banking website the user id and password.Then you must approve the payment using a TAC number.

Please select a payment method:

Malayan banks targeted by malicious apps

These copycat websites include buttons that claim to download apps from Google Play. However, these buttons do not actually lead to the Google Play store, but to malicious apps controlled by the attackers. The malicious apps pretend to offer goods and services for purchase while matching the interface of legitimate stores. At the payment step, victims are presented with a fake payment page and are asked to select one of eight Malaysian banks and then enter their online banking credentials.

Many other researchers also discovered new Android banking malware or new distribution vectors. *Check Point* [99] found Sharkbot disguised as security apps on the Google Play store, *Bitdefender* [100] identified new FluBot and TeaBot campaigns spreading through SMS messages asking "Is this you in this video?", while *Threat Fabric* [101] researchers analyzed another piece of Android banking malware – Medusa – that started a distribution scheme using the same SMS phishing service as FluBot. They *also* [102] discovered a new threat they dubbed Xenomorph, targeting users of 56 different European banks. All of the aforementioned threats are detected by ESET as variants of the Android/TrojanDropper.Agent trojan. According to ESET telemetry, countries with the biggest detections of this umbrella banking malware threat are Brazil, Mexico, Turkey, Argentina, and Ukraine.

And to show that Android can also suffer from high-impact vulnerabilities, *researchers at Tel-Aviv University* [103] discovered that Samsung phones were shipped with design flaws in Android's hardware-backed cryptographic key management services. The flaw affected millions of Samsung's flagship phones including the Galaxy S8, S9, S10, S20, and S21.

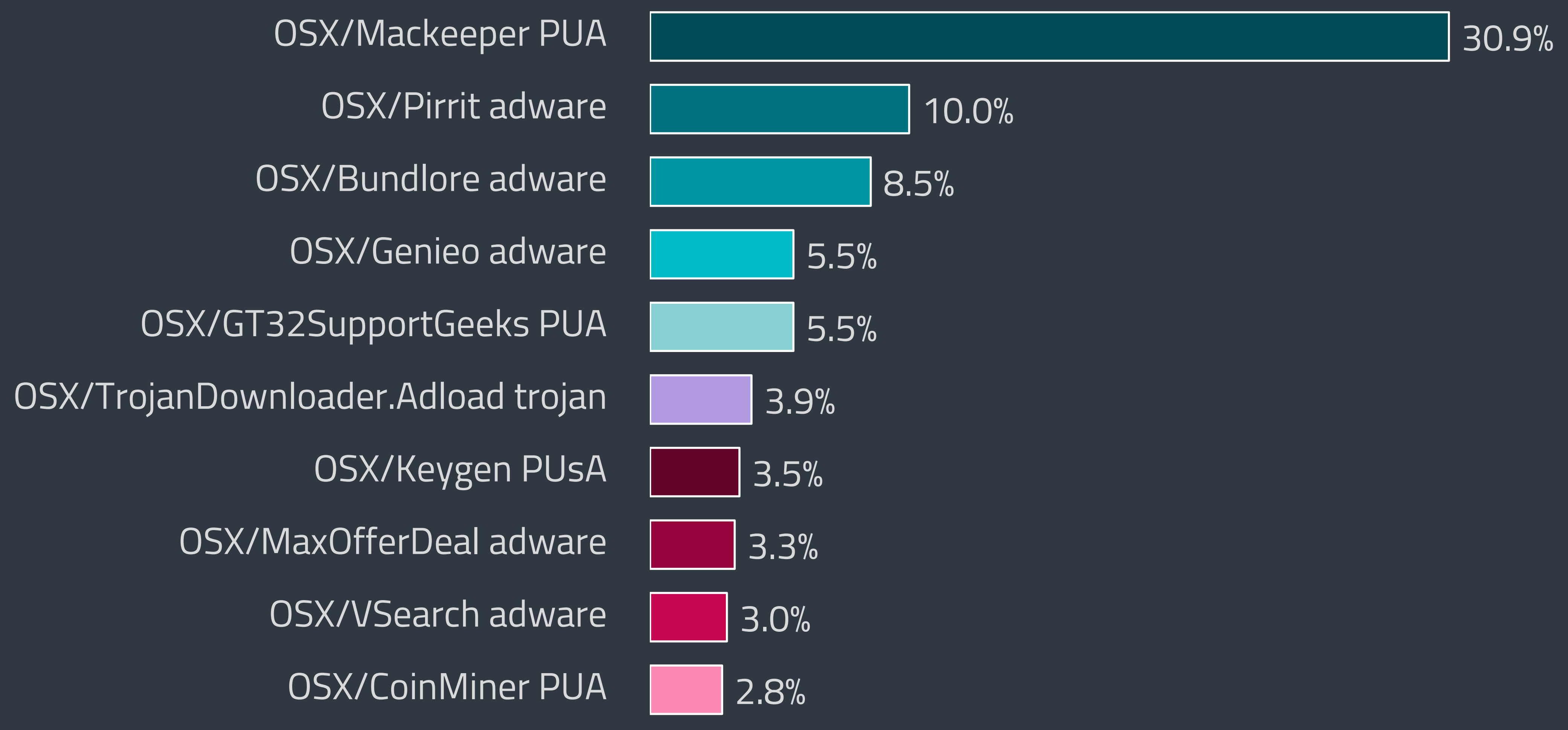
macOS AND iOS THREATS

macOS detection numbers saw a notable decline in T1 2022; compared to T3 2021 the biggest decrease was visible in the Trojans category.

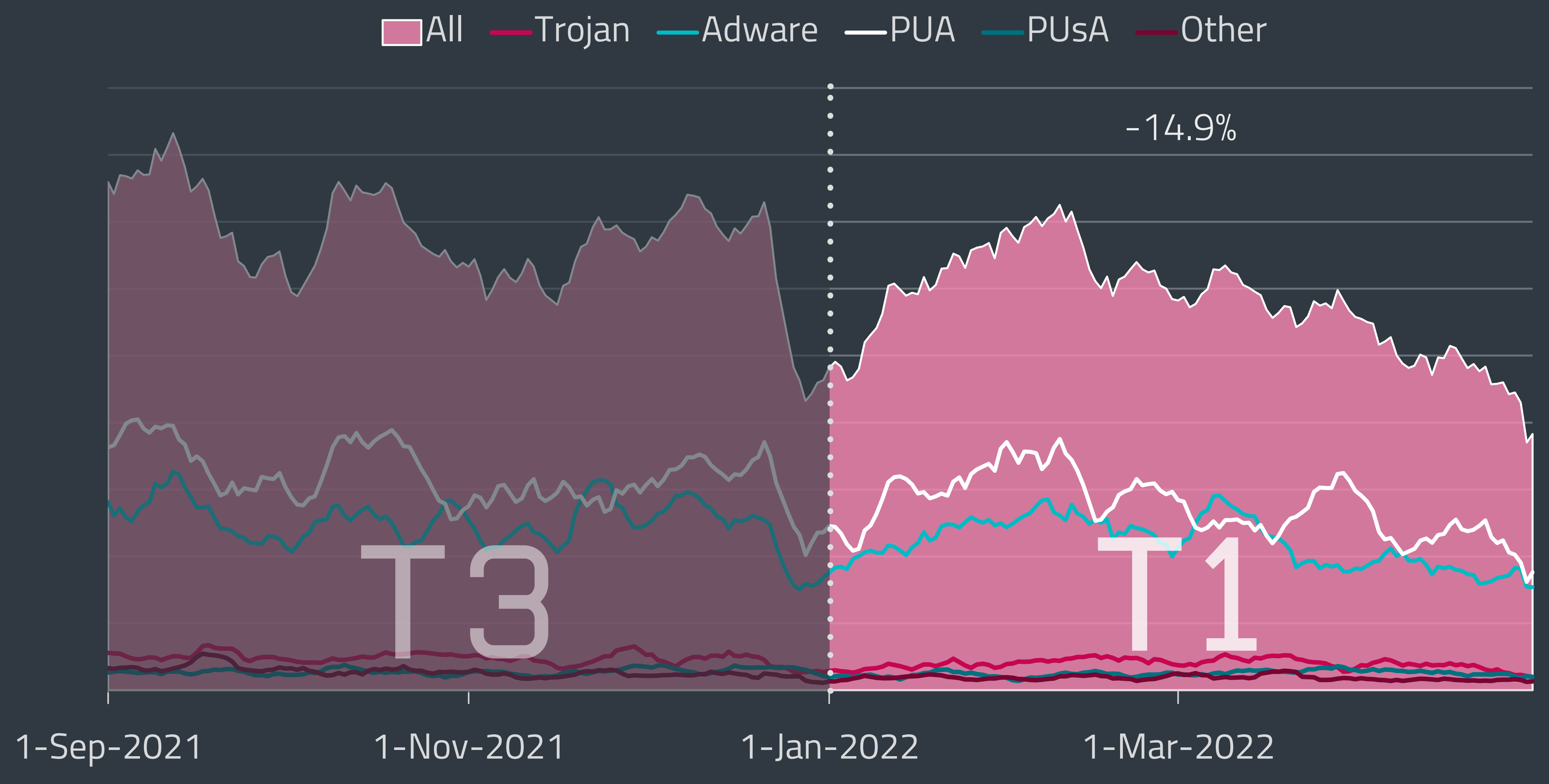
In T1 2022, detections of macOS threats saw a notable decline (14.9%) and, what's more, a notable decline was detected in all monitored macOS threat categories. Trojans experienced the biggest decline (-18.8%) compared to T3 2021, followed by Potentially unwanted applications (PUAs, -15.6%). This type of threat is the most widespread hazard targeting Mac systems; it accounted for around 47% of all macOS detections during the first four months of 2022, visible also in the top 10 macOS threats according to ESET telemetry. The number one macOS detection – OSX/Mackeeper PUA – has been the same since our Q1 2020 Threat Report, but now with higher prevalence. In T1 2022 it was responsible for more than 30% of all macOS threat detections. This PUA, displaying unsolicited ads, was most active in the United States and Japan.

Other examples of these types of apps – installed by users after being tricked by the description of an allegedly useful program – are OSX/GT32SupportGeeks PUA and OSX/CoinMiner PUA, which are number five and number ten on the top 10 macOS threat list. The first one is often presented as a macOS performance scanner that reports alleged issues on the system; the second one uses the system's resources to mine digital currency.

Adware (-13.8%) and Potentially unsafe applications (PUsAs, -12.7%) also declined in T1, with Adware being the second most prevalent macOS threat in T1 with 38% overall prevalence. In the top 10 macOS threat list, it is represented by OSX/Pirrit, OSX/Bundlore, OSX/Genieo, OSX/MaxOfferDeal, and OSX/VSearch. OXS/Bundlore is notoriously known for "bundling" adware applications with legitimate apps, while OSX/Genieo, OSX/MaxOfferDeal, and OSX/VSearch intercept internet searches. All of the above-mentioned adware apps display intrusive ads.



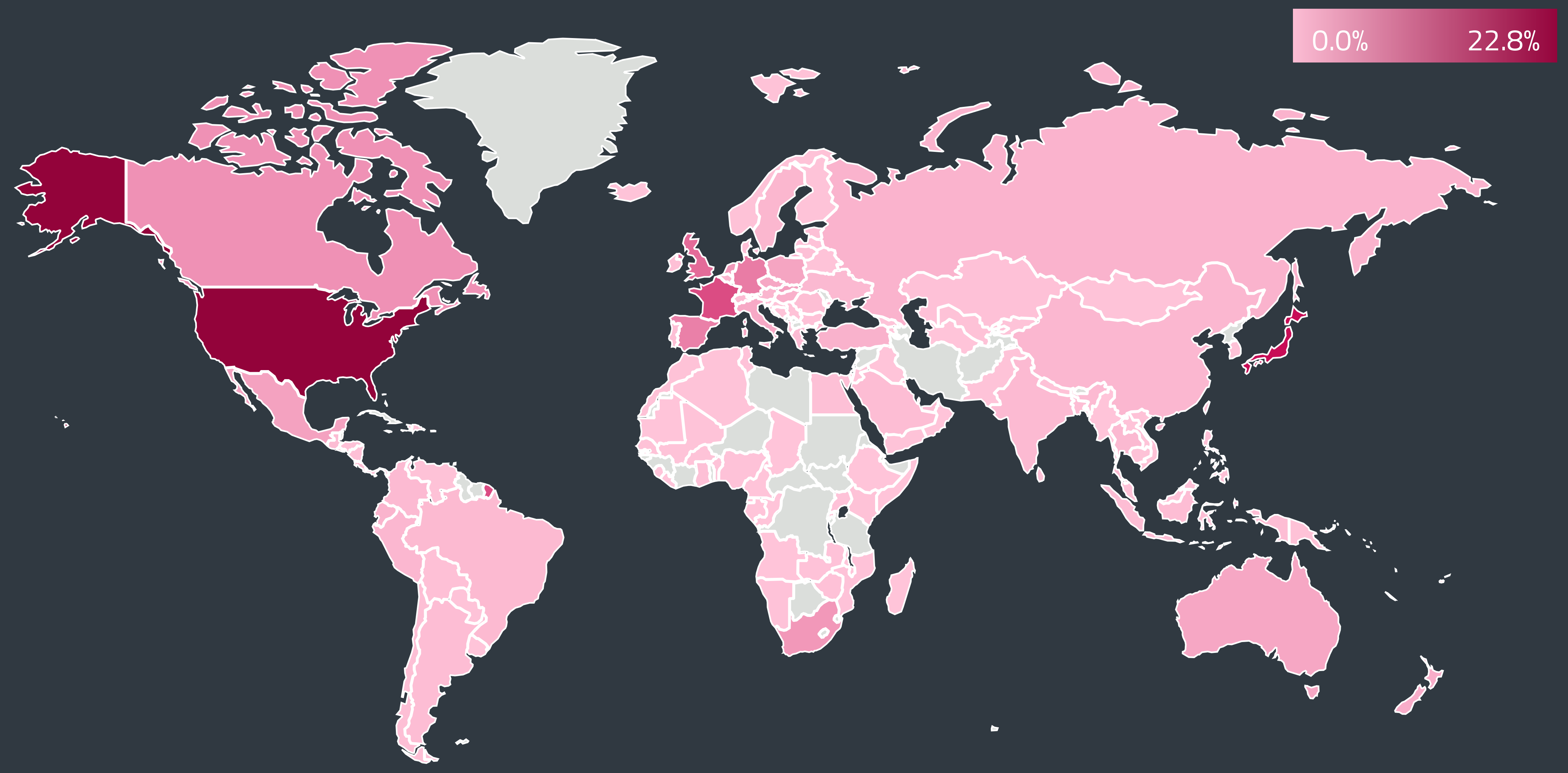
Top 10 macOS threat detections in T1 2022



macOS threat detection trend in T3 2021 – T1 2022, seven-day moving average

According to ESET telemetry, the most macOS detections in T1 2022 were found in the United States, with 21.6%, followed by Japan (12.8%), the United Kingdom (7.2%), South Africa (5.9%), and France (5%). The dip visible around the end of 2021 and the beginning of 2022 is similar to the one detected the year before, and could be attributed to this specific time of the year in which people around the world celebrate various religious and cultural festivities and simply don't use their computers that often.

It is important to note that, for the purposes of these Threat Reports, to describe and monitor threats faced by macOS systems in a more real-world way, we changed the methodology behind the analysis of macOS threat prevalence at the turn of the year. However, data from the previous period was also recalculated so that this report is able to analyze comparable data. And while the overall number of macOS detections is indeed decreasing, companies, organizations, and high-profile individuals should keep in mind that if a target is interesting enough, threat actors or APT groups will also deploy malware targeting non-Windows systems.



Global distribution of macOS threat detections in T1 2022

The latest ESET Research discovery of a case like this is a threat *compiled for both Intel and the newer Apple silicon processors* [104] used in the Mac lineup. This malware, detected by ESET as OSX/NukeSped.N, is an executable disguised as a job description document and ESET researchers think it is part of a campaign by the infamous Lazarus APT group, which has extensive experience in hiding malware in fake job lures.

At the beginning of the year, ESET researchers published their insights about a compromised Hong Kong pro-democracy radio station website that was serving a Safari exploit that installed cyberespionage malware on visitors' macOS devices. *DazzleSpy* [46], as it was dubbed by ESET, is macOS malware previously unseen by ESET telemetry. Its features include gathering information about the system; searching, downloading and uploading files; exfiltrating the macOS keychain; and providing access for the perpetrator via remote desktop. Comments in its code suggest it could also exploit iOS and PAC-enabled (Pointer Authentication Code) devices such as the iPhone XS and newer models. Given the complexity of the exploits used in this campaign, ESET researchers assess that the group behind this operation has strong technical capabilities.

EXPERT COMMENT

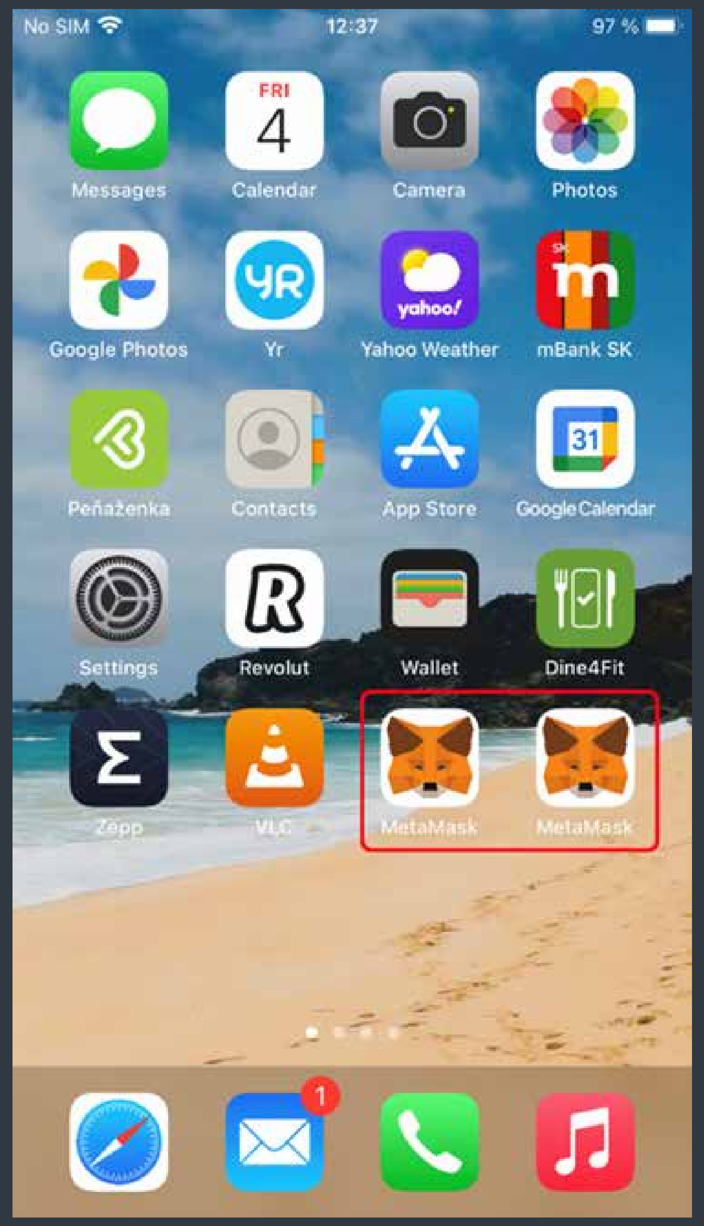
Seeing macOS threats declining should be a positive sign for users. However, as is shown not only by our own research, companies and organizations should stay on the lookout for targeted macOS malware, protect their systems accordingly and try to increase employee awareness also about non-Windows-based threats. Companies simply don't have homogenous networks and it takes only one device to be compromised, regardless of its operating system.

Marc-Etienne M.Léveillé, ESET Senior Malware Researcher

Another example of a cross-platform threat was discovered by researchers at Intezer. Called *SysJoker* [105], the macOS version is described more thoroughly by *Objective-See* [106]. SysJoker masquerades as a system update and is part of an espionage campaign; Intezer assess this backdoor is after specific targets. ESET telemetry suggests the same – SysJoker has a low prevalence with detections mainly in Asia and the United States. *Volexity* [107] also discovered a new macOS variant of a feature-rich, multiplatform malware family, dubbed Gimmick. It uses public cloud hosting services (such as Google Drive) for command-and-control channels.

Despite their built-in security features, iOS devices are also targets of cyberthreats and targeted attacks. As is described in the *Android* section, ESET researchers discovered *maliciously patched cryptocurrency wallets* [33] targeting not only Android but also iOS devices to steal victims' seed phrases. These malicious apps are not available on Apple's App Store; they must be downloaded and installed using configuration profiles, which add an arbitrary trusted code-signing certificate. Using these profiles, it is possible to download applications that are not verified by Apple, from sources outside the App Store.

It means the weakest security link in such cases is the user, but not every threat can be detected by safe user behavior and security features…such as the Pegasus phone hacking tool mentioned in ESET Threat Reports several times in the past. As new revelations come to light about the latest victims of this NSO Group spyware tool, for instance the *Spanish prime minister* [108] and *Finnish diplomats* [109], Reuters *uncovered* [110] that a second Israeli spy firm – QuaDream – used exploits similar to those employed by NSO Group. Besides that, *Google's Project Zero* [111] published its own in-depth analysis of the ForcedEntry exploit that can remotely compromise an iOS device for the purpose of installing the Pegasus spyware. For a typical user, Pegasus is impossible to detect; however, Apple patched the underlying issues in September 2021. It means that updated devices should be secure, but the discovery of other vulnerabilities *shows* [112] that updating must be done on a regular basis, while hoping one will not be targeted by another zero-day exploit in the meantime.



Trojanized wallet successfully installed on iPhone

IoT SECURITY

Mirai-based botnets still wreak havoc. Russia's war in Ukraine affects IoT.

In 2016, the noose around the necks of the authors of Mirai was tightening, yet before the police arrested them, they published the source code online. Six years later, researchers still track many IoT botnets that either use the original code or are built upon it. Gafgyt, BotenaGo, or Enemybot are only some of the names that fall within this category in ESET telemetry.

If we leave out the separately tracked Mozi and ZHtrap, Mirai-based botnets were responsible for close to 7.3 million attacks in T1 2022. Of those, 26% were aimed at the United States, 7% at the United Kingdom, and 6% at Germany. When focusing on the unique IPs facing these attacks, most were found in Germany (14%) and the US (12%). Japan, Mexico, and the UK each accounted for 5%.

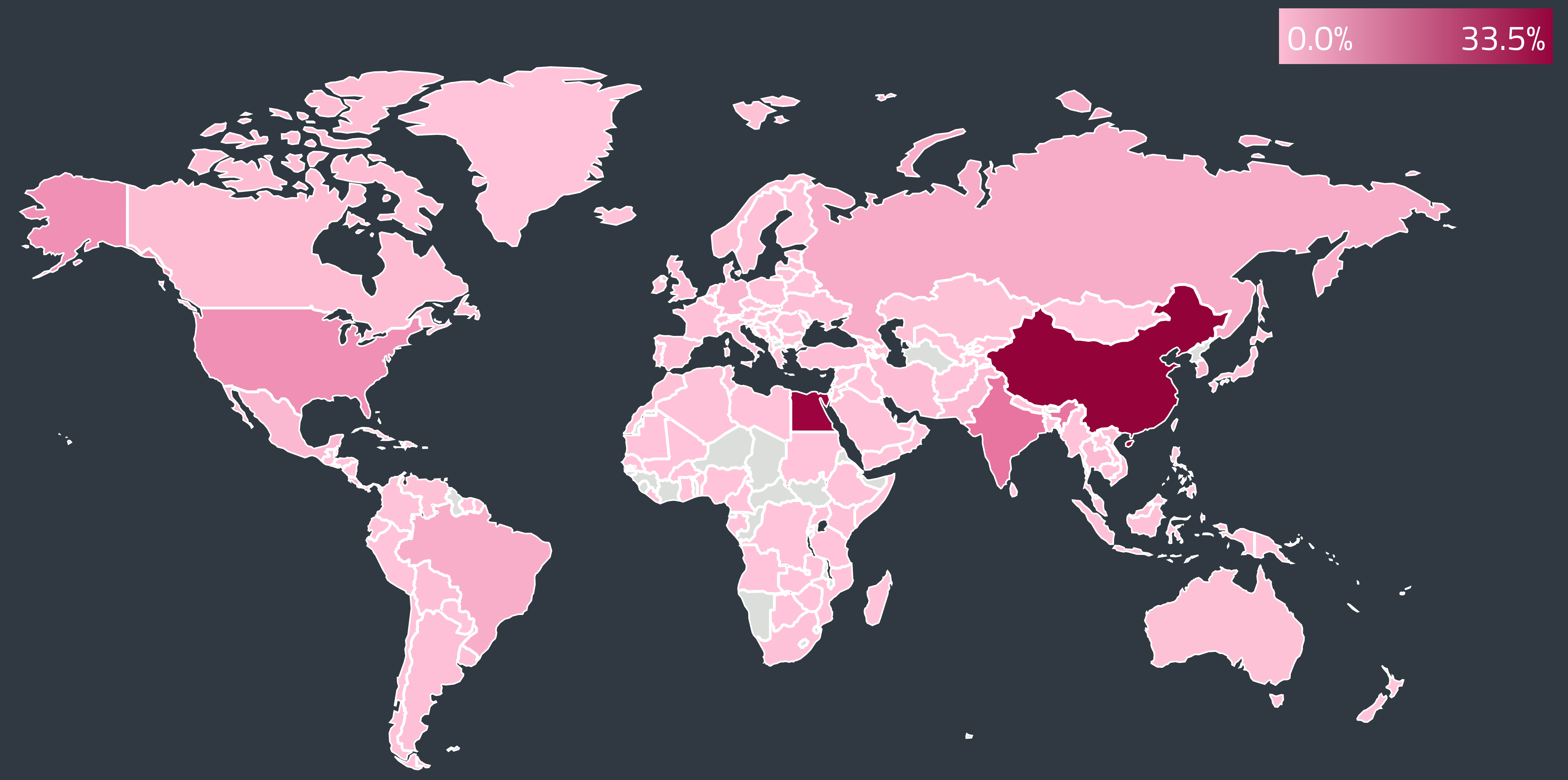
The origins of these attacks? The top three countries with the most *attackers' IPs* were China (33%), Egypt (30%), and India (7%). As for the largest amounts of malicious traffic produced, China leads the pack (22%), followed by Egypt (16%), South Korea (14%), and the US (14%). It's interesting that most of the 800+ payload servers – these being the servers delivering the final payload with their IPs embedded in the command injections in the exploits – were close to their victims, namely in the US (37%), the Netherlands (10%), and Germany (9%).

As for the spreading mechanism of Mirai-based botnets, the *ED 41471* [113] flaw – a shell command execution in MVPower DVR – was the most widespread, accounting for 84% of all attempts. A *Shodan search* [114] shows almost 67,000 such devices, although more than a third of them are tagged as honeypots. The second most exploited vulnerability was a 2017 command injection in ZyXEL P660HN routers (*CVE-2017-18368* [115]), amounting to 8% of attack attempts seen by ESET.

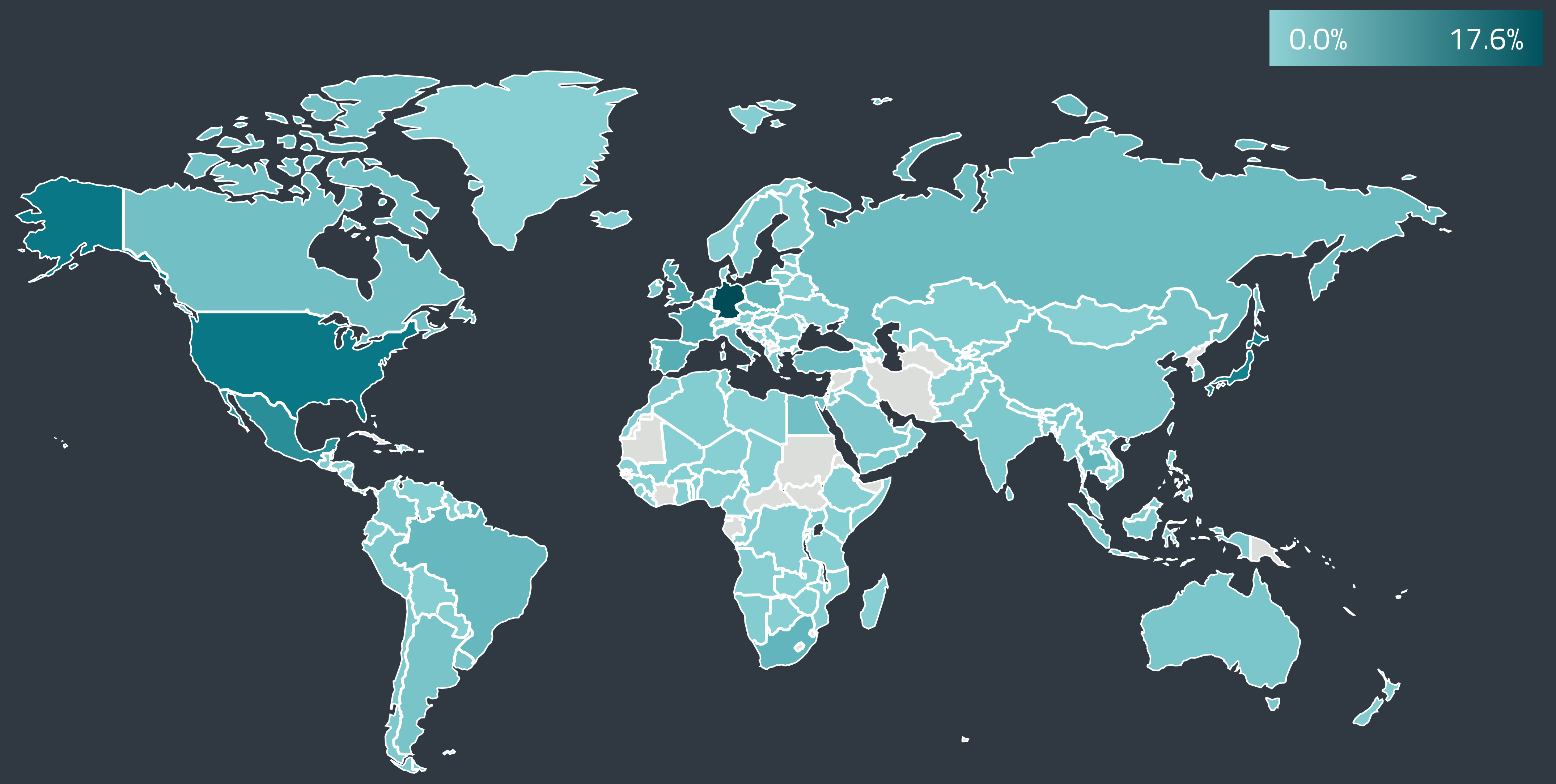
Another Mirai-based botnet tracked by ESET is ZHtrap. To broaden its ranks, its bots focused exclusively on *CVE-2015-2051* [116], a remote code execution flaw in the D-Link DIR-645 routers. ESET telemetry reported 106,000 attacks in T1 2022, a 9% increase in activity compared to T3 2021.

In T1 2022, ZHtrap's payload servers were most frequently seen in the Netherlands (41%), which is also the country where the highest number (29%) of the 106,000 detected attacks originated. The second most frequent source of malicious traffic was the US with 28%, followed by Romania with 12%, Germany with 11%, and Poland with 9%.

Although the US (13%), Germany (11%), and the UK (6%) led the list of unique IPs of ZHtrap targets, the biggest waves of the attacks made landfall in Taiwan (16%).



Global distribution of countries with IP addresses of Mirai-based bots in T1 2022



Global distribution of IP addresses targeted by Mozi botnet in T1 2022

EXPERT COMMENT

While Mirai started as a botnet targeting Minecraft infrastructure, it quickly evolved into a powerful botnet with global reach. The publication of its source code turned it into the basis of most new IoT botnets and gave birth to many mods, improvements, and additional features not seen in the original.

Mirai-based botnets also demonstrate why people need to patch their publicly accessible smart devices and systems. Devices past their ends-of-life and those that still sport patchable vulnerabilities are the prime targets enabling the continual spread of this threat.

Strong passwords and proper configuration are also key in preventing Mirai-like attacks, as the botnets themselves often brute-force their way into the weakly protected and exposed command line services such as Telnet and SSH.

Milan Fránik, ESET Malware Researcher

And then there is the biggest IoT botnet tracked by ESET, named Mozi. Its operators allegedly were *arrested* [117] by Chinese authorities in 2021, yet the botnet seems to survive and propagate further on its own – as any brain-eating zombie in a world full of vulnerable humans would.

In T1 2022, ESET detected close to 500,000 unique IPs compromised by Mozi, 11% less than in T3 2021. The geolocation of the attacker IPs was predominantly Chinese (59%) and Indian (30%). As for the targeted IPs, Germans were the most frequently hit with 17%, followed by victims in the US (8%) and Japan (7%).

If the number of attacks is considered, Mozi was detected 5.6 million times, a 6% growth compared to T3 2021. Close to a third of the attacks (30%) had to be fended off by the US.

The distribution of Mozi relied on the same intrusion vectors as in T3 2021, namely exploitation of vulnerabilities in Netgear DGN devices (EDB-25978), DASAN routers (CVE-2018-10562), D-Link routers (CVE-2015-2051), and Jaws web servers (EDB-41471). ESET data shows an increase in Mozi activity, detecting its attacks on 5.5 million occasions in T1 2022, a 6% growth vs. T3 2021.

In T1 2022, the number of router scans requested by customers as well as the number of unique-router checks remained almost identical to those in T3 2021 – oscillating around 270,000 and 164,000 respectively.

These scans also confirmed one positive trend seen in T2 and T3 2021, namely that use of weak or default passwords for routers is slowly declining. The latest checks found their ratio dropping by 7.5% compared to T3 2021. On a similarly positive note, the ratio of routers being vulnerable to one of the ESET-monitored flaws has also dropped, in this case by 15% between T3 2021 and T1 2022.

In April, reports of a new Enemybot botnet run by the Keksec group emerged. Fortinet researchers *described it* [118] as a potential update and rebrand of Gafgyt with additional features from Mirai. Its operators seem to have two main purposes in mind: DDoS and cryptomining. In contrast with other botnets mentioned in this category, Enemybot seems to use a wider set of vulnerabilities – including some very recent ones – to “recruit” bots among Seowon Intech, D-Link, and iRZ routers.

Around the same time, another new DDoS botnet called *Fodcha* [119] was observed by Qihoo 360’s Network Security Research Lab. According to their findings, the main targets for its further spread are various routers, DVRs, and servers, with the number of daily live bots surpassing 50,000.

When IoT security is mentioned, most people think of weak passwords in routers or hijackable IP cameras. But more expensive “smart” devices are up for grabs too. Security researcher David Colombo *discovered* [120] that, by abusing a flaw in a third-party app, he could take control of multiple features on Tesla cars, including tracking them, opening their doors and windows, and starting their engines.

As shown by multiple stories related to the invasion of Ukraine, IoT security can become key in future conflicts. Among them was the hack and sabotage of *Viasat’s KA-SAT network* [9]; a new variant of Cyclops Blink botnet (replacing VPNFilter) targeting network firewall devices by *WatchGuard* [121] and *ASUS* [122] routers, which was later *disrupted* [123] by the US authorities; and – although related only remotely – findings that vulnerable *MikroTik* [124] routers were abused in Glupteba and Trickbot campaigns. To find out more about attacks related to the war in Ukraine, read our *Featured story*.

EXPLOITS

RDP attacks dropped for the first time since the beginning of 2020; SQL and SMB followed.

Since the beginning of 2020, password-guessing attacks aimed at exposed RDP services had been constantly growing. After more than two years, this changed for the first time and the brute-force attempts have dropped by 41% between T3 2021 and T1 2022.

The shift came on January 10 as RDP attacks reached an all-time high. Since then, the detected attempts started to fall sharply. They reached the first low on January 15, then recovered partially only to drop again at the beginning of February. On February 20 – shortly before the Russian invasion of Ukraine – the password guesses fell again and oscillated at that level until the end of T1 2022.

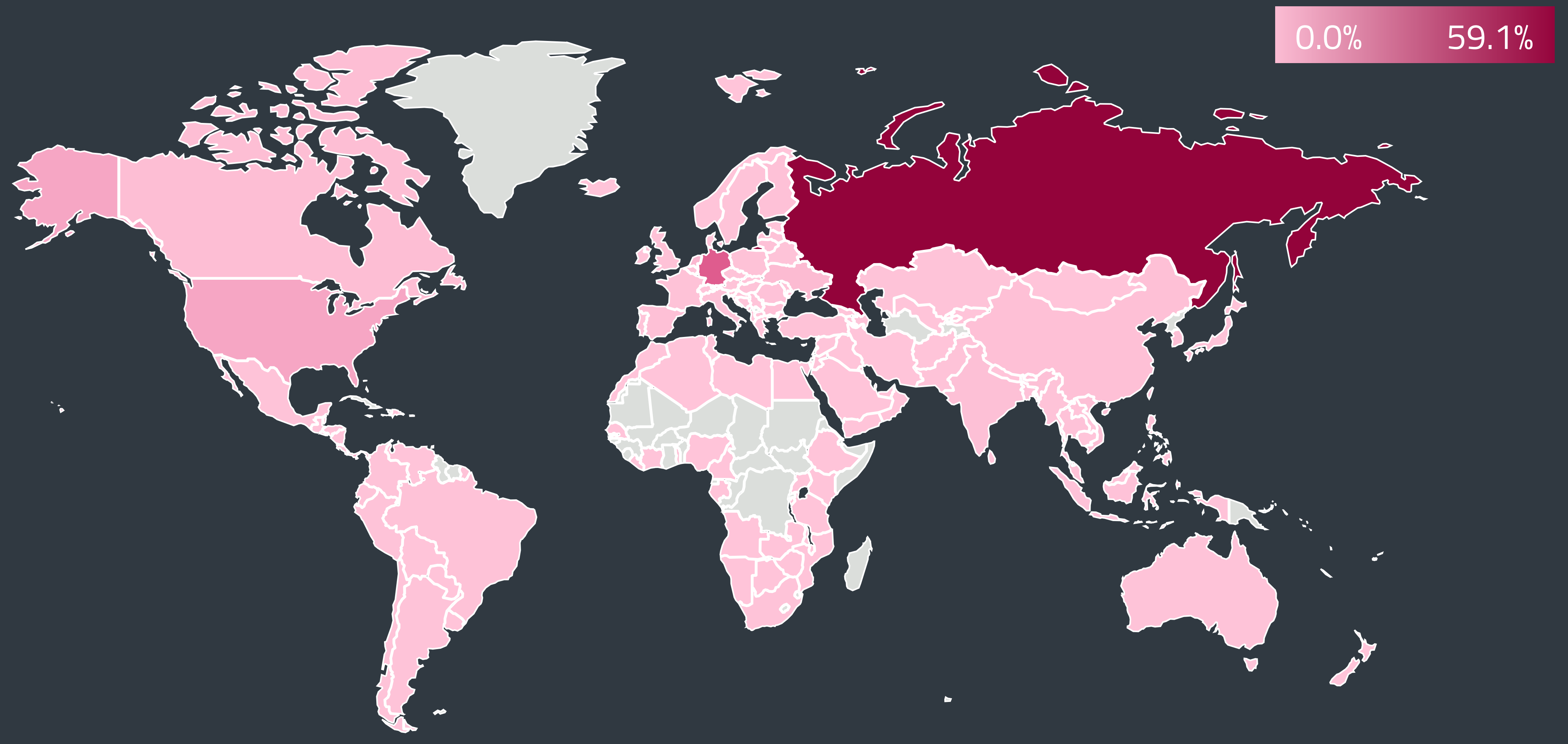
The number of unique clients reporting RDP attacks has followed a similar trajectory, dropping most notably at the turn of the year and overall, falling by 40% between T3 2021 and T1 2022. Consequentially, the average number of unique clients also decreased from 160,000 in T3 2021 to 97,000 in T1 2022.

Of the 121 billion RDP attack attempts seen in T1 2022, the top affected country was France (16%), followed by Spain (14%), Germany (8%), the United States (6%), and Italy (5%). Almost 60% of the incoming attacks came from Russia, followed in a distant second by Germany with 16% and the United States with 5%.

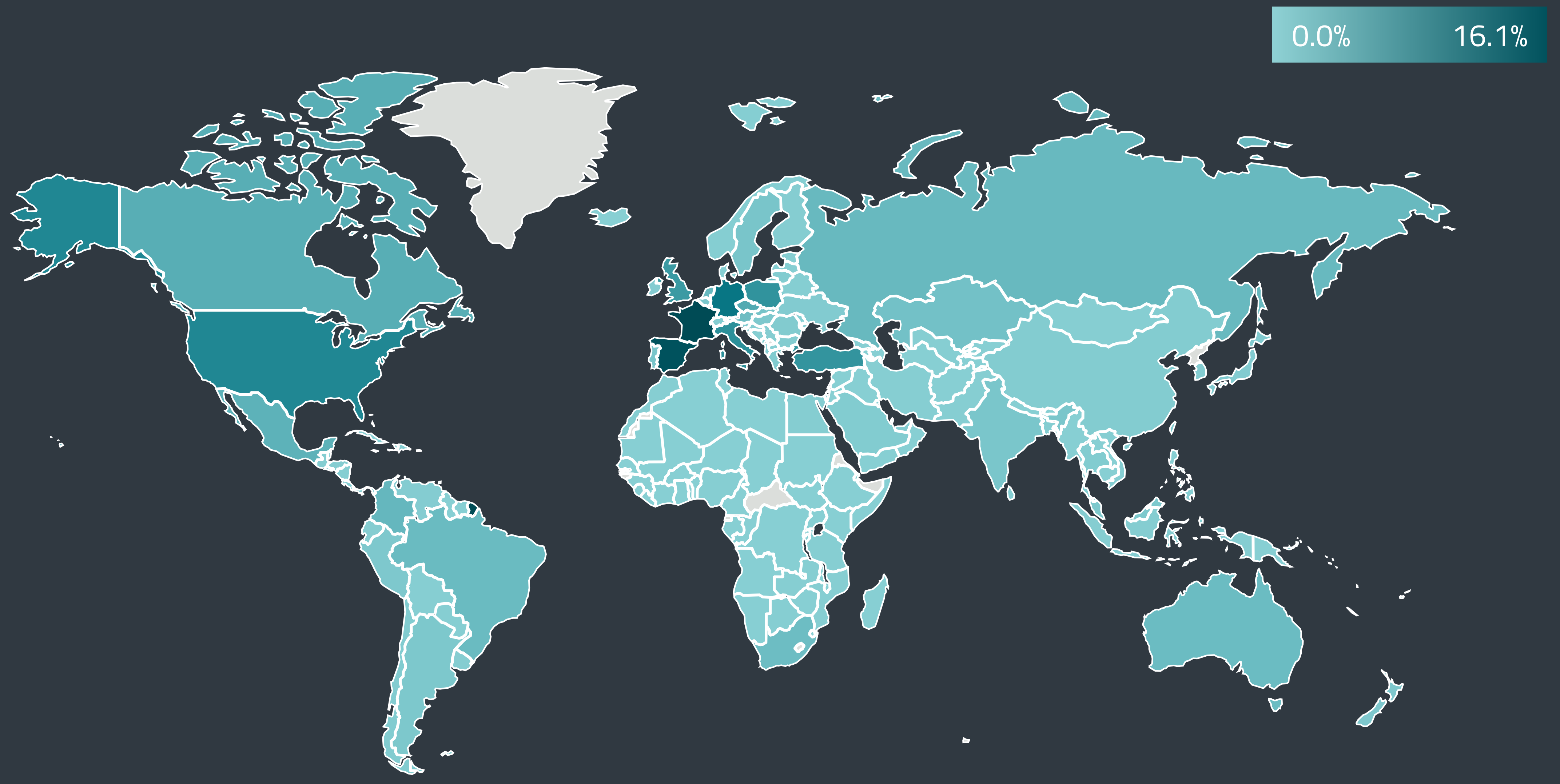
Interestingly, ESET telemetry shows an almost identical nosedive pattern for password guesses against exposed SQL services. As with RDP, SQL attack statistics reached an all-time high on January 10, followed by an extreme drop in the following days. In contrast to RDP, SQL numbers have not yet recovered. With 860 million attacks against SQL, T1 2022 saw a decline of 64% compared to T3 2021. The number of unique clients reporting malicious SQL connections decreased in the same period by 12%.

In the case of exposed SMB services, the decline started on January 9 and was slower and more gradual than in the case of RDP and SQL. Comparing T3 2021 with T1 2022, attacks targeting SMB dropped by 26%, and the number of unique clients went down by 6%.

As reported at the end of 2021, attackers also started using a new intrusion avenue – the critical *Log4J vulnerability* [125]. According to public reports, the beginning of 2022 only broadened the range of groups that adopted it into their toolkits, including *Prophet Spider* [126] and *NightSky* [78] ransomware on the criminal end and Magic Hound (also known as APT35, Charming Kitten, Phosphorus, TA453), *Hafnium* [127], *Deep Panda* [128], and *TunnelVision* [129] on the side of cyberespionage groups.



Global distribution of RDP password guessing attack attempt sources in T1 2022



Global distribution of RDP password guessing attack attempt targets in T1 2022

EXPERT COMMENT

There may be many reasons behind the decline in RDP attacks. First, the COVID-19 pandemic seems to be nearing its end and people are returning to offices. With less work being done remotely, there might be fewer interesting high-profile targets. Another factor that might have contributed to this positive development is increased awareness among IT departments and gradually improving security of corporate environments, removing exposed services and systems.

Russia's war against Ukraine has probably also played its part. Although the drop in RDP and SQL attacks started more than a month before the invasion, the physical and cyber-disruptions and the sanctions imposed after February 24 probably influenced the access to and availability of the infrastructure that was involved in the brute-force attacks.

Ladislav Janko, ESET Senior Malware Researcher

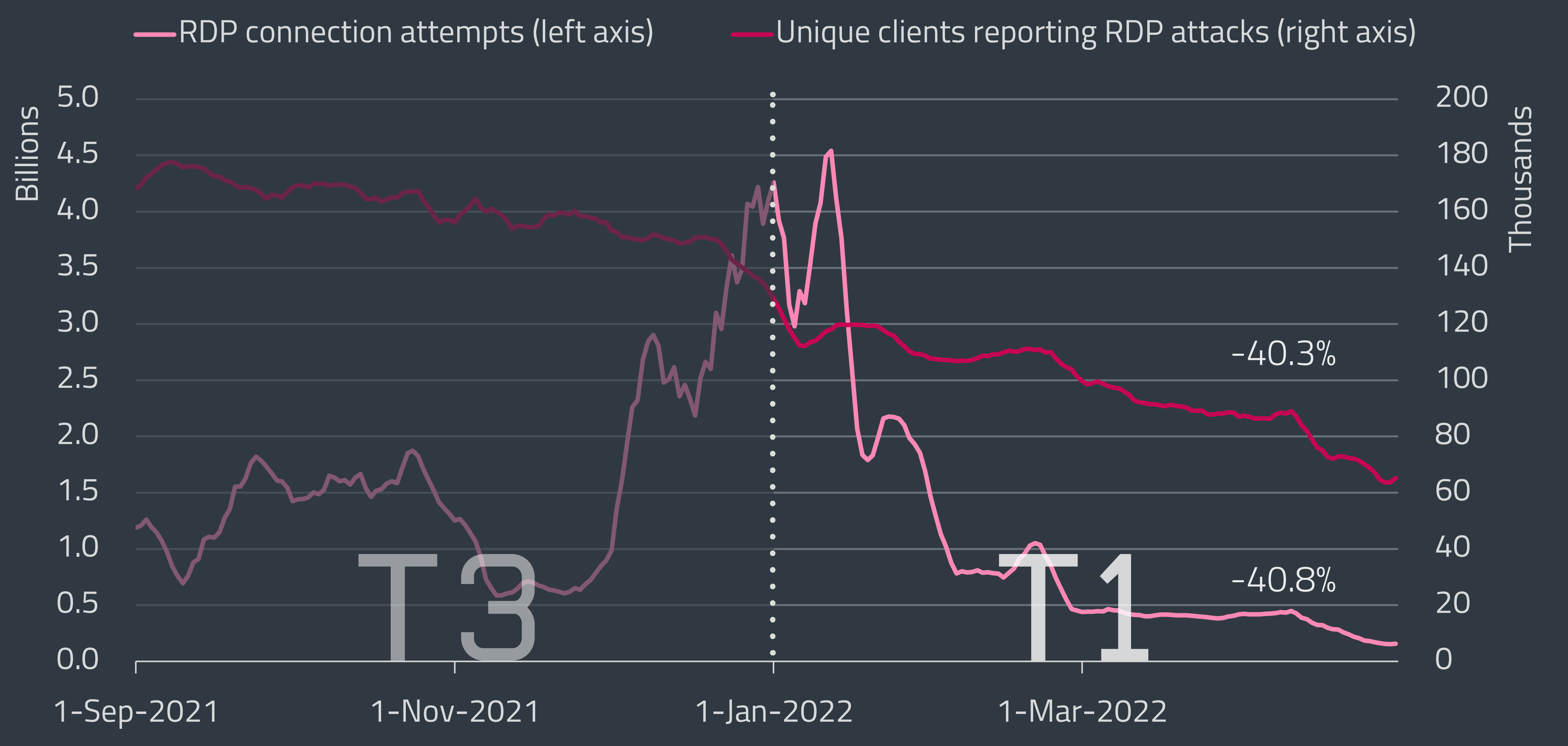
According to ESET telemetry, the number of Log4J exploitation attempts exploded after the vulnerability was published on December 10. Between January 1 and January 5, the numbers dropped from hundreds of thousands per day to tens of thousands per day, but it seems this was a short-lived holiday hiatus. After January 6, the activity of attackers – and probably also pentesters – jumped back to the levels from 2021.

Despite the gradual decline observable in our chart, Log4J isn't going away anytime soon as there are still many vulnerable applications in the wild. This has been confirmed by the Rezilion *report* [130], which identified *"over 90,000 potentially vulnerable internet-facing applications"*, acknowledging that this was probably only the tip of the iceberg.

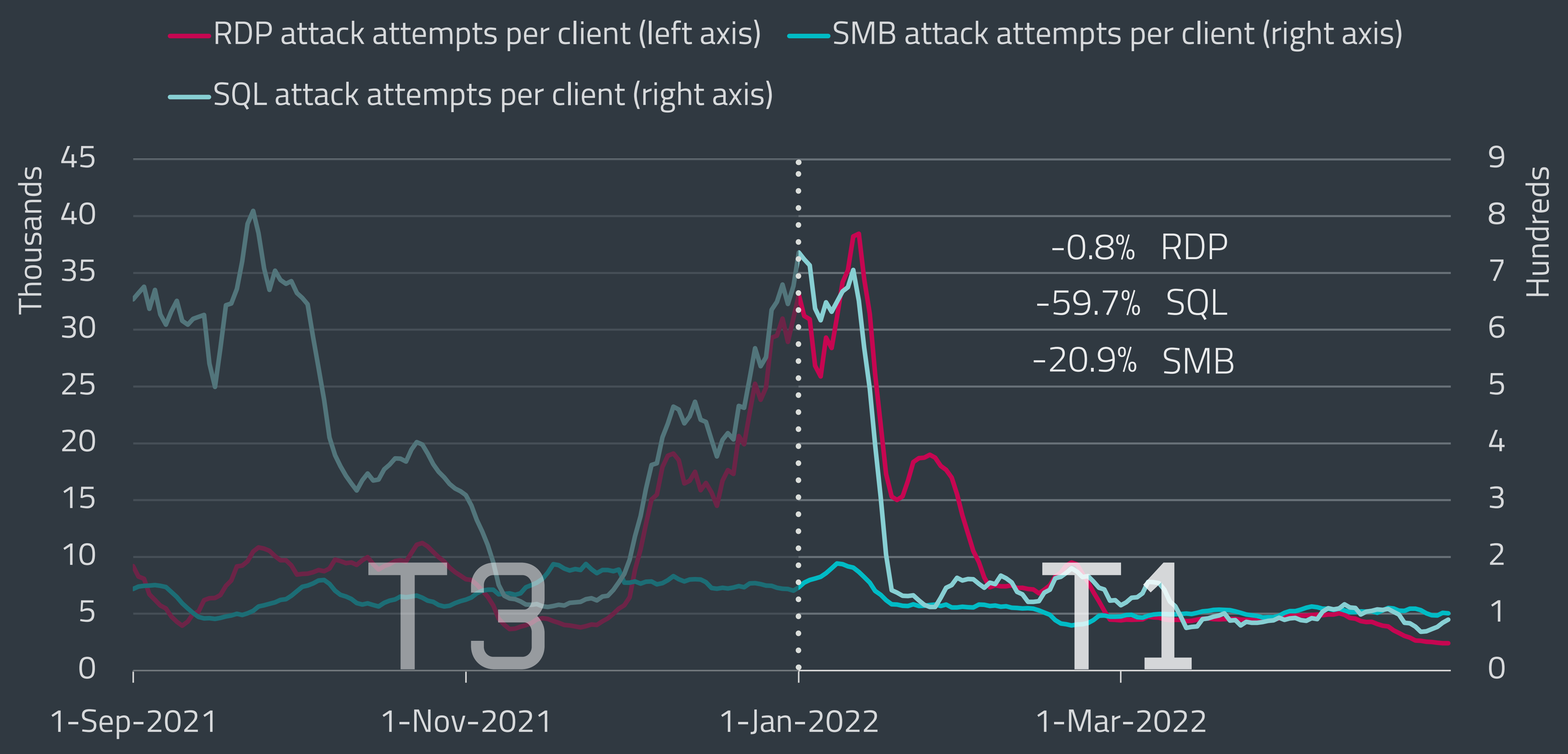
Another critical vulnerability appeared in April 2022, sporting a critical 9.8 CVSS score. The so-called Spring4Shell vulnerability (*CVE-2022-22965* [131]) has been found in the popular open-source VMWare Spring Core Java framework and allows the attackers to exploit the flaw for remote code execution (RCE) in all applications that run the unpatched version of the code.

Similar to Log4J, Spring4Shell can be exploited by sending a malicious query to the vulnerable server, allowing attackers to gain access to a broad range of the victims' data, credentials, and resources. While this makes Spring4Shell quite severe, the good news is that it is easier to identify and then to fix than Log4J.

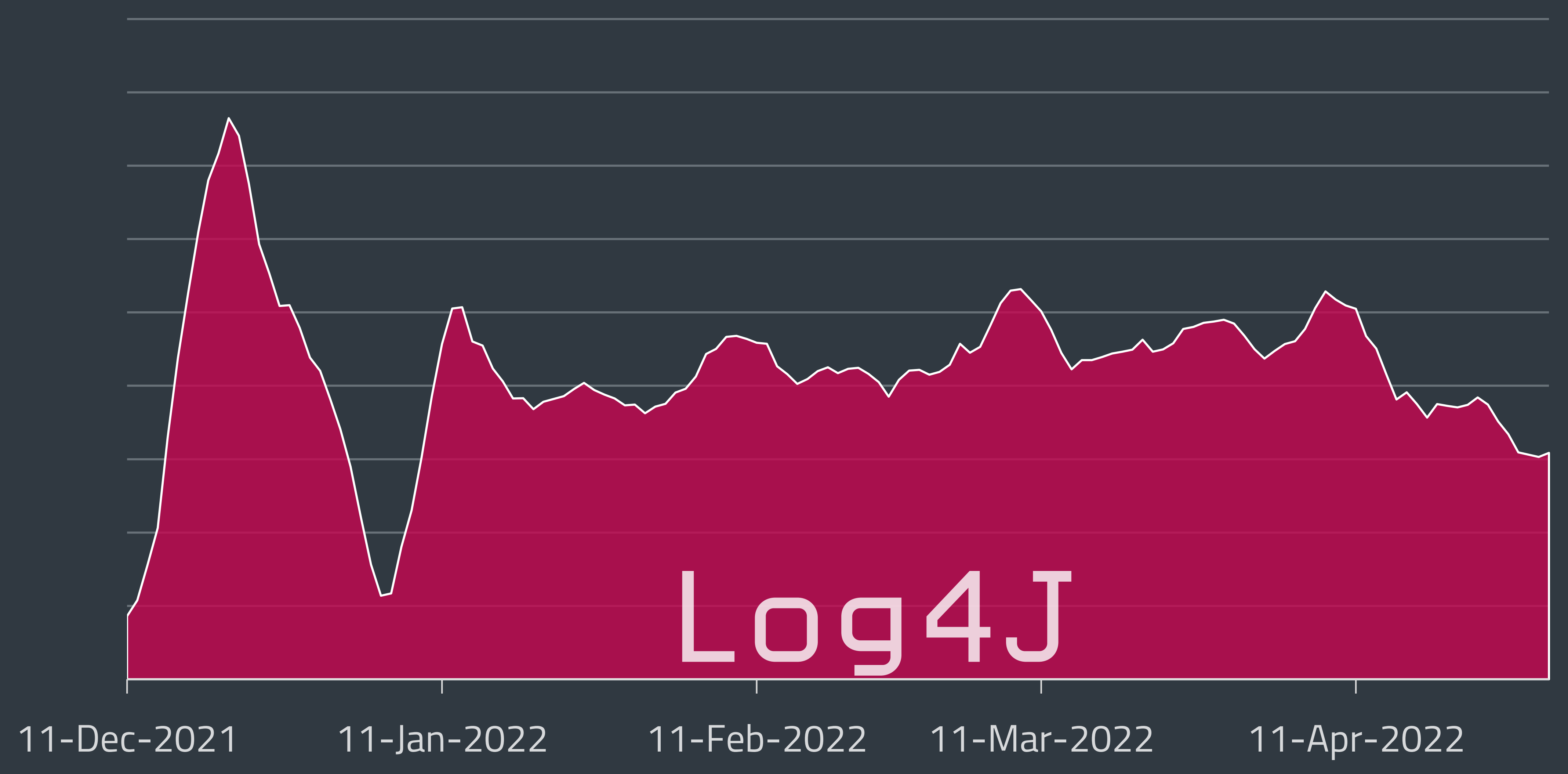
One month after its publication, ESET telemetry saw hundreds of thousands of attempts to exploit Spring4Shell. As in the Log4J case, we observed the biggest spike of activity shortly after the vulnerability was published.



Trends of RDP connection attempts and number of unique clients in T3 2021 – T1 2022, seven-day moving average

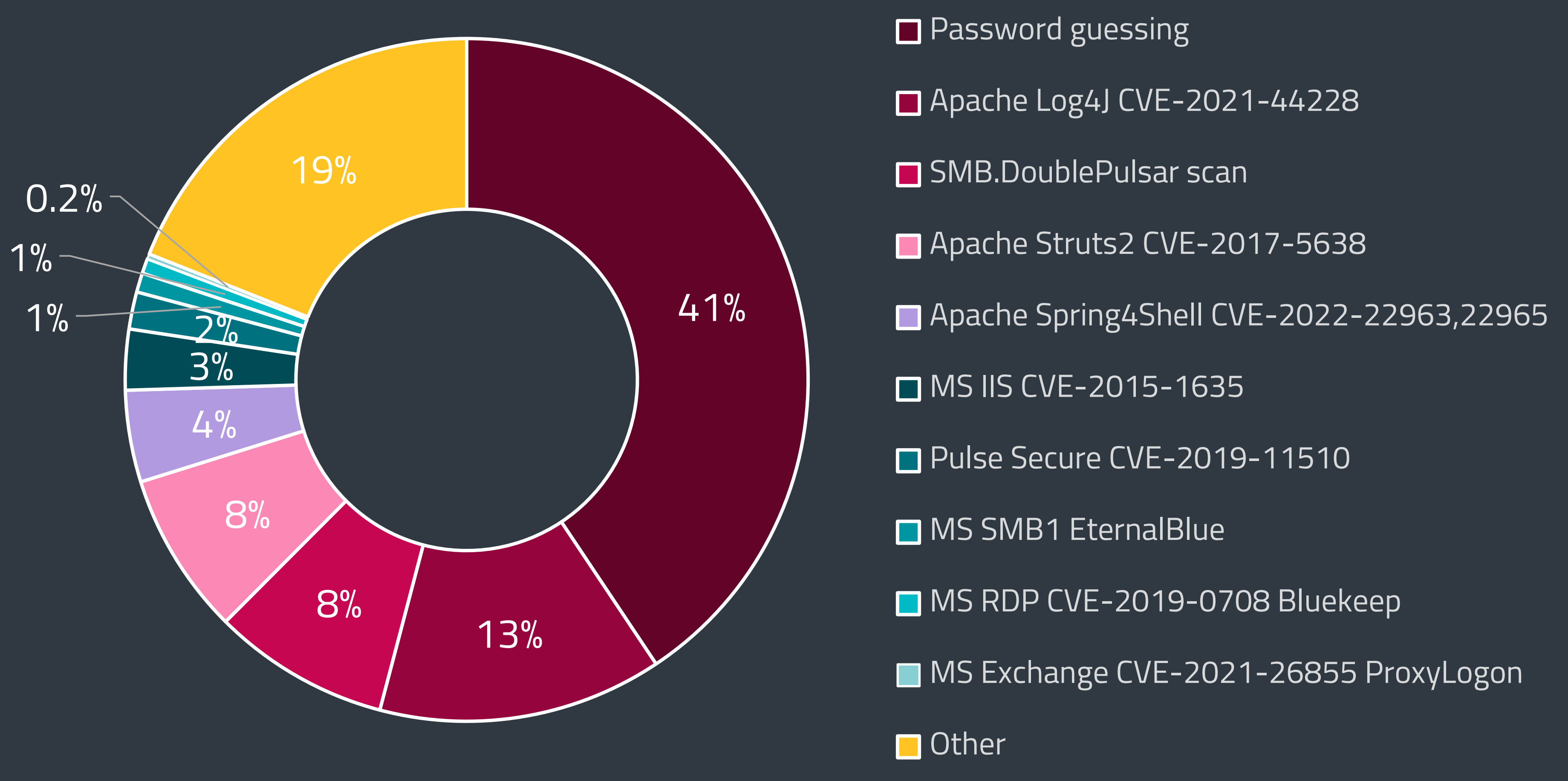


Trends of RDP, SMB and SQL attack attempts per client in T3 2021 – T1 2022, seven-day moving average

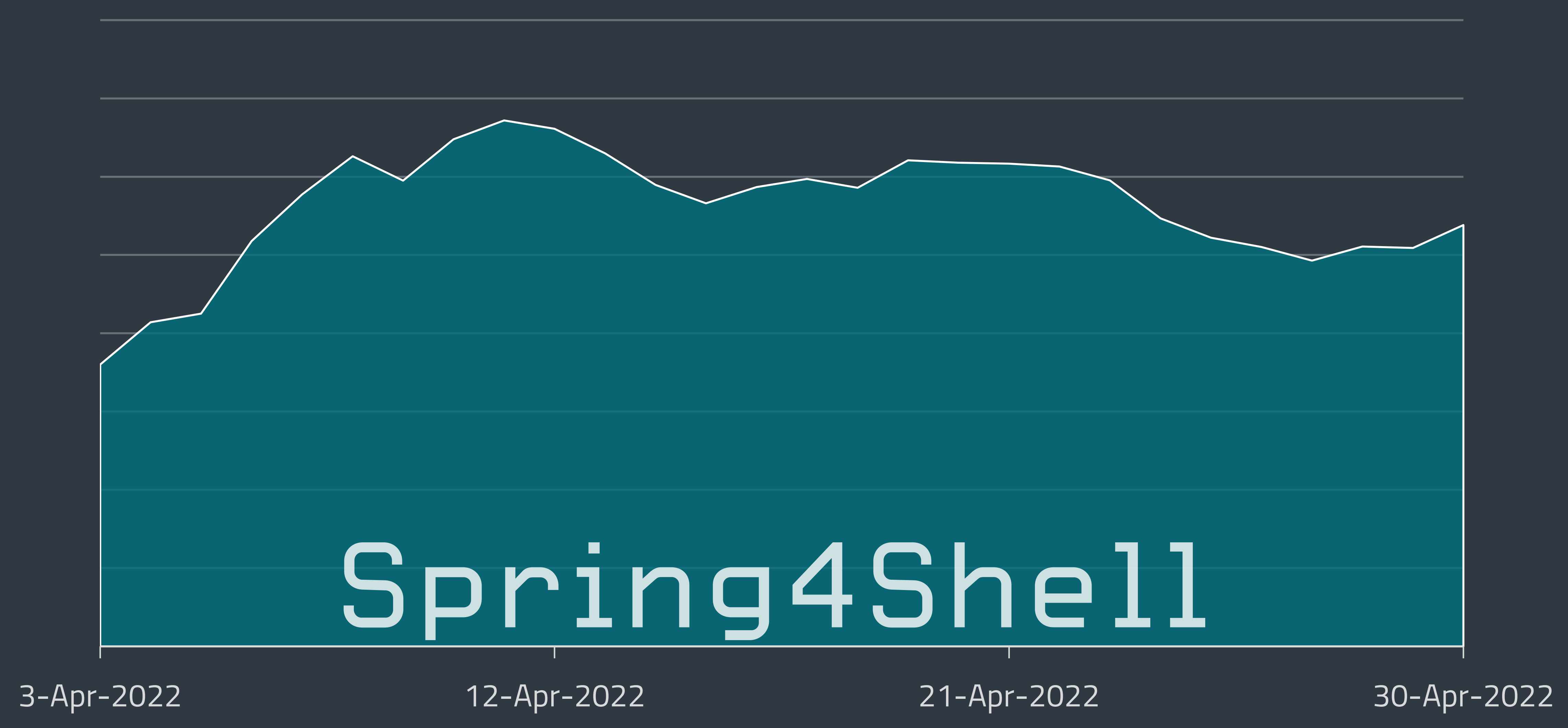


Log4J exploitation attempt trend, seven-day moving average

In the top 10 external network intrusion vectors, password guessing remains the most widespread. However, with 13%, Log4J became a solid number two in T1 2022, stealing most of the glory from *ProxyLogon* [132] – an RCE vulnerability chain in MS Exchange Servers. Our data suggests that ProxyLogon has become obsolete for offensive actors, since exploitation attempts targeting these flaws dropped from 14% in T3 2021 to less than 1% in T1 2022.



External network intrusion vectors reported by unique clients in T1 2022



Spring4Shell exploitation attempt trend in April 2022, seven-day moving average

Spring4Shell seems to be repeating Log4J's trajectory in the top 10 and despite being known only for a couple of weeks, it took fifth place, with 4% of detected exploitation attempts.

A new Linux vulnerability scoring 7.8 on the CVSS scale made noise in March. "Dirty Pipe" (*CVE-2022-0847* [133]) affects Linux kernel version 5.8 and later and was disclosed by security researcher Max Kellermann. According to his *public report* [134], the flaw makes "overwriting [of] data in arbitrary read-only files" possible. This allows attackers to inject their code into root processes and escalate their privileges on the victim's machine.

In T1 2022, Google Project Zero and Mandiant published summaries of their zero-day vulnerabilities findings in the previous year. *Google's team* [135] stated they found 58 previously unknown vulnerabilities; a two-fold jump compared to the 25 zero days uncovered in 2020. Researchers cited increased detection and disclosure as the possible reasons for the growth. Google also highlighted that only two of the 58 zero days stood out as novel, both related to a zero-click iMessage exploit FORCEDENTRY.

Mandiant's *findings* [136] are similar, although their list includes more zero days. In 2021, their researchers identified 80 new flaws, more than doubling the previous record of 32 from 2019. Mandiant also notes that the number of financially motivated actors deploying zero days is rising, mostly due to ransomware gangs utilizing them for initial access to environments of high-profile victims.

ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

UPCOMING PRESENTATIONS

RSA Conference 2022

ESPecter: Showing the future of UEFI Threats [137]

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, and the actors behind ESPecter bootkit think that compromising the bootloader is the way. This session by ESET director of threat research Jean-Ian Boutin and ESET malware researcher Martin Smolár will describe ESET's discovery of the aforementioned ESPecter – a previously undocumented real-world UEFI bootkit persisting on the EFI System Partition (ESP). This session raises awareness of UEFI threats affecting the ESP and provides guidance and resources for defenders to help secure their pre-OS environments. Boutin's and Smolár's analysis of this previously unknown, real-world UEFI ESP bootkit will help 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.

Black Hat USA 2022

Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again [138]

In this talk, ESET senior malware researcher Anton Cherepanov and ESET principal researcher Robert Lipovský will provide technical details of Industroyer2, a new version of the only malware to ever trigger electricity blackouts. Its latest variant was observed in Ukraine amidst the ongoing Russian invasion, aiming to cause a major electricity outage in a region with a population of more than two million, using components amplifying the impact. In the presentation, the researchers will show data linking this attack to the notorious Sandworm APT group and discuss why and how the attack was mostly unsuccessful. On top of that, actionable advice for defenders will be provided, including log entries to check; EDR rules to consider; configuration options to hamper Sandworm compromise and lateral movement; and detection/hunting rules for Snort and YARA.

Virus Bulletin 2022

Lazarus & BYOVD: Evil to the Windows core [139]

In this session, ESET senior malware researcher Peter Kálnai and ESET malware analyst Matěj Havránek will take 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 will shed more light on these mechanisms by demonstrating how they operate and what changes they make to system monitoring once the user-mode module is executed. Our researchers will also compare 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.

REcon 2022

Under the hood of Wslink's multilayered virtual machine [140]

Wslink is a unique loader, linked to the Lazarus group, that ESET researchers discovered and documented at the end of last year. 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 Hrčka analyzes the internals of the VM and describes ESET Research's semiautomated approach to seeing through the obfuscation techniques in a reasonable time. The approach is demonstrated on a few chunks of bytecode from a protected sample and the results are compared against a subsequently discovered non-obfuscated sample to confirm the validity of the method.

DELIVERED PRESENTATIONS

S4x22

Inside Industroyer2 and Sandworm's latest cyberattacks against Ukraine [141]

ESET's principal malware researcher Robert Lipovsky presented the work of the team that discovered Industroyer2, a new variant of Industroyer malware deployed by the infamous Sandworm group, that attempted to target a Ukrainian energy company after the outbreak of the war in Ukraine. Lipovsky talked about how the collaboration with CERT-UA mitigated this attack and compared it to the original Industroyer malware that switched off the lights in 2016. The presentation also looked at other recent Sandworm cyberattacks against Ukraine's critical infrastructure.

CARO Workshop 2022

Oil, water, and something fresh: Hunting Middle Eastern threat actors [142]

In this presentation, ESET's principal malware researcher Robert Lipovsky discussed hunting Middle Eastern threat actors OilRig, MuddyWater, and a new group ESET Research is calling FreshFeline. Based on the research of Adam Burgher, senior threat intelligence analyst at ESET, Lipovsky laid out the hunting methodology of ESET researchers and how it led to a newly discovered OilRig backdoor, several new campaigns from MuddyWater, and the backdoors and exploitation chain used by the FreshFeline group.

Behind the scenes of hunting InvisiMole [140]

Since ESETs discovery of this group in 2018, our researchers have been closely tracking activities of this highly targeted cyberespionage group. In this session, ESET senior malware researcher Anton Cherepanov and ESET malware researcher Zuzana Hromcová shared publicly unavailable information about hunting InvisiMole and discussed two previously undisclosed 2021 campaigns targeted at Ukraine and how the timing aligns with other geopolitical events in the region.

CARO Workshop 2022 Botconf 2022

TA410: APT10's distant cousin (CARO Workshop 2022) [140]

TA410: APT10's distant cousin (Botconf 2022) [143]

TA410 is a cyberespionage group first described in August 2019 and that shows interesting technical capabilities with its use of complex implants. TA410's activity shares some characteristics with past APT10 operations. As such, some public reports have misattributed TA410 activities to APT10. In this presentation, ESET malware researcher Alexandre Côté Cyr and senior malware researcher Matthieu Faou clarified what TA410 is and how its activities differ from the current activities of APT10. By leveraging ESET telemetry, they presented ESET Research's view of the main targets of TA410.

Botconf 2022 NorthSec

Jumping the air gap: 15 years of nation-state efforts (Botconf 2022) [144]

Jumping the air gap: 15 years of nation-state efforts (NorthSec) [145]

Air-gapping is used to protect the most sensitive of networks. In the first half of 2020 alone, four previously unknown malicious frameworks designed to breach air-gapped networks emerged, bringing the total, by ESET's count, to 17. ESET Research decided to revisit each framework known to date and to put them in perspective, side by side. This presentation by Alexis Dorais-Joncas, who leads the Canadian malware research team, and ESET security intelligence analyst Facundo Munõz, described how malware frameworks targeting air-gapped networks operate, and provided a side-by-side comparison of their most important TTPs.

Botconf 2022

ProxyChaos: a year-in-review of Microsoft Exchange exploitation [146]

Since the beginning of 2021, Exchange has been subject to several critical vulnerabilities, including the ProxyLogon and ProxyShell vulnerability chains, and their variations. ESET researchers have been closely monitoring malicious activities related to these vulnerabilities since they were made public and discovered multiple APT groups exploiting them. This presentation by ESET malware researcher Mathieu Tartare revisited the whole timeline of events and showed how attackers systematically exploited these vulnerabilities and for what purpose. For each vulnerability, the presentation gave an overview of the various groups that exploited it, including some yet undisclosed activities. Tartare also provided the attendees with a detailed timeline of the events and statistics from ESET telemetry, to show the wide scope of these attacks.

SeQCure

Disclosure of vulnerabilities: A challenge even in 2022 [147]

Finding vulnerabilities is not inherently associated with being a malware researcher. Yet ESET researchers regularly expose different types of vulnerabilities in the course of their work and actively participate in the coordinated disclosure process. This presentation by Alexis Dorais-Joncas, who leads the ESET security intelligence team, and ESET malware researcher Mathieu Tartare, explained how malware research can lead to the discovery of vulnerabilities. Throughout the presentation of real-world case studies, our researchers detailed the different types of vulnerabilities that are most frequently discovered, how the disclosure process works, and the lessons that were learned.

ESET World

Worldwide aerospace and defense contractors under attack by Lazarus [148]

Advanced threat actors operating under the Lazarus umbrella have been relentlessly targeting worldwide defense contractors and aerospace companies for years. In this presentation, ESET's director of threat research Jean-Ian Boutin explained the details of the group's newest campaigns against this critical sector. While the opening lure is still the same – a fake job offer through social media like LinkedIn – the campaign's sophistication and diversity keeps increasing.

ESET European cybersecurity day SEMAFOR

Past and present cyberwar in Ukraine (ESET European cybersecurity day) [149]

Past and present cyberwar in Ukraine (SEMAFOR) [150]

With the brutal escalation of the war against Ukraine, ESET's principal malware researcher Robert Lipovsky took a closer look at the "cyber" part of it. What has been happening in Ukraine? Could the cyberwar spill over to other European countries? Should users be worried? Lipovsky explained to the attendees of these events the most important cyberattacks related to the armed conflict – in the past weeks, as well as in the past eight years.

ESET European Cybersecurity Day

Will machine learning improve or disrupt the cybersecurity equilibrium? [151]

Machine learning-based technologies increasingly help fight large-scale fraud, evaluate and optimize business processes, improve testing procedures, and develop new solutions to existing problems. Juraj Jánošík, the leader of ESET's automated threat detection and machine learning team, spoke during his talk about how ESET recognized the potential of machine learning early on and employed it to improve malware detection starting over 20 years ago. Explaining that technological advances are not exclusively available to cybersecurity defenders, Jánošík also spoke about how cybercriminals do not hesitate to utilize machine learning-based technologies to make their malware and activities more efficient.

Zooming in on the current threatscape [152]

ESET security awareness specialist Ondrej Kubovič shared findings about the latest threats and trends detected in ESET telemetry during the last months of 2021. Among others, his presentation covered the hundreds of billions of password guesses aimed to break the protection of RDP remote access; the resurrection of Emotet, a threat described by Europol as the "most dangerous malware in the world"; and the over 400-fold increase in Android banking malware year-over-year.

WHITE PAPERS

Under the hood of Wslink's multilayered virtual machine [36]

ESET researchers recently described Wslink, a unique and previously undocumented malicious loader that runs as a server and that features a virtual-machine-based obfuscator. In this white paper, ESET malware researcher Vladislav Hrčka describes the structure of the virtual machine used in samples of Wslink and suggests a possible approach to see through the obfuscation techniques used in the samples analyzed. The virtual machine introduced a diverse arsenal of obfuscation techniques, which ESET researchers were able to overcome to reveal a part of the deobfuscated malicious code that is described in this document. This white paper also provides an overview of the internal structure of virtual machines in general, and introduces some important terms and frameworks used in our detailed analysis of the Wslink virtual machine.

ESET RESEARCH PODCAST

To increase the reach of ESET research among cybersecurity practitioners, administrators, researchers and the infosec community in general, we have decided to start our own podcast – the ESET Research podcast. New episodes are released every time we publish a major research story, which usually happens every few months.

The host of our podcast is ESET's Distinguished Researcher and infosec pioneer *Aryeh Goretsky* [153], who is talking to researchers, introducing them and their discoveries and offering the listeners a peek behind the curtain of how their research came to be.

You can listen to the latest episodes via the most popular podcast platforms including *Spotify* [154], *Google Podcasts* [155], *Apple Podcasts* [156] and *PodBean* [157].

MITRE ATT&CK CONTRIBUTIONS

ESET researchers regularly contribute to *MITRE ATT&CK®* [158] – a globally accessible knowledge base of adversary tactics and techniques. In T1 2022, ESETs *Process Injection: ListPlanting* [159] contribution was added to the ATT&CK knowledge base.

ListPlanting is a method of executing arbitrary code in the address space of a separate live process. Code executed via ListPlanting may also evade detection from security products since the execution is masked under a legitimate process. InvisiMole uses ListPlanting to inject code into a trusted process.

InvisiMole [160] is a modular spyware program that has been used by the InvisiMole APT group since at least 2013. The InvisiMole group also has two backdoor modules called RC2FM and RC2CL that are used to perform post-exploitation activities. It has been discovered on compromised victims in Ukraine and Russia. *Gamaredon group* [161] infrastructure has been used to download and execute the InvisiMole spyware against a small number of victims.

ESET has conducted extensive research into both of these APT groups. ESET researchers *revealed* [26] the modus operandi and extensive toolset of the elusive InvisiMole group, which targets military and diplomatic entities. Various tools used by Gamaredon are also *well known* [25] to ESET researchers and are frequently monitored and tracked by them.

The latest ATT&CK *v11 setlist* [162] also includes detections now paired with related Data Sources: Data Components, a beta version of sub-techniques for ATT&CK for Mobile, ATT&CK for ICS on *attack.mitre.org* [156], as well as regular updates and additions across Techniques, Software, and Groups.

MITRE ATT&CK EVALUATIONS

ESET participated in the latest round of MITRE ATT&CK evaluations that focused on tactics, techniques and procedures applied by the Wizard Spider and Sandworm nation-state APT groups: *Wizard Spider & Sandworm MITRE Engenuity ATT&CK evaluation* [163].

These evaluations are not a competitive analysis, as is stressed by *MITRE Engenuity* [164]. Some key parameters that the evaluations do not consider include performance and resource requirements, alerting strategy, noisiness (alert fatigue – any product could obtain a very high score on most of these results by producing alerts on every action recorded in the test environment), integration with endpoint security software, and ease of use. In ESET's case, this evaluation assessed *ESET Inspect* [165], our extended detection and response solution, which provides risk managers and incident responders with threat and system visibility.

The detection scenarios consisted of 19 steps (10 for Wizard Spider and 9 for Sandworm) spanning a spectrum of tactics listed in the ATT&CK framework, from initial access to lateral movement, collection, exfiltration, and so on. These steps are then broken down to a more granular level – a total of 109 sub-steps. ESET Inspect for Linux machines was not yet released at the time of the evaluation, so Linux-related steps and sub-steps were out of scope. That means 15 steps and 90 sub-steps were evaluated in ESET's case.

Out of the 15 applicable steps in the detection evaluation, ESET Inspect *detected all steps (100%)* [166]. Breaking the attack emulation down to a more granular level, out of the 90 applicable sub-steps in the emulation, ESET Inspect detected 75 sub-steps (83%) even without the modules present in ESET Inspect with Linux support. As the results indicate, ESET Inspect provides defenders excellent visibility of the attacker's actions on the compromised system throughout all attack stages. As already stated, ESET did not participate in the Linux part of the evaluation, but with the public launch of ESET Inspect with Linux support on March 30, 2022, the company's coverage of all major endpoint platforms, alongside Windows and macOS, is now complete.

To understand ESET's background, the company is a pioneer of research on Sandworm, with some of the most significant discoveries made about this threat group. ESET's outstanding visibility into this group is demonstrated by high-profile research, such as ESET's recent discovery of *Industroyer2* [14]. The discovery and cooperation with CERT-UA led to the prevention of the attack that was aimed at an energy provider in Ukraine. Other examples of ESET research analyzing Sandworm operations and tools include the *attacks against the Ukrainian power grid* [12], cyberattacks on *high-value targets in the Ukrainian financial sector* [167], the *supply-chain attacks against Ukraine* [168], and the devastating *NotPetya ransomware* [169], just to name a few.

Wizard Spider has been conducting ransomware campaigns using infamous tools like TrickBot, a botnet that has infected over a million computers. In 2020 ESET researchers participated in a global operation to *disrupt this botnet* [170]; however, it didn't take long and this infostealer was back in business with *new modules* [171].

OTHER CONTRIBUTIONS

ESET researchers discovered multiple vulnerabilities in various consumer Lenovo laptop models that allow an attacker with admin privileges to expose the user to firmware-level malware; they also identified an MSR vulnerability in the `AMDPowerProfiler.sys` kernel driver.

CVE-2021-26334 [172]

ESET researchers identified an MSR vulnerability in the `AMDPowerProfiler.sys` kernel driver, which is a part of *AMD μProf* [173] profiling software. Once the underlying software package is installed, the driver runs on every system boot. The unfiltered MSR IOCTL access combined with the lack of `FILE_DEVICE_SECURE_OPEN` flags and on-boot presence gives the attackers a good opportunity to exploit the driver even as an unprivileged user – this is an advantage compared to the BYOVD approach when the attackers need to load the driver themselves.

AMD *acknowledged* [174] the vulnerability and released a fix in its November 2021 *Patch Tuesday* [172] release. More information about malware that abuses vulnerabilities in kernel drivers is available in ESET Research's *blogpost* titled Signed kernel drivers – Unguarded gateway to Windows' core [30].

CVE-2021-3971 [37], *CVE-2021-3972* [38]

These two vulnerabilities affect UEFI firmware drivers originally meant to be used only during the manufacturing process of Lenovo consumer notebooks. Affected firmware drivers can be activated by an attacker to directly disable SPI flash protections (BIOS Control Register bits and Protected Range registers) or the UEFI Secure Boot feature from a privileged user-mode process during OS runtime. It means that exploitation of these vulnerabilities would allow attackers to deploy and successfully execute SPI flash or ESP implants, like *LoJax* [29] or ESET Research's latest UEFI malware discovery *ESPecter* [39], on the affected devices.

CVE-2021-3970 [40]

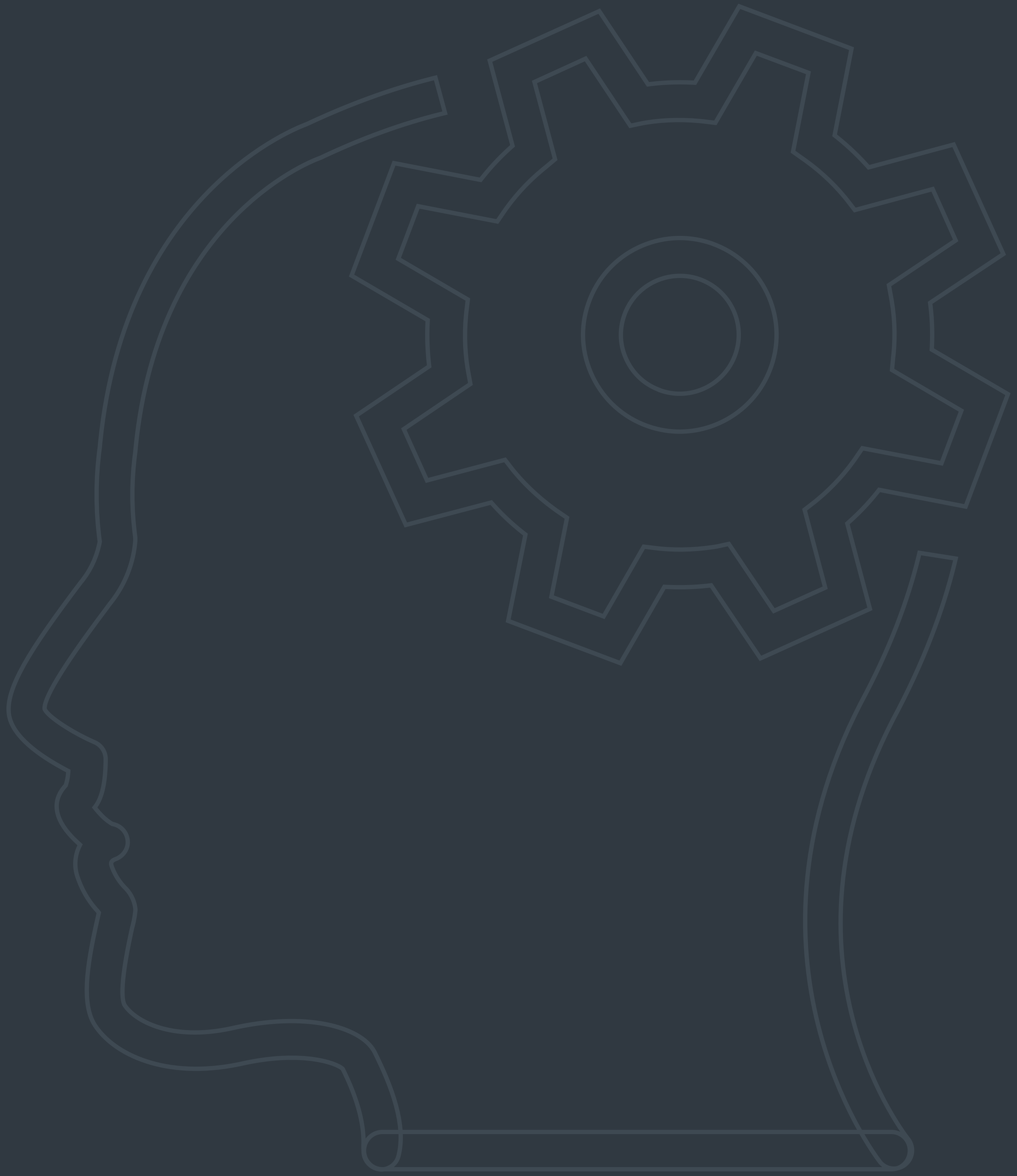
A third vulnerability – SMM memory corruption inside the SW SMI handler function – was discovered while ESET researchers investigated the aforementioned vulnerable drivers. This vulnerability allows arbitrary read/write from/into SMRAM, which can lead to the execution of malicious code with SMM privileges and potentially lead to the deployment of an SPI flash implant.

Lenovo confirmed the vulnerabilities on November 17, 2021 and published an advisory on April 18, 2022. Altogether, the list of affected devices contains more than one hundred different consumer laptop models with millions of users worldwide, from affordable models like Ideapad-3 to more advanced ones like Legion 5 Pro-16ACH6 H or Yoga Slim 9-14ITL05. The full list of affected models with active development support is published in the *Lenovo Advisory* [41]. In addition to the models listed in the advisory, several other devices we reported to Lenovo are also affected, but won’t be fixed due to them reaching End Of Development Support (EODS). More information is available in ESET Research’s *blogpost* [42] titled “When ‘secure’ isn’t secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer laptops”.

Frost & Sullivan’s Insights for CISOs series: Participation in the panel about implications of the war in Ukraine [175]

The war in Ukraine changed geopolitics in Europe and the NATO alliance faster than anyone could have imagined. According to research and consulting firm Frost & Sullivan, one aspect of the war that is under-reported is the cybersecurity dimension and the question of whether sanctions and technology sales bans will drive new waves of ransomware attacks and cyber-economic espionage.

Cybersecurity executives from all over the world came together with Frost & Sullivan, to discuss the potential cybersecurity implications of the largest war in Europe since World War 2. Jean-Ian Boutin, ESET’s director of threat research, shared the company’s insights into various threats ESET Research detected in Ukraine, not only during the outbreak of the war but also those preceding it. He described 2022 as the year of WhisperGate, HermeticWiper, IsaacWiper and CaddyWiper from the perspective of CISOs, and outlined how the vendor community can ensure these attacks are mitigated. He also discussed diverse APT groups like Mustang Panda exploiting the Ukraine conflict as a bait for adversarial actions and what it means for CISOs and their evolving role.



CREDITS

Team

Peter Stančík, Team Lead

Klára Kobáková, Managing Editor

Aryeh Goretsky

Branislav Ondrášik

Bruce P. Burrell

Hana Matušková

Nick FitzGerald

Ondrej Kubovič

Zuzana Pardubská

Foreword

Roman Kováč, Chief Research Officer

Contributors

Anton Cherepanov

Dušan Lacika

Igor Kabina

Jakub Souček

Jakub Tomanek

Ján Šugarek

Jean-Ian Boutin

Jiří Kropáč

Juraj Jánošík

Ladislav Janko

Lukáš Štefanko

Marc-Etienne M.Léveillé

Martin Červeň

Matthieu Faou

Michal Malík

Milan Fránik

Miroslav Legéň

Patrik Sučanský

Robert Kapp

Robert Lipovský

Vladimír Šimčák

Zuzana Legáthová

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 threats regardless of the targeted platform.

This data was processed with the honest intention to mitigate all known biases, in an effort to maximize the value of the information provided on the most significant in-the-wild threats.

Further, the data excludes detections of *potentially unwanted applications* [176], *potentially unsafe applications* [177] and *adware* [178], except where noted in the more detailed, platform-specific sections and in the Cryptocurrency threats section.

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://twitter.com/ESETresearch/status/1496581903205511181

[2] https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

[3] https://twitter.com/ESETresearch/status/1496614321442459655

[4] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

[5] https://twitter.com/AvastThreatLabs/status/1496663206634344449

[6] https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

[7] https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/

[8] https://cip.gov.ua/en/news/chergova-kiberataka-na-saiti-derzhavnikh-organiv-ta-banki

[9] https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

[10] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[11] https://twitter.com/ESETresearch/status/1483161464106098689

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

[13] https://cert.gov.ua/article/39518

[14] https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

[15] https://edition.cnn.com/2022/04/12/politics/gru-russia-hackers-ukraine-power-grid/index.html

[16] https://www.eset.com/int/ua-crisis/?utm_source=facebook&utm_medium=cpc&utm_campaign=ukraine-crisis&utm_term=eset-response-center&fbclid=IwAR2pu0PR2VThhA0GpRE0-Km9NmA3oELsHzsrR9l8DzNR_33I_2Sw0urrrD4#eset-helps

[17] https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/

[18] https://www.welivesecurity.com/2022/02/27/beware-charity-scams-exploiting-war-ukraine/

[19] https://www.welivesecurity.com/2022/03/11/eset-research-webinar-apt-groups-ukraine-cyber-battlefield/

[20] https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/

[21] https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

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

[23] https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/

[24] https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

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

[26] https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

[27] https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

[28] https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/

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

[30] https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/

[31] https://www.welivesecurity.com/2022/04/06/fake-eshops-prowl-banking-credentials-android-malware/

[32] https://appdefensealliance.dev/

[33] https://www.welivesecurity.com/2022/03/24/crypto-malware-patched-wallets-targeting-android-ios-devices/

[34] https://www.welivesecurity.com/2022/04/13/eset-takes-part-global-operation-disrupt-zloader-botnets/

[35] https://www.welivesecurity.com/2022/03/28/under-hood-wslink-multilayered-virtual-machine/

[36] https://www.welivesecurity.com/wp-content/uploads/2022/03/eset_wsliknkvm.pdf

[37] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3971

[38] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3972

[39] https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/

[40] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3970

[41] https://support.lenovo.com/us/en/product_security/len-73440

[42] https://www.welivesecurity.com/2022/04/19/when-secure-isnt-secure-uefi-vulnerabilities-lenovo-consumer-laptops/

[43] https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2017-11882

[44] https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/

[45] https://www.trendmicro.com/en_us/research/20/c/operation-poisoned-news--hong-kong-users-targeted-with-mobile-ma.html

[46] https://www.welivesecurity.com/2022/01/25/watering-hole-deploys-new-macos-malware-dazzlespy-asia/

[47] https://unit42.paloaltonetworks.com/thor-plugx-variant/

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

[49] https://twitter.com/ESETresearch/status/1506904404225630210

[50] https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/

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

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

[53] https://www.bleepingcomputer.com/news/security/malicious-powerpoint-files-used-to-push-remote-access-trojans/

[54] https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html

[55] https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

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

[57] https://twitter.com/ESETresearch/status/1494249522301743105

[58] https://twitter.com/ESETresearch/status/1485660697044398081

[59] https://krebsonsecurity.com/2022/01/at-request-of-u-s-russia-rounds-up-14-revil-ransomware-affiliates/

[60] https://www.bleepingcomputer.com/news/security/revils-tor-sites-come-alive-to-redirect-to-new-ransomware-operation/

[61] https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/

[62] https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/

[63] https://www.bleepingcomputer.com/news/security/oldgremlin-ransomware-gang-targets-russia-with-new-malware/

[64] https://edition.cnn.com/2022/03/30/politics/ukraine-hack-russian-ransomware-gang/index.html

[65] https://twitter.com/BrettCallow/status/1497249143663652865?s=20&t=NUaoFyINtpUfN4Vj2oxBEw

[66] https://twitter.com/contileaks

[67] https://www.washingtonpost.com/politics/2022/03/18/11-big-takeaways-conti-ransomware-leaks/

[68] https://twitter.com/uuallan/status/1498048260425977856?s=20&t=IiOyo7tgumTKlUnLqiermQ

[69] https://www.emsisoft.com/ransomware-decryption-tools/maze-sekhmet-egregor

[70] https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-trickbot-gangs-diavol-ransomware/

[71] https://decoded.avast.io/threatresearch/decrypted-targetcompany-ransomware/

[72] https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-yanluowang-ransomware-victims/

[73] https://decoded.avast.io/threatresearch/help-for-ukraine-free-decryptor-for-hermeticransom-ransomware/

[74] https://arxiv.org/abs/2202.08477

[75] https://krebsonsecurity.com/2022/03/estonian-tied-to-13-ransomware-attacks-gets-66-months-in-prison/

[76] https://www.bleepingcomputer.com/news/security/netwalker-ransomware-affiliate-sentenced-to-80-months-in-prison/

[77] https://www.bleepingcomputer.com/news/security/night-sky-is-the-latest-ransomware-targeting-corporate-networks/

[78] https://www.bleepingcomputer.com/news/security/

night-sky-ransomware-uses-log4j-bug-to-hack-vmware-horizon-servers/

[79] https://www.bleepingcomputer.com/news/security/qnap-warns-of-new-deadbolt-ransomware-encrypting-nas-devices/

[80] https://www.bleepingcomputer.com/news/security/a-look-at-the-new-sugar-ransomware-demanding-low-ransoms/

[81] https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/

[82] https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/

[83] https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

[84] https://www.bleepingcomputer.com/news/microsoft/microsoft-plans-to-kill-malware-delivery-via-office-macros/

[85] https://twitter.com/ESETresearch/status/1518923380782739458

[86] https://thehackernews.com/2022/04/emotet-testing-new-delivery-ideas-after.html

[87] https://thehackernews.com/2022/03/new-malware-loader-verblecon-infects.html

[88] https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-crash-continues/

[89] https://www.vice.com/en/article/g5qj9j/cryptocom-says-incident-was-actually-dollar30-million-hack

[90] https://www.bleepingcomputer.com/news/cryptocurrency/wormhole-cryptocurrency-platform-hacked-to-steal-326-million/

[91] https://thehackernews.com/2022/02/hackers-steal-17-million-worth-of-nfts.html

[92] https://twitter.com/ESETresearch/status/1497194165561659394

[93] https://www.welivesecurity.com/2021/05/17/android-stalkerware-threatens-victims-further-exposes-snoopers-themselves/

[94] https://techcrunch.com/2022/02/22/stalkerware-network-spilling-data/

[95] https://lab52.io/blog/complete-dissection-of-an-apk-with-a-suspicious-c2-server/

[96] https://blog.appcensus.io/2022/04/06/the-curious-case-of-coulus-coelib/

[97] https://www.wsj.com/articles/apps-with-hidden-data-harvesting-software-are-banned-by-google-11649261181

[98] https://blog.pradeo.com/spyware-facestealer-google-play

[99] https://blog.checkpoint.com/2022/04/07/android-banking-stealer-dubbed-sharkbot-found-disguised-as-legitimate-anti-virus-apps-on-the-google-play-store/

[100] https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered

[101] https://www.threatfabric.com/blogs/partners-in-crime-medusa-cabassous.html

[102] https://www.threatfabric.com/blogs/xenomorph-a-newly-hatched-banking-trojan.html

[103] https://eprint.iacr.org/2022/208.pdf

[104] https://twitter.com/ESETresearch/status/1521735320852643840

[105] https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/

[106] https://objective-see.com/blog/blog_0x6C.html

[107] https://www.volexity.com/blog/2022/03/22/storm-cloud-on-the-horizon-gimmick-malware-strikes-at-macos/

[108] https://www.politico.eu/article/pegasus-hacking-spyware-spain-government-prime-minister-pedro-sanchez-margarita-robles-digital-espionage-crisis/

[109] https://www.bleepingcomputer.com/news/security/finnish-diplomats-phones-infected-with-nso-group-pegasus-spyware/

[110] https://www.reuters.com/technology/exclusive-iphone-flaw-exploited-by-second-israeli-spy-firm-sources-2022-02-03/

[111] https://googleprojectzero.blogspot.com/2022/03/forcedentry-sandbox-escape.html

[112] https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/Apple-Iphone-Os.html

[113] https://www.exploit-db.com/exploits/41471

[114] https://www.shodan.io/search/report?query=jaws%2F1.0

[115] https://nvd.nist.gov/vuln/detail/CVE-2017-18368

[116] https://nvd.nist.gov/vuln/detail/CVE-2015-2051

[117] https://twitter.com/360Netlab/status/1420390398825058313

[118] https://thehackernews.com/2022/04/new-enemybot-ddos-botnet-borrows.html

[119] https://www.bleepingcomputer.com/news/security/new-fodcha-ddos-botnet-targets-over-100-victims-every-day/

[120] https://www.vice.com/en/article/akv7z5/how-a-hacker-controlled-dozens-of-teslas-using-a-flaw-in-third-party-app

[121] https://arstechnica.com/information-technology/2022/02/russias-most-cut-throat-hackers-infect-network-devices-with-new-botnet-malware/

[122] https://thehackernews.com/2022/03/new-variant-of-russian-cyclops-blink.html

[123] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

[124] https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html

[125] https://www.welivesecurity.com/2021/12/13/log4shell-vulnerability-what-we-know-so-far/

[126] https://thehackernews.com/2022/01/initial-access-broker-involved-in.html

[127] https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

[128] https://www.zdnet.com/article/chinese-hackers-deep-panda-return-with-log4shell-exploits-new-fire-chili-rootkit/

[129] https://securityaffairs.co/wordpress/128159/apt/tunnelvision-exploits-log4j-vulnerability.html

[130] https://www.rezilion.com/wp-content/uploads/2022/04/Log4Shell-4-Months-Later.pdf

[131] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965

[132] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

[133] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847

[134] https://dirtypipe.cm4all.com/

[135] https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html

[136] https://www.mandiant.com/resources/zero-days-exploited-2021

[137] https://www.rsaconference.com/usa/agenda/session/ESPecter%20First%20Real-World%20UEFI%20Bootkit%20Persisting%20on%20ESP

[138] https://www.blackhat.com/us-22/briefings/schedule/#industroyer-sandworms-cyberwarfare-targets-ukraines-power-grid-again-27832

[139] https://www.virusbulletin.com/conference/vb2022/

[140] https://recon.cx/2022/conference.html

[141] https://whova.com/embedded/session/xfYtdNgvSv-eYXY1By4aWq606%4092h9NXnd7hwTzd-z4=/2292486/?widget=primary

[142] https://caro2022.org/agenda/

[143] https://botconf2022.sched.com/event/1199o/ta410-apt10s-distant-cousin

[144] https://botconf2022.sched.com/event/119AL/jumping-the-air-gap-15-years-of-nation-state-efforts

[145] https://nsec.io/speakers/

[146] https://botconf2022.sched.com/event/119A0/proxychaos-a-year-in-review-of-microsoft-exchange-exploitation

[147] https://www.seqcure.org/en/#speakers

[148] https://www.esetworld.com/growth.protected/event-agenda/detail/157

[149] https://eecd.eset.com/agenda/detail/112

[150] https://www.computerworld.pl/event/semaforeng

[151] https://eecd.eset.com/agenda/detail/117

[152] https://eecd.eset.com/agenda/detail/120

[153] https://www.welivesecurity.com/author/goretsky/

[154] https://open.spotify.com/show/1WDjY2A3A3s5FKycrOVkhg

[155] https://podcasts.google.com/feed/aHR0cHM6Ly9mZWVkLnBvZGJlYW4uY29tL2VzZXRyZXNlYXJjaC9mZWVkLnhtbA

[156] https://podcasts.apple.com/us/podcast/eset-research-podcast/id1596306608

[157] https://esetresearch.podbean.com/

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

[159] https://attack.mitre.org/techniques/T1055/015/

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

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

[162] https://attack.mitre.org/resources/updates/updates-april-2022/

[163] https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-and-sandworm/

[164] https://attackevals.mitre-engenuity.org/using-attack-evaluations/

[165] https://www.eset.com/int/business/solutions/xdr-extended-detection-and-response/

[166] https://www.eset.com/blog/awards-and-testing/hunting-down-sandworm-and-wizard-spider-how-eset-fared-in-the-attckr-evaluation/

[167] https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

[168] https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

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

[170] https://www.eset.com/int/about/newsroom/press-releases/research/eset-takes-part-in-global-operation-to-disrupt-trickbot-a-botnet-that-has-infected-over-a-million-c/

[171] https://twitter.com/ESETresearch/status/1409495354534473728

[172] https://github.com/eset/vulnerability-disclosures/commit/0b456d6fd13abb60407c2491904fd11613ead6c9

[173] https://developer.amd.com/amd-uprof/

[174] https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1016

[175] https://www.brighttalk.com/webcast/5567/537094

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

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

[178] 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.

WeLiveSecurity.com
@ESETresearch
ESET GitHub

Digital Security
Progress. Protected.