Digital Security
Progress. Protected.

ESET 脅威レポート

2023 年下半期

2023 年 6 月～ 2023 年 11 月

(eset):research

目次

エグゼクティブサマリー

Android

Android アプリをスパイウェアにする SpinOk

SDK？それともスパイウェア？多数の正規の Android アプリがスパイウェアとして暗躍していましたが、サードパーティの SDK（ソフトウェア開発キット）がその原因でした。

IoT ボットネット

Mozi をテイクダウンしたのは誰？ IoT を標的とする Mozi ボットネットの活動が急減か？

ESET の研究者は、広く拡散していた IoT ボットネットをテイクダウンさせたキルスイッチを発見、分析しました。

Web に関する脅威 AI

悪意のあるドメインでの ChatGPT 名の悪用

OpenAI の API キーと ChatGPT の名前を取り巻く新たな経済圏が生まれており、合法的な参加者とサイバー犯罪組織の両方を引き付けています。

暗号通貨の脅威 情報窃取型マルウェア サービスとしてのマルウェア

クリプトスティーラーとして急激に人気が高まった Lumma Stealer

不正なクリプトマイニングの脅威は廃れつつありますが、Lumma Stealer の成功は、暗号通貨ウォレットが依然としてサイバー犯罪者の標的となっていることを示しています。

IoT Android ボットネット

Android TV Box への攻撃：Pandora、DDoS 攻撃用のボットネットを構築

Mirai をベースとした新たな脅威が、悪意のあるストリーミングアプリを使用して、ラテンアメリカ地域のデバイスを乗っ取っています。

情報窃取型マルウェア Web に関する脅威

e コマースに亡霊のようにつきまとうサイバー攻撃組織「Magecart」

Magecart の攻撃は決して止むことはなく、2023 年下半期も例外ではありませんでした。

Web に関する脅威

Web サイトを利用するユーザーを狙う悪意あるスクリプト

JS/Agent の検出数が増加し、約 45,000 の Web サイトが悪意のある JavaScript コードの被害に遭っていることが明らかになりました。

ランサムウェア

Cl0p と MOVEit のハッキング：大規模な標的型攻撃

1 人の攻撃者が 2 年前に悪用したゼロデイの脆弱性が、どのように世界的なサイバーセキュリティの悪夢を引き起こしたのでしょうか？

序文

2023 年下半期の ESET 脅威レポートをご覧いただきありがとうございます。

2023 年下半期にも、重大なサイバーセキュリティインシデントが多くありました。これまで大規模なランサムウェア攻撃を実行してきたサイバー犯罪組織「Cl0p」は、ファイル転送ツール「MOVEit」に対する大規模なハッキングによって衆目を集めましたが、意外なことに、このハッキングではランサムウェアは展開されていません。この攻撃は、グローバル企業や米国政府機関などを標的としていました。Cl0p の戦略で見られた重要な変化は、身代金が支払われなかった場合に、窃取した情報を世界中の Web サイトに公開するものでした。ALPHV ランサムウェア組織もこのような戦略を取り入れています。FBI は、ランサムウェア組織の他の新たな戦略として、ランサムウェアの複数の亜種を同時に展開する手法や、データを窃取して暗号化した後に、ワイパー型マルウェアを使用する手法も挙げています。

IoT 環境における脅威については、ESET の研究者が重要な発見を行いました。これは、Mozi IoT ボットネットを機能させないために使用されたキルスイッチを特定したことです。Mozi は、過去 3 年間にわたって ESET が監視してきたボットネットの中でも最大級のボットネットです。Mozi が突然停止された原因は、キルスイッチがボットネットの作成者によって使用されたのか、中国の法執行機関による対策であったのか、未だに不明なままです。Android/Pandora という新たな脅威が登場し、スマート TV、TV Box、モバイルデバイスなどの Android デバイスを侵害し、DDoS 攻撃に利用しています。

AI を悪用する攻撃についての議論が白熱する中で、ChatGPT のようなツールを利用するユーザーを標的としたキャンペーンも確認されています。また、ChatGPT チャットボットと関連性があるように見せかけるため、「chapgpt」に似せた名前の悪意のあるドメインが多く使用されています。これらのドメインから発信されている脅威には、OpenAI の API キーを安全に処理していない Web アプリも含まれており、OpenAI API キーのプライバシーを保護する重要性が増しています。

また、SpinOk モジュールが使用されている Android アプリがスパイウェアとして利用される事案が大幅に増加しています。この悪意のあるソフトウェアはソフトウェア開発キット（SDK）として配布され、さまざまな正規の Android アプリケーションに含まれています。2023 年下半期に最も多く記録された脅威の 1 つは、JS/Agent として検出された 3 年前の悪意のある JavaScript コードです。このコードは、侵害された Web サイトから長年にわたって読み込まれています。クレジットカード情報を窃取する脅威である Magecart も、この 2 年間同じように、パッチが適用されていない無数の Web サイトを標的にして拡大し続けています。これら 3 つの脅威については、開発者や管理者が適切なセキュリティ対策を講じていれば、攻撃を防ぐことができたはずです。

これまではビットコインの価値の上昇に伴って暗号通貨の脅威も増加する傾向にありましたが、今期はそうではありませんでした。しかし、情報窃取型ツール「Lumma Stealer」が暗号通貨ウォレットを狙う「サービスとしてのマルウェア」（MaaS）として提供されるようになり、クリプトスティーラーが大幅に増加しました。これらの傾向は、サイバーセキュリティ環境が常に進化しており、サイバー攻撃者はさまざまな戦術を駆使していることを示しています。

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。

ESET 脅威検出部門ディレクター
Jiří Kropáč

脅威環境の動向

Android

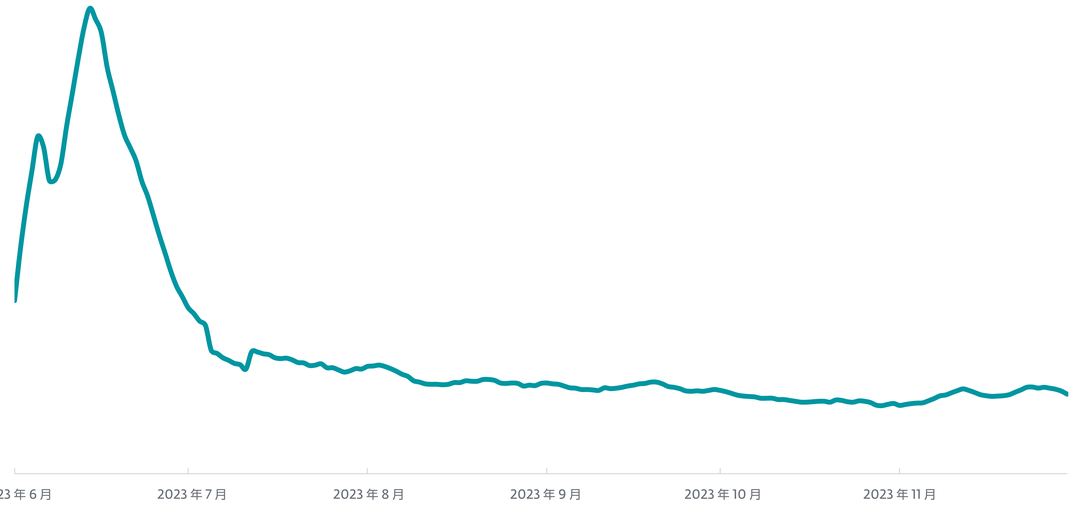
Android アプリをスパイウェアにする SpinOk

SpinOk は SDK なのでしょうか、それともスパイウェアなのでしょうか？多くの正規の Android アプリがスパイウェアとして動作していることが明らかになりました。その原因は、サードパーティのソフトウェア開発キットでした。

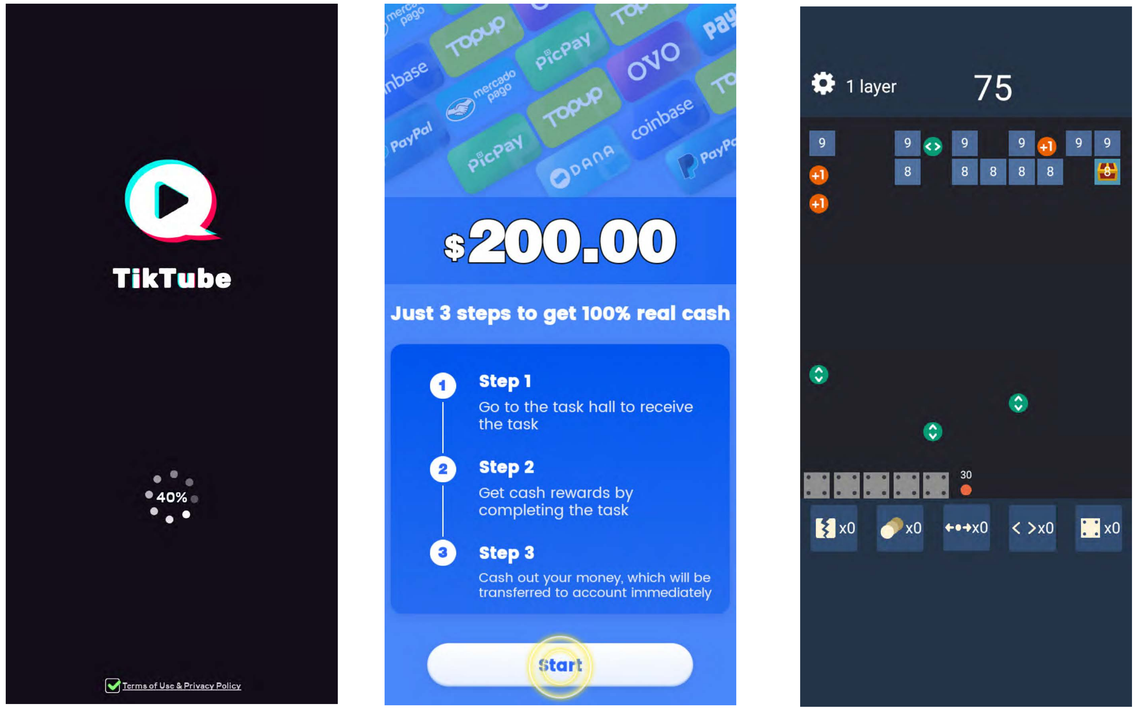
2023 年下半期、ESET のテレメトリ（監視データ）から、Android スパイウェアの検出数が大幅に増加（89% 増）したことが判明しました。この増加の原因は主に、モバイルマーケティングのためのソフトウェア開発キット（SDK）であり、ESET の製品はこの脅威を SpinOk スパイウェアとして識別します。驚くべきことに、この SDK は多くの正規の Android アプリケーションに組み込まれており、これらのアプリは公式のマーケットプレイスで公開されていたのです。その結果、SpinOk スパイウェアは、2023 年下半期に検出された Android の脅威の 7 位に上昇し、この期間に最も拡散したスパイウェアとなりました。ESET のテレメトリで検出されたスパイウェアの約 3 分の 1 が SpinOk でした。

ESET やその他のサイバーセキュリティベンダーが SpinOk スパイウェアを検出したアプリには、OKSpin という名前の企業が提供するモバイルマーケティング用の SDK の特定のバージョンが含まれていました。開発者やマーケティング担当者は SDK をモバイルアプリに統合して、ユーザーデータの収集、ユーザーの行動の分析、パーソナライズしたコンテンツの配信、その他のマーケティング戦略を実行できるようになります。今回の脅威では、OKSpin SDK は、アプリのトラフィックを収益化するためのゲームプラットフォームをアプリ開発者に提供していました。開発者は、この SDK を、公式の Android マーケットプレイスにあるアプリを含め、さまざまなアプリやゲームに組み込むことができます。しかし、OKSpin SDK を搭載したアプリがインストールされると、スパイウェアのように動作し、コマンドアンドコントロールサーバーに接続し、機密性の高いデータが含まれるクリップボードのコンテンツなどのさまざまなデータをデバイスから外部に送信します。

SpinOk はまた、デバイスのジャイロスコープと地磁気センサーから収集されたデータを分析して、エミュレートされた環境を識別します。SpinOk が仮想化環境であると判断すると、



2023 年下半期の **Android/SpinOK の検出の傾向**、7 日移動平均線



スパイウェアとして動作する SDK が含まれるさまざまなアプリの例

サンドボックスや研究者による検出を回避するために動作を変更します。

サイバーセキュリティ企業の **Doctor Web** は、Google Play にある SpinOk スパイウェアが含まれる 101 個のアプリを特定しました。そのすべてが Google Play から削除されたにもかかわらず、ESET のテレメトリは、世界中の Android デバイスにインストールされたこれらの膨大な数のアプリを引き続き検出しています。Doctor Web の調査結果が公開された後に、OKSpin はモジュールを更新しました。

スパイウェアのように動作する SDK が、なぜこれほど多くのアプリに組み込まれ、4 億 2100 万回以上もインストールされた原因は解明されていません。OKSpin のモバイルマーケティング分野におけるプレゼンスは増していますが、自社の情報をオンラインでは大々的に公開していません。同社は、Web サイトで会社の詳細情報を提供していませんが、ESET は同社が**香港で登録されている**ことを特定しました。この会社の住所は、集合オフィスであり、多くの会社が香港にある**同じオフィスビル内**の同じ部屋を本社所在地にしています。これは、OKSpin が**ペーパーカンパニー**であり、その住所は郵便物を受け取り、香港に所在しているように見せかけるためだけに使用されており、実際の業務は別の場所で行われていることを示唆しています。さらに疑念が深まっている理由は、国際的な租税回避詐欺を暴露した**オフショアリークスレポート**に、OKSpin の所在地に隣接する部屋を登記している会社が存在しているためです。

OKSpin が提供している SDK を使用したあるアプリの**代表者**は、この SDK を使用するに至った経緯を説明しており、この SDK がこれだけ多くのアプリケーションに取り入れられた方法が明らかになりました。この代表者によると、OKSpin との最初の接触は、ビジネス開発の代理店が「収益を拡大するプログラム」を提案してきたときでした。このアプリの開発者は、この企業に対する徹底的な調査（デューデリジェンス）を怠ったことを告白しています。このサードパーティ SDK をアプリに組み込む前に適切な評価を行わなかったため、自社の正規のアプリが Google Play から削除されることになりました。この SDK を除去した後に、この開発者は同アプリを Google プラットフォームに再び公開するまでに、長期間にわたる複雑なプロセスを経なければならなくなりました。SpinOk の今回のケースは、公式ストアからアプリをダウンロードしている一般的なユーザーが、アプリにマルウェアや潜在的に望ましくないコードが含まれているかどうかを見分けることができない問題を浮き彫りにしています。サイバーセキュリティ対策のためのアプリは、このようなシナリオで潜在的な脅威を検出する重要な役割を担います。さらに、このケースはアプリ開発者への教訓にもなっています。サードパーティのテクノロジーを十分に調査せずに性急に統合することにはリスクが伴います。不正なコードが含まれている場合、収益源のアプリを稼働することも、公式のアプリストアで公開することもできなくなる恐れがあります。

SpinOk に牽引され、スパイウェアカテゴリの検出数は急増し、他の Android 脅威の検出数が全般的に減少している中で際立っています。SpinOk は、2023 年下半期に Android 検出数が全体で 22% 増加した一因にもなりました。アドウェアは、Android 環境の恒常的な脅威であり、下半期には検出された脅威の総数の 36% を占めました。アドウェアが恒久的に蔓延している原因の 1 つは、押し付けがましい多くの広告を取り入れている無料のモバイルゲームが普及していることです。クリッカーは大幅な増加傾向にあり、検出数は 63% 増加しました。クリッカーの増加は、広告付きアプリの配信が増加していることに関連しています。これは、サイバー犯罪者が利益を挙げることができる戦略にもなっています。しかし、隠しアプリは検出率が 3% ほど微減したものの、Android の脅威の中で最も多く検出されています。検出数が増加した唯一のカテゴリはストーカーウェアであり、5% 増加しました。

アドウェア、クリッカー、隠しアプリは、それぞれ異なる方法で広告を悪用する Android の脅威です。アドウェアは主に、ユーザーのデバイスに迷惑な広告を表示します。一方で、隠しアプリはインストール後にデバイスに巧妙に潜伏し、煩わしい広告を表示するなど、さまざまな悪意のある（少なくとも望ましくない）活動を実行します。一方、クリッカーは、ユーザーに知られることなく自動で広告をクリックし、不正に広告収入を得るように設計されています。広告配信型のトロイの木馬と広告配信型の PUA はそれぞれ、2023 年下半期に検出された Android の脅威トップ 10 に入りました。広告配信型のトロイの木馬が隠しアプリのカテゴリに分類されるのに対し、広告配信型の PUA は PUA（望ましくないアプリケーション）に分類されます。両者は類似していますが、検出されるこれらの 2 つの脅威は Android デバイスで若干異なる挙動を示します。

バンキングマルウェアとクリプトスティーラーを含む金融関連の脅威は 14% 減少し、2023 年上半期から減少傾向が続いています。2023 年の後半には、SMS の脅威（23%）、ランサムウェア（22%）、クリプトマイナー（10%）詐欺アプリ（9%）の検出数も大幅に減少しました。

ESET のエキスパートの解説

SpinOk の問題は、アプリ開発者がサードパーティーベンダーのテクノロジーをアプリに取り入れる場合には、慎重を期する必要があるという教訓になりました。サードパーティテクノロジーのプロバイダーが開発者に営業することは多くありますが、これらのテクノロジーが安全でアプリに適しているかどうか、詳細かつ慎重に評価することが極めて重要です。

SDK のセキュリティを確保するには、プロバイダーが信頼できるかどうかを包括的に調査するなど、さまざまな検証が必要となります。この検証プロセスでは、SDK の機能を理解し、そのドキュメントを調査し、可能であれば、ソースコードに不審な点がないか精査することが求められます。開発者は、本来の機能とは異なる不要な動作や潜在的な脆弱性を発見するために静的解析ツールを活用し、ネットワークトラフィックも監視して予期せぬデータが転送されていないか検証する必要があります。また、検討しているサードパーティ SDK を試験的に統合した後に、実績のあるセキュリティ製品を使用してアプリをスキャンすることも可能です。SDK やプロバイダーがセキュリティ認証や監査を受けているかどうかを確認することも有益です。開発者フォーラムや開発者グループからのフィードバックも確認しておくと良いでしょう。SDK をアプリに組み込む前には、安全な環境でテストを実施し、その動作やパフォーマンスを評価することをお勧めします。SDK をアプリに統合すると、SDK はアプリ内のすべてのデータにアクセスできるようになります。SDK を評価するための十分なリソースが自社になければ、サードパーティの SDK を使用するべきではありません。

ESET シニアマルウェアリサーチャー
Lukáš Štefanko

IoT　ボットネット

Mozi をテイクダウンしたのは誰? IoT を標的とする Mozi ボットネットの活動が急減か?

ESET の研究者は、最も広く拡散していた IoT ボットネットをテイクダウンさせたキルスイッチを発見して分析しました。

2 年以上にわたって、ESET 脅威レポートでは Mozi IoT ボットネットについて取り上げてきました。Mozi IoT ボットネットは自動で運用されており、その検出数は徐々に減少していました。2023 年 8 月にこのボットネット活動の検出が急激に低下しました。まず 2023 年 8 月 8 日にインドで、そしてその 1 週間後の 8 月 16 日にはこれまで最も多くのデバイスを乗っ取ってきた中国で、その活動が検出されなくなりました。ESET が詳細に分析したところ、これは意図的に実行されたテイクダウンでしたが、テイクダウンを実行できる組織は 2 つしか考えられません。

Mozi ボットネットの作成者は、2021 年 7 月に中国当局によって逮捕されました。それ以降も、このボットネットは脆弱性の攻撃を続け、毎年何十万台もの新しい IoT デバイスに侵入していましたが、運用者が逮捕されており、この大規模なボットネットネットワークが利用されることはなく、Mozi ボットコードのアップデートが展開されることもありませんでした。Mozi は主に、脆弱な Netgear DGN デバイス（EDB-25978）、DASAN Networks GPON ホームルーター（CVE-2018-10562）、D-Link ルーター（CVE-2015 2051）、Jaws Web サーバー（EDB-41471）を侵害しますが、このボットネットの拡散力は時間とともに低下していました。2022 年 1 月から 4 月にかけて、このボットネットは、主に中国とインドにある約 50 万台の新しいユニークなデバイスを配下に加えました。その後 4 か月間に乗っ取ったデバイスの台数は 38 万 3,000 台に減少し、2022 年の最後の 4 か月では 28 万 9,000 台にまで減少しました。

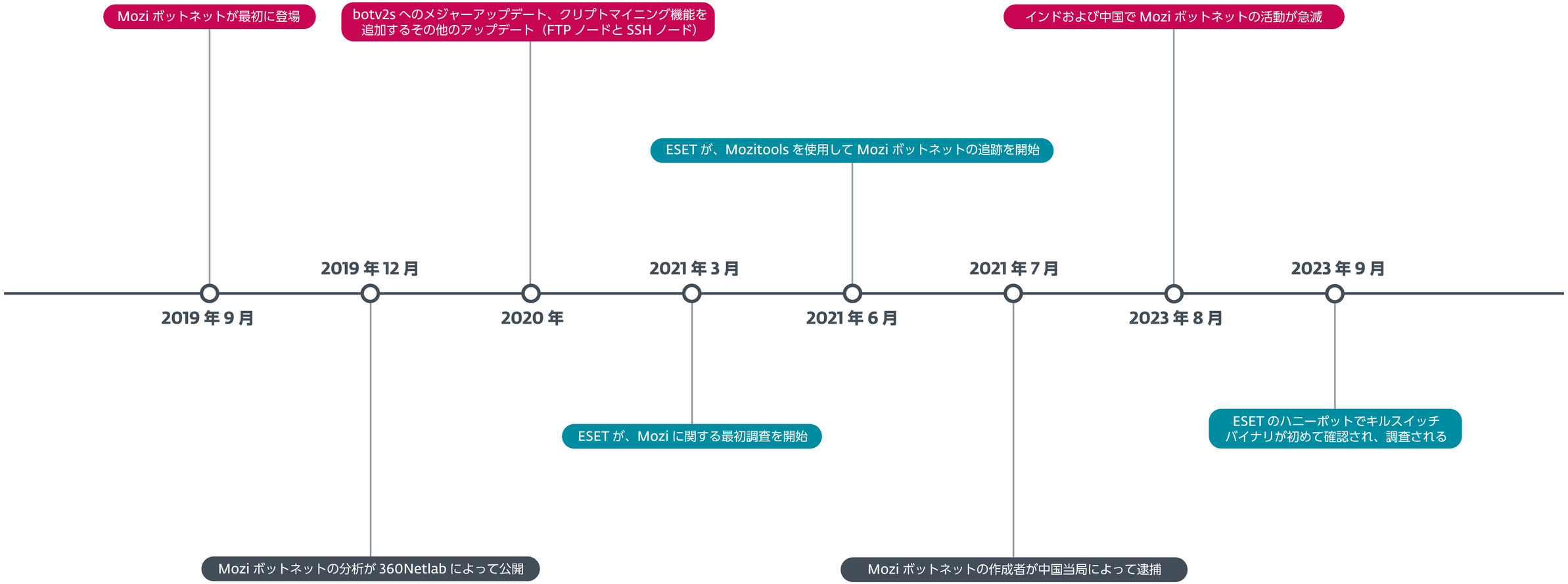
このような傾向の中で、理論的には、侵害するデバイスを見つけられなくなるまで Mozi の活動が継続する可能性もありましたが、突如としてその活動は急激に減少しました。2023 年 8 月、Mozi ボットの拡散が突然停止し、ESET のハニーポットで確認されたユニーク IP の数は、わずか数日間で 89% も減少しました。

この突然の崩壊について ESET が調査した結果、キルスイッチとして機能する制御ペイロード（設定ファイル）を発見できました。このペイロードが配信されると、マルウェアを拡散して伝搬させるすべての試みが停止され、Mozi ボットのほぼすべての機能が削除されます。

```
int __fastcall recursive_dir_crawler_sub_EA24(const char *a1, int a2)
{
  int v4; // r6
  int v6; // r0
  int v7; // r4
  int v8; // r5
  int v9; // r0
  int v10; // r0
  _BYTE v11[1024]; // [sp+0h] [bp-818h] BYREF
  char v12[1048]; // [sp+400h] [bp-418h] BYREF

  v4 = _GI_opendir();
  if ( !v4 )
    return 0;
  while ( 1 )
  {
    v6 = _GI_readdir(v4);
    v7 = v6;
    if ( !v6 )
      break;
    v8 = v6 + 11;
    if ( strcmp(v6 + 11, ".") && strcmp(v7 + 11, "..") )
    {
      v9 = *(unsigned __int8 *)(v7 + 10);
      if ( v9 == 8 )
      {
        v10 = _GI_strrchr(v7 + 11, 46);
        if ( v10 )
        {
          if ( !strcmp(v10, ".sh") )
          {
            memset(v11, 0, sizeof(v11));
            _GI_sprintf(v11, "%s/%s", a1, (const char *)(v7 + 11));
            processSHfile_sub_E848(v11, a2);

          }
        }
      }
      else if ( v9 == 4 )
      {
        memset(v12, 0, 1024);
        _GI_strcpy(v12, a1);
        strcat(v12, "/");
        _GI_strcat(v12, v8);
        if ( !_GI_strstr(v12, "/proc/")
          && !_GI_strstr(v12, "/tmp/")
          && !_GI_strstr(v12, "/var/")
          && !_GI_strstr(v12, "/lib/")
          && !_GI_strstr(v12, "/dev/")
          && !_GI_strstr(v12, "/sys/") )
        {
          recursive_dir_crawler_sub_EA24(v12, a2);
        }
      }
    }
  }
  _GI_closedir(v4);
  return 1;
}
```

```
int __fastcall recursive_dir_crawler_sub_8A60(const char *a1, int a2)
{
  int v4; // r6
  int v6; // r0
  int v7; // r4
  int v8; // r5
  int v9; // r0
  int v10; // r0
  _BYTE v11[1024]; // [sp+0h] [bp-818h] BYREF
  char v12[1048]; // [sp+400h] [bp-418h] BYREF

  v4 = _GI_opendir();
  if ( !v4 )
    return 0;
  while ( 1 )
  {
    v6 = _GI_readdir(v4);
    v7 = v6;
    if ( !v6 )
      break;
    v8 = v6 + 11;
    if ( strcmp(v6 + 11, ".") && strcmp(v7 + 11, "..") )
    {
      v9 = *(unsigned __int8 *)(v7 + 10);
      if ( v9 == 8 )
      {
        v10 = _GI_strrchr(v7 + 11, 46);
        if ( v10 )
        {
          if ( !strcmp(v10, ".sh") )
          {
            memset(v11, 0, sizeof(v11));
            _GI_sprintf(v11, "%s/%s", a1, (const char *)(v7 + 11));
            if ( !access(v11, 2) )
            {
              if ( !sub_898C() )
              {
                sub_83E0(v11, a2);
                sub_F3E4(0);
              }
              sub_101B4(1);
            }
          }
        }
      }
      else if ( v9 == 4 )
      {
        memset(v12, 0, 1024);
        _GI_strcpy(v12, a1);
        strcat(v12, "/");
        _GI_strcat(v12, v8);
        if ( !_GI_strstr(v12, "/proc")
          && !_GI_strstr(v12, "/haha")
          && !_GI_strstr(v12, "/tmp")
          && !_GI_strstr(v12, "/var")
          && !_GI_strstr(v12, "/lib")
          && !_GI_strstr(v12, "/dev")
          && !_GI_strstr(v12, "/sys") )
        {
          recursive_dir_crawler_sub_8A60(v12, a2);
        }
      }
    }
  }
  _GI_closedir(v4);
  return 1;
}
```

元の Mozi の検体のコードスニペット（左）と 2023 年に確認されたキルスイッチの検体（右）



Mozi のタイムライン

ESET の研究者は、BitTorrent の分散型のスロッピーハッシュテーブル（BT-DHT）プロトコルの典型的なカプセル化が欠落しているユーザーデータグラムプロトコル（UDP）メッセージ内に、キルスイッチが存在していることを特定しました。テイクダウンを実行した人物は、この制御ペイロードを利用可能な各ボットに 8 回送信し、常に HTTP 経由でアップデートをダウンロードしてインストールするようにデバイスに指示していました。

この制御ペイロードはいくつかの他の機能も実行します。例えば、親プロセスを終了し、元の Mozi ファイルをこのペイロードに置き換える、sshd や Dropbear などのシステムサービスを無効にする、ルーター / デバイス設定コマンドを実行する、特定のポートセットへのアクセスを無効にするなど機能を行います。

Mozi ボットネットの機能は大幅に削減されましたが、活動自体は持続しています。また、リモートサーバーに ping コマンドを実行していますが、これはおそらく、統計を取ることが目的でしょう。これらの操作が実行されていることは、Mozi の突然の停止が、意図的かつ計算された行為であることを示しています。さらに詳細に調査したところ、このキルスイッチはボットネットの元のソースコードと密接に関係しており、バイナリの署名には正しい秘密鍵が使われていました。

これらの事実から、このボットネットの元の作成者またはこの作成者からの協力を強制した中国当局がこのボットネットの機能を一時的に除去した可能性があるという仮説を ESET は立てています。

最も拡散している IoT ボットネットが終焉するケースは、サイバーフォレンジックの観点からも調査すべき重要なケースであり、このようなボットネットが作成、運用、解体される方法について興味深い技術的な知見をもたらしてくれます。今後数か月のうちに、ESET の研究者が詳細な分析結果を WeLiveSecurity.com で公表する予定です。

2023 年下半期の **Mozi の活動の世界的な急減**、7 日移動平均

ESET のエキスパートの解説

IoT マルウェアは、検出や監視が困難であり、対策を講じることができないことも多く、この数年間は十分な対応がなされていませんでした。しかし、Mirai やその系統のボットネットの脅威は、スマートデバイスを悪用して大規模な DDoS ネットワークや匿名ネットワークを構築したり、VIP ユーザーを標的として追跡したりすることを可能にしており、重大なリスクになっています。

IoT を保護するための優れたセキュリティ対策や標準は存在しますが、すべてのメーカーが対策や規格を積極的に取り入れているわけではありません。その理由は、コストの問題や怠慢などさまざまです。また、多くのエンドユーザーは、IoT のセキュリティ向上を真剣に求めていません。ルーターや防犯カメラのレコーダーが一部不正な活動をしていても、エクスペリエンスには大きな影響がないため、無関心になっているのです。

一方で、サイバー攻撃者は脆弱性を悪用し、増え続ける弱点やデバイスの種類を、驚くべき熟練度で悪用しています。そのため、このような行動を監視するハニーポットが極めて重要な意味を持つようになり、Mozi の停止のような事態を特定するのに役立ってきました。結局のところ、インターネットのデジタルセキュリティを向上させていくためには、新たに出現するあらゆる潜在的なサイバー脅威を把握して対処することが重要です。

ESET マルウェアリサーチャー、
Milan Fránik

Web に関する脅威 AI

悪意のあるドメインでの ChatGPT 名の悪用

OpenAI の API キーと ChatGPT の名前を取り巻く新たな経済圏が生まれており、合法的な企業とサイバー犯罪組織の両方を引き付けています。

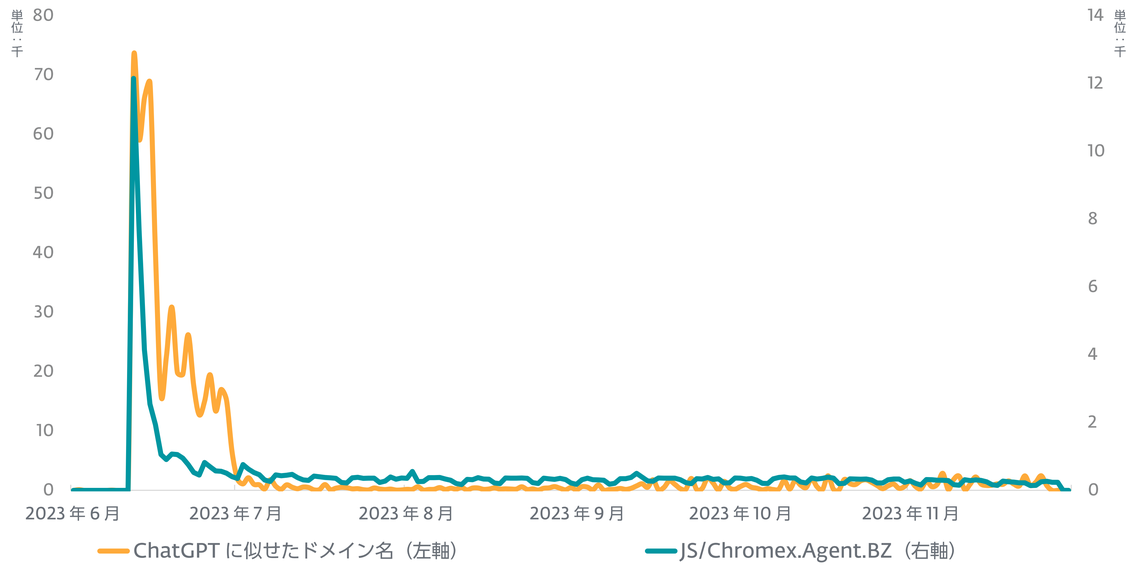
2023 年下半期の ESET テレメトリの記録では、ChatGPT のチャットボットを明らかに意識した文字列である `chapgpt` や類似テキストが名前に含まれる悪意のあるドメインへのアクセス試行が 650,000 件以上ブロックされています。これらの攻撃の多くは 6 月にブロックされましたが、その後数か月間も、OpenAI のサービスを提供すると偽って宣伝する悪意のあるドメインが次々と登場しました。

このようなドメインからは、OpenAI API キーを安全に処理しない Web アプリや、ChatGPT 向けの悪意のある Google Chrome ブラウザ拡張機能などが配信されています。

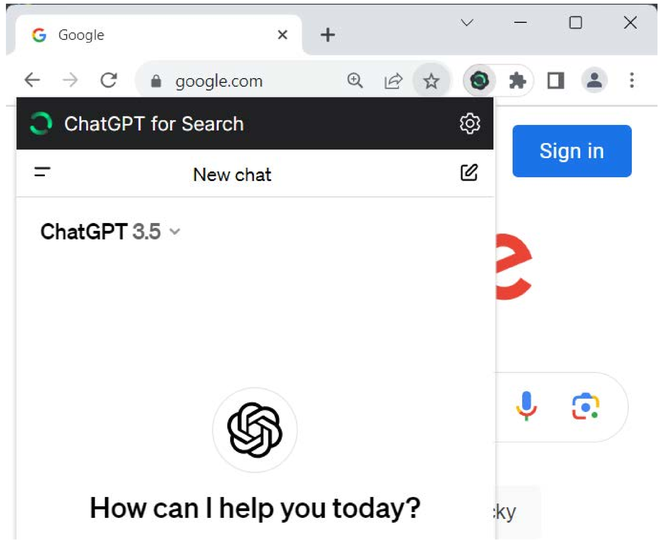
OpenAI は、GPT、DALL-E、Whisper など、**OpenAI によって訓練された AI モデル**にアクセスする API を提供しています。API を使用するには、OpenAI からキーを取得し、そのキーを **HTTP 認証ヘッダー**で `api.openai.com` エンドポイントに送信する必要があります。その後で、OpenAI は各 API キーのユーザーにトークンの使用数に応じて課金します。

従って、API キーのプライバシーを保護することは、API を予算内で利用するためにも非常に重要です。しかし、一部の開発者は、ユーザーに代わって `api.openai.com` への呼び出しを行うという触れ込みで、ユーザーの OpenAI API キーを要求する BYOK（Bring Your Own Key：独自の鍵の持ち込み）アプリを構築しています。このアプリが開発者のサーバーにキーを送信している場合、OpenAI API への呼び出しが行われているとしても、このキーが漏えいや悪用されない保証はほとんどありません。そのために、OpenAI は、**API キーは秘密**であり、他者と共有したり、ブラウザやアプリなどのクライアントサイドのコードでは公開したりしないように、何度も**忠告しています**。

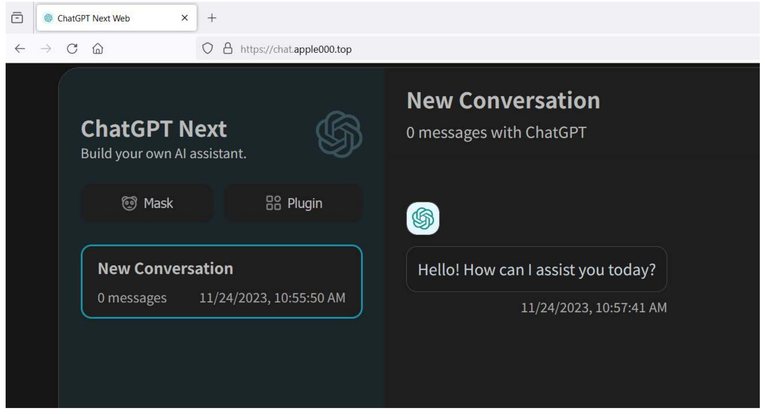
`chat.apple000[.]top` でホスティングされている ChatGPT Web アプリが、ユーザーに OpenAI API キーの入力を求め、自身のサーバーに送信しているケースもありました。



ChatGPT に似せた悪意のあるドメイン名と JS/Chromex.Agent.BZ の検出数、2023 年下半期



ブラウザ拡張機能「ChatGPT for Search Chrome」は JS/Chromex.Agent.BZ として検出される



OpenAI の API キーを自身のサーバーに送信する ChatGPT Web アプリ

この Web アプリは、作成元の **GitHub のオープンソースコード**にリンクしています。「ChatGPT Next Web」というタイトルを使用している HTML Web ページの **Censys クエリー**を実行したところ、7,000 台以上のサーバーがこの Web アプリのコピーをホストしている可能性があることが分かりました。これらのコピーが、OpenAI の API キーのフィッシングキャンペーンの一環として作成されたのか、別の理由でインターネットに公開されたのかを判断することはできませんが、信頼できないサーバーに送信しているアプリに OpenAI の API キーを入力することは決してお勧めできません。

これらの Web アプリ以外では、2023 年後半に ChatGPT と関連するように見せかけた悪意のあるドメイン名がブロックされたほぼ全てのケースは、JS/Chromex.Agent.BZ として検出される Chrome 拡張機能に関連していました。この脅威は 6 月に初めて検出されています。

例えば、`gptforchrome[.]com` は、Chrome Web ストアにある不正な拡張機能 **ChatGPT for Search - Support GPT-4** にリンクしていたため、ESET は、この問題を Google に報告しました。6 月には、別のデベロッパーもこの拡張機能が悪意のある可能性があることを**報告しています**。

この Chrome 拡張機能は**「Service Worker」**を使用して、`tracker.js` ファイルから JavaScript をインポートし、`gptforchrome[.]comserver` に以下の情報を定期的に送信します。

- 拡張機能 ID
- 拡張機能のバージョン
- 拡張機能によって割り当てられた固有のユーザー ID
- 現在のタイムスタンプ

サーバーが応答として URL を送信する場合、この拡張機能はその URL を新しいブラウザタブに表示できます。この機能は開発者によって明らかにされておらず、悪意のある Web ページに誘導される可能性があります。

ESET のエキスパートの解説

ブラウザの同期をオンにしている場合、悪意のあるブラウザ拡張機能を削除しただけでは、再度侵害される恐れがあります。同期プロセスが実行されるときに、拡張機能などの他のデバイスのブラウザデータが、現在のデバイスのブラウザでも利用できるようになるためです。そのため、同期を有効にしている場合、悪意のあるブラウザ拡張機能はすべてのデバイスで削除する必要があります。さらに良い対策は、ブラウザ拡張機能をインストールする前に慎重に調査し、これらの機能に悪意のあるコードが潜在していないかどうかを検出できる、信頼性の高い多層防御ソリューションを使用することです。

ESET 脅威検出部門ディレクター、
Jiří Kropáč

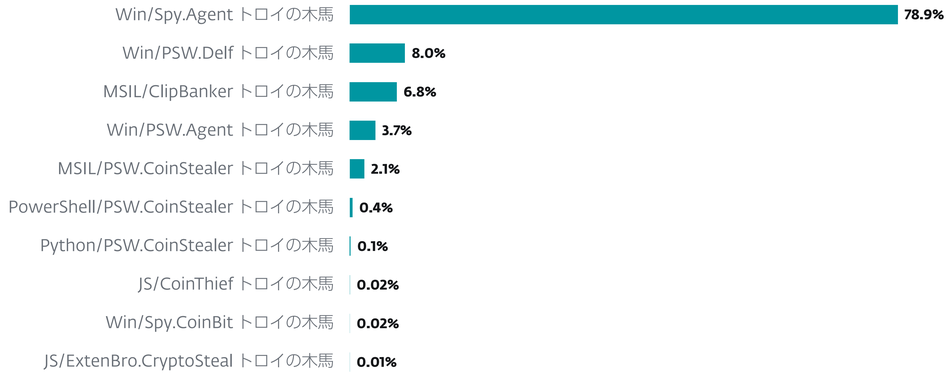
暗号通貨の脅威 情報窃取型マルウェア サービスとしてのマルウェア

クリプトスティーラーとして急激に人気が高まったLumma Stealer

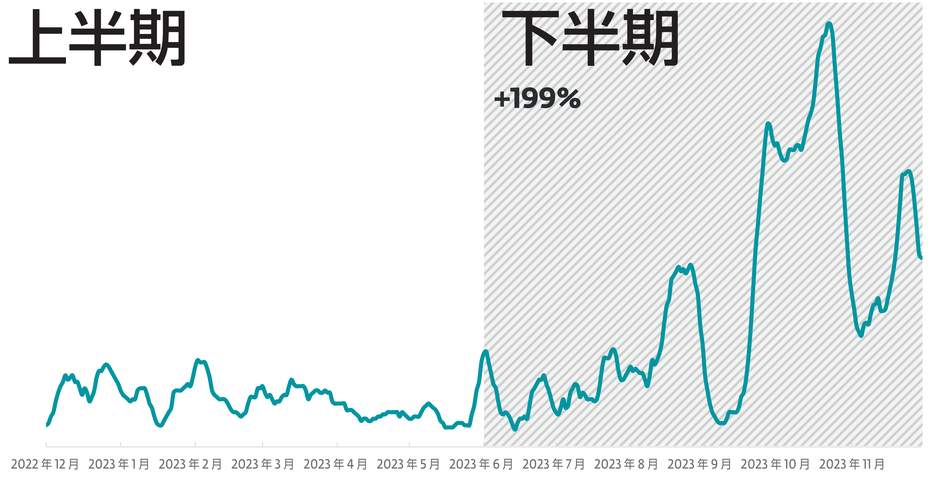
不正なクリプトマイニングは廃れつつありますが、Lumma Stealer の成功は、暗号通貨ウォレットが依然としてサイバー犯罪者の標的であることを示しています。

2023 年下半期も、前回の**脅威レポート**で説明した状況が続きました。ビットコインの為替レートは上昇を続けましたが、暗号通貨の脅威は増加しませんでした。ESET が検出した暗号通貨の脅威の大半を占めるクリプトマイナーが再び急減（21% 減）した一方で、クリプトスティーラーは増加する傾向にありました。2023 年下半期に、クリプトスティーラーの脅威は 68% 以上増加しました。このカテゴリの急増は、このカテゴリで検出されたトロイの木馬の約 80% を占める、たった 1 つの脅威である Win/Spy.Agent.PRG によって引き起こされたため、暗号通貨の脅威がマイニング（採掘）から窃取へ大きく変わったと断定することはできません。

ESETのテレメトリデータに登録されている検体とVirusTotalで検出された検体を照合した結果、Win/Spy.Agent.PRGは情報窃取型ツールであることが判明しました。**Lumma Stealer** と呼ばれる、サービスとしてのマルウェア（MaaS）として提供されているこのマルウェアは、LummaC2 Stealerとも呼ばれ、C 言語で書かれており、暗号通貨ウォレット、ユーザーの認証情報、二要素認証ブラウザの拡張機能を標的にしています。また、侵害したマシンから情報を外部に送信します。2023 年上半期から下半期にかけて、Lumma Stealer の検出数は 3 倍に増加しました。Win/Spy.Agent.PRG が最も多く検出されたのは下半期の後半であり、10 月にピークを記録しています。



2023 年下半期の**クリプトスティーラーのトップ 10**（クリプトスティーラー検出数に占める割合）



2023 年上半期～下半期の **Lumma Stealer の検出傾向**、7 日移動平均線

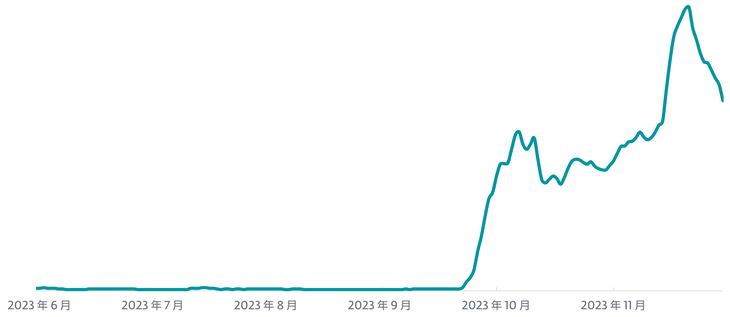
この新しく活発な MaaS は 2022 年 8 月に初めて登場し、地下フォーラムやテレグラムで販売されています。サービスレベルに応じて、250 米ドルから最大で 2 万米ドルまでの価格で**提供されています**。最高のサービスレベルでは、購入者は情報窃取型マルウェアのソースコードにアクセスでき、このマルウェアを自分で販売することも可能です。

実は、2022 年以前に ESET は Win/Spy.Agent.PRG を検出しています。サイバーセキュリティ企業 **Sekoia.io** とユーザー **Fumik0** が X（旧 Twitter）で共有した情報に基づき、ESET は、2022 年以前の検出は、情報窃取型ツール Mars、Arkei、Vidar に属しており、これらのツールに共通するコードベースが、Lumma Stealer を作成するために再利用されたと考えています。

Lumma Stealer の人気がサイバー犯罪者の間で高まっている背景には、販売可能であり、その機能が暗号通貨の窃取だけではないことが主な要因です。2023 年上半期の ESET 脅威レポートでは「RedLine Stealer」について取り上げましたが、直ぐに使用できる商品としてマルウェアが販売されており、技術的なスキルの低いサイバー攻撃者でも簡単に利用できるようになっていることが、悪意のあるキャンペーンの拡散に拍車をかけています。Lumma Stealer は、幅広い機能を提供することで、サイバー攻撃者にとって魅力的な製品となっています。

この情報窃取型ツールは、主に VLC や ChatGPT のようなソフトウェアをハッキングして拡散していますが、他の配信方法も確認されています。例えば、2023 年 2 月には韓国の YouTuber が、ゲーム会社のバンダイナムコになりすましたスピアフィッシングによって**標的になっています**。サイバー攻撃者はまた、人気の高いチャットプラットフォーム Discord の**コンテンツデリバリネットワーク**を介して、このツールを拡散させています。さらに、Lumma Stealer は、最近発生した偽のブラウザアップデートキャンペーンで使用されているペイロードの 1 つとして利用されている可能性もあります。このキャンペーンでは、侵害された Web サイトにオーバーレイが表示され、サイトにアクセスするために**ブラウザのアップデート**するようにユーザーに求めていました。更新ボタンをクリックすると、RedLine、Amadey、Lumma Stealer などのマルウェアがユーザーのマシンに配信されます。

ESET は、Lumma Stealer が Win/TrojanDownloader.Rugmi トロイの木馬によって配信されていることも確認しています。このマルウェアは、暗号化されたペイロードをダウンロードするダウンローダー、内部リソースからペイロードを実行するローダー、そしてディスク上の外部ファイルからペイロードを実行するローダーの 3 種類のコンポーネントが含まれるローダーです。Lumma Stealer 以外にも、Win/TrojanDownloader.Rugmi は、Vidar、Rescoms、RecordBreaker などの他の情報窃取型ツールを配信するために使用されています。このローダーの検出数は下半期に急増し、1 桁であった 1 日の検出数が数百件にまで増加しました。



2023 年下半期の **Win/TrojanDownloader.Rugmi の検出傾向**、7 日移動平均線

暗号通貨の強奪と詐欺

暗号通貨を標的とするマルウェアの検出率は過去と比較すると鈍化していますが、2023 年下半期には暗号通貨に関連する大規模なサイバー犯罪が目立ちました。

NFT の開発者を装った暗号通貨詐欺

FBI は、犯罪者が正規の NFT 開発者を装い、暗号通貨資金を窃取している詐欺について**警告しました**。これらの詐欺師は、一般に公開していない NFT を獲得するチャンスがあると主張する投稿によってユーザーを引き付けて、正規の NFT の開発者になりすました Web サイトに誘導します。ユーザーがこの Web サイトから NFT を購入しようとすると、サイバー攻撃者はこのユーザーの暗号通貨ウォレットの資金を盗み出します。

約 9 億米ドル相当の暗号通貨を窃取した Lazarus

2022 年 7 月から 2023 年 7 月までの間に、APT グループである Lazarus が、クロスチェーン犯罪によって約 9 億米ドルの暗号通貨を**洗浄しました**。クロスチェーン犯罪とは、犯罪者が暗号通貨資産の出所を特定されないように、あるトークンやブロックチェーンから別のトークンやブロックチェーンに繰り返し変換する行為です。

イーロン・マスク氏になりすました暗号通貨詐欺が、新たなプラットフォームを悪用

イーロン・マスク氏が暗号通貨をプレゼントするという詐欺は、X や Instagram では以前から多く行われてきました。現在、詐欺師は動画共有プラットフォーム **TikTok** で、マスク氏が対話しているディープフェイクを使用して、新たな標的を見つけています。宣伝された報酬を受け取るために、登録料を事前に入金をするように要求されますが、その詐欺サイトへの入金はそっくりそのまま盗まれます。

パスワードマネージャーの LastPass が侵害され 440 万米ドル相当の暗号通貨が盗まれる

10 月にハッカーは流出した LastPass のデータベースのプライベートキーとパスフレーズを使用して、440 万米ドル相当の暗号通貨を**盗みました**。LastPass は 2022 年に 2 回侵害されており、サイバー攻撃者は同社の顧客データにアクセスできるようになりました。

IoT Android ボットネット

Android TV Box への攻撃：Pandora、DDoS 攻撃用のボットネットを構築

Mirai をベースとした新たな脅威が、悪意のあるストリーミングアプリを使用して、ラテンアメリカ地域のデバイスを乗っ取っています。

インターネットに接続されるあらゆるデバイスは、サイバー犯罪者の標的になる恐れがあります。スマートテレビやその周辺機器も例外ではありません。2023 年 9 月、新たな IoT ボットネットが誕生しました。ESET はこのボットネットを Android/Pandora として検出します。Doctor Web によって初めて報告されたこの脅威は、Android デバイス（特に Android TV Box）を Mirai ベースのマルウェアによって侵害します。このマルウェアに乗っ取られたデバイスは、ボットネットの運営者によって DDoS 攻撃を実行するために使用されます。

ESET のテレメトリから、Android/Pandora は何万台もの Android デバイスを侵害しようとしていることが分かりました。これらの試行の約5分の1が ESET Smart TV Security によって検出され、ユーザーのテレビで直接ブロックされています。

最も攻撃が活発化したのは 9 月 8 日で、2,000 回以上の攻撃がありました。攻撃の第一波が去った後には、攻撃回数が 1 日 500 回程度に減少しました。最も多くのユーザーが標的となった地域はラテンアメリカであり、ブラジルがトップ（20%）で、メキシコ（13%）、ペルー（11%）が続いています。

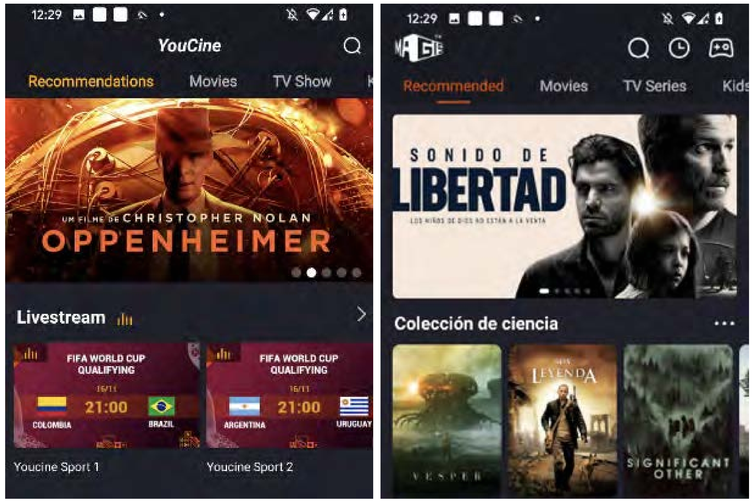
Android/Pandora マルウェアを配信する方法としては 2 つが考えられます。最初の方法は、悪意のあるファームウェアアップデートを使用するものです。このアップデートは、再販業者によって Android TV Box にプリインストールされた、あるいは、無防備なユーザーがダウンロードおよびインストールした可能性があります。

しかし、主な配信方法は、「MagisTV」、「Tele Latino」、「YouCine」といった名前の悪意のあるアプリを拡散している Web サイトと考えられます。これらのアプリは、テレビ、スマートフォン、タブレット、Android TV Bpx だけでなく、Amazon や Xiaomi の TV スティック向けにも提供されています。これらのアプリをインストールすると、ストリーミングサービスや海賊版のコンテンツが提供され、無料、トライアル、またはプレミアムアカウントで利用できるようになります。ユーザーから見ると、このアプリは不正な要素の全く見せることなく、約束されたすべての機能とコンテンツを提供しています。さらに、有料プランに加入したユーザーは、デバイスからこのマルウェアを自発的に削除しようとしないと考えられます。

2023 年 9 月から 2023 年 11 月までの **Android/Pandora の検出傾向**

ANDROID TV BOX

ANDROID TV BOX は、IoT の周辺機器であり、通常はボックスやドングルとして提供されます。これらのボックスやドングルをテレビに接続することで、TV の従来の機能ではサポートされていなかったストリーミングアプリやコンテンツにアクセスできるようになります。



悪意のあるこのアプリのユーザーインターフェイス

アプリの権限リストには、スパイウェア機能を示すような侵入的な権限はないように見えますが、Pandora は Smart TV にインストールされると、スーパーユーザー権限またはルート権限を要求します。しかし、この要求を実行するためには、アプリをインストールした時点ですでにデバイスがルート化されている必要があります。このアプリはデバイス自体をルート化しません。

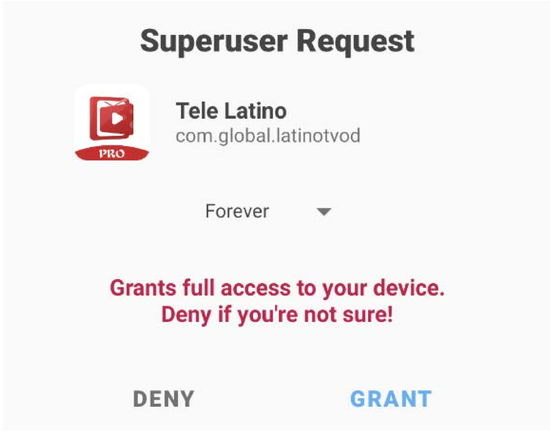
その他の Mirai ベースのボットネット

Pandora ボットネットが台頭する一方で、ESET が追跡している他の Mirai ベースのボットネットである Gafgyt、BotenaGo、Dofloo、Tsunami、Zero などは減退しました。ESET のテレメトリによると、ボット化された IoT デバイスのこれらのネットワークが 2023 年下半期に実行した攻撃数は 750 万件にとどまり、2023 年の上半期と比較すると 59% 減少しました。これらの攻撃が最も多かったのはアメリカ（22%）、ドイツ（7%）、イギリス（7%）でした。

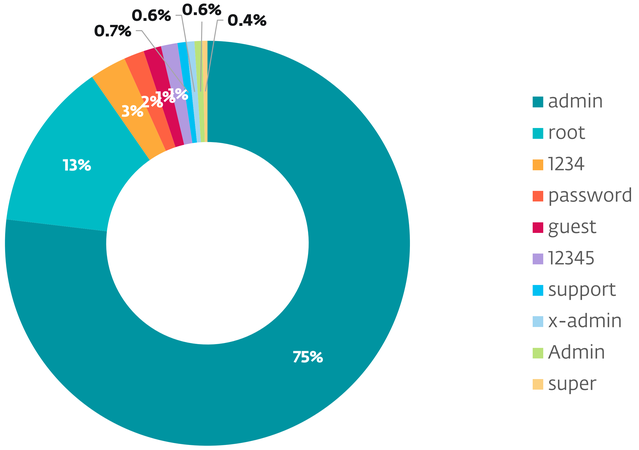
多少の違和感があるかもしれませんが、これらのボットネット用に修正された Mirai ペイロードを配信しているサーバー台数はわずか 3%（わずか数十台）しか減少しておらず、Mirai をベースとする IoT ボットネットは、2023 年の上半期と下半期の間に 106,000 台から 168,000 台以上へと 58% 増加しています。

この増加のうち最も大きな割合を占めたのはエジプトで、検出された侵害デバイスのうち 110,000 台（65%）近くをホストしており、2023 年上半期の 42,000 台（39%）と比べて 164% も急増しました。一方で、Mirai ベースのボットネット攻撃を受けたユニークデバイスの割合が最も高かったのは、ドイツ（16%）、米国（9%）、メキシコ（7%）でした。

Mirai ベースのボットネットは、CVE-2023-26801 を攻撃するようになり、2023 年下半期に悪用された脆弱性のリストにも影響を及ぼしています。CVE-2023-26801 は、最近報告された LB-LINK ルーターのコマンドインジェクションの脆弱性であり、過去 6 か月間で 2 番目に多く悪用されており、検出された攻撃試行数の 10% を占めました。



Pandora は、Android Smart TV でスーパーユーザー（root）権限を要求する



2023 年に使用された最も一般的で脆弱な IoT デバイスのパスワードトップ 10

情報窃取型マルウェア Web に関する脅威

e コマースに亡霊のように常につきまとうサイバー攻撃組織「Magecart」

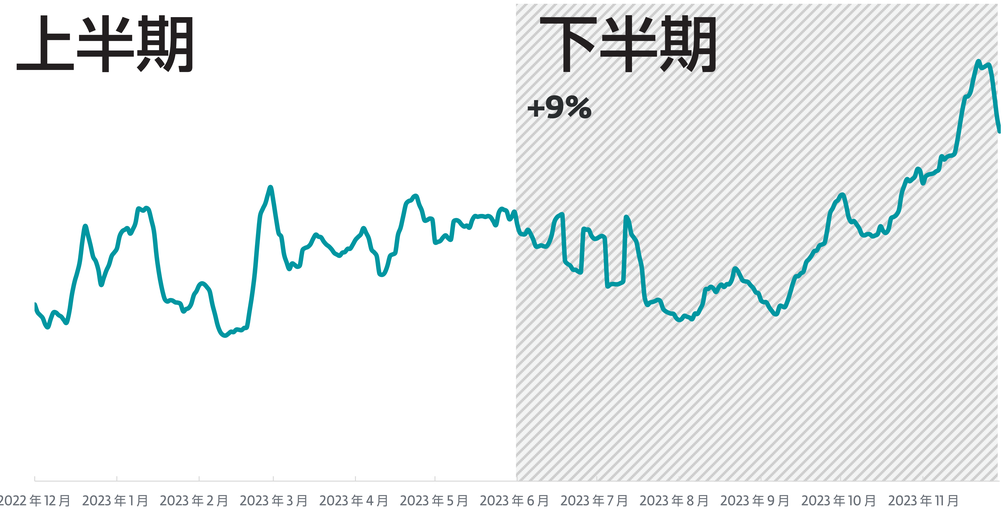
Magecart による攻撃は決して止むことはありません。2023 年下半期も例外ではありませんでした。

Magecart は 2015 年から、オンラインショッピングとホスピタリティプラットフォームを標的にした攻撃を成功させてきましたが、その勢いは今後も止まりそうにありません。ESET のデータによると、このマルウェアの増加傾向が始まってから 2023 年下半期で 2 年目になります。しかし、Magecart がこれほどまでに蔓延している理由はどこにあるのでしょうか？

ESET テレメトリでは、Magecart は JS/Spy.Banker として検出され、Web スキミング攻撃に分類されます。Web スキミング攻撃とは、ハッキングした Web サイトやパッチが適用されていない Web サイトのコードに悪意のあるオンラインスクリプトを挿入し、これらの Web サイトを閲覧するユーザーから情報を盗むことを目的としています。Magecart は主にクレジットカードのデータを窃取することを狙っており、Magento や WordPress プラットフォームでホストされている Web サイトを標的にしています。Magecart 攻撃を操っているサイバー攻撃組織は 1 つではありません。ESET は、Magecart を使用しているいくつかのグループの活動を追跡しています。

このマルウェア系統は、ESET が最も多く検出した情報窃取型マルウェアの統計で常に上位にランクインしています。2023 年下半期には 2 位となり、検出数は数万件を数え、Magecart よりも多く検出された情報窃取型マルウェアは Agent Tesla のみとなりました。JS/Spy.Banker の検出は Web サイトへのユニークアクセス数に基づいているため、メールの添付ファイルやダウンローダーのペイロードとして配信される脅威と比較すると、一般的に検出数は多くなります。

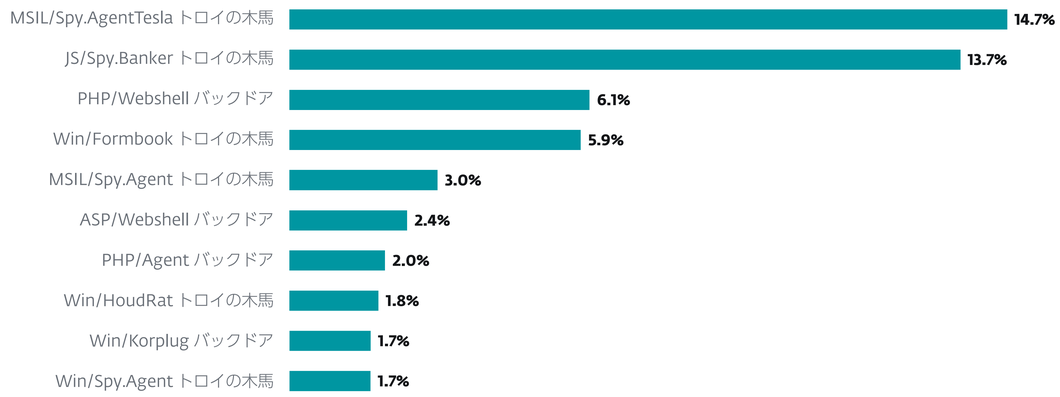
しかし、Magecart の脅威が非常に広がっていることに疑いの余地はありません。ESET のデータを見ると、JS/Spy.Banker は 2021 年末から増加しており、2021 年から 2023 年の間の全体検出数の増加率は 343% に達しています。2023 年下半期に着目すると、このマルウェア系統は劇的に増加したわけではありませんが（9% 増）、検出数は 10 月から増加し始め、11 月を通じて検出率は増加しています。11 月下旬から年末にかけては、多くの国でホリデーシーズンとなり、オンラインショッピングが増える時期でもあるため、Magecart の検出率が増加するのは驚くことではありません。



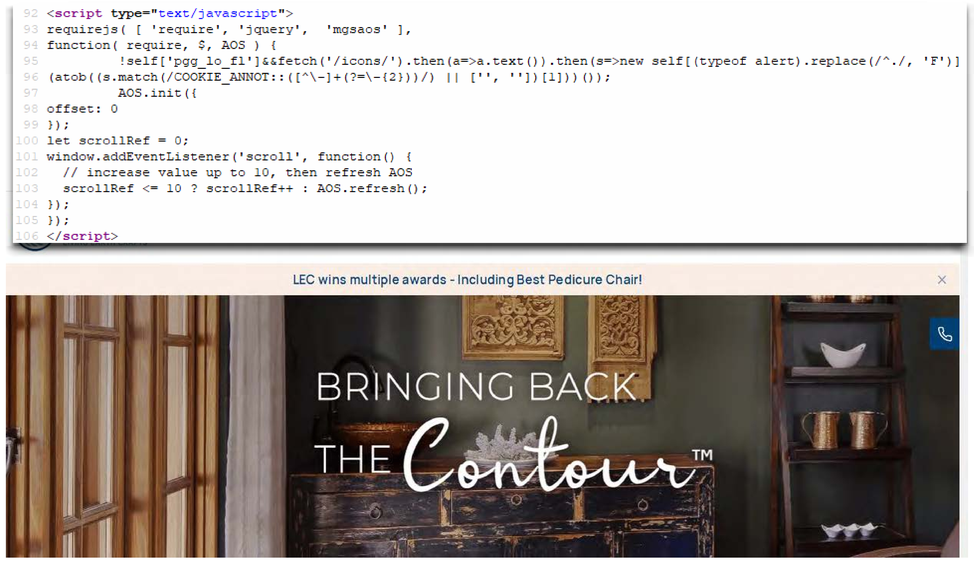
2023 年上半期～下半期の **JS/Spy.Banker の検出傾向**、7 日移動平均線

Magecart の攻撃は、他のサイバー犯罪と比較しても決して派手でも洗練されてもいませんが、何年もの間、サイバー犯罪者によって悪用され続けています。比較的簡単にコーディングできるスクリプトを使用しており、その簡便さが有利に働いている一方で、パッチが適用されていない無数の Web サイトが格好の標的となっています。また、現在の AI ブームも Magecart にとって好都合になっている可能性があります。研究者は、ChatGPT を悪用して、Web スキミング攻撃のためのスクリプトを記述でき、より多くのサイバー犯罪者がこのタイプのマルウェアを利用できるようになっている可能性があると**指摘しています**。

金銭や個人情報がサイバー犯罪者の手に渡るなどの、侵害された Web サイトの顧客に対する明らかな影響とは別に、Magecart 攻撃によって標的となった企業は壊滅的な打撃を受ける恐れもあります。顧客からの信頼を失い、顧客数が減少することで収益が低下し、これらの企業は金銭的な影響を受けることになります。また、法的な問題が生じる可能性もあります。例えば EU では、これらのデータ漏洩が発生した企業は GDPR に違反し、多額の罰金を科される恐れがあります。IBM が公開した最近の**レポート**では 2023 年におけるデータ侵害の平均コストは 445 万米ドルと試算されています。



2023 年下半期の**情報窃取型マルウェアの検出率トップ 10**（情報窃取型マルウェア検出数に占める割合）



JS/Spy.Banker によって侵害された Web サイトと、そのページにリンクされた悪質なコード

しかし、Magecart の Web スキミング攻撃から自社を守ることは可能です。Web サイトの侵害を防止するには、Web サイトのサーバーと CMS で最新のソフトウェアが実行されていることを確認し、これらのリソースを管理するアカウントが強力な認証方法（強力なパスワードや二要素認証の使用など）で保護されていることを確認する必要があります。

2023 年下半期には、e コマース Web サイトを侵害する方法でいくつかの注目すべき攻撃の進化が見られました。これは、Magecart が少なくとも現在まで停滞することなく、悪用されているもう 1 つの理由になっています。

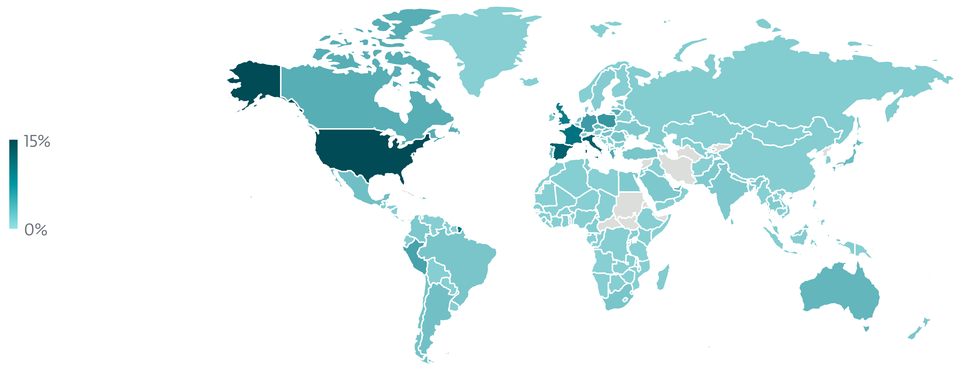
Akamai 社のアナリストは、このようなさらに巧妙な攻撃を調査した 2 つの記事を公開しています。そのうちの**1 つ**は、サイバー犯罪者が正規の Web サイトを悪用して、他の Web サイトを攻撃する方法について説明しています。最初に、脆弱なサイトに Magecart のコードを挿入し、このサイトでコードをホストします。次に、既に侵害している脆弱な Web サイトから完全なコードを取得するローダーとして、悪意のある JavaScript コードスニペットを使用して、実際の標的を攻撃します。

ESET も、リンク先の記事に記載されているのと同じ機能を持つスクリプトを検出しています。スキミング攻撃用のコードが標的の Web サイトにない場合には、ESET 製品は通常、このコードをロードするスクリプトを検出します。これらのスクリプトは、多くの場合、JS/Redirector や JS/Agent 系統のマルウェアに属します。

もう 1 つの調査レポートは、404 エラーページに Magecart スクリプトを隠蔽する方法を解説しています。ユーザーが購入した商品の代金を支払おうとすると、悪意のあるコードがスキミング攻撃のスクリプトが含まれる 404 ページを呼び出し、チェックアウトページを精巧に偽装した支払フォームをそのページ上にオーバーレイとして表示し、ユーザーが入力したデータを取得します。ESET は、404 ページに隠蔽されたコードスニペットローダーを JS/Spy.Banker.MC として検出します。

HTML エラーページを悪用する手法は、サイバー犯罪者の常套手段となっています。例えば、今はなき TeslaCrypt ランサムウェアは、HTML タグの中に C&C コマンドを隠していました。幸いなことに、Magecart スクリプトは、サイバー攻撃者が独創的な方法で隠蔽している場合でも、通常サイバーセキュリティ製品によって容易に検出されます。ESET の検出エンジンも、侵害されたサイトに Magecart スクリプトが含まれている場合、このスクリプトを検出してブロックします。

Magecart による攻撃は米国で最も多く検出されており、JS/Spy.Banker による攻撃の 15% 近くを占めます。この脅威は、実際に米国で最も検出された情報窃取型マルウェアであり、米国で検出された情報窃取型マルウェア全体の 3 分の 1 を占めます。これは、JS/Spy.Banker の検出数が世界で 2 位となったイタリア（11%）でも同様です。この脅威は、ESET のテレメトリにおける情報窃取型マルウェアの検出の 42% を占めています。



2023 年下半期における **JS/Spy.Banker の検出の地理的な分布**

情報窃取型マルウェアに関するその他の洞察

macOS のパスワード窃取ツールが増加

macOS プラットフォームは、アドウェアや PUA（望ましくないアプリケーション）の標的となることが多くありますが、ESET のテレメトリでは、2023 年下半期に macOS のパスワード窃盗ツールが 290% も増加しており、懸念される状況となっています。PSW は、ESET が macOS プラットフォームで検出する情報窃取型マルウェアのサブセットの 1 つであり、ユーザーのシステムから機密情報を盗むように設計されたマルウェアの一種です。パスワード窃取ツールは、バックグラウンドで秘密裏に動作して、キー入力の記録やスクリーンショットのキャプチャを実行するほか、ユーザーのブラウザやその他のアプリケーションで保存されたパスワード直接盗み出すことができます。

この急増に拍車をかけているのが、2023 年下半期にセキュリティ研究者によって発見された、Metastealer、Pureland、Realst Infostealer、ShadowVault macOS Stealer、MacStealer、AMOS などの新しく登場した多数のパスワード窃取ツールです。これらの情報窃取型マルウェアは、特定のファイルや便利なアプリを装って、悪意のある Web サイト、不正な広告、フィッシングによって拡散します。これらのマルウェアは、パスワードを盗んだり、さまざまな種類のファイルを外部に流出させたりするだけでなく、クレジットカード情報を窃取したり、暗号通貨ウォレットを標的にすることもあります。パスワード窃取ツールが急増したにもかかわらず、macOS の情報窃取型マルウェアのカテゴリ全体の検出数は 2023 年下半期には 10% の増加にとどまっています。

Qbot の運営のテイクダウン

2023 年 8 月、悪名高い Qbot マルウェア（Qakbot とも呼ばれる）は、複数の国の法執行機関や、ユーロポール、FBI などの組織による国際的な協調作戦によって、テイクダウンされました。この作戦を実施する過程で、捜査当局は約 800 万ユーロの暗号通貨を押収しました。Qbot のインフラストラクチャを調査した結果、世界中で 70 万台以上のコンピュータが侵害されていたことが明らかなりました。

ESET のテレメトリデータを見ると、このマルウェアはその時点ですでに活動をほぼ停止していました。今年の半ば以降は Qbot の活動は多く見られなくなり、最後に実行されたキャンペーンは 6 月下旬でした。テイクダウンの後も、Qbot の C&C サーバーが検出されるケースが時折ありますが、これらの C&C サーバーのいくつかは捜査当局によってすでに無力化されています。

Web に関する脅威

Web サイトを利用するユーザーを狙う悪意あるスクリプト

JS/Agent の検出数が増加し、約 45,000 の Web サイトが悪意のある JavaScript コードの被害に遭っていることが明らかになりました。

JS/Agent は、2023 年下半期に 111% 上昇し、ESET テレメトリによって記録されたすべての脅威の中で 2 位になりました。この検出名は、侵害された Web ページによって読み込まれる悪意のある JavaScript コードを意味します。2023 年 9 月以降、JS/Agent が大規模に検出されるようになりました。これは、過去 3 年間では見られなかった高い検出率です。

Magecart のセクションでも説明しましたが、サイバー攻撃者は Web サイトの脆弱性を悪用し、Web ページに悪意のある JavaScript コードを挿入する手法を取り入れています。このようなコードは通常、攻撃者が悪意のあるスクリプトを追加でダウンロードする連鎖型攻撃の起点となっており、このコードによって、サイトの管理者権限を乗っ取ったり、悪意のある Web プラグインをインストールしたり、バックドアなどのペイロードを配信したりすることが可能になります。

JS/Agent の検出数が増加した主な原因は、JS/Agent.PHC の亜種が 136% 増加したことと、.RAN および .RAW の亜種が出現したことでした。.PHC の亜種には、2022 年 6 月に Sucuri 社が報告した ndsj マルウェアが含まれます。このマルウェアは簡易な手法で難読化された JavaScript で構成されており、これらの JavaScript が次の攻撃段階を実行します。通常、悪意のある PHP スクリプトが侵害された Web サーバーにすでに存在しており、C&C サーバーから JavaScript ペイロードを取得します。

JS/Agent.PHC が最も多く検出されたのは、日本（10%）、スペイン（8%）、米国（6%）でした。ESET のテレメトリでは、9 月から 11 月にかけて、14,500 の Web サイトが .PHC の亜種によって侵害されたことが記録されています。

2021 年 1 月から 2023 年 11 月までの **JS/Agent の検出傾向**、7 日間移動平均

ESET のエキスパートの解説

Web サイトの管理者は、特に WordPress などを使用している場合には、インストールするプラグインによって攻撃対象領域が劇的に広がる恐れがあるため、注意しなければなりません。管理者は、必ずパッチ適用のポリシーを定め、アップデートが入手可能になったら速やか適用する必要があります。Web 開発者には、データサニタイズ、安全な HTTP ヘッダー、コンテンツセキュリティポリシーなどのセキュアコーディングを実践する方法をトレーニングし、さまざまなタイプのスクリプト挿入攻撃を防止しなければなりません。

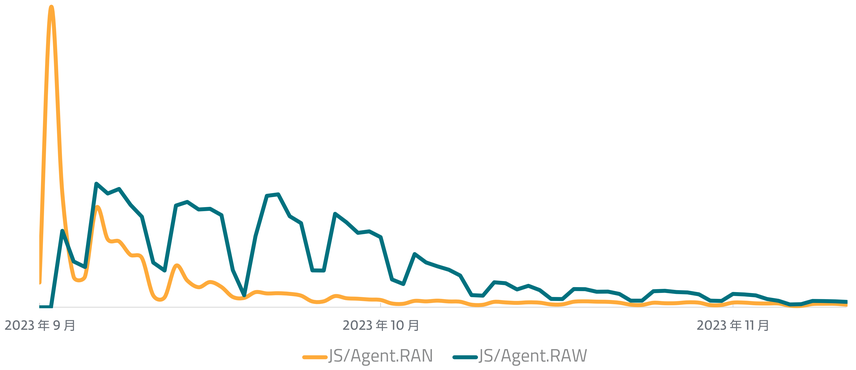
ESET シニア検出エンジニア、
Ján Adámek

.RAN と .RAW の亜種には、2023 年 10 月に Sucuri 社によって報告された **Balada Injector キャンペーン**の一部として検出された悪意のある JavaScript が含まれています。これらの亜種はどちらも難読化されたスクリプトですが、C&C サーバーから次の攻撃で使用する JavaScript コードをダウンロードするという目的は共通しています。例えば、いくつかの .RAN の検体は、`stay.decentralappps[.]` からスクリプトをダウンロードし、いくつかの .RAW の検体は `cdn.statisticscripts[.]com` にアクセスします。

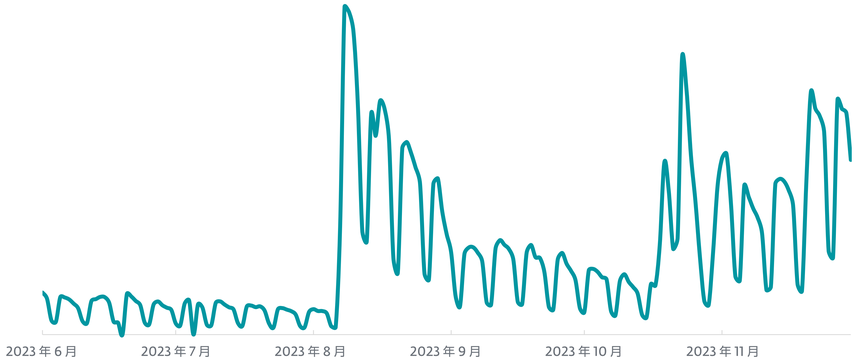
.RAN の亜種は 9 月 21 日に過去 3 年間で最大となる急増を記録しました。その後も何度か検出数が急増しましたが、これらは主に RAW の亜種が原因でした。

.RAN と .RAW の亜種と、その他の 37 の関連する JS/ Agent の亜種を合わせると、2023 年の下半期で 90 万件以上検出されています。これは、**ESET のセキュリティフォーラム**で報告されているように、攻撃者が WordPress 用のプラグイン **tagDiv Composer** の特定のバージョンに影響する **CVE-2023-3169** のような脆弱性を Web サイトで悪用したことで、この期間に多くの Web サイトが侵害されたことを示しています。

これらの 39 件の亜種が最も多く検出されたのは、イタリア（10%）、チェコ（7%）、ポーランド（7%）でした。9 月から 11 月にかけて、ESET のテレメトリは 6,700 の Web サイトが .RAW の亜種によって侵害され、23,500 の Web サイトが .RAW の亜種によって侵害されたことを記録しています。



2023 年 9 月から 2023 年 11 月までの **JS/Agent.RAN および JS/Agent.RAW の検出傾向**



2023 年下半期における **JS/Agent.PHC の検出傾向**

ランサムウェア

ClOp と MOVEit のハッキング：大規模な標的型攻撃

1 人の攻撃者が 2 年前に悪用したゼロデイの脆弱性が、どのように世界的なサイバーセキュリティの悪夢を引き起こしたのでしょうか？

2023 年下半期に最も大きな話題となったのは、ランサムウェアを使用しないランサムウェア攻撃です。「MOVEit のハッキング」をこの章で取り上げるのは、大規模なハッキングでランサムウェアを使用することで悪名高い ClOp（別名 Lace Tempest、FIN11、TA505、または Evil Corp）として知られるサイバー犯罪組織によって実行されたためです。ClOp が実行した最新のキャンペーンは、あまりにも大規模であり、すべてのユーザーのデータを暗号化するためには多くの時間と労力を要するようになった可能性があります。

すべては 5 月 27 日、戦没将兵追悼記念日（メモリアルデー）の長期休暇の初日に、このサイバー犯罪者が、多くのユーザーに使用されているファイル転送アプリ「MOVEit」のゼロデイ脆弱性（CVE-2023-34362）に対する大規模な攻撃を開始したことから始まりました。この攻撃者は、2021 年からこの脆弱性を温めていた可能性があります。最終的に攻撃者は特権を昇格させ、保存されたデータや転送されたデータに不正にアクセスできるようになっています。

それから 1 週間が経過すると、BBC、ブリティッシュ・エアウェイズ、アイルランドの航空会社であるエアリンガスなどの大企業が被害を受けているとの情報が入り始め、この攻撃による影響の範囲が明らかになり始めました。ClOp 組織がこの攻撃を実行していることを、Microsoft が最初に発表したのもほぼ同時期であり、ClOp 組織はメディアを通じて、この攻撃を実行したことを認め、侵害した企業の数は数百にのぼると吹聴しました。

Emsisoft 社の監視データによると、最初の攻撃から半年が経過し、被害を受けた組織の数は 2,600 社を超えています。被害を受けた企業や組織には、米国の政府機関、学校、大学、医療機関や、ソニー、アーンスト・アンド・ヤング、プライスウォーターハウスクーパースなどのグローバル企業が含まれます。IBM が試算しているセキュリティ侵害によって流出した記録 1 件あたりの平均コストである 165 米ドルを、今回流出した 8,300 万人分の個人データを乗算すると、このハッキングの推定被害は 140 億米ドルに達します。これは、大きく報道された NotPetya のインシデントによる 100 億米ドルの被害額よりも多い額です。

ESET のエキスパートの解説

2023 年を振り返ると、ランサムウェアは 2022 年よりも活発だったと言って差し支えないでしょう。公開されている情報と ESET が調査したインシデントでは、要求される身代金が増加しています。これは、攻撃者がさらに貪欲になっているのか、被害を受けた組織が身代金を支払わなくなっているために、攻撃者はより多くの身代金を要求せざるを得なくなったのか、あるいはインフレによる影響なのか、評価が難しいところです。

最も印象に残った攻撃は、MOVEit のハッキングでした。キャンペーンの規模だけでなく、攻撃を操っていた ClOp 組織の技術力の高さが際立っていたことも、印象的であった理由です。サイバー攻撃者は、新しいゼロデイ脆弱性を見つけて武器化しておき、好機を待って展開していることが明らかになっています。

現在の主要なサイバー攻撃組織はアフィリエイトプログラムの拡充に注力しており、2024 年も本書で説明したトレンドの大半は継続すると予測されます。大規模なサイバー攻撃組織は、別のサイバー犯罪者を自分のスキームに組み入れることによって、新たな競争相手が出現しないように取り組んでいるのです。

ESET シニアマルウェアリサーチャー、Jakub Souček

当初の試算では、Cl0p は被害を受けた組織から **7,500 万米ドルから 1 億米ドル**を奪取できる可能性があると言われていました。インシデントの重大さと、米国とカナダに攻撃が集中している可能性が高いことから、米国国務省は犯人の逮捕と有罪判決につながる情報に対して **1,000 万米ドルの懸賞金**を出しています。

MOVEit のハッキングは、Cl0p が窃取した情報を流出させるために**クリアウェブ**を利用し始めたように、ランサムウェア環境が新しい局面を迎えたことを示している可能性があります。このような攻撃は、2023 年 6 月に ALPHV ランサムウェア組織（別名 BlackCat）で初めて検出されました。サイバー攻撃のインシデントが外部からも透過的になることで、被害を受けた企業は対応を迅速に迫られることになります。窃取したデータの量が膨大であることから、Cl0p はテイクダウンを回避するために、情報の一部を**トレント**経由で流出させています。

2023 年下半期には、**FBI** が他の 2 つの新しいトレンドを指摘しています。最初の傾向は、同じインシデントで 2 つ以上のランサムウェアの亜種が展開されることです。通常は、AvosLocker、Diamond、Hive、Karakurt、LockBit、Quantum、Royal の各系統のランサムウェアが展開されます。もう 1 つの傾向は、データ窃取とランサムウェアによる暗号化に加えて、ワイパー型マルウェアが使用されるようになっていることです。ワイパー型マルウェアを使用すると、攻撃者は、侵害したシステムのデータを一定時間後に完全に破損させることが可能となり、被害を受けた組織へのプレッシャーがさらに高まることになります。

CosmicBeetle、これまで使用していた Scarab ランサムウェアを独自の ScRansom に変更

2023 年下半期に、ESET の研究者は、Spacecolon（Sc）ツールセットを使用して世界中にランサムウェアを展開しているトルコ語を使用するサイバー攻撃者である CosmicBeetle を詳しく調査しました。

ESET の研究者はまた、開発中の新しいランサムウェア系統を発見し、ScRansom と命名しました。ESET は、このランサムウェアが CosmicBeetle によって開発されたと確信しています。ESET がこの攻撃組織に関する調査を最初に**公開**したときには、ScRansom を使用した攻撃は実環境では観測されていませんでしたが、すぐに状況が変化し、これまで主要なペイロードとして選択されていた Scarab ランサムウェアに代わって、現在、CosmicBeetle グループはこのランサムウェアの亜種を主に展開するようになりました。

最近の複数の攻撃では、このサイバー攻撃者は LockBit になりすます目的で身代金メモを変更しており、LockBit のように偽装した Web リークサイトも立ち上げています。このリークサイトでは、直近の LockBit の被害を受けた組織のデータをコピーし、さらに CosmicBeetle による被害者のデータもいくつか追加しています。CosmicBeetle は、LockBit の知名度を悪用して、被害者へのプレッシャーを強めていると考えられます。

攻撃のための最初の足がかりを構築するために、CosmicBeetle は RDP ブルートフォースや ZeroLogon 脆弱性（**CVE-2020-1472**）などのいくつかの攻撃手法を使用します。確証は得られていませんが、ESET の研究者は、コード中に「Forti」という文字列が見つかったことや、被害を受けた組織の多くが FortiOS を実行しているデバイスを使用しているという事実から、CosmicBeetle が FortiOS の脆弱性を攻撃している可能性があります。

Spacecolon のツールセットは 3 つのツールで構成されています。メインのオーケストレーターは ScHackTool と呼ばれ、小規模なコンポーネントである ScInstaller を展開するために使用され、CosmicBeetle のバックドアである ScService をインストールします。ScService は、攻撃者がコマンドを実行し、被害者のシステムに関する情報を取得し、ペイロードをダウンロードして実行することを可能にします。詳細については、ESET の**分析レポート**を参照してください。

注意が必要な新たな攻撃組織とリブランドした攻撃組織

3AM

Rust ベースの新しいランサムウェアが 9 月に大きな話題となり、研究者の注目を集めましたが、その理由は、LockBit ランサムウェアの実行に失敗した後のバックアップ用の亜種として展開されていたためです。それ以来、3AM は 10 社の組織を攻撃するのに使用され、新たに開設された Tor リークサイトからこれらの組織の情報が流出しました。

LostTrust

LostTrust ランサムウェアは、同じサイバー犯罪者が使用している MetaEncryptor ランサムウェアをリブランドしたものである可能性が高いです。

SophosEncrypt

サイバー犯罪者がサイバーセキュリティの研究者や企業にその犯罪をなすりつけようとすることは決して珍しくありません。SophosEncrypt はランサムウェアの一例であり、このサイバー攻撃者は、有名なセキュリティ企業であるソフォスの製品のように装って、このランサムウェアを「販売」しています。

NoEscape

2023 年 7 月、NoEscape と呼ばれる新しいランサムウェア系統が研究者やメディアの注目を集めました。この暗号化ソフトのコードの類似性から、専門家は、過去に大規模に拡散されたランサムウェア系統である Avaddon がリブランドされた可能性を指摘しています。NoEscape のダークウェブリークサイトのリストから、NoEscape グループは 2023 年下半期に少なくとも 100 社を侵害した可能性があります。

Hunters International

Hive が復活したのでしょうか？ 2023 年下半期、Hunters International という名前の新しい「サービスとしてのランサムウェア」が開始されました。その暗号化ツールを分析したところ、複数のセキュリティ研究者が、2023 年上半期の前半に法執行機関が侵入してテイクダウンしたサイバー犯罪向けのサービスである Hive とそのコードが大きく重複していることを発見しました。Hunters International を運用しているサイバー攻撃組織は、Hive との関係を否定しており、以前の運営者から古いコードを購入して修正したと主張しています。Hunters International のリークサイトには、侵害された米国とヨーロッパの組織が表示されています。

逮捕／活動停止／復号鍵の提供

ハッキング：**Trigona**

ランサムウェア組織の「Trigona」は、ウクライナの活動家によってサーバーに侵入されデータを消去されました。また、Ukrainian Cyber Alliance（UCA）は、Trigona のシステムからソースコード、組織内のコミュニケーション、データベースレコード、およびその他のデータも取得したと述べています。収集したデータには、復号鍵が含まれている可能性もありますが、UCA は詳細な最新情報を提供していません。

逮捕されたサイバー攻撃者：**Ragnar Locker**

10 月下旬、警察当局は「Ragnar Locker」ランサムウェアに対する捜査を行い、5 人の容疑者に事情聴取を行い、首謀者一人を逮捕しました。チェコ、スペイン、ラトビアではアジトへの家宅捜索が行われ、オランダ、ドイツ、スウェーデンでは攻撃に使用されていたインフラストラクチャが差し押さえされました。ダークウェブサイトもテイクダウンされ、この解体作戦に関する情報に置き換えられました。Ragnar Locker は、2019 年から活動を開始しており、ポルトガルの国営航空会社やイスラエルの医療機関などの重要インフラストラクチャを攻撃していました。

コードの流出：**HelloKitty**

さらに多くのランサムウェアのソースコードが流出しましたが、今回は HelloKitty ランサムウェアを操っているサイバー攻撃者が自ら漏えいさせた可能性があります。HelloKitty ランサムウェアの最初のバージョンのコードは、ロシア語圏のフォーラムに掲載され、さらに強力で新しい暗号化ソフトウェアを開発しているという説明も加えられていました。流出したこれらのコードは、ランサムウェアを攻撃に手を染めようとする多くの新しいサイバー攻撃者を生み出す可能性があります。

逮捕されたサイバー攻撃者：**LockBit（アフィリエイト）**

LockBit のアフィリエイトが逮捕されたのは 2023 年の初めでしたが、米国当局が容疑とその刑罰を明らかにしたのは 2023 年 6 月でした。米国司法省は、ロシア人の Ruslan Magomedovich Astamirov を最高で懲役 25 年の刑罰に処すよう裁判所に求めています。

復号ツール：**Key Group**

「Key Group」ランサムウェアの暗号化スキームの欠陥を突いて、研究者は、復号化ツールを作成しました。このランサムウェアの初期バージョンに感染したユーザーは、この無料のツールを使用して被害を回復できる場合があります。Key Group は 2023 年から活動しており、ロシア語圏のサイバー攻撃組織と考えられています。

復号ツール：**Akira**

2023 年以来、世界中のさまざまな業界を攻撃している Akira ランサムウェアに対しても、復号化ツールが提供されています。

懸賞金：**Cl0p**

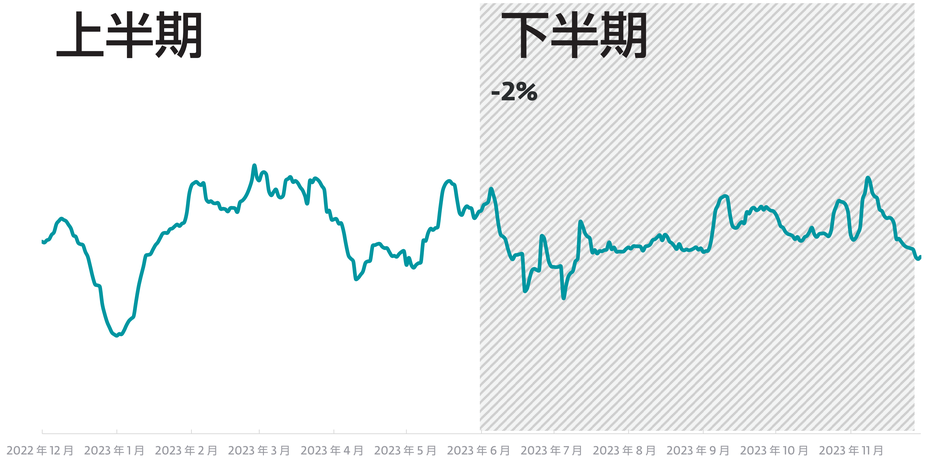
MOVEit のハッキングの問題が深刻であることから、米国国務省は Cl0p と呼ばれる犯人の逮捕と有罪判決につながる情報に対して、1,000 万米ドルの懸賞金を懸けました。

逮捕されたサイバー攻撃者：**MegaCortex、HIVE、LockerGoga、Dharma**

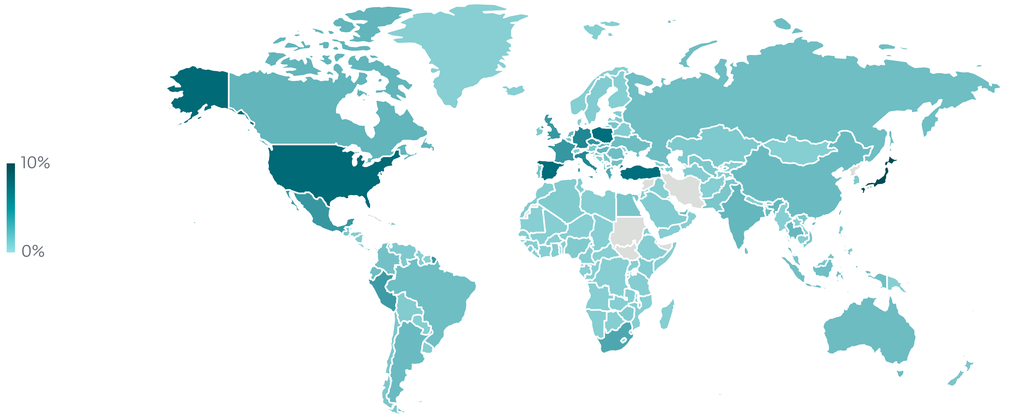
欧州警察機構（ユーロポール）、欧州司法当局（ユーロジャスト）、および 7 カ国の捜査機関は、71 カ国で 1,800 社以上の組織に被害を与えたランサムウェア組織を解体しました。32 歳の首謀者を含む 5 人の容疑者全員がウクライナで拘束されました。合計で 30 カ所の組織の拠点が捜索されています。今回の捜査は、2021 年の一度目の逮捕劇に続くものでした。

脅威テレメトリ

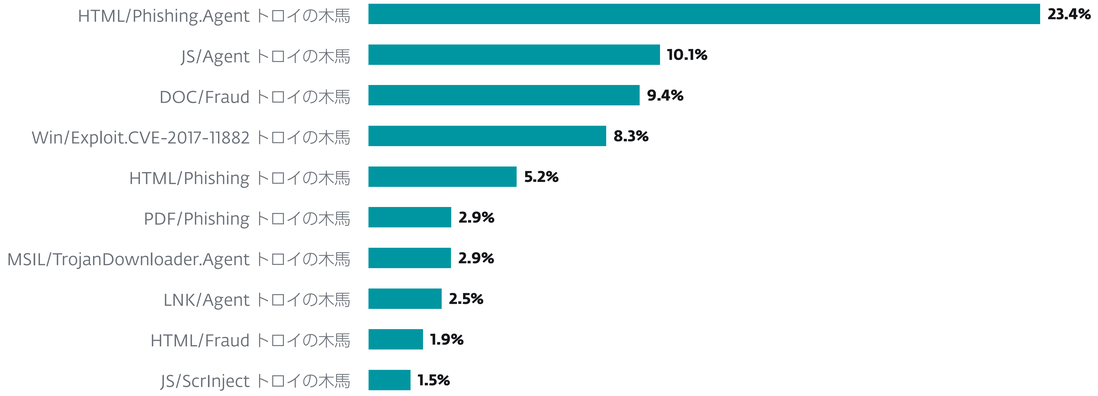
すべての脅威



2023 年上半期～ 2023 年下半期の**脅威全体の検出傾向**、7 日移動平均線

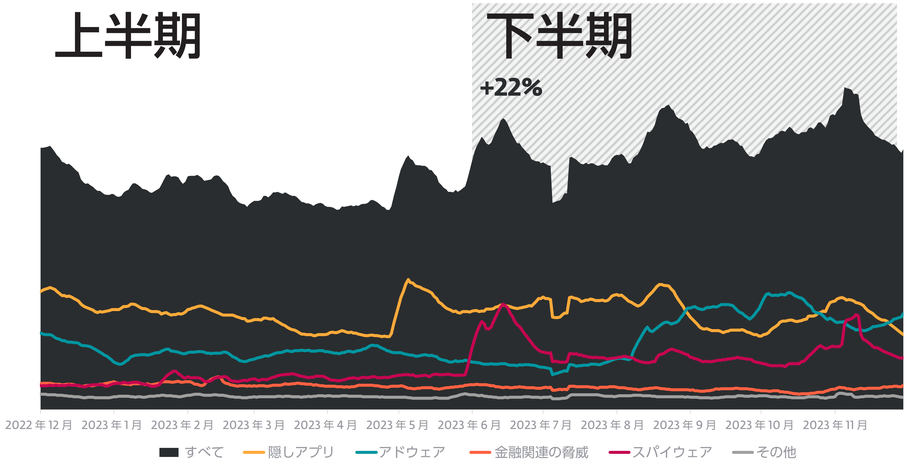


2023 年下半期における**マルウェア検出の地理的な分布**

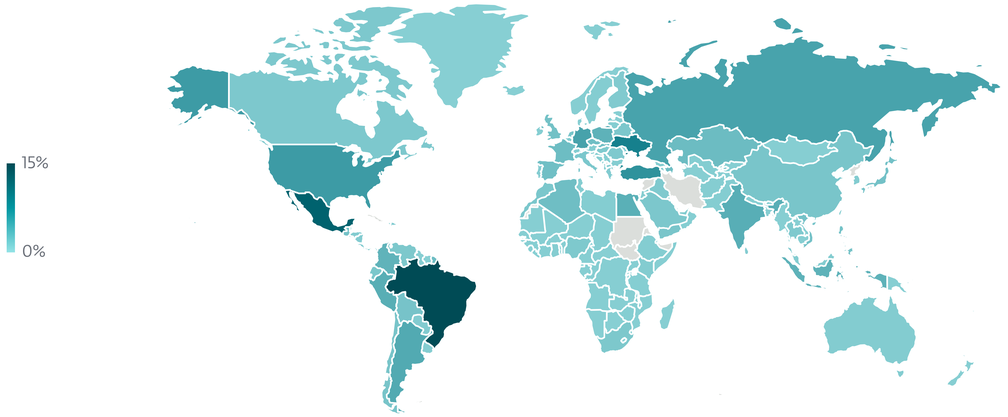


2023 年下半期における**マルウェアの検出数トップ 10**（マルウェア数に占める割合）

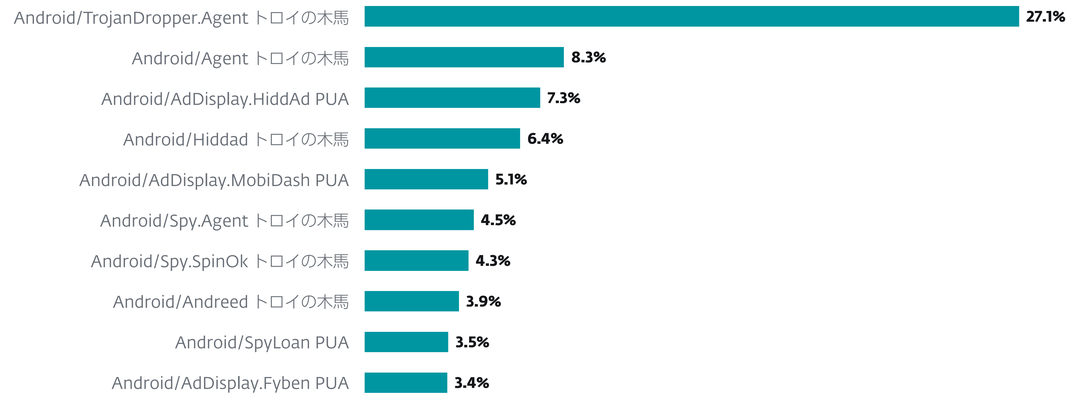
Android



2023 年上半期～ 2023 年下半期の **Android に関する脅威カテゴリの検出傾向**、7 日移動平均線
（クリッカー、クリプトマイナー、ランサムウェア、詐欺アプリ、SMS トロイの木馬、ストーカーウェアの傾向は、「その他」の傾向線に統合）

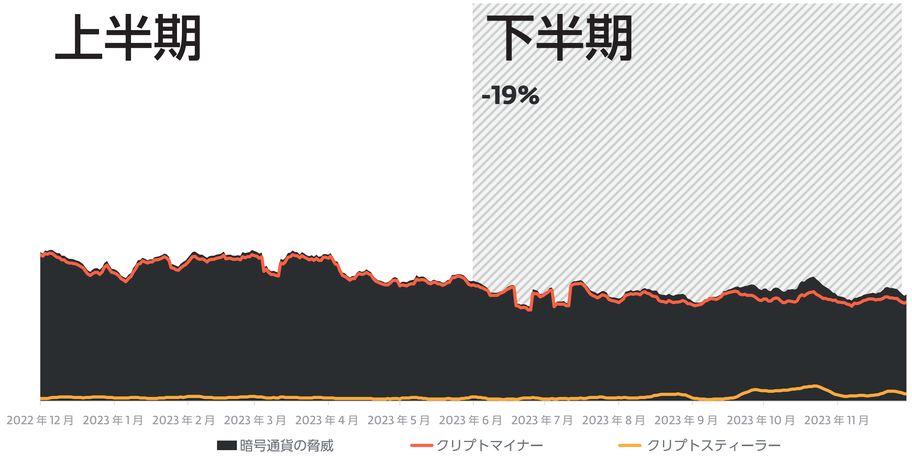


2023 年下半期における **Android に関連する脅威検出の地理的な分布**

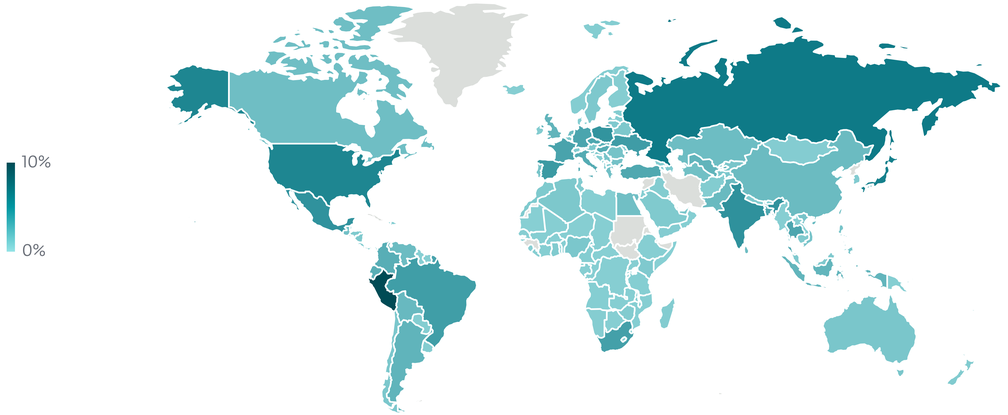


2023 年下半期における **Android に関連する脅威の検出数トップ 10**（マルウェア数に占める割合）

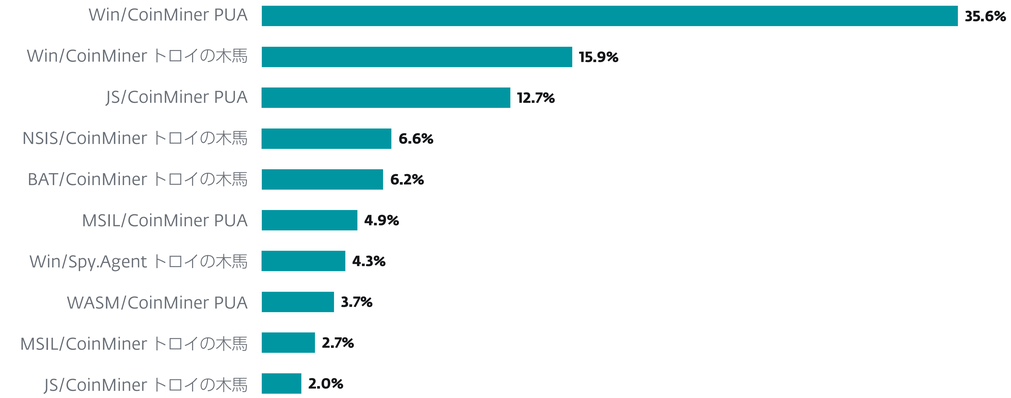
暗号通貨の脅威



2023 年上半期～ 2023 年下半期の**暗号通貨に関する脅威の検出傾向**、7 日移動平均線

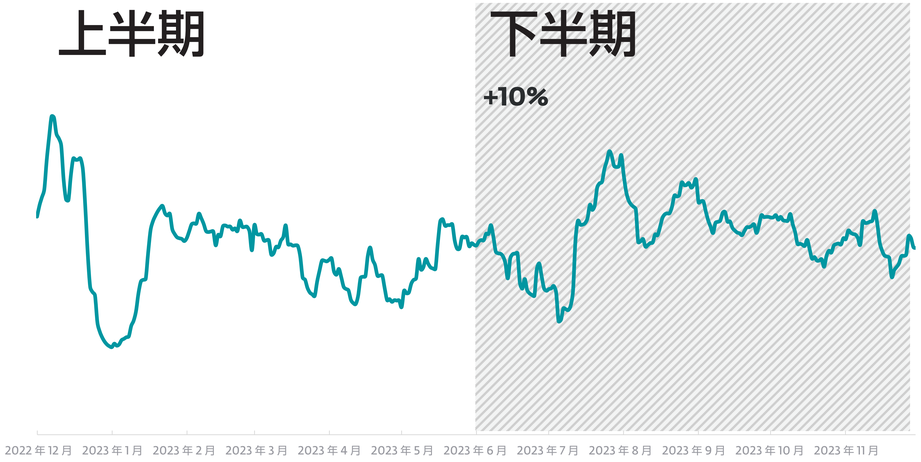


2023 年下半期における**暗号通貨の脅威の検出数の地理的な分布**

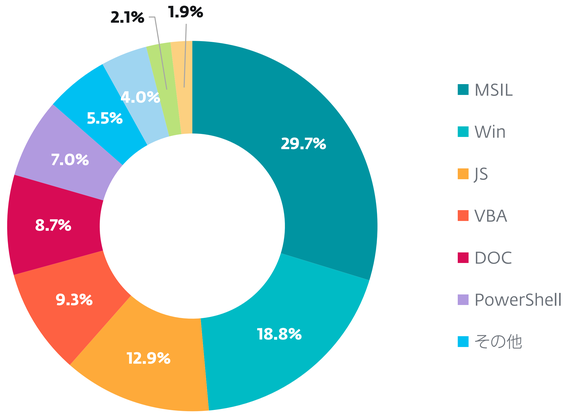


2023 年下半期における**暗号通貨の脅威の検出数トップ 10**（マルウェア数に占める割合）

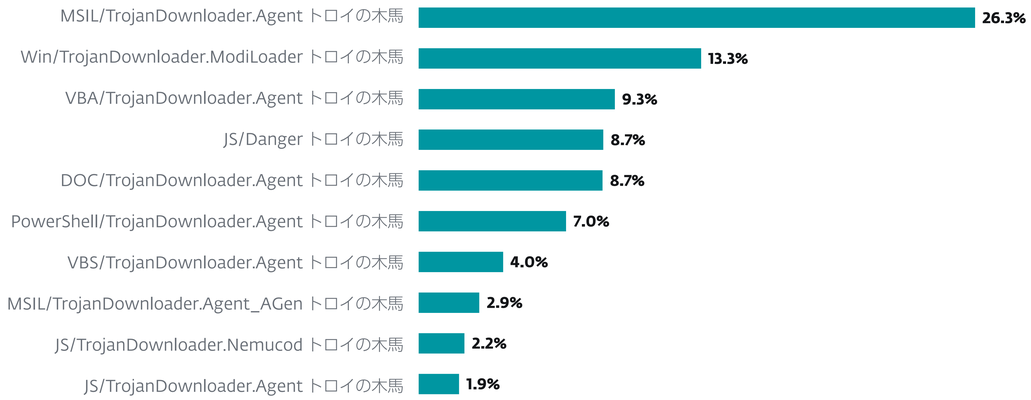
ダウンローダー



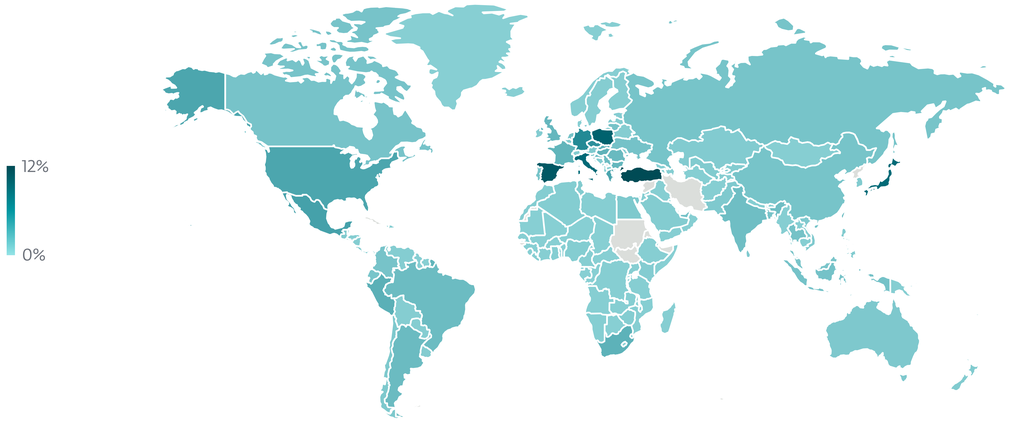
2023 年上半期～ 2023 年下半期の**ダウンローダーの検出傾向**、7 日移動平均線



2023 年下半期の**ダウンローダータイプ別の検出率**

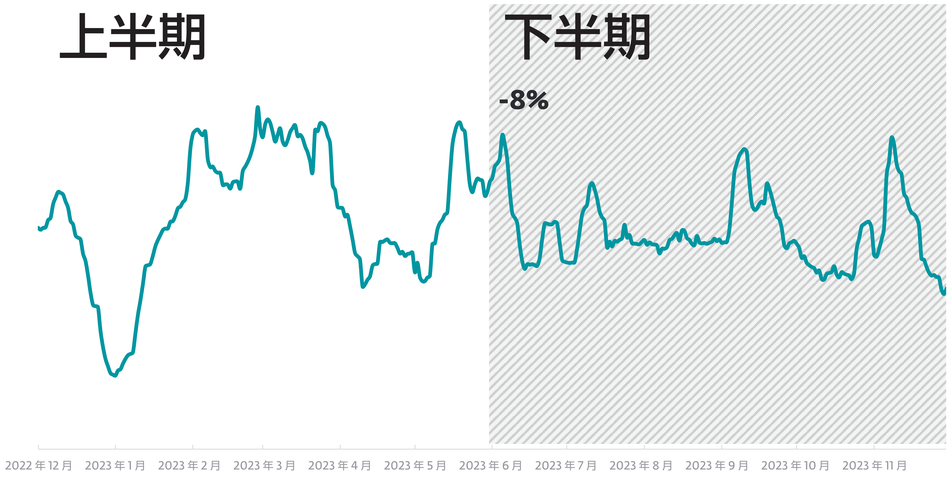


2023 年下半期における**ダウンローダーの検出数トップ 10**（マルウェア数に占める割合）

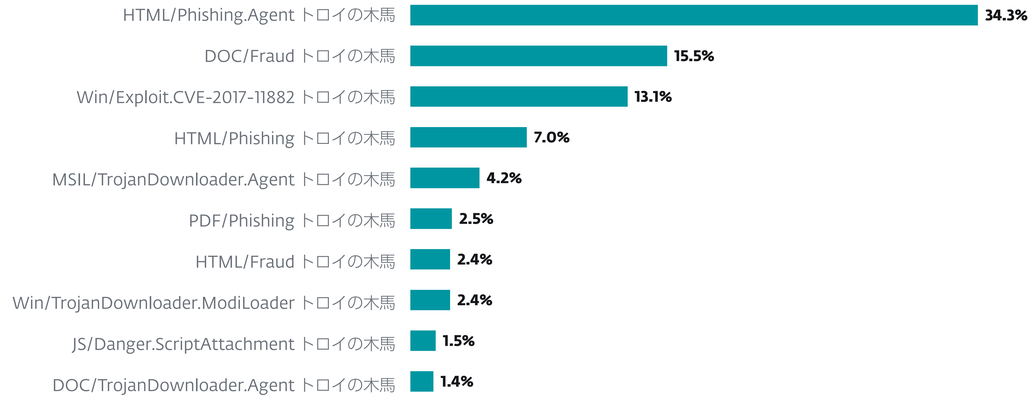


2023 年下半期における**ダウンローダー検出数の地理的な分布**

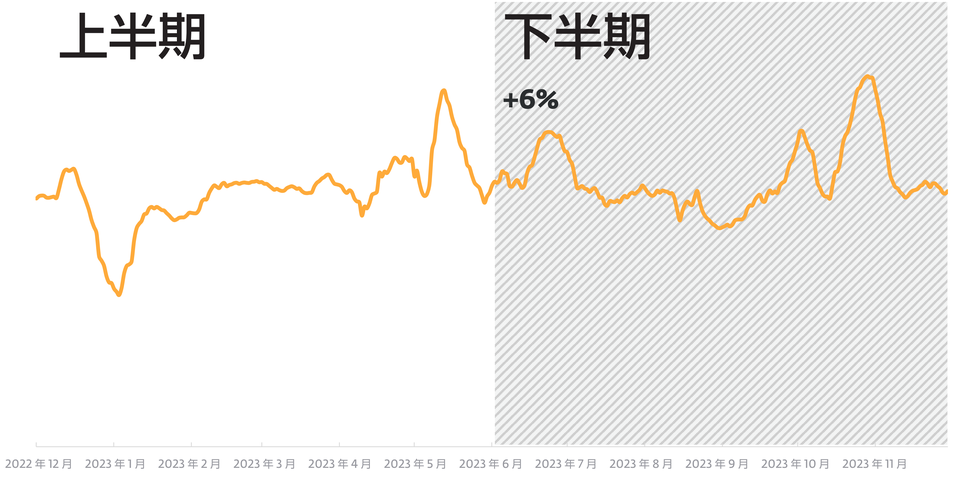
電子メールに関する脅威



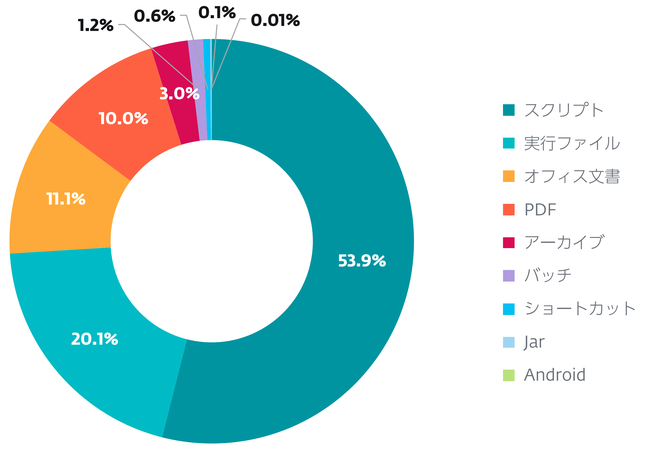
2023 年上半期～ 2023 年下半期の**悪意のあるメールの検出傾向**、7 日移動平均線



2023 年下半期に**検出されたメールの脅威トップ 10**

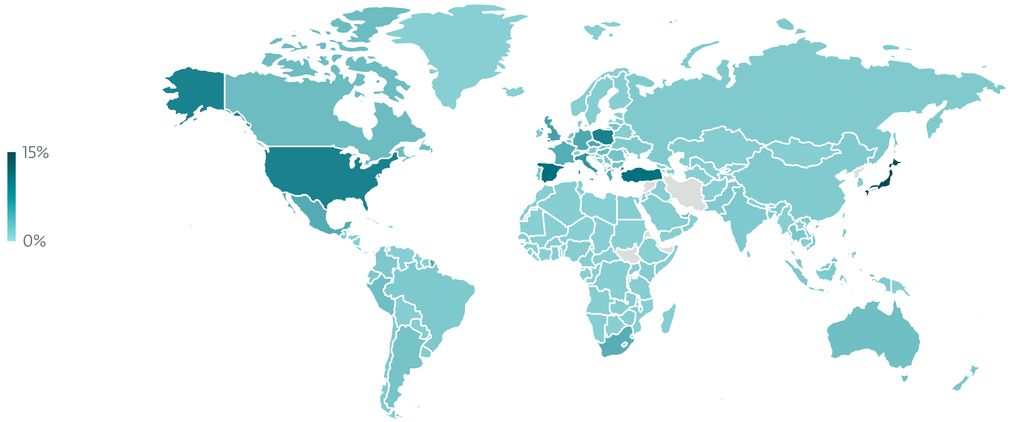


2023 年上半期～ 2023 年下半期の**スパムの検出傾向**、7 日移動平均線



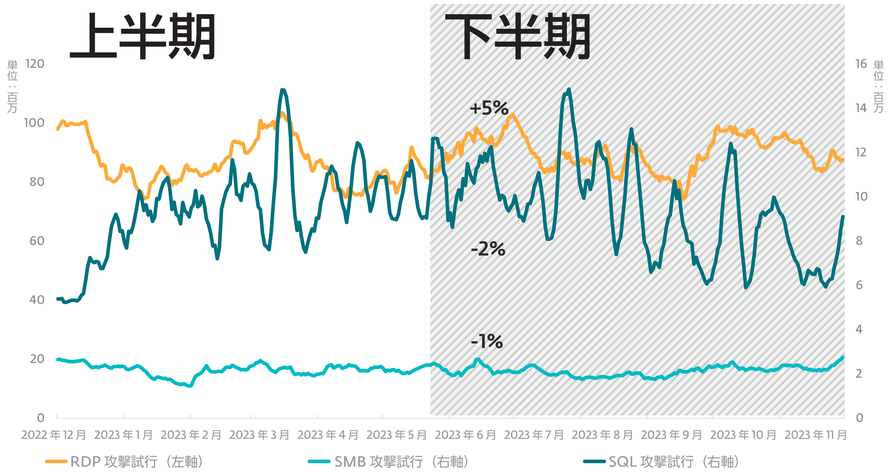
2023 年下半期の**主な悪意のある電子メールの添付ファイルのタイプ**

電子メールに関する脅威

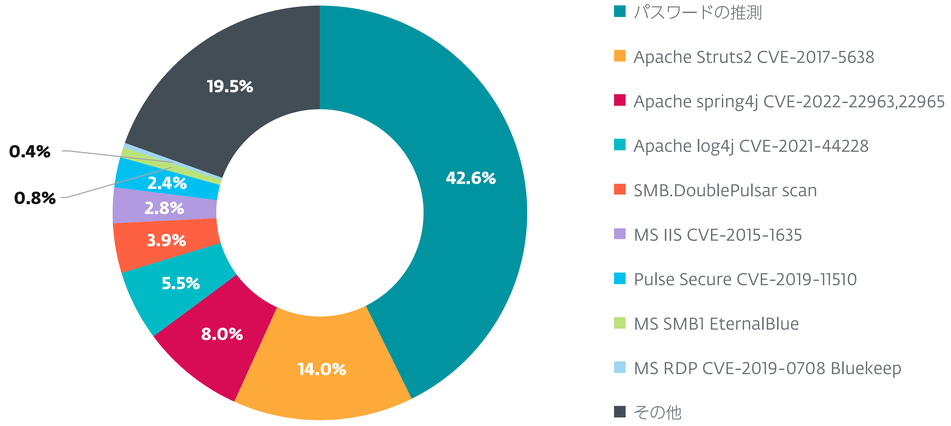


2023 年下半期における**メール脅威の検出数の地理的な分布**

エクスプロイト

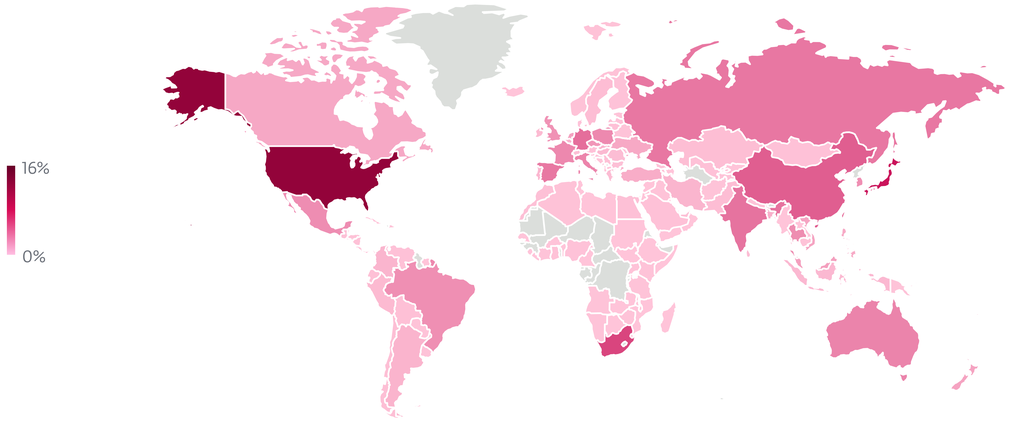


2023 年上半期および 2023 年下半期における **RDP、SMB、SQL 攻撃試行の傾向**、7 日間移動平均線

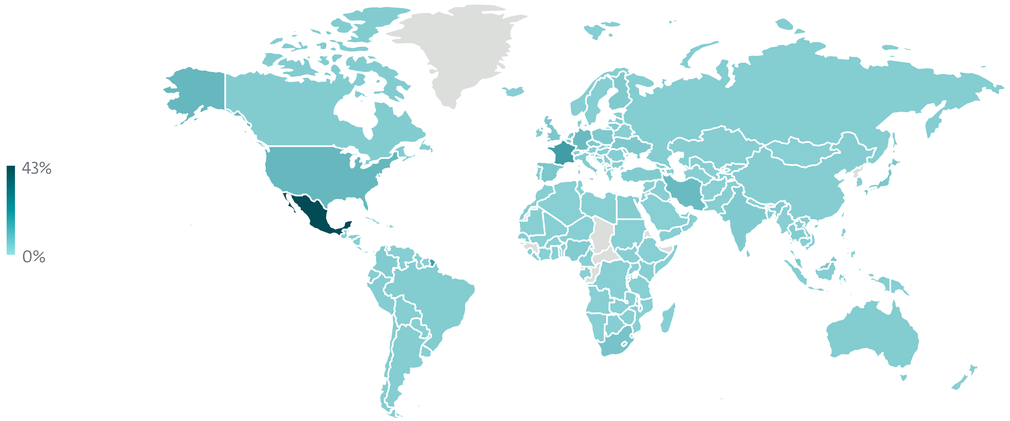


2023 年下半期にユニーククライアントから報告された**外部からのネットワークへの侵入方法**

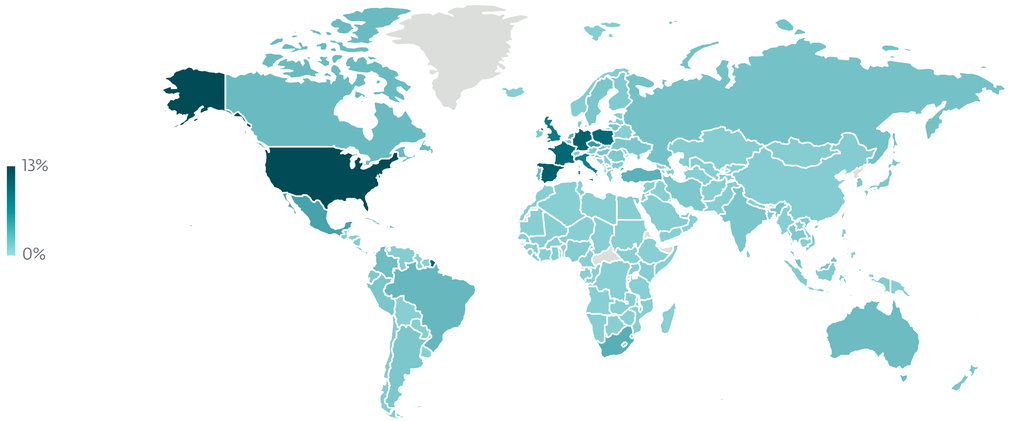
エクスプロイト



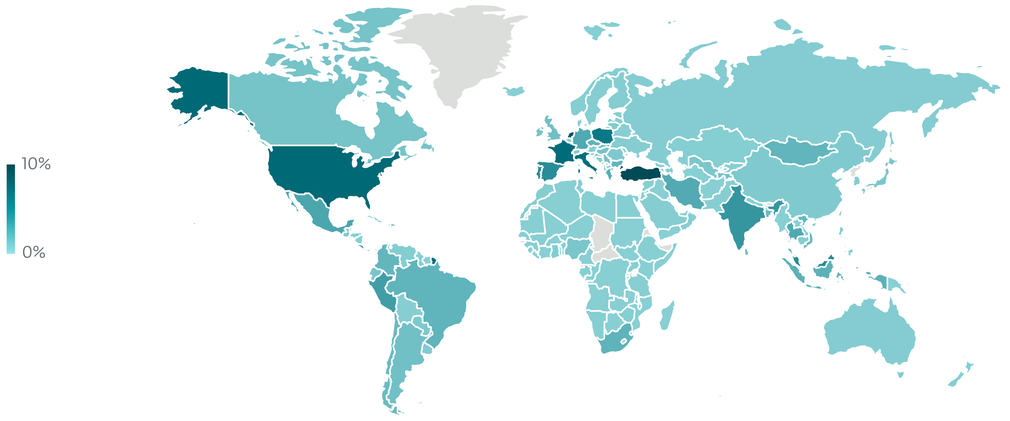
2023 年下半期に **RDP パスワード推測攻撃を実行したソースの地理的な分布**



2023 年下半期に **SMB パスワード推測攻撃が実行された標的の地理的な分布**

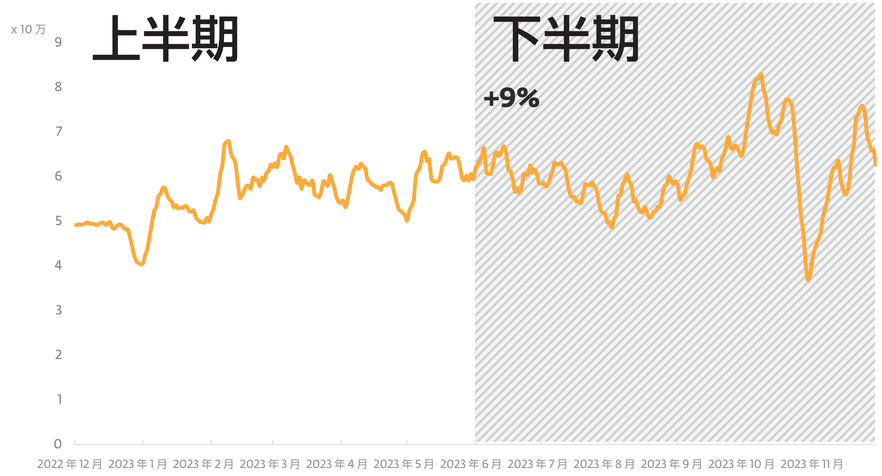


2023 年下半期に **RDP パスワード推測攻撃が実行された標的の地理的な分布**

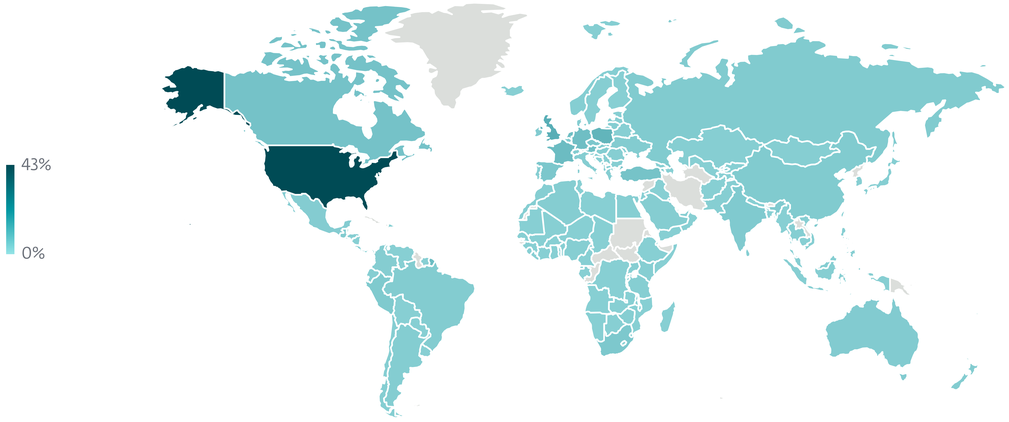


2023 年下半期に **SQL パスワード推測攻撃が実行された標的の地理的な分布**

エクスプロイト

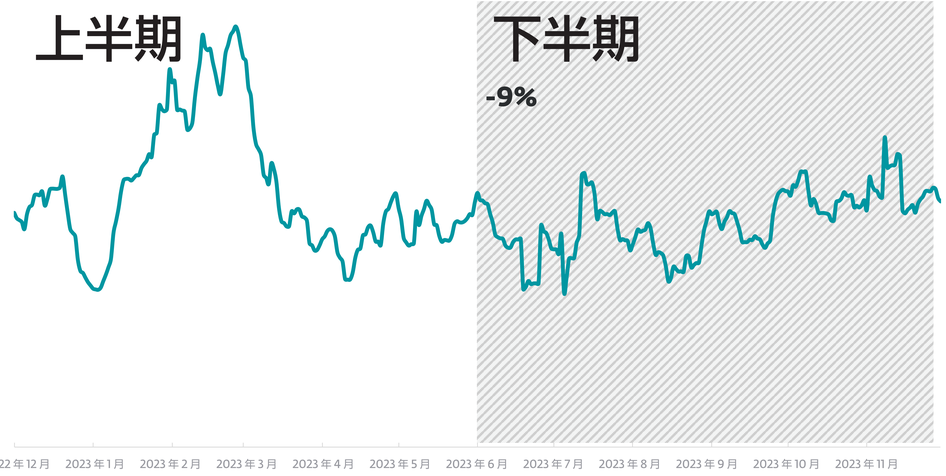


2023 年上半期と 2023 年下半期における **Log4Shell 攻撃試行の検出傾向**、7 日間移動平均線

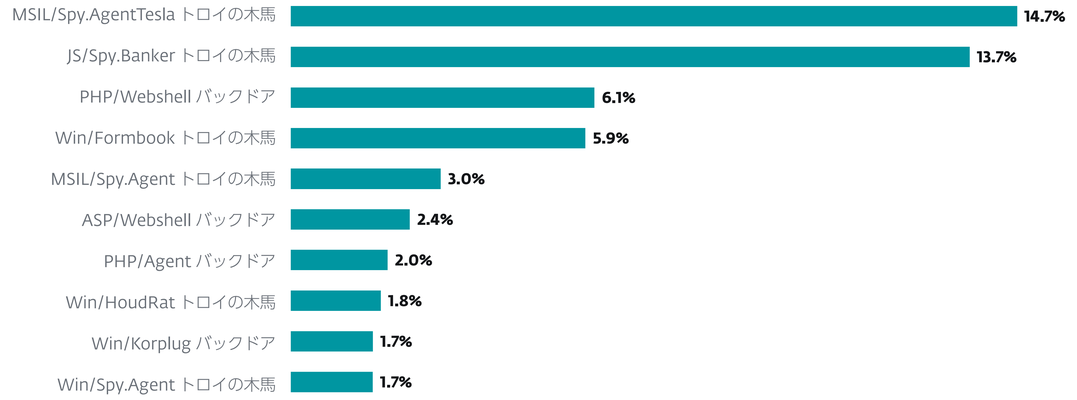


2023 年下半期における **Log4Shell 攻撃試行の地理的分布**

情報窃取型マルウェア

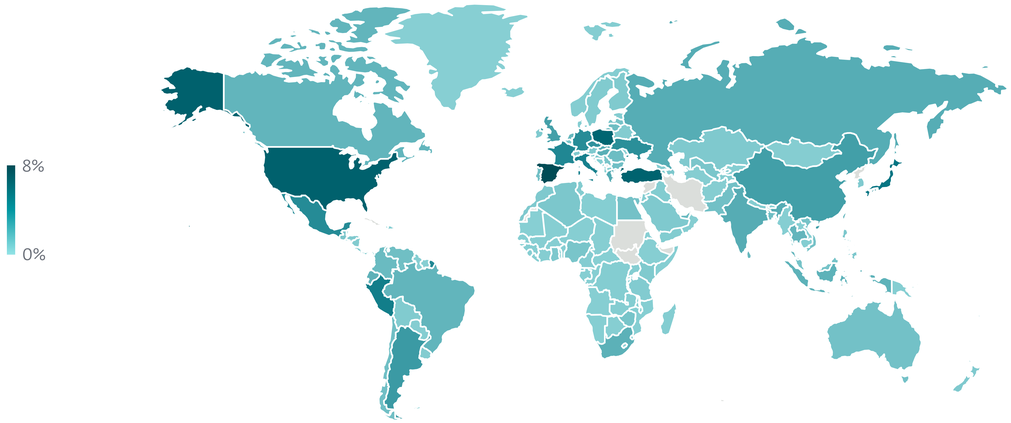


2023 年上半期と 2023 年下半期の**情報窃取型マルウェアの検出傾向**、7 日間移動平均線



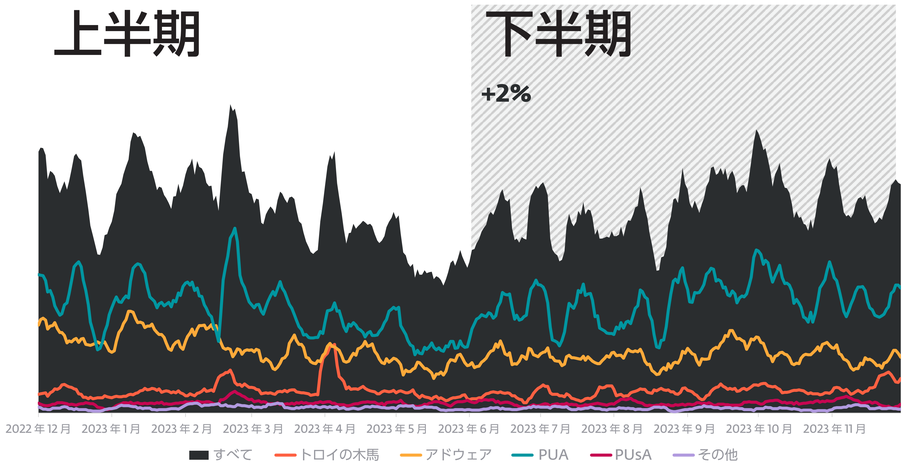
2023 年下半期における**情報窃取型マルウェアのトップ 10**（情報窃取型マルウェアの検出に占める割合）

情報窃取型マルウェア

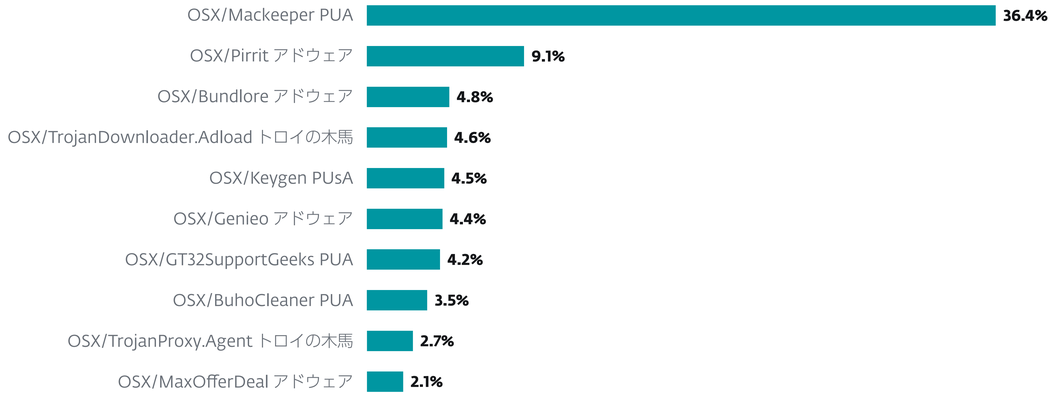


2023 年下半期における**情報窃取型マルウェアの検出の地理的な分布**

macOS

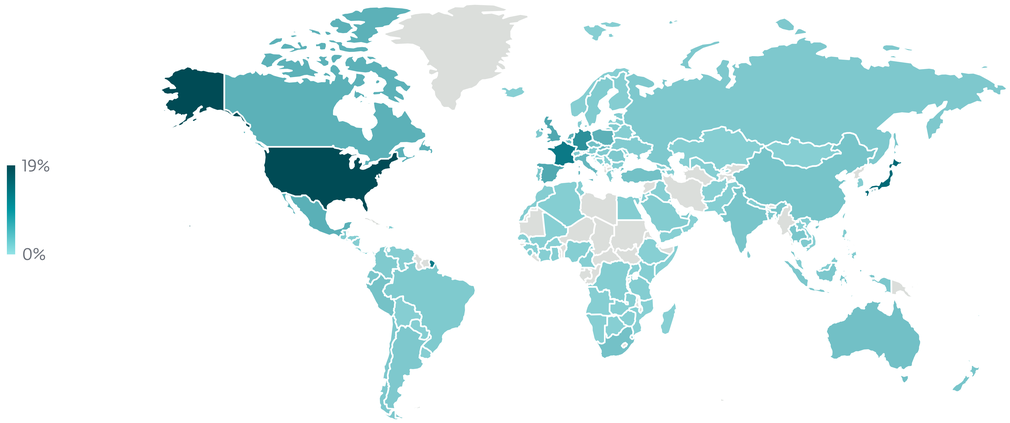


2023 年上半期と 2023 年下半期の **macOS の脅威の検出傾向**、7 日間移動平均線



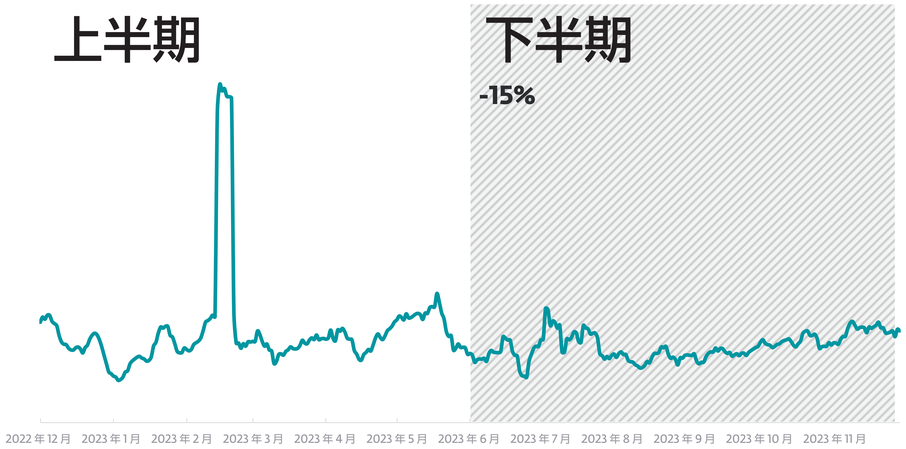
2023 年下半期の **macOS の脅威の検出率トップ 10**（macOS の脅威の検出数に占める割合）

macOS

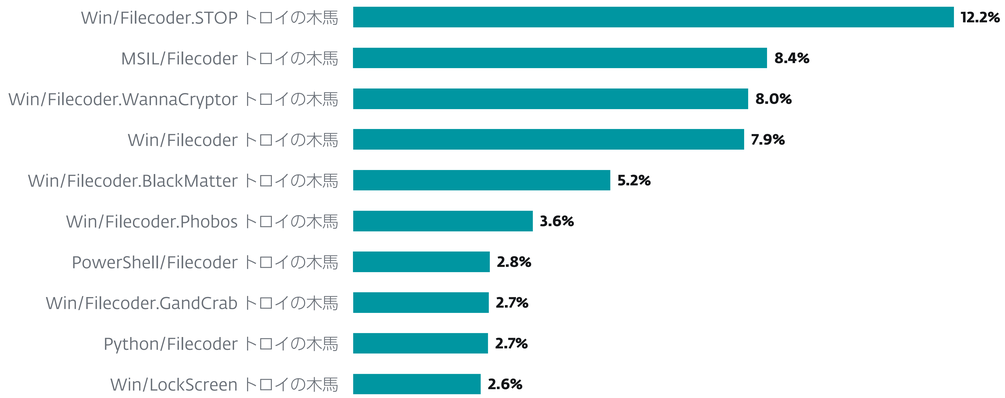


2023 年下半期における **macOS の脅威の検出の地理的な分布**

ランサムウェア

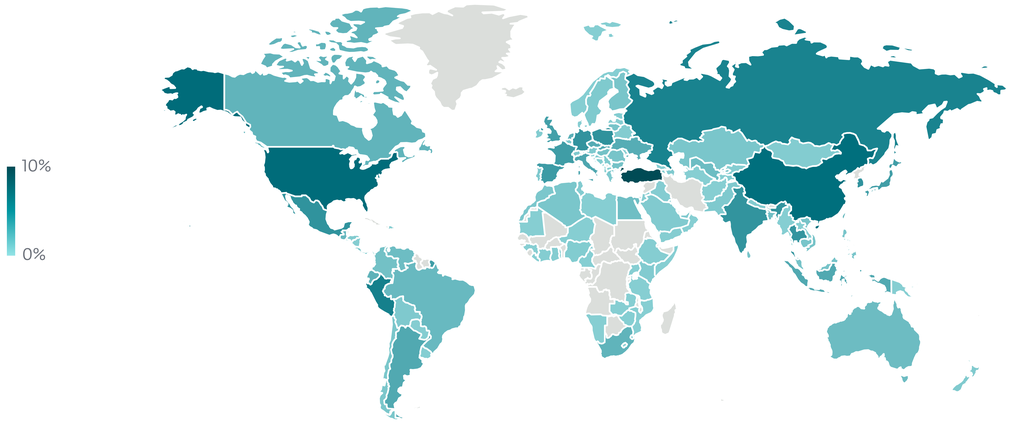


2023 年上半期～ 2023 年下半期の**ランサムウェアの検出傾向**、7 日移動平均線



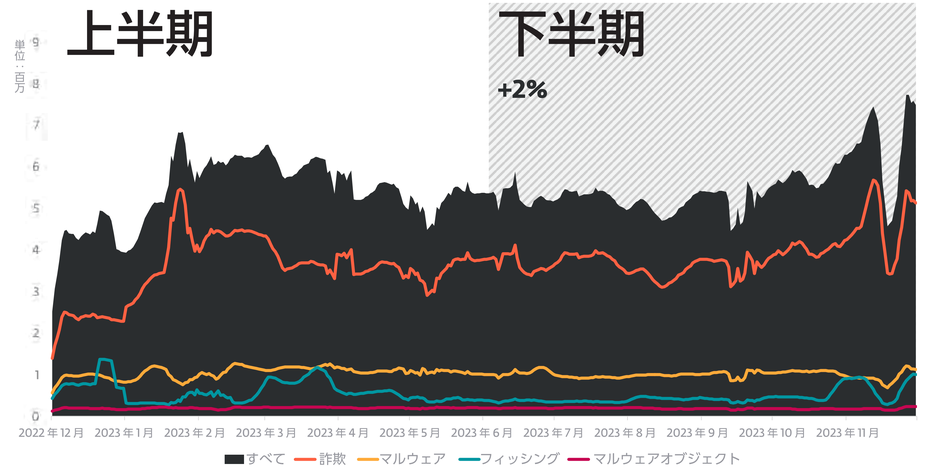
2023 年下半期の**ランサムウェア検出率トップ 10**（ランサムウェア検出数に占める割合）

ランサムウェア

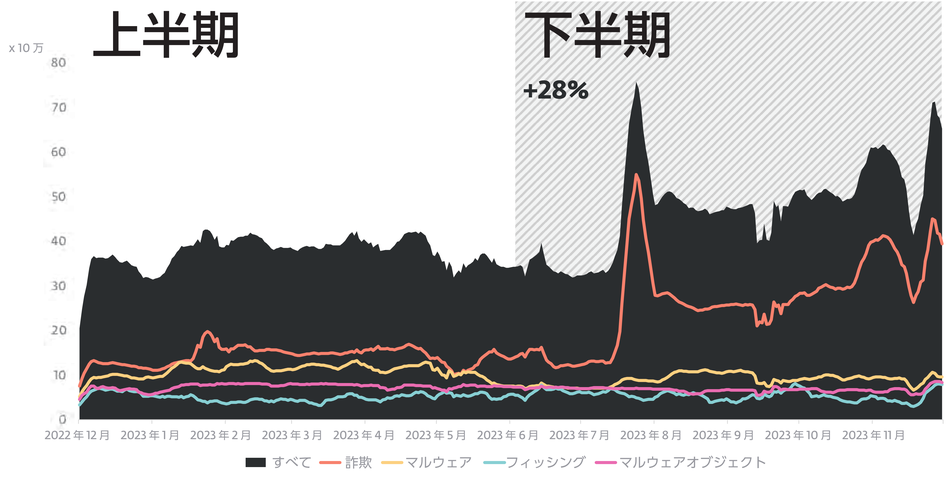


2023 年下半期における**ランサムウェアへの検出の地理的な分布**

Web に関する脅威

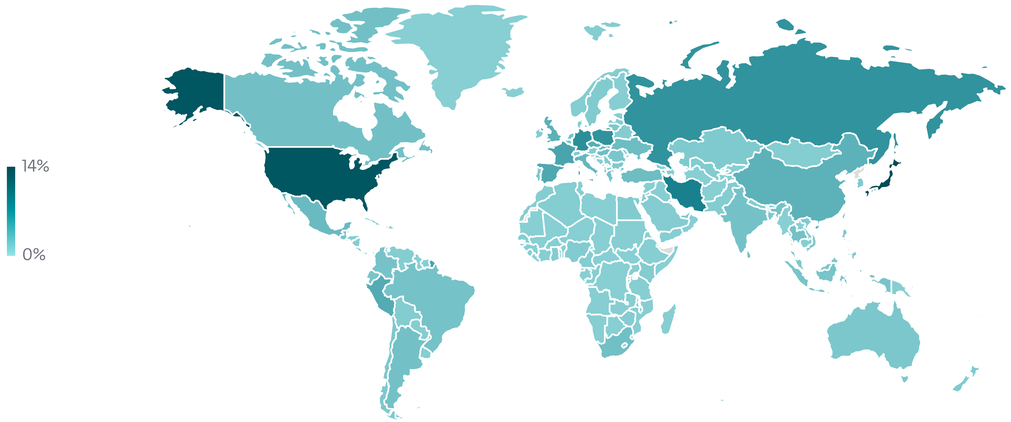


2023 年上半期～ 2023 年下半期に**ブロックされた Web 脅威の傾向**、7 日移動平均線

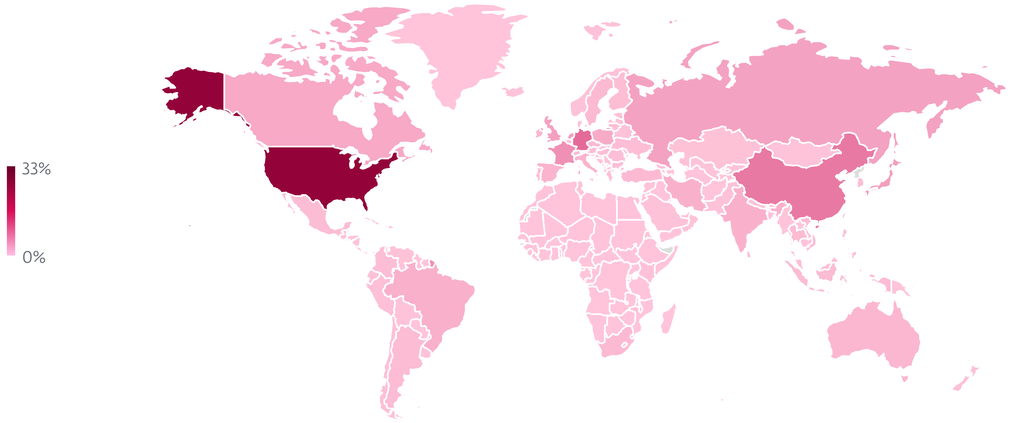


2023 年上半期～ 2023 年下半期に**ブロックされたユニーク URL の傾向**、7 日移動平均線

Web に関する脅威



2023 年下半期に**ブロックされた Web 脅威の世界的な分布**



2023 年下半期に**ブロックされたドメインホストの検出数の世界的な分布**

調査レポート

Asylum Ambuscade：クライムウェアか、それともサイバースパイか？

サイバー犯罪とサイバースパイの両方を実行している特異な攻撃者

WhatsApp のバックアップを狙う Android GravityRAT

WhatsApp のバックアップファイルを盗み出し、ファイル削除コマンドを受け取るスパイウェアである GravityRAT の最新バージョンを ESET の研究者が分析しました。

Emotet の現状

2021 年 11 月に Emotet が復活してからの活動の概要

ESET Research のポッドキャスト：BlackLotus ブートキットの分析

ゲームのチート行為を分析することで、UEFI の重大な脅威が見つかったエピソードを紹介します。

MoustachedBouncer：ベラルーシ駐在の外国外交官に対するスパイ活動

C&C との通信に使用されるメールベースのプロトコル、C++ で記述されたモジュール型のバックドア、中間者攻撃の一種である AiTM 攻撃（Adversary-in-the-Middle 攻撃）などの特徴のある外交官に対するスパイ活動が長期にわたって行われています。これらの攻撃は Turla との共通点が多くあることから、ESET は詳細な検証を行いました。

ESET Research のポッドキャスト：MoustachedBouncer の正体を暴く

ESET の脅威リサーチ部門のディレクターである Jean-Ian Boutin が、ベラルーシの外国大使館を標的に攻撃している APT グループ「MoustachedBouncer」の TTP（戦術 / 技術 / 手順）を明らかにしました。

不特定多数の Zimbra ユーザーを標的とする大規模なキャンペーン

ESET の研究者は、NikoWiperZimbra Collaboration メールサーバーのユーザーを標的とした新たなフィッシングキャンペーンを確認しました。

脆弱なサーバーを標的として攻撃する Scarabs ランサムウェア

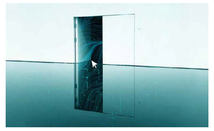
脆弱なサーバーに Scarab ランサムウェアを展開するために使用されるツールセット「Spacecolon」と、そのオペレーターである CosmicBeetle を ESET が分析しました。

Telekopye：Telegram として運用される多機能ツールキット

オンラインマーケットプレイスでサイバー犯罪者による詐欺を支援する Telegram ボットの分析

Signal と Telegram アプリをトロイの木馬化し、Android ユーザーを標的とする BadBazaar スパイツール

ESET の研究者は、GREF として知られる中国政府とつながりのある APT グループが実行しているキャンペーンを発見しました。GREF は、過去にウイグル自治区を標的としたスパイコードを展開しています。



APT グループ Ballistic Bobcat が使用するバックドア「Sponsor」

ESET Research は、APT グループ「Ballistic Bobcat」が使用する Sponsor バックドアによる「Sponsoring Access」キャンペーンを発見しました。

ESET Research のポッドキャスト：セクストーション、デジタル空間での法外な金利貸し、SQL ブルートフォース

侵入経路を封鎖されたサイバー犯罪者は、これまでの攻撃手法を見直すだけでなく、新たな攻撃方法を探さなければならなくなりました。

APT グループ OilRig がイスラエルを対象に実行した 2 つのキャンペーン「Outer Space」と「Juicy Mix」

ESET の研究者が、2021 年と 2022 年にイスラエルの組織を標的に OilRig が実行した「Outer Space」と「Juicy Mix」キャンペーンを分析しました。

Stealth Falcon グループによる新しい高度なモジュラーバックドア「Deadglyph」

ESET の研究者は、悪名高い Stealth Falcon グループが中東でのスパイ活動に使用していた高度なバックドア「Deadglyph」を発見しました。

Lazarus、採用の一貫としてコーディングの課題にトロイの木馬を仕込む手法で従業員を攻撃：スペインの航空宇宙関連企業のケース

航空宇宙企業の従業員を標的とする Lazarus に攻撃を分析しているときに、ESET の研究者は、新たしいバックドアを発見しました。

Jacana 作戦：ガイアナのホビット族を発見せよ

ESET の研究者が、ガイアナの政府機関に対するサイバースパイキャンペーンを発見しました。

Mozi をテイクダウンしたのは誰？IoT を標的とする Mozi ボットネットの活動が急減か？

IoT を標的とする Mozi ボットネット活動が急激に減少した理由を探る。ESET Research は、最も拡散しているボットネットの 1 つをテイクダウンするために使用されているキルスイッチを特定しましたが、誰が何の目的でこのキルスイッチを使用しているのは謎のままです。

2023 年第 2 四半期～第 3 四半期 ESET APT 活動レポート

2023 年第 2 四半期および第 3 四半期に ESET Research が調査および分析した APT グループの活動の概要をお伝えします。

ツタンカーメン作戦：ラテンアメリカにおける脅威環境

ESET の研究者は、ラテンアメリカ地域に影響を及ぼす脅威が、回避の手法を取り入れ、価値の高い標的を選定して、さらに巧妙化していることを明らかにしました。

未知のマルウェア「Kamran」：ギルギット・バルティスタンのウルドゥー言語の住民を監視する Android マルウェア

ESET の研究者が、Hunza News のウルドゥー語圏の読者を監視する未知のマルウェア Kamran を発見しました。

Winter Vivern、Roundcube Webmail サーバーのゼロデイ脆弱性を攻撃

ESET Research は、Roundcube Webmail を速やかに最新バージョンにアップデートすることを推奨しています。

Telekopye：ネアンデルタール人の秘密の部屋

オンラインマーケットで詐欺を働く Telekopye ボットを運用するグループの調査結果

クレジット

チーム

Peter Stančík、チームリーダー

Hana Matušková、マネージングエディター

Aryeh Goretsky
Branislav Ondrášik
Bruce P. Burrell
Klára Kobáková
Nick FitzGerald
Ondrej Kubovič
Rene Holt
Zuzana Pardubská

貢献者

Anton Mäčko
Dušan Lacika
Igor Kabina
Ivan Bešina
Jakub Souček
Ján Adámek
Ján Šugarek
Jiří Kropáč
Ladislav Janko
Lukáš Štefanko
Martin Červeň
Michal Kopera
Michal Malík
Michal Škuta
Milan Fránik
Miloš Čermák
Patrik Sučanský
Vladimír Šimčák
Witold Gerstendorf

本レポートにおけるデータについて

本レポートに示されている脅威の統計と傾向は、ESET のグローバルテレメトリ（監視チーム）データに基づいています。特に明記されていない限り、検出に含まれるデータは標的となったプラットフォーム別にはなっていません。

さらに、詳細なプラットフォーム固有のセクションと「暗号通貨の脅威」のセクションで記載されている場合を除いて、これらのデータでは望ましくないアプリケーション（PUA）、潜在的に危険なアプリケーション、およびアドウェアの検出数が除外されています。

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

本レポートのほとんどのグラフは、絶対数ではなく、検出傾向を示しています。このような表示を行っている主な理由は、ほかのテレメトリデータと直接比較する場合にデータについてさまざまな誤解を招きやすいためです。ただし、有益であると思われる場合は、絶対値または桁数を表示しています。

ESET について

ESET は 30 年以上にわたり世界中の個人および法人に向けて、業界をリードする革新的な IT セキュリティソフトとサービスを開発し、サイバーセキュリティ脅威に対する包括的な多層防御ソリューションを提供してきました。ESET は長年にわたり、マルウェアの予防、検出、対応を行う機械学習とクラウドテクノロジーのパイオニアとして活動しています。ESET は、科学的な研究開発を世界的に推進している非公開会社です。

WeLiveSecurity.com

@ESETresearch

ESET GitHub

ESET 脅威レポートと APT アクティビティレポート

Digital Security
Progress. Protected.

(eset):research