サイバー脅威レポート

2024 年 6 月

専門家、センサー、テレメトリ、インテリジェンスから成るグローバル ネットワークから得られたインサイト

主なテーマ

APT 状況における急速かつ重大な変化

ランサムウェア エコシステムを活発にさせる LockBit

拡大する攻撃者のツールボックス

提供

Trellix ADVANCED RESEARCH CENTER

あなたと同じ業界のある組織で、エンドポイント検出 / 対応機能を遮断するために、EDR 回避ツールが使用されました。

サイバー セキュリティは攻撃者の一歩先を行こうと努めているものの、正規のセキュリティ ツールの悪用を阻止することはますます難しくなっています。

CISO は、アジリティ、スピード、自信、コントロールを伴って行動する必要があります。CEO と取締役会は、ロギングとアラート ツールに関する情報を求めています。CISO はギャップの特定をチームに課し、特定されたギャップに対処する計画を練ります。

サイバー セキュリティのレースはトライアスロンのようなものです。CISO は、SecOps、技術、インテリジェンスを競っています。レースは始まっています。そしてここでは忍耐力が問われます。

防御メカニズムはますます高度になっていますが、国家支援型の攻撃者やサイバー犯罪者が使用する攻撃ツールや戦術も同様です。

サイバー脅威レポート

Trellix の Advanced Research Center による本レポートは、(1) サイバー セキュリティ脅威について、複数のソースの重要なデータから得られたインサイト、インテリジェンス、ガイドラインを紹介し、(2) このデータの専門的、合理的、妥当な解釈を展開して、サイバー防衛のベスト プラクティスにつながる情報をお届けします。今回のレポートでは、主に 2023 年 10 月 1 日から 2024 年 3 月 31 日までに収集されたデータとインサイトに焦点を当てています。

1. APT 状況における急速かつ重大な変化
2. ランサムウェア エコシステムを活発にさせる LockBit
3. EDR キラーの登場
4. 米国大統領選挙をテーマにした詐欺
5. 生成 AI とサイバー犯罪者の地下活動

序文

CISO にとって、実用的な脅威インテリジェンスや、あらゆる脅威に関するコンテキストを、組織環境に提供できる能力がかつてないほど重要になっています。

少ない労力でより多くを行うことが求められている CISO とその SecOps チームは、脅威に先手を打つ、組織を標的にしている最も関連性の高い脅威を特定して備える、最も可能性の高い脅威や攻撃者に対するプログラムや予算を調整する、そして最終的には、リアクティブからプロアクティブな体制へと移行することを可能にする、脅威インテリジェンスを求めています。

Trellix の「カスタマーゼロ」として、私は、対応チームが動き、戦略を立てる方法を形成する上で役立つインテリジェンスの可能性をかつてないほど感じています。

こうした情報を取り込んで吸収し、戦略的計画、予算の合理化、取締役会の教育、オペレーション サポートで使用しましょう。このインサイトが教育的で情報とメリットをもたらし、APT に対する計画、準備、存続の方法を導き、影響を与える足がかりとなることを願っています。



Harold Rivas
CISO、TRELLIX

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

まえがき

このレポートや、Trellix のすべてのレポートは、Trellix が観察したものに、インテリジェンスやコンテキストといった構造を付け加えることを目的としています。

状況

ここ 6 か月はこれまでにない激動の期間でした。ポリクライシスは依然として続き、サイバー犯罪者や攻撃者による活動が世界的にますます活発になっています。活動に以下のような急激な変化が確認されています。

- ランサムウェア エコシステムは、法執行機関活動を受けて不規則な動きを見せています。
- 自律的なグループは、自身のペネトレーション テスト ツールや代替の攻撃手法をランサムウェア グループに販売しています。
- イスラエルでの戦争により直接的な国家支援型の攻撃やハクティビズムが引き起こされています。
- 攻撃者は、より巧妙になることを求めており、夜通しエキスパートになれるような、安い、または無料の生成 AI ベースのツールを利用しています。
- EDR の回避や無効化を可能にするツールは、攻撃者にとってますます重要になっています。

いたちごっこ

エンドポイント検出 / 対応 (EDR) ソリューションは幅広く実装されており、サイバー セキュリティのいたちごっこはますます複雑になっています。Trellix は、EDR を解除するために犯罪ツールを使用する攻撃者の増加に着目しています。また、それに伴って、従来のマルウェアベースのツールの使用から急激にコースが変更されています。

防御側の私たちもコースを変更する必要があります。EDR が、マルウェア、ランサムウェア、APT グループの活動を効果的に検出することは実証済みですが、EDR が無効化されてしまった場合、組織と CISO は何をすべきでしょうか？普段では見られない行動がシステム上で発生したときにそれを見逃さないために、ロギング、アラート、実用的な脅威インテリジェンスが必要です。新たな役割を担うレイヤーです。

Trellix では、敵に先手を打つための弊社の基本的価値観である脅威インテリジェンスをコミュニティと共有し、広範囲でキャンペーンや脅威グループを追跡することに取り組んでいます。

状況はかつてないほど変化しています。私たちの目的は、防御の強化、対応策の作成、ギャップの特定に必要なインテリジェンスにより、顧客と業界を広範囲でサポートすることです。

このいたちごっこに、私たちは、勝利を目指して取り組まなければなりません。



John Fokker
THREAT INTELLIGENCE 責任者、TRELLIX

目次

序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

はじめに : サイバー脅威レポート : 2024 年 6 月

サイバー分野に影響する地政学的事象

2023 年 10 月 1 日～ 2024 年 3 月 31 日の間に Trellix Advanced Research Center が実施した活動調査では、脅威活動に大きな変化が見られました。地政学上の目的をもつサイバー攻撃活動が大幅に増加しました。中でも、軍事演習、政治サミットまたは経済サミット、政党大会、選挙といった、地域イベントや国際イベントが、サイバー脅威活動を推進していました。

Trellix アナリストは、攻撃者がこうしたイベントに焦点を当て、相手に関するインテリジェンスの収集、プロアクティブにネットワークを調査して状況を把握するための情報の収集、今後の攻撃に向けて戦略的に IT ネットワークへの攻撃を準備していることを、ある程度の確信をもって推測しています。

- **サンフランシスコでのバイデン大統領と習近平主席の会談** 2023 年 11 月、Trellix のテレメトリ検出データは、APEC (アジア太平洋経済協力) 会議の一環としてサンフランシスコで開かれたバイデン大統領と習近平主席の会談のわずか数日前に、中国が関与する APT グループによる悪意のある活動の増加を確認しました。脅威活動は、バイデン大統領と習近平主席の会談後、また APEC サミット期間中は大幅に減少しました。

  APEC サミットの終わりが近づくにつれて、脅威活動レベルも 2023 年 11 月には最低ポイントまで低下しました。中国が関与する攻撃者グループによるこうした脅威活動パターンからおそらく、中国の国家支援型攻撃者グループは、APEC などの地政学的イベントに大きく影響されていると考えられます。これはまた、中国の APT グループが、おそらくパブリック イメージや国際的な評判を守るために、大きな政治イベント中はハイジャック活動を意図的に控えた可能性があることを示しています。
- **イスラエルとハマスの戦争** : イランが関与する APT グループによる脅威もまた、イスラエルとハマスの戦争に関わる政治的な変動によって引き起こされたものです。Trellix のグローバル テレメトリ データによると、米国では (2023 年 11 月と 12 月を除く) ここ 6 か月でイランが関与する APT グループによる悪意のある活動が定期的に増加していることが確認されています。具体的にいうと、Trellix のグローバル テレメトリでは、イランがハマスを支持することを公表し、米国がガザ地区での人道的停戦を求めた際、2023 年 11 月下旬から 12 月に行われたイスラエルの人質交換と停戦協定で、米国の組織を標的にしたイランが関与する APT グループによる脅威活動の減少が見られました。また、このテレメトリでは、イランが関与する APT グループが、レポート対象期間に、イスラエルの組織を標的にしたフィッシング、情報窃取、バックドア、ダウンローダー、悪意のある WebShell、広く悪用されている脆弱性など、さまざまな TTP (戦術、手法、手順) を用いていることを示しています。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

- **軍事演習**：また、戦争への備えを強化するための複数国の合同軍事演習も、悪意のある活動を増加させる一因となっています。最近では、2024 年 3 月 4 日～ 3 月 14 日の間、米国と韓国の大規模な合同軍事演習の際に脅威活動が繰り返し増加したことが、2024 年 3 月の Trellix のグローバル テレメトリ データによって確認されました。これらの軍事演習は、「韓国の作戦区域」を反映し、北朝鮮による、拡大する核の脅威に対抗するものです。具体的には、2024 年 3 月 7 日～ 13 日の間、韓国で通常の 20,000 件を上回る、1 日 150,000 以上の脅威が検出されました。
- **ロシアとウクライナの戦争**：この地域で今もなお続くキネティックな戦いに伴い、大小のサイバー イニシアチブが生まれています。特筆すべきは、ロシアが関与する攻撃者が、新しい高度なワイパー マルウェアを積極的に活用して、ウクライナの電気通信事業者である Kyivstar を攻撃し、数千の仮想サーバーや PC を消去している事実が確認されたことです。Kyivstar への攻撃は、2022 年にロシアがウクライナに侵攻してから、最も大きな影響を与えた壊滅的なサイバー攻撃の一つです。

ハイライト概要

レポートは、さまざまな業務活動で実施された調査のリポジトリとしての役割を担っていますが、主要なテーマは一貫しています。

1. APT 状況における急速かつ重大な変化
    a. **ロシアが関与する Sandworm の増加**：地政学的な緊張が高まるにつれ、APT の活動もエコシステム全体に広まりました。APT の脅威は全体的に増加しており、中でもロシアが関与する Sandworm は、このレポートの観察期間に検出数が 40% 増加しました。
    b. **依然として活発な中国**：中国が関与する脅威グループは、APT 活動を起こしているグループとしては依然として最も活発で、Trellix では、中国が関与するグループによる脅威活動を 2,100 万件以上確認しています。検出された悪意のある活動の 23% は、世界中の政府機関を標的にしたものでした。
    c. **Volt Typhoon による活動が急増**：比較的新しい中国による国家支援型の APT グループ、Volt Typhoon は、その独自の行動パターンや標的の定め方が際立っています。Trellix のテレメトリでは、2024 年 1 月中頃から、Volt Typhoon が関与する悪意のある活動が 7,100 件以上検出され、2024 年 1 月から 3 月にかけて定期的な増加が見られています。

目次

序文
まえがき
はじめに：サイバー脅威レポート：2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論：データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス：LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い：サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途：本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

2. **ランサムウェア エコシステムを活発にさせる LockBit**
    a. **国際的な法執行機関の活動「Operation Cronos」の実施後、Trellix は、LockBit のなりすましを確認しました。グループは必死に面目を保ち、詐欺活動を再開しようとしました。**
    b. **米国は依然として最大のターゲットに**: 米国は依然として、ランサムウェア グループの最大のターゲットになっており、トルコ、香港、インド、ブラジルがこれに続きます。
    c. **最も被害を受けたのは運輸業**: 2023 年第 4 四半期と 2024 年第 1 四半期に、ランサムウェア攻撃者によって最も脅かされた業種は、運輸業です。全体的なランサムウェア検出数のうち、2023 年第 4 四半期では 53%、2024 年第 1 四半期では 45% を占め、金融業がこれに続きます。
    d. **法執行機関による判決**: このレポートの最終稿を確定する前に、国際的な法執行機関が LockBit の首謀者の正体を明かしました。ランサムウェア犯罪者に対する措置が 5 月 1 日に講じられました。Kaseya などの多くの組織を攻撃した REvil アフィリエイトが、懲役 13 年、1,600 万米ドルの返済を言い渡されました。
3. **EDR キラーの登場**
    a. **D0nut ランサムウェア グループの登場**: D0nut ランサムウェア グループの登場は、EDR キラー ツールの使い方が革新的であったことから特に注目すべきです。エンドポイントの検出を回避し、攻撃の有効性を強化するといった高度な戦術を用いています。
    b. **電気通信事業者を標的にした Spyboy の EDR 回避ツール**: 2024 年 1 月、Spyboy という開発者による EDR「キラー」ツール、「Terminator」が新しいキャンペーンで使用されました。このツールは、EDR ソリューションを回避するためのものであり、検出された脅威の 80% が電気通信事業を標的にしたものでした。
4. **米国大統領選挙をテーマにした詐欺**
    a. **依然として盛んなフィッシング**: 11 月に行われる米国大統領選挙の結果に世界中が注目している中で、選挙でのイメージを利用したり、寄付を募ったりする詐欺が確認されています。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
    - 活発な国家と APT グループ
    - APT グループと拠点国
    - 標的とされる国と地域
    - 悪意のあるツール
    - 悪意のないツール
    - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
    - 概要
    - 攻撃活動のタイムライン
    - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
    - オペレーション クロノス : LockBit を阻止する法執行機関活動
    - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
    - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
    - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
    - 選挙資金寄付詐欺
    - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
    - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
    - インフォスティーラーに導入される生成 AI
    - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

5. **生成 AI とサイバー犯罪者の地下活動**

   a. **AI を活用した無料のツール :** Trellix は、無料の ChatGPT 4.0 Jabber ツールがサイバー犯罪者のアンダーグラウンドの世界で入手可能であることを確認しました。このツールにより、開発者は、攻撃者が生成 AI を活動に利用できるようにしたり、生成 AI ナレッジ ベースを作成して他のサイバー犯罪者から学んだり、さらにはアイデアやツールを盗んだりすることができます。

   b. **増加するインフォスティーラーの導入 :** 生成 AI ベースの機能を搭載した 2 つのインフォスティーラーが、サイバー犯罪者によって使用されていることが確認されました。MetaStealer と LummaStealer はそれぞれ、検出を回避する生成 AI、ログ リストにあるボットを検出する生成 AI を搭載しています。生成 AI 機能により、これらの犯罪者の戦術は、見つけるのも阻止するのも困難になっています。

方法論 : データの収集および分析方法について

Trellix の Advanced Research Center に所属する専門家は、本レポートを構成する統計、トレンド、インサイトを、クローズドかオープンかを問わずグローバルな幅広いソースから収集しています。収集されたデータは、弊社の Insights および ATLAS プラットフォームへ送られます。機械学習、自動化、そして人間の鋭敏な感覚を活用して、チームは集中的、統合的、反復的なプロセスをひととおり実施します。つまり、データを正規化して情報を分析し、全世界でサイバー セキュリティの最前線にいるサイバー セキュリティ リーダーや SecOps チームにとって有意義なインサイトを導き出すというプロセスです。弊社の手法の詳細については、本レポートの末尾をご覧ください。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

レポート分析、インサイト、データ

国家と APT (Advanced Persistent Threat)

2023 年 10 月～ 2024 年 3 月、Trellix では、以前の 6 か月と比較して、APT 関連の検出数の増加が 17% だったことを確認しました。前回のレポート では 50% も増加したことをふまえると注目すべき点です。APT エコシステムは 1 年前とはその根本から変わっており、より攻撃的で狡猾、より活発になっています。

急速に進化するサイバー脅威状況において、APT (Advanced Persistent Threat) グループは、世界のサイバー セキュリティに重要で高度な課題を投げかけています。

Trellix は、2023 年第 4 四半期から 2024 年第 1 四半期の間に検出された APT (Advanced Persistent Threat) 関連の活動を徹底的に分析することを目指しました。こうした脅威の発生源、主な標的、攻撃活動で使用されたツールが分析の焦点となっています。増加・減少率と占有比率の変化率といった、2 つの主要メトリックスを使用して、この期間の調査結果を、2023 年前半 (第 2 四半期～第 3 四半期) のデータと比較します。

- **増加・減少率** : このメトリックスは、特定の APT グループの活動、特定の国が標的にされている状況、または特定のツールの使用について、増加、減少、または横ばいのいずれであるかを示します。これを理解することにより、こうした攻撃者の行動がどのように変化しているか、サイバー脅威の状況がどのように進化しているかを追跡できます。
- **占有比率の変化** : このメトリックスは、活動の変化をそのまま示すだけでなく、サイバー セキュリティ脅威環境全体に対し、このような変化がどのような位置にいるかを示すことで、コンテキストを追加します。たとえば、ある攻撃者の検出数が大幅に増加したとしても、脅威環境全体がそれ以上に拡大していれば、これは総サイバー脅威数のわずかな部分を占めるだけかもしれません。反対に、ある攻撃の検出数が減少したとしても、それ以外の脅威環境がそれ以上に縮小していれば、この攻撃者はどちらかといえば深刻であるといえます。

これらのメトリックスを用いることで、APT 活動の変化のわずかな違いも把握し、戦略的な目的、優先的な方法、こうした活動がもたらすサイバー セキュリティの課題に関するインサイトを導き出すことができます。以下のセクションでは、これらの調査結果を徹底的に調査し、APT の複雑な世界や、こうした巧妙な脅威から保護するために続けるべき取り組みにスポットライトを当てています。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

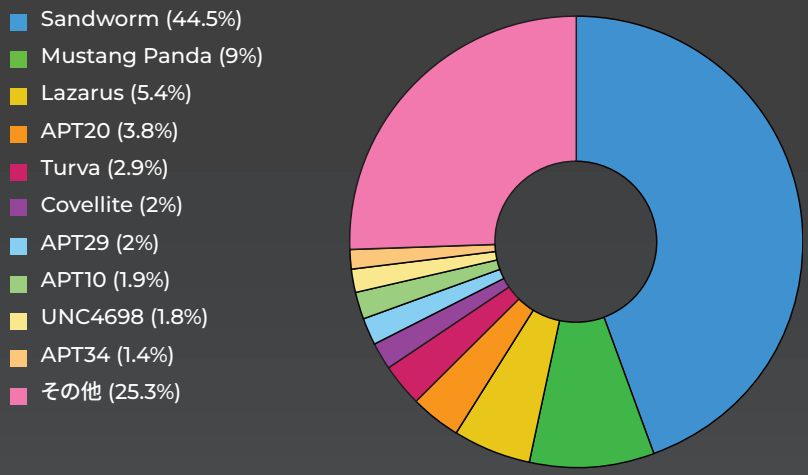
リソース

- Trellix Advanced Research Center について
- Trellix について

活発な国家と APT グループ

また、2023 年 10 月～ 2024 年 3 月の期間では、さまざまな APT グループの活動に大きな変動が確認されました。こうした変動から、サイバー脅威の動的な性質だけでなく、これらの巧妙な攻撃者の活動の焦点や手法も変わってきていることが読み取れます。

2023 年第 4 四半期～ 2024 年第 1 四半期の間に検出された上位 10 の APT



サイバー脅威グループ活動における変化 : 増加・減少率と占有比率の変化率

高度な持続型脅威	増加・減少率	占有比率の変化率
Sandworm	1669.43%	40.34%
Mustang Panda	-2.19%	-6.14%
Lazarus	66.87%	0.07%
APT28	18.67%	-1.49%
Turla	2.95%	-1.74%
Covellite	85.30%	0.23%
APT29	123.98%	0.53%
APT10	80.46%	0.17%
UNC4698	368.75%	1.14%
APT34	96.73%	0.23%
その他	-28.99%	-33.33%

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

- **戦術の転換**: 破壊的なサイバー活動で古くから知られている Sandworm は、その検出数が 1669% も増加し、占有比率も 40% 上昇しています。この記録すべき上昇は、ロシアが関与するグループによるサイバー活動がかつてないほど増加していることを示唆しています。
- **繰り広げられる活動**: 広くサイバー スパイを展開してきた歴史をもつ APT29 は、検出数が 124% 増加し、活動がかなり活発化しました。同様に、APT34 と Covellite も検出数がそれぞれ 97%、85% と大幅に増加しており、活動の頻度が高まっている、または新たなキャンペーンが実行されていることがうかがえます。
- **変化なし**: 対照的に、Mustang Panda、Turla、APT28 などのグループでは活動レベルに大きな変化はなく、Mustang Panda の場合は検出数が 2% のわずかな減少、Turla では 3% のわずかな上昇が見られたのみです。
- **新たな攻撃者の登場**: 注目すべきは UNC4698 の登場です。検出数は 363% 増加しており、APT 状況に対して大きな影響力を持ちうる新たな攻撃者が台頭してきていることがうかがえます。

UNC4698 についてわかっていることは？

このグループについてあまり多くのことはわかっていませんが、研究者は、グループの活動としての行動であることを認識できるものの、どのように分類してよいかはわかっていません。

そうした中でも、UNC4698 についてわかっているのは、産業スパイ活動に焦点を当て、業務上の機密データを収集していることです。こうしたデータは、支援に当たっている国家の経済的な目的または国家安全上の目的をサポートするために使用されていると思われ、攻撃の性質や標的の地域を考慮すると、中国が関与していると考えられます。

主な標的は、アジアの石油・ガス関連の組織です。

このグループは、通称「SNOWYDRIVE」のマルウェアを用いていることがわかっています。

UNC4698 は、USB フラッシュ ドライブ経由で配布されるマルウェアの使用を中心とした、さまざまな戦術、手法、手順 (TTP) を用いています。この攻撃者に関連した主な TTP は以下のとおりです。

- **感染 USB デバイス経由での初期アクセス**: 主な感染方法として、ホスト システムでバックドアを作成するために設計された、悪意のあるソフトウェアが含まれる USB ドライブが使用されます。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

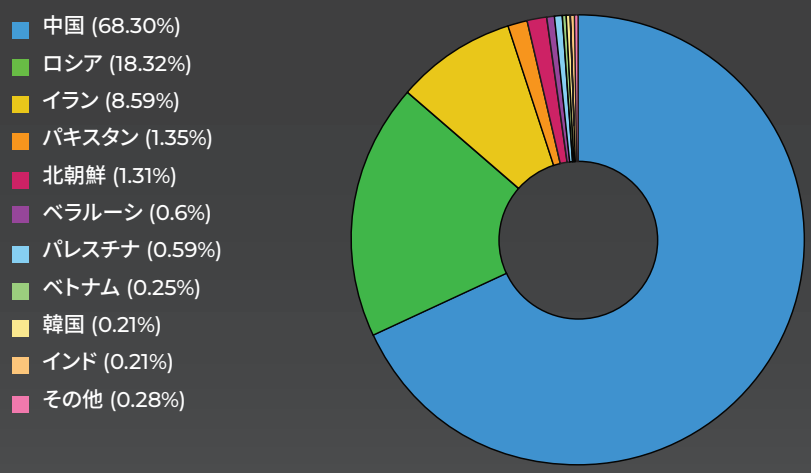
UNC4698 についてわかっていることは？ (続き)

- **悪意のあるファイルを介した実行** : このマルウェアには通常、悪意のある実行ファイルや DLL をディスクに書き込むドロッパーが含まれます。これらのファイルは多くの場合、検出を回避するために正規のソフトウェアに偽装しており、さらなるコントロールを確立するために実行されます。
- **滞留とレジストリの変更** : UNC4698 は、Windows レジストリを変更することで感染システムに滞留します。これにより、マルウェアは、システムが起動すればいつでも自動的に開始することができます。
- **コマンド & コントロール (C2) コミュニケーション** : マルウェアは、リモート コミュニケーションの手法を設定します。これにより、攻撃者は、侵害されたシステムに対し、遠隔でコマンド & コントロールを実行することができます。
- **リムーバブル メディア経由でラテラル移動** : マルウェアは、他の USB デバイスが感染マシンに接続すれば自動でコピーされるため、簡単に他のシステムに感染を広げることができます。

あまり知られていない、または特定されていないグループについては、検出数が 62% 増加しており、これまで十分に情報が収集されてきた APT 組織よりも、脅威の多様化と成長が進んでいることを示しています。総検出数に対するこのグループの占有比率は 8% 上昇していることから、サイバー脅威が確実に進化・多様化していることが読み取れます。

APT グループと拠点国

2023 年第 4 四半期～ 2024 年第 1 四半期の間、キャンペーンに関連した検出に基づく、APT に関与した上位 10 か国



目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

サイバー分野に影響する地政学的事象

ハイライト概要

方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

国家と APT (Advanced Persistent Threat)

活発な国家と APT グループ

APT グループと拠点国

標的とされる国と地域

悪意のあるツール

悪意のないツール

まとめ

Volt Typhoon: 中国が関与する国家支援型 APT 脅威

概要

攻撃活動のタイムライン

戦術、手法、手順 (TTP)

進化するランサムウェア状況

オペレーション クロノス : LockBit を阻止する法執行機関活動

ランサムウェアの総合的考察

EDR キラーの登場と回避ツール

Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン

確認される EDR キラーの増加

メールは依然として攻撃者が盛んに用いる手段

選挙資金寄付詐欺

税金関連のフィッシング

生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見

ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト

インフォスティーラーに導入される生成 AI

「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

用途 : 本レポートの情報の使用方法

本レポートで分析を理解する方法

リソース

Trellix Advanced Research Center について

Trellix について

拠点国について見ると、2023 年 10 月～ 2024 年 3 月の Trellix のテレメトリでは、国家支援型のサイバー活動の状況も大きく変化していることが確認されています。



中国が関与する脅威グループは依然として APT 活動を最も多く生み出しています

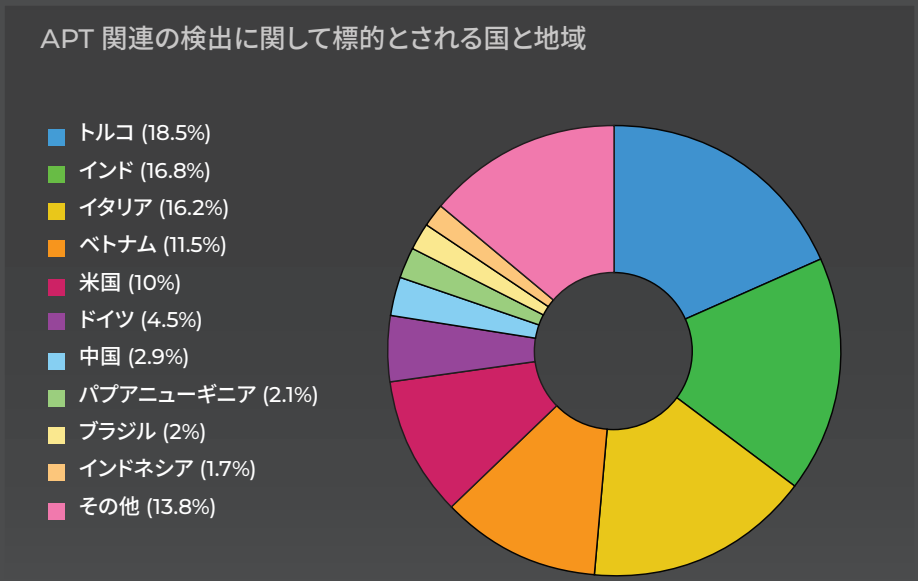
- **大幅に増加する攻撃活動**：さまざまな国で、地政学上の目的やサイバーセキュリティの能力は進化しています。Trellix のテレメトリでは、以下が確認されています。
  a. ロシアが関与する脅威グループは、APT の検出数が 31% も増加しており、占有比率も 4% 上昇しています。これは、サイバー攻撃がかなり増加していることを示しており、拡大する戦略目的または世界的なサイバーセキュリティ ダイナミクスへの対応を反映したものと考えられます。
  b. イランが関与する脅威グループもまた、サイバー活動が著しく増加しており、検出数は 8% 増加し、占有比率は 3.89% 上昇しています。これは、地政学上の目的やイスラエルとハマスの戦争への関与に沿って、イランのサイバー活動が大幅に拡大していることを強調しています。
- **広まる多様化**：中国は、検出数こそわずかに 1% 増加したものの、依然として APT 活動を最も多く生み出している国です。しかし、総検出数に対する占有比率は -1% というわずかな減少を見せており、この期間に APT 拠点国の多様化が進んでいることを示唆しています。また、今年 2 月には、米国の重要なインフラストラクチャを狙った中国支援型の APT、Volt Typhoon による活動が活発であったことが報告されています。詳しくは次のセクションをご覧ください。
- **戦略の転換**：対照的に、北朝鮮、ベトナム、インドが関与するグループは APT 活動が大幅に減少しており、北朝鮮関連の検出数は 82%、ベトナムは 80%、インドは 82% 減少しています。特に、北朝鮮の占有比率が 6% も下降していることは注目すべきです。これはおそらく注力する対象、戦略、または能力が転換したものと思われます。
- **台頭するその他の国**：パキスタンが関与するグループやベラルーシが関与するグループでは、APT 活動が大幅に増加しており、その検出数はそれぞれ 55%、2019% も増加しています。ベラルーシ関連の爆発的な検出数の増加をはじめとしたこのような上昇は、APT の分野で、新しい攻撃者やこれまでは無名に近かった攻撃者が台頭してきていることを示しています。

  「その他」カテゴリについては、検出数が 121% 増加していることから、APT 活動は頻繁に話題になる国に限定されているわけではないことが読み取れます。こうした多様化は、サイバー脅威の世界的な性質を表しており、広範に及ぶ適応型サイバー セキュリティ体制が求められることを示しています。

弊社では、これらの新しいパターンを今後数か月にわたって注視していきます。

目次

序文
まえがき
はじめに：サイバー脅威レポート：2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論：データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス：LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い：サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途：本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について



標的とされる国と地域

このセクションでは、2023 年第 4 四半期から 2024 年第 1 四半期の間に、Trellix によって、APT グループによる APT 関連の活動が検出された国や地域にスポットを当て、こうしたサイバー攻撃者が注力する対象や戦略における重要な転換を明らかにします。

> **データは、サイバー脅威の全体的な性質や、各国が APT グループに対し向けている注意のレベルを表しています。**

Trellix Advanced Research Center は、特定の国や地域で検出された活動に影響を与えたのが以下の要素であることをある程度の確信をもっています。



トルコでは APT 関連の検出数がかつてないほど増加しました

攻撃活動の目的 :
トルコを標的にした脅威の検出数は、実に 1458% 増加し、総検出数に対する占有比率は 16% 上昇しています。この顕著な上昇は、トルコに焦点を当てたサイバー脅威の大きな転換を表しており、広範な地政学的な緊張または APT グループの活動上の目的を反映したものと考えられます。

- **戦略的重要性 :** インドとイタリアでも検出数は大幅に増えており、それぞれ 614%、308% も増加しています。両国が標的リストの中で重要な位置を占め始めていることは、経済的、政治的、または技術的な要素によって、サイバー分野における戦略的重要性が高まっていることを示唆しています。

目次

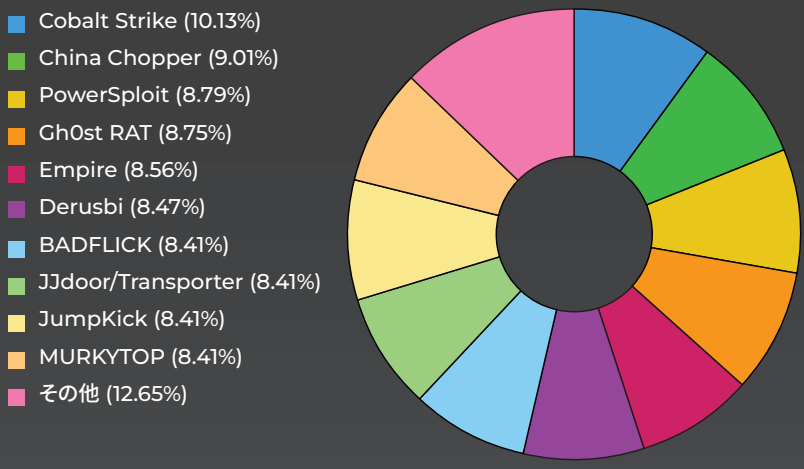
序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

- **拡大する対象地域**：興味深いのは、ベトナムと米国では、APT 検出数が依然として高いものの、傾向が変わってきていることです。ベトナムの検出数は 9% 増加しましたが、その占有比率は 9% 減少しており、標的にされる国が広がっていることを示しています。米国では検出数が 15% 増加と、ある程度増加したものの、その占有比率は 7% 減少しており、APT グループによる標的の戦略が多様化していることを示しています。
- **地政学的な状況変化**：ドイツ、中国、パプアニューギニア、ブラジルは、いずれも検出数が増加しており、ドイツと中国では占有比率も大きく変化しています。こうした標的の多様化は、世界的なサイバー セキュリティ体制や地政学的な状況変化に対応するために、APT グループが戦略や機会を調整していることを表しています。
- **国レベルでセキュリティを強化**：対照的に、インドネシアでは、検出数が -48% という注目すべき減少を見せ、占有比率も 4% 減少しています。この減少は、インドネシアの標的としての優先度が一時的に低下している、またはサイバー セキュリティ対策が国規模で強化されていることによるものであると考えられます。
- **焦点の集中**：「その他」カテゴリは、Trellix によって APT 関連の活動が検出されたさまざまな国を総合したものであり、検出数は 23% 減少し、占有比率は 21% 減少しています。この減少は、この期間に APT グループが高い利益を見込める特定の標的に焦点を当てたケースが積み重なったためと思われます。

Trellix では、地政学的な傾向によって状況は急激に変わり続けると予測しています。

悪意のあるツール

2023 年第 4 四半期～ 2024 年第 1 四半期の間に検出された上位 10 の悪意のあるツール



目次
序文
まえがき
はじめに：サイバー脅威レポート：2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論：データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス：LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い：サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途：本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

2023 年第 4 四半期から 2024 年第 1 四半期の間、APT キャンペーンで使用された悪意のあるツールを分析すると、サイバー攻撃者の好みや攻撃戦術に関して注目すべき傾向が明らかになりました。検出率や占有比率の変化から、進化するサイバー脅威状況や、こうした巧妙なグループが使用するツールの転換の動きに関するインサイトが得られます。

確認された動向は以下のとおりです。

- **攻撃ツールはますます強力に**：Cobalt Strike は、検出数が 17% 減少したものの、依然として多くの脅威グループが好むツールです。一方で占有比率は 1% のわずかな減少にとどまったことから、サイバー攻撃活動において変わらず人気で効果的であると思われ、汎用性が高く、広く使用されているこの攻撃ツールに対する対策の課題も強く残っています。
- **Web シェル、PowerShell、リモート アクセスの攻撃の利用**：China Chopper、PowerSploit、Gh0st RAT も、それぞれ 23%、24%、24% という大幅な減少を見せています。このような減少にもかかわらず、占有比率の変化はわずかであったことから、これらのツールが依然として攻撃者のツールキットに不可欠であることがわかります。Web シェル攻撃、PowerShell エクスプロイト、リモート アクセスにおいて能力を発揮することで知られるこれらのツールは、サイバー攻撃活動の際にさまざまな目的で使える実証済みのツールとして今もなお多用されていることがうかがえます。
- **検出されにくいツール**：Empire、Derusbi、BADFLICK、JJdoor/Transporter、JumpKick、MURKYTOP では、同様の検出数の下降傾向が見られ、いずれも 25% 以上減少しました。このように一斉に減少したのは、攻撃者グループが好むツールが大きく転換したこと、または対応策や検出手法に対抗するために検出されにくい新しいツールへの移行が進んだためと考えられます。
- **絶えず続くイノベーション**：「その他」の悪意のあるツール カテゴリは、検出数に関して 30% という大幅な増加が見られ、占有比率も 6% と注目すべき上昇がありました。この上昇からは、攻撃者が検出を回避し、目的を達成するための新たなツールや手法を模索しながら、継続的にイノベーションを続け、状況に適応していることが読み取れます。

悪意のあるツールの好みが進化していることは、成長するサイバー セキュリティに対応しようとする、サイバー攻撃者の適応型の性質を表しています。

> **防御メカニズムはますます高度になっていますが、APT グループが使用する攻撃ツールや戦術も同様です。**

「その他」の検出数の増加から読み取れるように、使用されるツールが幅広くなっているため、進化するサイバー脅威がもたらすリスクを低減するためには継続的な調査、脅威インテリジェンス、適応型の防御戦略が必要です。

目次

序文

まえがき

はじめに：サイバー脅威レポート：2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論：データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス：LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い：サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

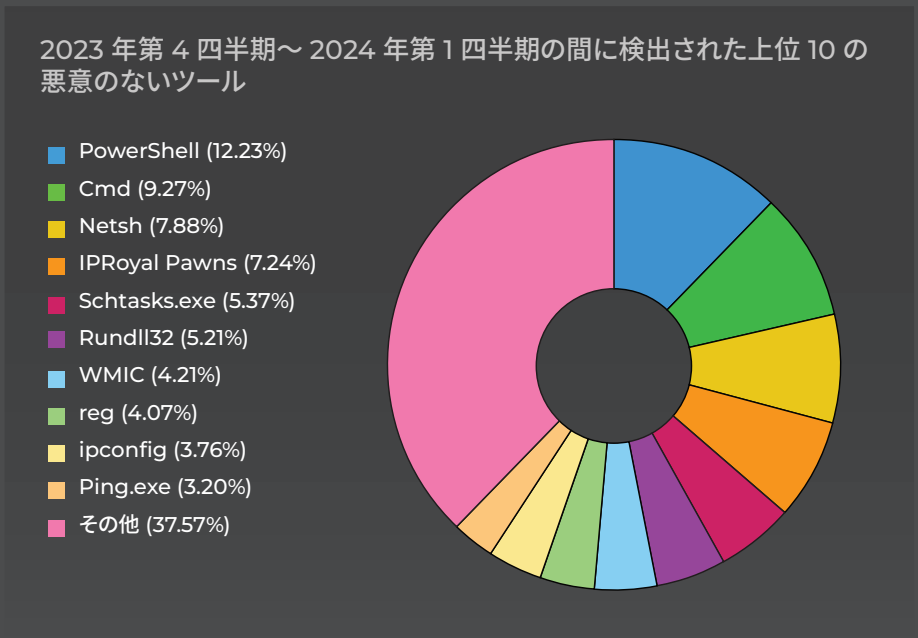
方法論

- 用途：本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

悪意のないツール



> 「Living off the Land (環境寄生)」として知られるこの手法は、検出が困難で、この手法を採用する攻撃者の巧さを示しています。

2023 年第 4 四半期から 2024 年第 1 四半期の間、悪意のないツールが APT グループによるサイバー攻撃活動で使用されたことは、最新のサイバー脅威の重要な側面を表しています。攻撃者は、正規のシステム ツールを活用して悪意のある目的を達成しようとしているということです。「Living off the Land (環境寄生)」として知られるこの手法は、検出が困難で、この手法を採用する攻撃者の巧さを示しています。統計では、このようなツールの使用状況に著しい変化が見られ、サイバー攻撃活動におけるその戦略的重要性が明らかになっています。

- **汎用性 :** PowerShell は、検出数に 105% という劇的な増加が見られ、占有比率では 1% の上昇がありました。この急激な増加は、このツールがさまざまな目的で使用できること、偵察からペイロード配布にいたるまで幅広く、悪意のある活動を自動化できる能力があることを示しています。
- **ネットワーク操作へのフォーカス :** Netsh と IPRoyal Pawns は、検出数がそれぞれ 99%、102% と大幅に増加しています。これらのツールは多くの場合、ネットワーク構成やプロキシ トラフィックに使用されていることから、攻撃者はネットワーク操作や回避手法に戦略的に焦点を当てていることが読み取れます。
- **拡張の自動化 :** Schtasks.exe は、リストに掲載されたツールの中で 138% という最高の上昇率を記録しました。これは、攻撃者による直接的な操作が不要で、悪意のあるペイロードを滞留させて実行するために、スケジュール タスクの利用が高まっていることを表しています。

目次

序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

- **戦術的な転換**：対照的に、Rundll32 と WMIC は検出数こそ増加しましたが、占有比率は減少しています。これらのツールはユーティリティとして変わらず使用されているものの、APT グループの戦術の好みが変わってきていることがうかがえます。
- **ツールの多様化**：Windows システムの古き良きコマンドライン インタープリター、Cmd もまた、検出数が 65% と大幅に増加しました。ただし占有比率は 2.5% 減少しており、APT グループが使用するツールの多様化が進んでいることが読み取れます。

  「その他」カテゴリは、あまり使用されていない、または専門性の高いさまざまなツールが該当するもので、検出数は 42% 増加しています。しかし、占有比率については 21% の大幅な減少が確認されたことから、サイバー攻撃者が使用するツールの幅が広がっていることがうかがえます。

このように、APT グループによる悪意のないツールの使用に関する状況は進化しているため、巧妙なサイバー脅威を検出してそれを防ぐことはますます複雑になっています。悪意のないツールが戦略的に選ばれ、使用されていることから、攻撃者は標的の環境をよく理解しており、検出されないために対策を練っていることが読み取れます。

> **CISO へのヒント**：上記の理由から、サイバー セキュリティ防御は、従来のマルウェア検出にとどまることなく進化する必要があります。振る舞い分析や異常検出を取り入れるなど、正規のツールがサイバー攻撃活動で悪用された場合に対処できるようにしておく必要があります。

Trellix ATLAS グローバル センサーにより収集されたデータと、Trellix Advanced Research Center によって提供され、精査された業界レポートによる戦略的インサイトとを組み合わせることで、顧客は、顧客のセクターを標的にする攻撃者を特定し、振る舞い分析を使用して環境内の異常な行動を検出することができます。

目次

序文

まえがき

はじめに：サイバー脅威レポート：2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論：データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス：LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い：サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途：本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

まとめ

2023 年第 4 四半期から 2024 年第 1 四半期の APT (Advanced Persistent Threat) 活動の分析は、ますます複雑になるサイバー脅威状況の動的な性質を表しています。APT グループの拠点国、標的の国、悪意のあるツールや悪意のないツールの使用に関する統計を調査することにより、サイバー攻撃者の戦略が進化していることを示す主な傾向がいくつか明らかになりました。

APT グループは依然として以下の面で高いレベルを示しています。

1. 適応性と巧妙さ
2. 悪意のあるツールを組み合わせて活用
3. 正規のシステム ユーティリティを悪用し、スパイ活動、業務の妨害、機密情報の窃取を実行

APT グループの標的の定め方や攻撃戦術には大きな変化が見られましたが、これは戦略上の目的が変化しただけでなく、世界的なサイバー セキュリティの成長や防御対策に適応した結果によるものであると考えられます。

一部の国では APT 関連活動の大幅な増加が見られるなど、標的の定め方は大きく変動しており、地政学的な理由がサイバー攻撃活動に影響を与えていることがわかります。同様に、「Living off the Land (環境寄生)」戦術の利用が目立つなど、使用するツールも変化していることから、悪意のある活動とそうでない活動がますます複雑に絡み合う状況下で、APT 脅威を検出してそれに対抗するという課題も依然として強く残っています。

さらに、APT の拠点は多様化が進み、標的戦略も拡大していることから、サイバー攻撃能力が世界的に成長していることが読み取れ、サイバー セキュリティに対する統合型の協同アプローチが求められています。

> **こうした巧妙な攻撃者の攻撃に対し、免疫のある国や組織は皆無であることは明らかです。**

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

Volt Typhoon: 中国が関与する国家支援型 APT 脅威

2023 年第 4 四半期～ 2024 年第 1 四半期には、国家支援型の攻撃者グループが依然として、世界中の商業セクターおよび公共セクターの組織に重大な脅威をもたらしています。これらの攻撃者は多くの場合、装備が十分で、サイバー脅威を巧妙に仕掛けることに長けており、ライバルのサイバー犯罪者またはハクティビストよりも優れた人材とリソースを備え、長期間にわたって容赦なくネットワークを狙います。

23%

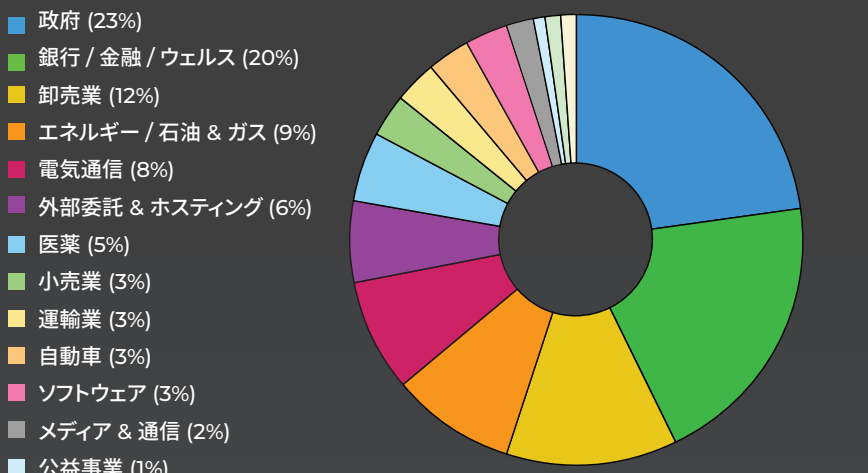
検出された悪意のある活動の 23% は、世界中の政府機関を標的にしたものでした。



中国が関与する攻撃者グループによる脅威活動が 2,100 万件以上確認されました

具体的には、Trellix のテレメトリ検出によると、中国が関与する国家支援型攻撃者グループは、世界中の政府機関にますます脅威をもたらしています。Trellix のデータによると、2023 年 10 月～ 2024 年 3 月の間に、中国が関与する攻撃者グループによる脅威活動が 2,100 万件以上確認されました。

中国が関与する APT グループの業界別の検出



(出典 : ATLAS)

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

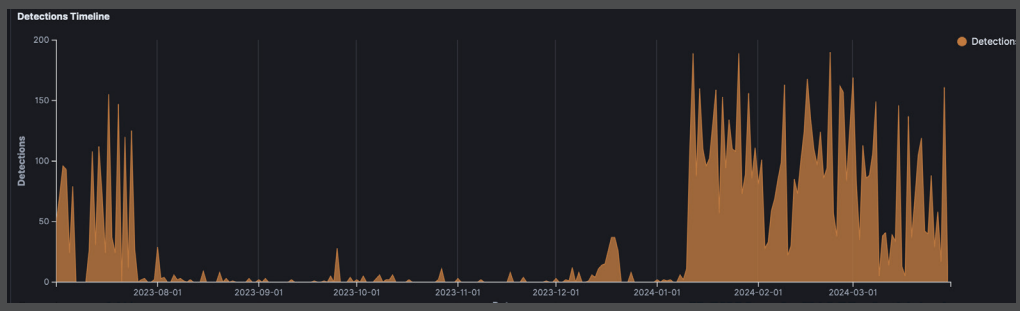
- Trellix Advanced Research Center について
- Trellix について

概要

比較的新しい中国による国家支援型の APT グループ、Volt Typhoon は、その独自の行動パターンや標的の定め方が際立っています。その手法は、従来のサイバー スパイ活動や、中国が関与する他の APT グループが行っている情報収集とは大きく異なるものです。以前のオープンソースのレポートでは、この中国の APT グループは、産業制御系 IT ネットワークにあらかじめ侵入してラテラル移動をスムーズに行い、地政学的な危機または戦争が発生したときに運用技術 (OT) の資産や機能を中断させたことが確認されています。Trellix のテレメトリ データによると、Volt Typhoon は、2024 年 1 月に攻撃活動を再開して以降、「Living off the Land (環境寄生)」戦術を用いながら、米国などの政府機関を繰り返し標的にしています。

攻撃活動のタイムライン

Trellix のグローバル テレメトリ データによると、Volt Typhoon が初めて検出されたのは 2021 年中頃でしたが、2023 年 8 月～ 2024 年 1 月の間は活動がわずか、または全く見られないような休止状態でした。このような休止状態が続いたのは、Volt Typhoon に関する初のベンダー レポートが 2023 年 5 月に発表され、これが世界の注目を浴びた後、さまざまな脅威調査が数か月にわたって行われたためであると考えられます。また、Volt Typhoon の存在が公に知れ渡るようになったことから、この期間に攻撃インフラストラクチャを転換した可能性もあり、それゆえに検出された脅威活動も少なかったのかもしれません。



2023 年 7 月～ 2024 年 3 月の Volt Typhoon 検出タイムライン (出典 : Trellix ATLAS)

Volt Typhoon は、2024 年 1 月中旬に攻撃活動を再開したことが Trellix のテレメトリ データで確認されています。Trellix のテレメトリでは、2024 年 1 月中頃から、Volt Typhoon が関与する悪意のある活動が 7,100 件以上検出され、2024 年 1 月から 3 月にかけて定期的な増加が見られています。



2024 年 1 月～ 3 月の Volt Typhoon の検出に関する詳細

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

戦術、手法、手順 (TTP)

Trellix の検出データによると、Volt Typhoon は、2024 年 1 月中旬に攻撃活動を再開して以降、一貫して多くの Windows ネイティブのツールや機能を活用して、さまざまな悪意のある目的でコマンドを実行しています。これらのツールは、「Living off the Land (LOTL、環境寄生)」ツールと呼ばれ、2 つの目的で使用されているツールです。正規のソフトウェアまたは機能としてシステムに搭載されながら、Volt Typhoon などの中国が関与する国家支援型攻撃者グループの間でも広く使用されるようになっています。Netsh.exe は、悪意のあるさまざまな目的で使用できる、こうしたツールの一つです。ファイアウォール設定の無効化や、プロキシ トンネルの設定によって感染ホストへのリモート ホスト アクセスを可能にすることなどができます。Ldifde は、Volt Typhoon 攻撃者が情報収集のために活用するツールです。

ドメイン コントローラーへのアクセスに成功した攻撃者は、Ldifde.exe を使用して機密データをエクスポートしたり、ディレクトリへの承認済み変更を実行したりすることができます。同様に、Volt Typhoon 攻撃者は、ntdsutil も使用して悪意のある試みを仕掛けています。Ntdsutil は、管理者がデータベース メンテナンスを実行するための正規のツールです。しかし、アクティブ ディレクトリのダンプを作成して、認証情報を取得したり、機密データを抜き出したりすることも可能です。

Volt Typhoon 攻撃者は、依然として FRP、Impacket、Mimikatz といったオープンソースのツールを攻撃活動で使い続けています。2023 年 2 月から 3 月に Trellix のテレメトリで確認された、Volt Typhoon が使用していた LOTL のツールやコマンドは以下のとおりです。

- Comsvcs
- Dnscmd
- Ldifde
- MiniDump
- Net
- Netsh
- Ntdsutil
- reg
- ping
- PowerShell
- PsExec

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

サイバー分野に影響する地政学的事象

ハイライト概要

方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

国家と APT (Advanced Persistent Threat)

活発な国家と APT グループ

APT グループと拠点国

標的とされる国と地域

悪意のあるツール

悪意のないツール

まとめ

Volt Typhoon: 中国が関与する国家支援型 APT 脅威

概要

攻撃活動のタイムライン

戦術、手法、手順 (TTP)

進化するランサムウェア状況

オペレーション クロノス : LockBit を阻止する法執行機関活動

ランサムウェアの総合的考察

EDR キラーの登場と回避ツール

Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン

確認される EDR キラーの増加

メールは依然として攻撃者が盛んに用いる手段

選挙資金寄付詐欺

税金関連のフィッシング

生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見

ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト

インフォスティーラーに導入される生成 AI

「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

用途 : 本レポートの情報の使用方法

本レポートで分析を理解する方法

リソース

Trellix Advanced Research Center について

Trellix について

Trellix のテレメトリで確認された、Volt Typhoon が使用していた主な MITRE ATT&CK ツールは以下のとおりです。

- 初期アクセス – T1190: 公開アプリケーション エクスプロイト
- 実行 – T1106: ネイティブ API
- 永続性 – T1546: イベントにトリガーされる実行
- 特権昇格 - T1546: イベントにトリガーされる実行
- 防御策回避 – T1070.001: Windows イベント ログのクリア
- 防御策回避 – T1070: ファイル削除
- 防御策回避 – T1027: ファイル / 情報の難読化
- 認証情報アクセス – T1003.003: NTDS
- 認証情報アクセス – T1003: OS 認証情報ダンプ
- 認証情報アクセス – T1110: ブルートフォース
- 認証情報アクセス – T1555: パスワード ストアからの認証情報
- 検出 – T1069.002: ドメイン グループ
- 検出 – T1069.001: ローカル グループ
- 検出 – T1083: ファイル / ディレクトリ検出
- 検出 – T1057: プロセス検出
- 検出 – T1010: アプリケーション ウィンドウ検出
- 収集 – T1560: 収集したデータのアーカイブ
- 収集 – T1560.001: ユーティリティでアーカイブ
- コマンド & コントロール – T1090.002: 外部プロキシ
- コマンド & コントロール – T1105: イングレス ツール転送
- コマンド & コントロール – T1132: データのエンコード

進化するランサムウェア状況

2023 年第 4 四半期、サイバー脅威状況では、ランサムウェア攻撃の増加が見られました。この年から新たなファミリーが登場し、その影響はますます深刻になっています。

- **EDR キラー ツール :** EDR キラー ツールの中でも、D0nut ランサムウェア グループの登場は、ツールの使い方が革新的であったことから特に注目すべきです。エンドポイントの検出を回避し、攻撃の有効性を強化するといった高度な戦術を用いています。詳しくは、次のセクションをご覧ください。
- **脆弱性の悪用 :** この期間にはまた、ランサムウェアをよりスムーズに展開するために重大な脆弱性を悪用する傾向も引き続き見られました。中でも、Citrix Bleed と呼ばれる CVE-2023-4966 が、LockBit 3.0 アフィリエイトによって悪用されたことから、依然として重要なインフラストラクチャに潜む脆弱性が、巧妙なサイバー攻撃に寄与していることがわかります。また、Confluence Data Center および Confluence Server では CVE-2023-22518 の悪用が確認され、攻撃者が広く使用されているビジネス プラットフォームに侵入してランサムウェアを展開しようと目論んでいることが読み取れます。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

Cactus ランサムウェア キャンペーンは、新しく発見された脆弱性を悪用して Qlik Sense 環境を狙っていたことからも、攻撃者がセキュリティ状況に適応し、新たな脆弱性を悪用するアジリティに優れていることがわかります。2023 年第 4 四半期は、ランサムウェア グループが活発な四半期でした。

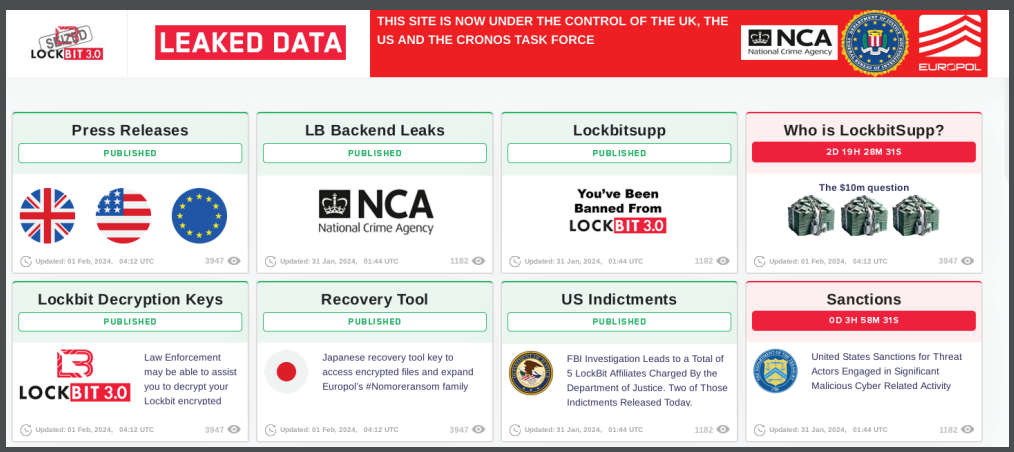
しかし、2024 年第 1 四半期には、法執行機関による重要な措置によって状況が一変しつつありました。

Operation Cronos: LockBit を阻止する法執行機関活動

2024 年 2 月 19 日より、国際的な法執行機関活動、Operation Cronos が実施されました。悪名高い LockBit グループを労せずして阻止し、長く君臨していた犯罪グループに苦汁をなめさせました。法執行機関は、よく知られている削除通知を提示しただけでなく、最終的には、犯罪グループのリーク サイトを手中に収め、このグループを世に知らしめながら、グループ自体の情報を公表しました。いくつもの起訴が行われ、アクティブなアフィリエイトが LockBit バックエンドにログインすると丁寧なウェルカム メッセージが表示されて、その身元が露見したことがはっきり示されました。

この措置は、LockBit の攻撃活動を阻止するためだけでなく、その評判に傷をつけ、グループ内部での信頼関係を崩すことを目的としていました。

このレポートが最終稿になる頃には、Operation Cronos で新たな展開が見られました。国際的な法執行機関は第 2 ラウンドを開始し、LockBit の首謀者の正体を明かしました。法執行機関の勝利はこれだけではありません。5 月 1 日に、Kaseya などの多くの組織を攻撃した REvil アフィリエイトは、懲役 13 年、1,600 万米ドルの被害に対する返済を言い渡されました。Trellix Advanced Research Center がサポートした REvil の事件について詳しくは、こちらでご確認ください。



目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

昨年、Trellix の 2 月 レポートは LockBit を、身代金を要求する最も攻撃的なグループとして認識しました。このサイバー犯罪者グループは、2018 年とかなり前に発見された脆弱性の悪用など、さまざまな手法を用いて、キャンペーンを実行しています。2023 年中も、LockBit は変わらず最も目立っているランサムウェア グループでした。多くの被害者が、グループの運営する名前公表サイトでさらされていました。主に、北米と欧州のさまざまな業界の組織を標的にし、中でも最も影響を受けた業界は、産業財・サービスでした。2023 年、LockBit は進化を続け、新たなツールや方法をランサムウェア プログラムに導入していました。Conti ランサムウェアの流出したコードをベースに開発された LockBit Green 暗号化プログラムや、macOS を標的にした LockBit 亜種が登場しました。さらに、LockBit RaaS が 2023 年、オペレーション不能となった ALPHV や NoEscape といった RaaS プログラムのアフィリエイト向けに新たな拠点を用意したことが確認されました。

阻止活動の余波で、Trellix では、LockBit が必死に面目を保ち、詐欺活動を再開しようとしていることを確認しました。これは、LockBit の犯罪活動の知名度を思えば、当然なことのように思えますが、サイバー犯罪者のアンダーグラウンドの世界では、サーバーは長年の信頼よりも簡単に取り戻せます。法執行機関が LockBit の攻撃活動や正体、LockBit のアフィリエイトについてどれだけの情報を得ているかはいまだわかりません。

> **この不確かさにより、LockBit とその (かつての) チームとの協力関係を望むサイバー犯罪者にとって大きなリスクが生まれています。**

法執行機関による措置が講じられた後、犯罪者どうしの食うか食われるかの世界となったことは非常に明白です。Trellix Advanced Research Center は、流出した LockBit Black バージョンを使用してこの有名なブランドになりすまし、詐欺をはたらいていた攻撃者を確認しました。

なりすましかそうでないかにかかわらず、こうしたグループが被害をもたらしたことは事実で、この 2 つの四半期で確認されたこれらの出来事は、映画になるくらいのものです。

ランサムウェアの総合的考察

Trellix は、2024 年第 1 四半期のランサムウェア活動に関する調査で、リーク サイト、テレメトリ、公開レポートといった複数のソースを調査しました。以下は、各カテゴリに関する簡単な説明です。

- **リーク サイト :** このようなサイトは、恐喝されたものの、身代金要求に応じなかった被害者を暴露するものとして設計されました。犯罪者グループの活動内容も確認することができます。ただし、リーク サイトは必ずしも状況を正確に表しているわけではないことにも注意が必要です。そもそも犯罪者によって運営されているわけですから、すべての内容が信用に足るものであり、正確であるとは限りません。さらに、たとえ、本当であったとしても、身代金を支払った組織は公開されないことから、全体像を把握するには十分ではありません。本レポートで使用されているデータは、複数のリーク サイトからの動向を総合的にまとめたものなので、効果的に全体像を把握できます。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

サイバー分野に影響する地政学的事象

ハイライト概要

方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

国家と APT (Advanced Persistent Threat)

活発な国家と APT グループ

APT グループと拠点国

標的とされる国と地域

悪意のあるツール

悪意のないツール

まとめ

Volt Typhoon: 中国が関与する国家支援型 APT 脅威

概要

攻撃活動のタイムライン

戦術、手法、手順 (TTP)

進化するランサムウェア状況

オペレーション クロノス : LockBit を阻止する法執行機関活動

ランサムウェアの総合的考察

EDR キラーの登場と回避ツール

Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン

確認される EDR キラーの増加

メールは依然として攻撃者が盛んに用いる手段

選挙資金寄付詐欺

税金関連のフィッシング

生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見

ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト

インフォスティーラーに導入される生成 AI

「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

用途 : 本レポートの情報の使用方法

本レポートで分析を理解する方法

リソース

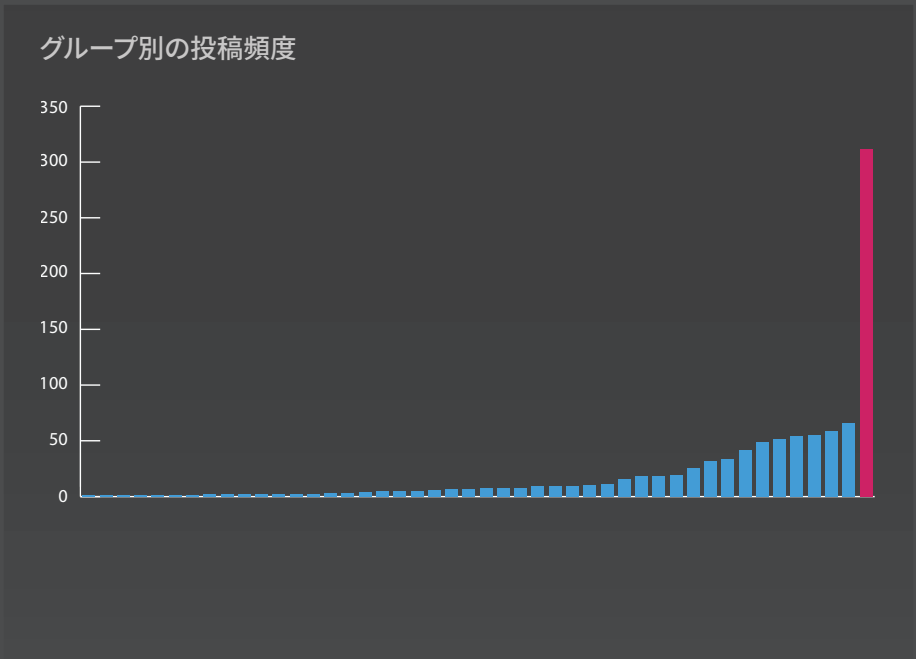
Trellix Advanced Research Center について

Trellix について

- **テレメトリ**：テレメトリは、Trellix のセンサー エコシステムから提供され、検出結果は、ファイル、URL、IP アドレス、その他の指標を弊社のいずれかの製品が検出し、弊社に報告したときに表示されます。検出が必ずしも感染を意味するのではなく、特定のファイルの検出をテストして、組織内のルールを調整することができ、またこれは集約ロギングで確認できます。そのため、トレンドが示しているように、全体像を把握したいときはこのようなデータが役立ちます。
- **公開レポート**：Advanced Research Center は、ベンダーや個人によるレポートを確認し、特徴を分析して動向を導き出します。どのレポートにもバイアスはつきもので、たとえば、ある地域ではあるベンダーが他のベンダーよりも存在感が強いなどといったこともあります。このような違いにより、報告内容がレポートによって異なる状況が生まれる可能性があります。Trellix では、参照したレポートのバイアスはさまざまであることをふまえ、特定のフィルターを適用していません。

活発なランサムウェア グループ

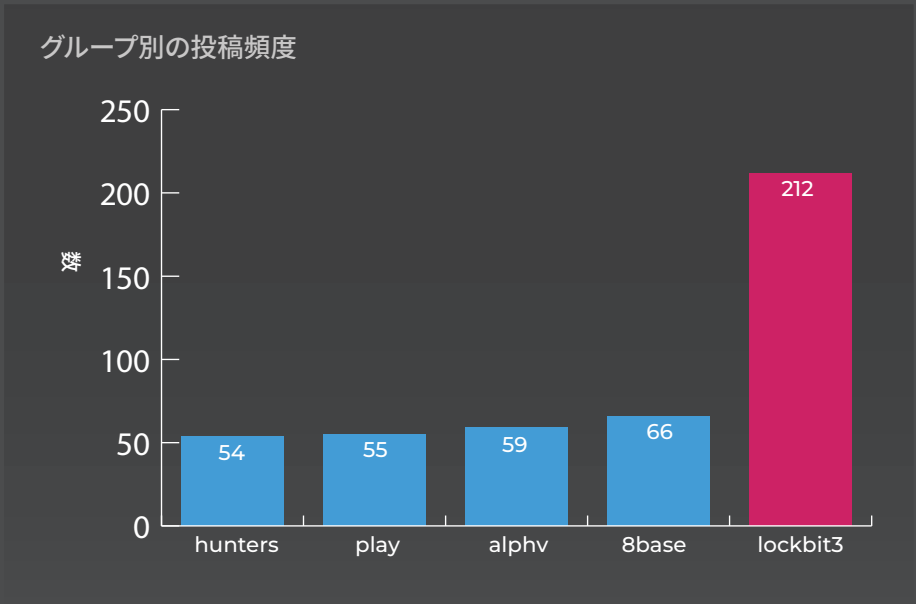
2024 年第 1 四半期から集約されたリーク サイトの投稿を見てみると、多くの投稿で活動の兆候が見られます。時には、リーク サイトは一般的なお知らせを投稿していることが確認されたものの、多数は、恐喝の「証明」または被害者のデータの流出です。また、多くの場合、1 つの被害組織を何度も投稿しており、データで同じ被害組織が複数回カウントされるような、インフレを招いています。



目次

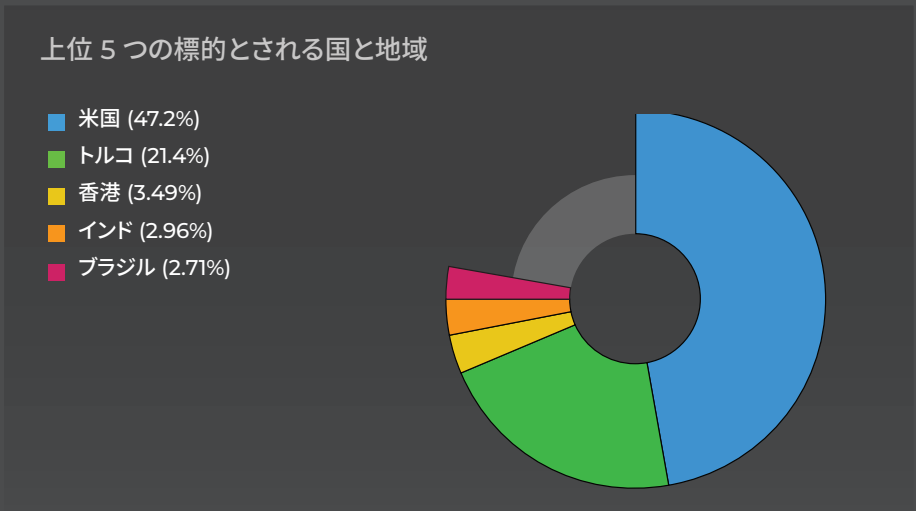
序文
まえがき
はじめに：サイバー脅威レポート：2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論：データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス：LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い：サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途：本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

最も活発な 5 つのランサムウェア グループのリーク サイトの頻度を見ると、LockBit の投稿頻度がグラフで飛びぬけています。LockBit を除いたグループは、1 四半期あたり平均 50 件超を投稿しており、これは 2 日と空けずに 1 つの被害組織を投稿していることになります。前述のとおり、この数字は、身代金要求に応じなかった被害者の数を表しているため、実際の数を知る方法はないものの、さらに多いことが予想されます。



標的とされる国と地域

ランサムウェア グループによる活動は絶え間なく続いていることから、Trellix のテレメトリではランサムウェアの検出状況が確認できます。検出数が最も多いのは米国で、トルコ、香港、インド、ブラジルがこれに続きます。



目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

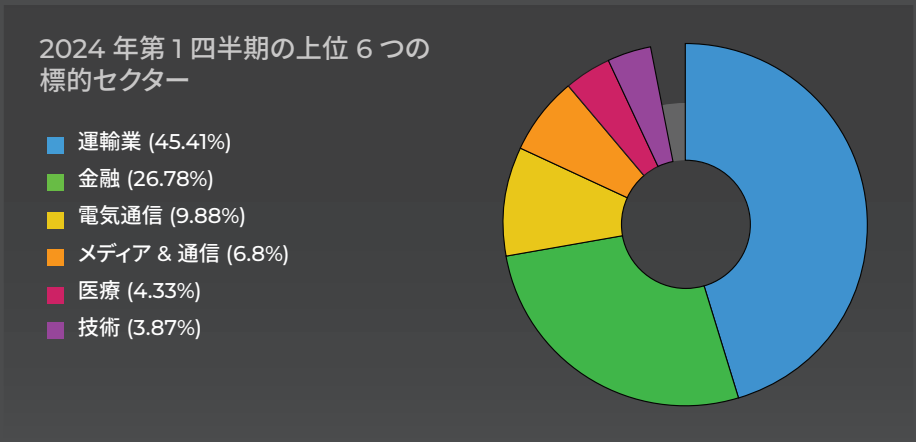
- Trellix Advanced Research Center について
- Trellix について

ランサムウェアがほぼあらゆる地域のすべてのセクターにとって脅威であることを考慮すると、顧客の数と照らした検出メトリックスが有効です。

前四半期のテレメトリも、インドと中国における検出数の増加を除いて、同様の結果が見られました。これらの国に対し特別なキャンペーンがあった形跡はありませんが、マルウェアのテストが行われ、これによって検出数も増加した可能性があると思われます。

標的のセクター

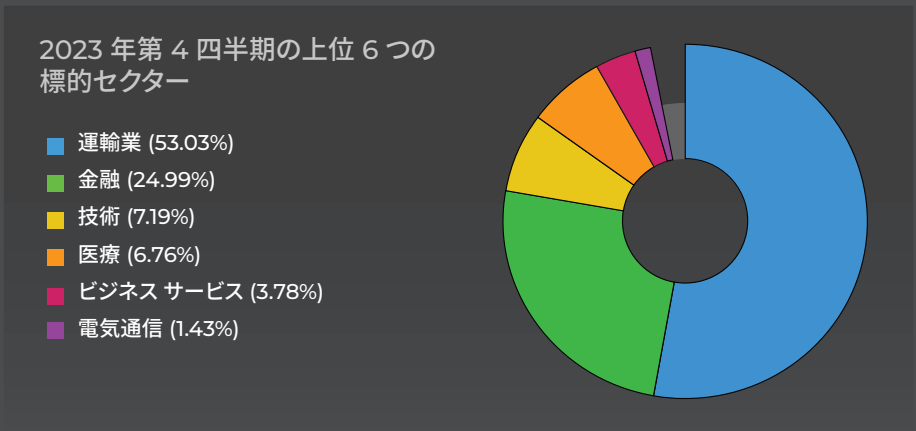
グローバル テレメトリのセクターごとの集計によると、検出数の半数が運輸業で確認されており、金融サービスが 4 分の 1 超を占めています。これら 2 つのセクターが総検出数の 72% 以上を占めており、それはもっともなことです。サービスの可用性が最も重要だからです。運送会社がランサムウェア攻撃により荷物を運べなければ、業務を続けることはできず、経済的に大きな負担がかかります。同様に、金融業界は信用で成り立っており、ランサムウェア攻撃によって機密データが流出したり、業務が停止したたりすれば、致命的な痛手となります。



2023 年第 4 四半期では、上位の標的セクターはわずかに変動したものの、上位 2 つのセクターは変わっていません。むしろこれら 2 つのセクターが占める割合は合わせて 78% と、より拡大しています。技術と医療のセクターは、2024 年第 1 四半期に前四半期と比べて減少したものの、この変動が何か特別な理由によるものかどうかはわかっていません。

目次

序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について



ツールと手法

取り上げた 3 つのソースのうち、最後は公開レポートです。収集したレポートに基づいて、MITRE 手法、関連ツール、コマンドラインを抽出できます。

> **CISO へのヒント**：これらは、検出の観点から、組織のブルー チームが使用できるものです。最も使用されている手法やツールに焦点を当て、最も効果的なものから始めながら、さまざまな攻撃者によるさまざまな攻撃を緩和することができます。また、これらの手法に焦点を当てた、レッド チームとパープル チームによる演習を行い、用いられるさまざまな検出方法をテストすることができます。

以下の表は、手法を頻度の高い順に並べたものです。

MITRE ATT&CK 手法	キャンペーンの種類の数
影響を与えるためのデータ暗号化	31
ファイル / ディレクトリ検出	23
PowerShell	23
イングレス ツール転送	21
システム情報検出	21
難読化されたファイル / 情報	19
レジストリの変更	18
Windows Command Shell	17
ファイル / 情報の難読化解除 / デコード	16
サービス停止	16

ランサムウェアの目的を考慮すると、データの暗号化やファイル / ディレクトリ検出の手法が上位にランクインするのは十分に理解できます。これらの手法を、2023 年第 4 四半期で広く用いられていた手法と比較すると、順位に若干の違いはあるものの、ほとんどの上位の手法は類似しています。

目次

序文
まえがき
はじめに：サイバー脅威レポート：2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論：データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス：LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い：サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途：本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

MITRE ATT&CK 手法	キャンペーンの種類の数
影響を与えるためのデータ暗号化	45
PowerShell	29
難読化されたファイル / 情報	25
ファイル / ディレクトリ検出	24
Windows Command Shell	24
システム リカバリの阻害	23
公開アプリケーション エクスプロイト	21
イングレス ツール転送	21
プロセス検出	21
サービス停止	21

APT に関する前述のセクションと同様に、攻撃者は依然として、正規のツールを犯罪に利用し続けています。使用されるツールは確認された手法に影響しています。ツールとは目的を達成するための手段ですが、ここでは、1 つの手法です。たとえば、PowerShell と Windows Command Shell は、多くの場合システムで追加コマンドを実行するために使用されるものです。中でもシャドーコピーの削除は、「システム リカバリの阻害」手法を実行する上で重要な役割を担います。そのため、以下の表が示すように、これらは重宝されているツールです。

CLI ツールの名前 (attr)	キャンペーンの種類の数
Cmd	7
PowerShell	6
VSSAdmin	5
wevtutil	4
curl	4
Rundll32	4
reg	4
Schtasks.exe	3
BCDEdit	3
wget	2

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

VSSAdmin、BCDEdit、wevtutil が使用されていることから、ランサムウェアが、被害者のシステムが侵害される前の通常の状態に戻せないようにしていることがわかります。レジストリの変更のために reg が使用されていますが、これはさまざまな理由があります。マルウェアは多くの場合、滞留するためにレジストリを使用しますが、ランサムウェアは、暗号化ができてしまえば目的達成なので滞留にこだわっていません。代わりに、他の設定を変更し、通常では不可能であるような操作を行えるようにします。Rundll32 は多くの場合、動的リンクライブラリのロードや実行に使用されますが、プロセス インジェクションの目的でも頻繁に使用されます。

2023 年第 4 四半期と同様、PowerShell とコマンド プロンプトは、同じ理由でリスト上位にランクインしています。VSSAdmin と BCDEdit もランクインしていますが、Windows Event Log Utility (wevtutil) はありません。取り上げたツールについて、両四半期に最も頻度の高いものでも 13 件であり、全体的に発生件数は多くないことをふまえると、すべてのキャンペーンが同じツールを使用しているわけではないことが簡単に読み取れます。偏差が小さい場合、このようなツールは除外されている可能性があります。

CLI ツールの名前 (attr)	キャンペーンの種類の数
PowerShell	13
Cmd	9
WMIC	6
Net	6
echo	5
VSSAdmin	4
msiexec	3
Schtasks.exe	3
Rundll32	3
BCDEdit	3

ランサムウェアの脅威は今もなお続きます。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

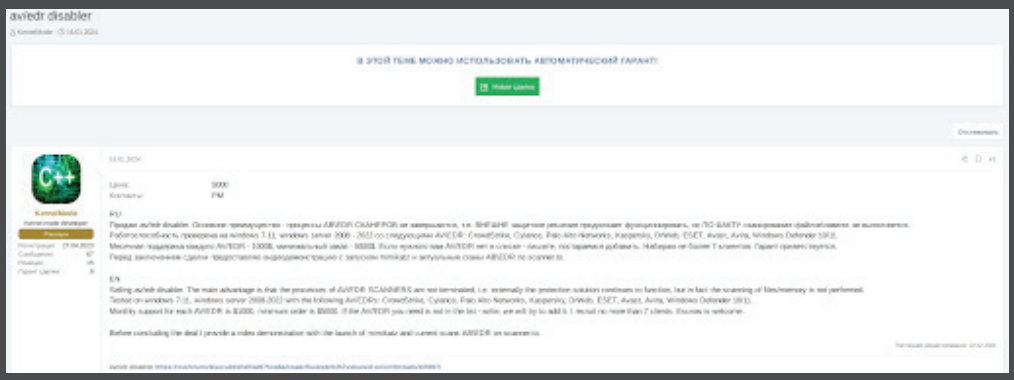
リソース

- Trellix Advanced Research Center について
- Trellix について

EDR キラーの登場と回避ツール

世界的に多くの組織が EDR ソリューションを導入していることから、より巧妙な攻撃を効果的に検出して理解し、これに対応できる能力が実証されていることがわかります。昨今の攻撃者は、多くの場合、「Living off the Land (環境寄生)」バイナリ (LOLBin) やより複雑な攻撃方法を活用していますが、EDR 技術のおかげで、攻撃者が検出されずに済むことは少なくなってきています。

とはいえセキュリティは、相変わらずいたちごっこのようなもので、攻撃者は、EDR ソリューションを回避または無効化する方法を模索しています。このような動きから、EDR キラーや回避ツール / 手法の大きな波が生まれ、中にはサイバー犯罪者のアンダーグラウンドのフォーラムで入手可能なものもあります。Trellix では、たとえば、早期に D0nut ランサムウェア グループが自身の EDR キラーにより台頭してきたことを確認しました。



アンダーグラウンドのフォーラム、XSS に投稿された EDR 無効化ツールに関する宣伝

Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン

脆弱性のあるドライバーを悪用して特権が必要なコードを実行するといった手法は、BYOVD (Bring Your Own Vulnerable Driver) 攻撃と呼ばれ、広く用いられています。

この方法の例として、Spyboy と呼ばれる攻撃者が提供する、EDR「Terminator」ツールがあります。Terminator ツールは、Zemana マルウェア対策ツールに含まれる、正規であるものの脆弱性のある Windows ドライバーを利用し、おそらく CVE-2021-31728 を悪用しながら、Windows カーネル内で任意コードを実行します。Terminator は 2023 年中頃にオンライン上に登場し、Trellix は、このツールの活動領域に関する詳細なナレッジ ベース記事を発表しました (詳しくはこちら)。

2024 年 1 月 11 日～ 17 日の間、Trellix Advanced Research Center では、Trellix のテレメトリで通常とは異なる数の Spyboy の Terminator を発見しました。新しいキャンペーンです。この Terminator キャンペーンは、この 6 日間で 3 日にわたり急増し、1 つの政府機関、1 つの公益事業会社、1 つの衛星通信会社で複数回検出されました。Trellix は、これらの特定の標的をふまえ、攻撃がロシアとウクライナの戦争に関連したものであるとの推測にかなりの確信をもっています。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

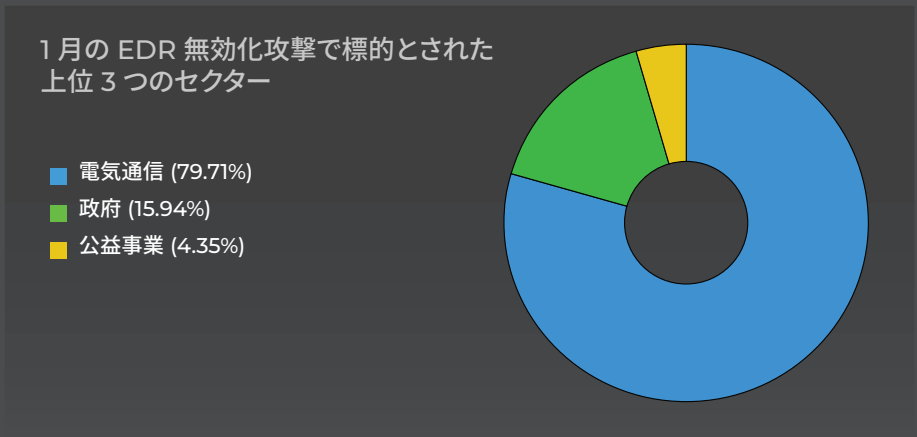
最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

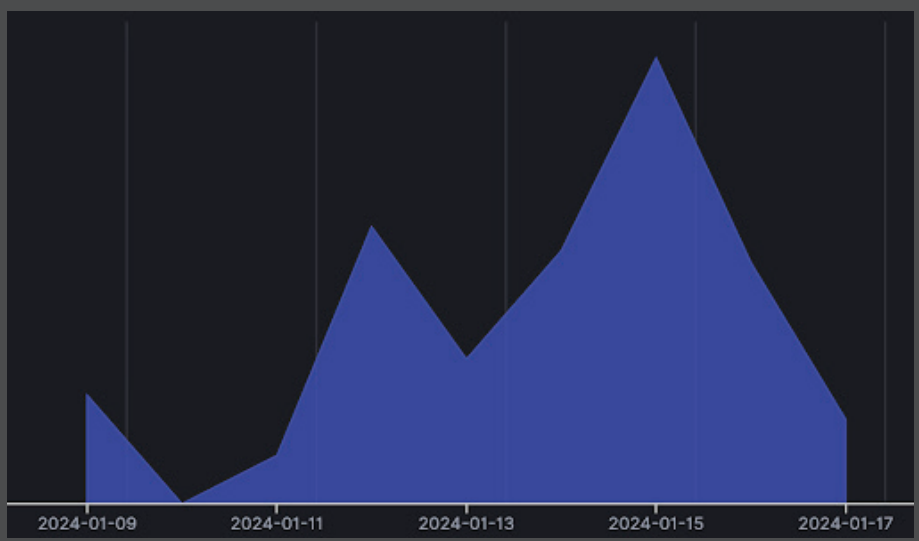




Trellix ATLAS で検出された、ウクライナを標的にした 1 月の EDR Terminator キャンペーン

確認される EDR キラーの増加

2023 年初頭、同様の目的をもったツール、AuKill が Sophos によって明らかにされました。これもまた、付属の脆弱性のあるドライバーを使用していました (BYOVD)。EDR Terminator と AuKill のケースで使用されていたドライバーは異なりますが、どちらも無害なドライバーです。反対に、2022 年のあるキャンペーンでは、類似のツールが、インストールされた悪意のあるカスタム ドライバーを使用していたことが確認されました。



目次

序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

無害なドライバーをこのような目的で悪用するため、攻撃の検出が難しく、また、前述の LOLBin の使用と共通するところがあります。バイナリとドライバーは技術的に異なるものですが、全く同じとは言わずとも意図と動機は似ています。無害なドライバーを用いたものとしては、2022 年の HermeticWiper もあります。このケースでは、ウイルス対策の無効化ではなく、マシンを消去するためにドライバーが使用されました。前述の EDR Terminator と使い方は似通っている部分がありますが、HermeticWiper の特徴は、ロシアのプロの攻撃者が使用していることです。

また、Trellix は、Discord のコンテンツ デリバリ ネットワークが、マルウェア配布のためにラテンアメリカの顧客の一社で使用されているケースを確認しました。Trellix のチームは、マルウェア攻撃で Discord が依然として使用されていることを確認しています。

> **CISO へのヒント**：EDR の密接な監視は、どの SoC にとっても不可欠です。もし EDR ツールが無効化されれば、直ちに SoC に通知され、適切な措置を講じることができるように、アラートやロギングを設定しておく必要があります。EDR ツールが停止した場合、改ざんが疑われます。攻撃者によるネットワークへのアクセスを制限するために、速やかに行動することが大切です。また、ネットワークの検出と対応 (NDR) プラットフォームなどの他のツールが潜在的なインシデントを検出できるよう、多層防御戦略を採用することも極めて重要です。そして、攻撃者によるネットワークへのアクセスを制限するために、速やかに行動することが大切です。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

メールは依然として攻撃者が盛んに用いる手段

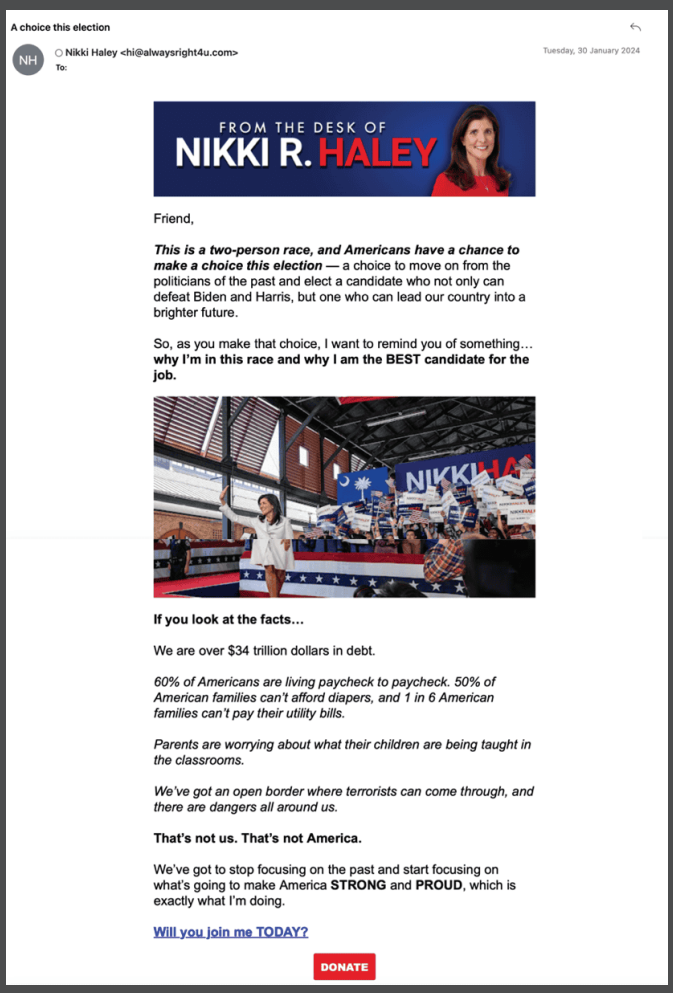
Trellix では、1 日あたり 20 億件のメール サンプルと、9,300 万のメール添付ファイルを処理しています。これにより、膨大なデータが生まれ、攻撃者がメール経由で被害者を狙うために用いる新たな手法を観察する機会も増えています。

選挙資金寄付詐欺

選挙資金の寄付に関するフィッシング詐欺は、個人の善意につけこみ、候補者の支援を悪用するものです。愛国心や候補者の知名度を利用します。2024 年第 1 四半期、Trellix の研究者は、サイバー犯罪者が正規のマーケティング サービスを悪用し、魅力的な寄付募集ページを作成していたことを確認しました。米国の旗と共に候補者の画像を掲げ、サイト訪問者に寄付を募るものでした。

この詐欺は、本物のマーケティング サービスの URL を使用して訪問者を騙し、メールが正規のものであると信じ込ませようとするものでした。しかし、送信されたメールは、人の寛大さにつけこんだものでした。メールに記載されたリンクをクリックすると、寄付ページが表示され、口座情報を入力するか、相手方の口座またはウォレット アドレスに寄付するよう要求されます。

メールの調査にあたった Trellix の研究者は、選挙資金の寄付を募った、以下の悪意のあるメールを確認しました。



A choice this election

NH ○ Nikki Haley <hi@alwaysright4u.com>
To:

Tuesday, 30 January 2024

FROM THE DESK OF
NIKKI R. HALEY

Friend,

This is a two-person race, and Americans have a chance to make a choice this election — a choice to move on from the politicians of the past and elect a candidate who not only can defeat Biden and Harris, but one who can lead our country into a brighter future.

So, as you make that choice, I want to remind you of something… **why I'm in this race and why I am the BEST candidate for the job.**

If you look at the facts…

We are over $34 trillion dollars in debt.

60% of Americans are living paycheck to paycheck. 50% of American families can't afford diapers, and 1 in 6 American families can't pay their utility bills.

Parents are worrying about what their children are being taught in the classrooms.

We've got an open border where terrorists can come through, and there are dangers all around us.

That's not us. That's not America.

We've got to stop focusing on the past and start focusing on what's going to make America **STRONG** and **PROUD**, which is exactly what I'm doing.

Will you join me TODAY?

DONATE

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について





税金関連のフィッシング

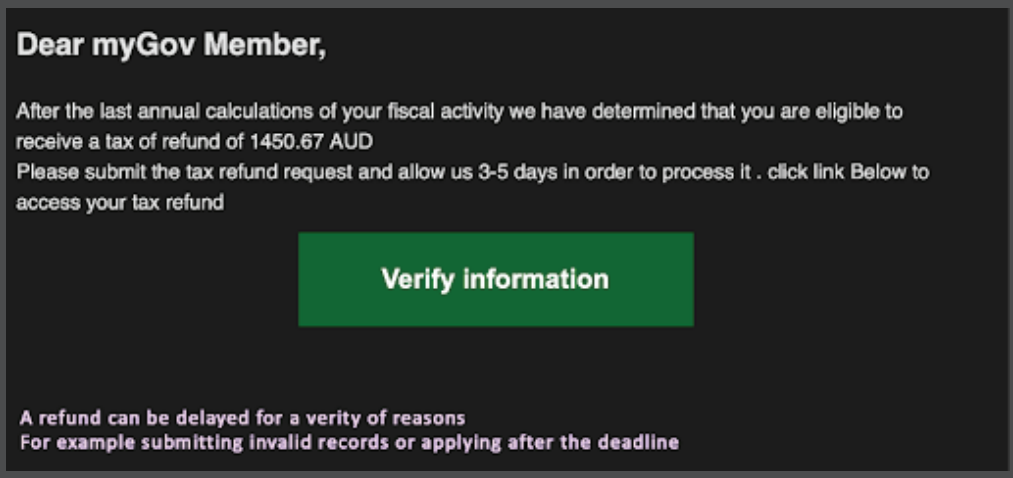
税金に関連したフィッシング攻撃は、特に懸念すべき問題です。詐欺師は政府機関、税務当局、定評ある税務署類作成サービスになりすまし、個人情報を提供させようと個人を騙します。詐欺師は、未払いの税金や申告漏れがある、または還付金の対象であるなどと伝えます。ここでの最終目標は、社会保障番号や銀行口座情報などの貴重なデータを手に入れることです。メールに記載されたリンク先は、政府機関または税務当局の Web サイトを装いながらも、実際はデータを盗むために設計された詐欺サイトへと誘導するものです。

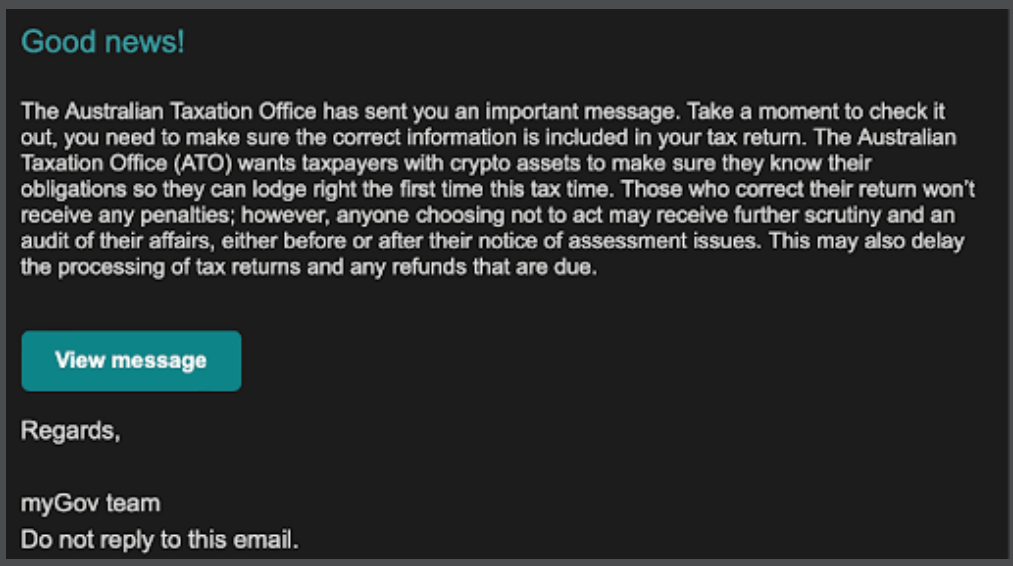
Trellix はまた、2024 年第 1 四半期に、オーストラリアの税務当局からのものであると装ったメールの急激な増加も確認しました。これらは正常に検出されました。

目次

序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

以下は、このキャンペーンのサンプルです。還付金を受け取るためにリンクをクリックさせようと、攻撃者が緊急性をもたせていることがはっきりとわかります。





生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見

AI と機械学習は、もはや資金豊富な組織だけが利用できるものではありません。ChatGPT などは、誰でも使用できるものです。犯罪者もです。そのため、良識ある人と攻撃者の間で AI を取り巻くせめぎ合いが生まれています。AI はパワフルで、ビジネス目標を推進するために確実に活用できるものといえますが、組織は、攻撃者にこのメリットを利用させてはいけません。サイバー犯罪者の戦術はより巧妙になり、彼らが用いる武器はより危険なものになっていることから、彼らの一歩先を行くために、新たな方法が発見されれば導入する必要があります。

目次

序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

CISO へのヒント : CISO は、このように進化する状況を乗り切るものと期待されていることから、その役割はさらに重要になっています。サイバー攻撃は増加し、AI への対応の圧力は高まり、責任も重くのしかかる中で、CISO の 90% がますますプレッシャーを感じていることもうなずけます。AI や生成 AI についていくことは不可欠であり、ほとんどの CISO が、組織はより多くのことをこなせるはずだと同意しています。詳しくは、Trellix の最新レポート、「Mind of the CISO: Decoding the GenAI Impact」(CISO の考え方 : 生成 AI の影響を読み解く) でご確認ください。

生成 AI は、その処理能力の速さと入手しやすさから、攻撃者にとって魅力的です。最も重要なのは、専門的な作業もこなせることです。攻撃者は、生成 AI を用いて、ロゴやログイン情報を追加し、どの言語でも完璧な文法でスピア フィッシング メールを作成することができます。優秀なスキルがなくとも、10 倍の速さでエクスプロイトを見つけ、書き出し、テストすることができます。

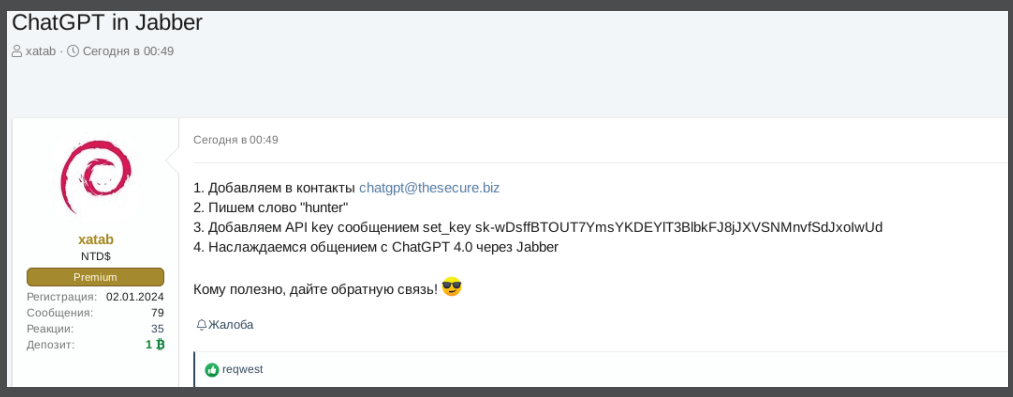
Trellix Advanced Research Center チームは、動向を探るべく、定期的にサイバー犯罪者の地下活動を調査しています。生成 AI は、サイバー犯罪者によってますます弾みをつけています。サイバー犯罪者は自身の成功体験を共有し、所有するツールを販売しています。Trellix では、前回のレポート以降、2024 年初頭より以下を確認しました。

ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト

1 月、Trellix では、アンダーグラウンドのフォーラム、XSS の重要人物である xatab が、API と使用手順と共に、「ChatGPT 4.0 in Jabber」を作成できる開発者を探していることを発見しました。

LLM 統合の導入にも積極的で、「ChatGPT in Jabber」プロジェクトの背景にある xatab の意図や動機は、攻撃者のやり取りを傍受して収集する、攻撃者の要求内容を窃取してサイバー犯罪者が興味のあるものや、生成 AI を活用した違法活動の主な目的と範囲に関する情報や知識を得ることであると考えられます。

Trellix では以下を確認しました。



xatab は XSS フォーラムで「ChatGPT in Jabber」の手順と API キーを提供

目次

序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

```
Python
1. Add to your contacts chatgpt@thesecure.biz
2. Write a keyword "hunter"
3. Add API key in the message: set_key <OPENAI_API_KEY>
4. Enjoy the conversation with  ChatGPT 4.0 via Jabber

If useful share your feedback!
```

2024 年 1 月 31 日、**xatab** は、XSS フォーラムで「ChatGPT in Jabber」プロジェクトへの参加報酬として 2,000 ドルを提示しました。**germans** と名乗る人物が要求されたボットを作成したものの、最初は **xatab** により無視されたため、**germans** が最近、XSS で苦情を寄せると、1,500 ドルで Jabber での ChatGPT ボットを開発することに合意したようです。このボットは、Exploit フォーラム (@exploit[.]im) と XSS (@thesecure[.]biz) Jabber サーバー向けに作成され、**xatab** は、Exploit と XSS のダークネット フォーラムにこれを投稿しました。おそらくこのボットをテストし、フォーラム メンバーからのフィードバックを募るためであったと考えられます。このボットは、xmppgpt プロジェクトをベースにしていると思われます。

xatab は、Exploit/XSS フォーラムで何度か投稿し、(特定のサークルではペンテスターを経験したことで知られる) APT チームとして、攻撃活動を成功させるために、米国 / 英国 / カナダ / オーストラリアの組織へのアクセス ブローカーを募集していることを伝えました。アクセスが成功するごとに収益の 20% を分配することを提示し、Exploit と XSS のフォーラムに 1 BTC を預けることで、彼らの意図と真剣さをアピールしました。

無料の ChatGPT 4.0 をサイバー犯罪者コミュニティに提供することにより、**xatab** は 2 つのことを達成しました。

1. 攻撃者が攻撃活動に革新をもたらし、活動に生成 AI を導入できるよう積極的にサポートする、ファシリテーターおよびイネーブラーになること
2. 生成 AI ナレッジ ベース / プールを作成して他のサイバー犯罪者から学んだり、さらには革新的なアイデアやツールを盗んだりすること

Trellix では、指定の手順に従って「ChatGPT in Jabber」プロジェクトをテストしてみましたが、攻撃者の説明どおり機能しているようです。

インフォスティーラーに導入される生成 AI

2024 年 2 月 21 日、Trellix の研究者は、攻撃者である MetaStealer が、MetaStealer の新たな改良バージョンを XSS ファーラムで宣伝していたことを確認しました。MetaStealer は、2021 年に初めて登場し、有名なインフォスティーラー、Redline から派生したバージョンであると考えられています。MetaStealer のいくつかのバージョンが広まっていることが確認されていますが、Trellix が特定した最近のバージョンは、生成 AI ベースの機能を搭載し、さらに検出を回避しています。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

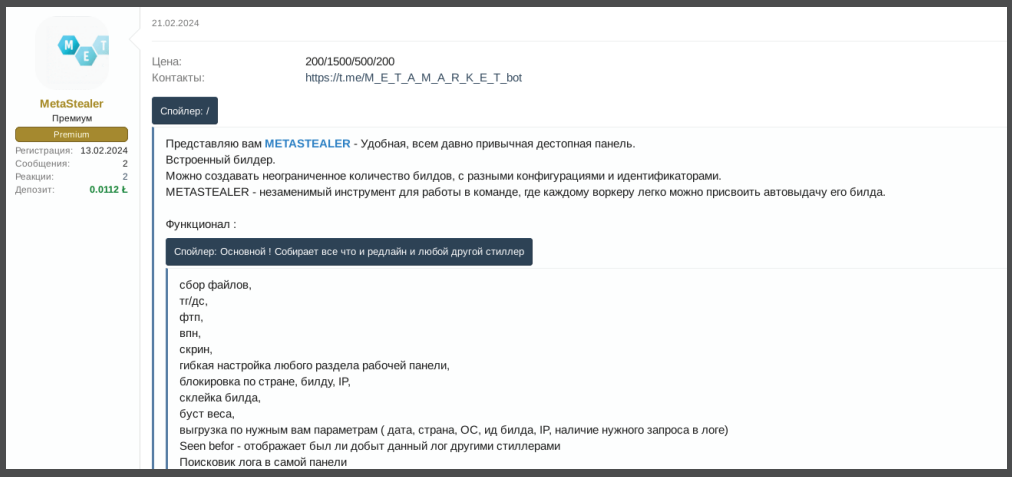
最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

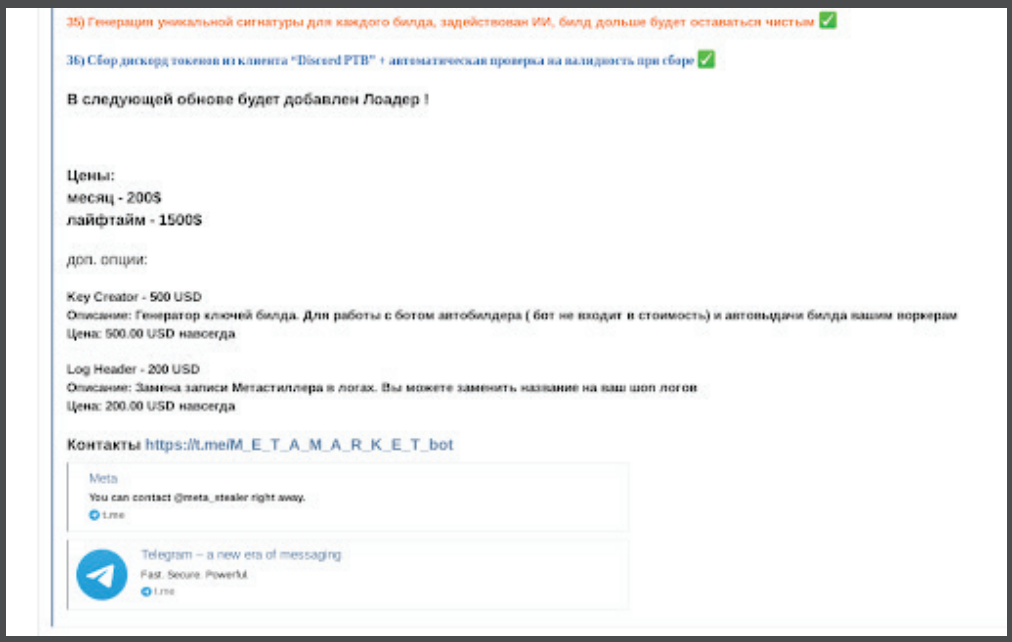
リソース

- Trellix Advanced Research Center について
- Trellix について



MetaStealer は XSS フォーラムで MetaStealer の改良バージョンを提供

以下のスクリーンショットでは、35) のオレンジ色のテキストは、「各ビルドに一意の署名を生成、ここでは AI を使用、ビルドは長期間クリア (検出不可) を維持」を意味し、MetaStealer の開発者は、新たな生成 AI ベースの機能をスティーラーに埋め込み、これにより MetaStealer の一意のビルドを作成して検出を回避したり、かつてないほど長期間にわたり AV/EDR システムによって捕捉されないようにしたりできます。



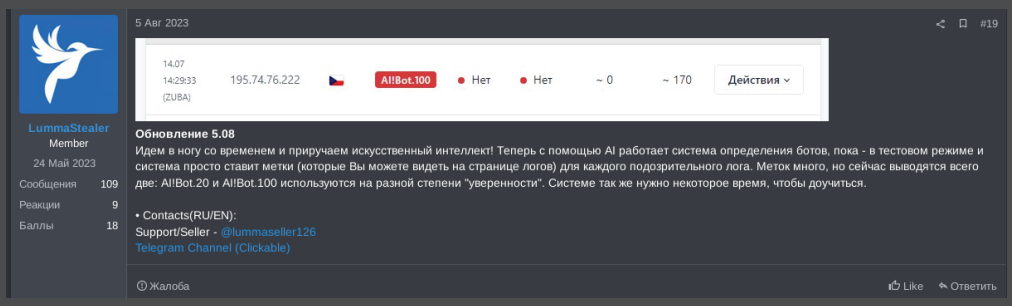
改良バージョンの MetaStealer は生成 AI ベースの機能を搭載して防御を回避

もう一つの例として、LummaStealer と呼ばれる十分に確立されたインフォスティーラーがあります。2023 年 8 月以降、Trellix では、LummaStealer チームが、このインフォスティーラー ユーザーがログ リストからボットを検出できる、AI ベースの機能をテストしていることを確認しました。LummaStealer に埋め込まれたこの AI ベースのシステムは、カスタム ニューラル ネットワークの

目次

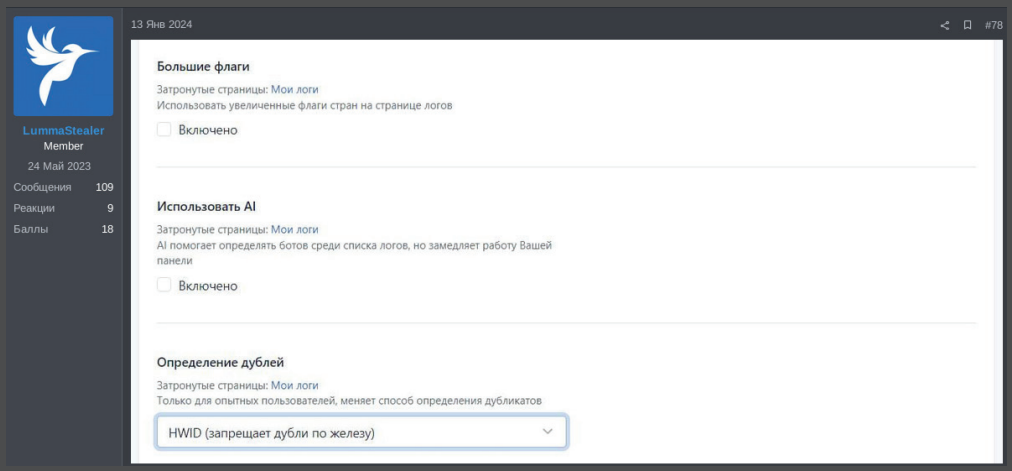
序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

可能性を持ち、不審なユーザー ログがボットであるかどうかを検出するようトレーニングされています。LummaStealer は、ラベル AI!Bot.< 数字 > を使用して、検出されたログをボットとして分類します。< 数字 > は、0 ～ 100 の数字が割り当てられ、検出されたボットを表しています。



インフォスティーラーは AI ベースの機能を搭載してスティーラーのログ リストからボットを検出できることを説明した、RAMP ファーラムでの LummaStealer の投稿

LummaStealer は、ニューラル ネットワークは引き続きトレーニング中で、検出精度を改善するにはいくらか時間がかかることをユーザーに伝えました。さらに 2024 年 1 月、LummaStealer は、LummaStealer パネルの処理速度を低下させることから、生成 AI ベースの機能はデフォルトで無効になっていることを伝えました。



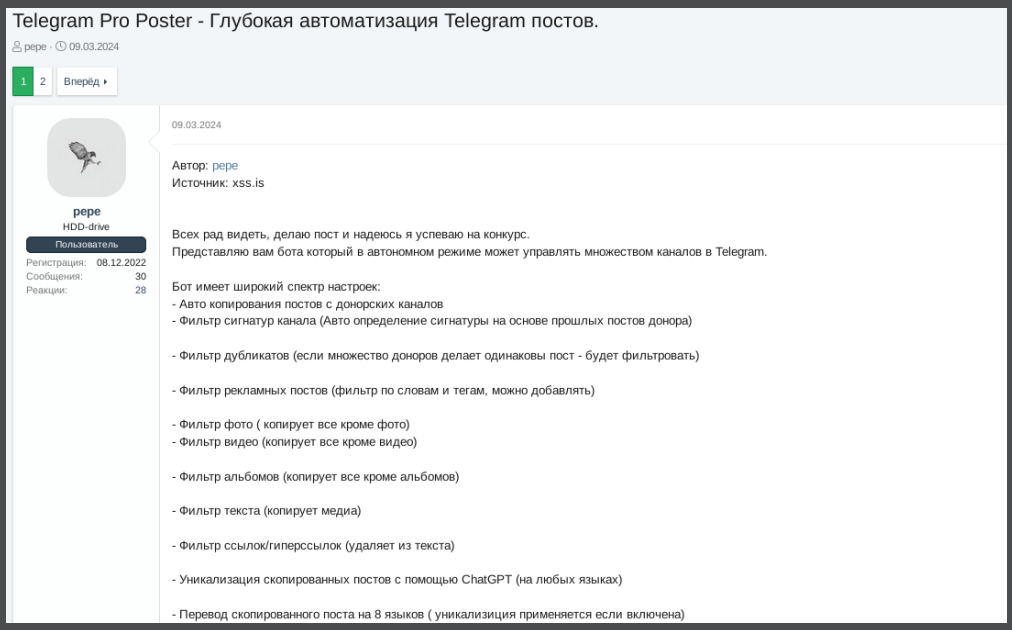
AI ベースのボット検出はデフォルトで無効になっていることを説明した、RAMP ファーラムでの LummaStealer の投稿

「Telegram Pro Poster」ボット プロジェクト

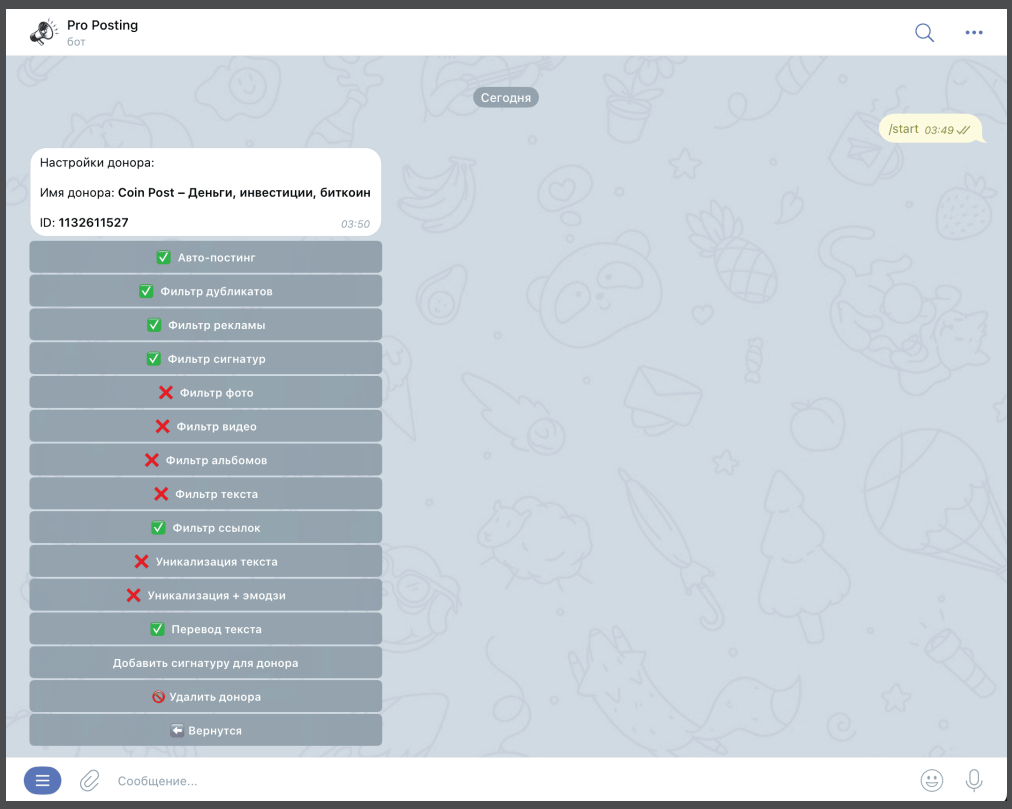
2024 年 3 月上旬、Trellix では、攻撃者の pepe が、悪意のあるツール / ソフトウェアのアンダーグラウンドの競争の一環として、「Telegram Pro Poster」プロジェクトを XSS フォーラムに投稿したことを確認しました。Telegram Pro Poster は、「Telegram 投稿のディープ オートメーション」のボットです。この Python ベースのボットにより、ユーザーは、複数 (無制限) の Telegram チャネルを自律的に管理できます。投稿は、「ドナー」Telegram チャネルから標的のチャネルに自動でコピーされます。投稿フィルタリング機能はいくつもありますが、中でもこのボットは、2 つの生成 AI 搭載機能を使用して Telegram のメッセージを翻訳したり、ChatGPT を使用して特定の投稿を書き換えたりすることができます。

目次

序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について



Telegram Pro Poster の生成 AI ベースのボットに関する XSS フォーラムでの投稿



デフォルトでは無効の「unique-alisation」機能など、Telegram Pro Poster のフィルタリング機能

Trellix は、Telegram Pro Poster のソース コードを入手し、コードから以下のテキストを確認しました。ドナー チャネルからコピーされた投稿を、ChatGPT API 経由で 8 つの言語に翻訳するもので、その後標的の Telegram チャネルに送信されます。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

```
Unset
API_ID = 99999999 #APP TELEGRAM ID
API_HASH = "HASH" # APP TELEGRAM HASH
BOT_TOKEN = "API" # BOT API
DATABASE_PATH = 'database.db'
OPEN_AI_KEY = 'API KEY' # OPEN AI KEY


language_codes = {
    'Ukranian': 'украинский',
    'Russian': 'русский',
    'English': 'английский',
    'Indian': 'индийский',
    'Italian': 'итальянский',
    'Brasilian': 'бразильский',
    'Germany': 'немецкий',
    'Indonesian': 'индонезийский'
}
...
def gpt_translate(input_text, language):
    print(f'Перевожу этот текст: {input_text}')
    if len(input_text) > 10:
        openai.api_key = OPEN_AI_KEY
        language = language_codes[language]

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": f"Когда ты получаешь текст то ты
должен перевести его на {language}."},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        return unique_text
    else:
        return input_text
```

2 つ目の機能は「unique-alization」と呼ばれるもので、デフォルトでは無効になっていますが、有効にすると、OPEN_AI_KEY を使用して、指定のテキストを希望の言語に、時には絵文字を加えながら書き換えるものです。

```
Python
def unique_text(input_text, is_emoji_need):
    print(f'Уникализирую этот текст: {input_text}')
    if len(input_text) > 5:
        openai.api_key = OPEN_AI_KEY

        if is_emoji_need:
            content_text = "Перефразируй текст и добавь эмодзи: "
        else:
            content_text = "Перефразируй текст:"

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": content_text},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        token_count = response['usage']['total_tokens']
        return unique_text


    else:
        return input_text
```

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

サイバー犯罪者コミュニティの XSS では、すでに「Telegram Pro Poster プロジェクト」に関するポジティブなフィードバックが共有されており、「興味深いプロジェクトであり、使いこなすことができれば必ず役に立つだろう」といった感想が寄せられています。XSS フォーラムのスレッドでは、このボットがすでにさまざまな Telegram チャネルで実際に使用されていることを指摘する攻撃者もいました。

最後に

レースは始まっています

実用的な脅威インテリジェンスは、特定のサイバー脅威の性質、意図、タイミングに関するインサイトを提供します。攻撃者の戦術、手法、手順 (TTP) に関する情報を含む、戦術的インテリジェンスよりも情報とコンテキストが豊富です。

組織は、こうした実用的なインテリジェンスを用いて、サイバー攻撃の動機や方法など、幅広いコンテキストを理解できるため、セキュリティ チームは特定の種類の攻撃にあらかじめ備えることができます。

私が業務の中で顧客と関わってきた経験上、どの CISO にとっても最重要目的は、組織へのリスクを抑えることです。実用的な脅威インテリジェンスを適用することは、こうしたリスクを抑えるための確実な方法です。そうすれば CISO や SecOps チームは先を見据え、足がかりを得ることができます。また、組織の環境全体でセキュリティ対策に潜むギャップを特定し、敵の情報をつかみ、追い出すことが期待できます。

Trellix は、貴社が今後重要な決定を下す上で役立つ、事実に基づいた堅牢なプラットフォームを提供するために、弊社の脅威インテリジェンスを提供します。Trellix の目的は、貴社がサイバー防御を十分に向上させ、攻撃者を倒せるようサポートすることであり、貴社が目指す次のステージがどのようなものであろうと進めるようにすることです。

始めましょう!



Ashok Banerjee
チーフ テクノロジスト、TRELLIX

目次

序文
まえがき
はじめに : サイバー脅威レポート : 2024 年 6 月
サイバー分野に影響する地政学的事象
ハイライト概要
方法論 : データの収集および分析方法について
レポート分析、インサイト、データ
国家と APT (Advanced Persistent Threat)
活発な国家と APT グループ
APT グループと拠点国
標的とされる国と地域
悪意のあるツール
悪意のないツール
まとめ
Volt Typhoon: 中国が関与する国家支援型 APT 脅威
概要
攻撃活動のタイムライン
戦術、手法、手順 (TTP)
進化するランサムウェア状況
オペレーション クロノス : LockBit を阻止する法執行機関活動
ランサムウェアの総合的考察
EDR キラーの登場と回避ツール
Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
確認される EDR キラーの増加
メールは依然として攻撃者が盛んに用いる手段
選挙資金寄付詐欺
税金関連のフィッシング
生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
インフォスティーラーに導入される生成 AI
「Telegram Pro Poster」ボット プロジェクト
最後に
方法論
用途 : 本レポートの情報の使用方法
本レポートで分析を理解する方法
リソース
Trellix Advanced Research Center について
Trellix について

方法論

データ収集：Trellix と弊社の Advanced Research Center に所属する世界でもトップクラスの専門家は、本レポートを構成する統計、トレンド、インサイトをグローバルな幅広いソースから収集しています。

- **クローズドのソース**：場合によっては、Trellix のセキュリティ ソリューションにより、世界中の公共と民間の両方のネットワークに配備されている顧客のサイバー セキュリティ ネットワークと防御フレームワーク上でテレメトリが生成されます。ネットワークには、技術、インフラストラクチャ、データ サービスを提供するものなどが含まれます。このようなシステムは数百万に上り、10 億個のセンサーからデータを生成しています。
- **オープン ソース**：その他のケースで、Trellix は特許取得済み、プロプライエタリ、オープンソースのツールを組み合わせて、インターネット上のサイト、ログ、データ リポジトリをスクレイピングしており、攻撃者がランサムウェアの被害者に関する情報や被害者の情報を公開する「リーク サイト」のようなダーク ウェブも活用することがあります。

正規化：収集されたデータは、弊社の Insights および ATLAS プラットフォームへ送られます。機械学習、自動化、そして人間の鋭敏な感覚を活用して、チームは集中的、統合的、反復的なプロセスをひととおり実施します。つまり、データを正規化して結果を補強し、個人データを削除して、攻撃手法やエージェント、業種、地域、戦略、結果などに関する相関関係を特定します。

分析：次に Trellix は、(1) 脅威インテリジェンスの広範なナレッジ ベース、(2) 高い評価と認定を受けた情報ソースからのサイバー セキュリティ業界レポート、(3) Trellix のサイバー セキュリティ アナリストや調査員、リバース エンジニアリング専門家、フォレンジック研究者、脆弱性専門家の経験と洞察力を参考にして、この膨大な情報を分析します。

解釈：最後に、Trellix チームは、サイバー セキュリティ リーダーと SecOps チームが (1) サイバー脅威の環境における最新のトレンドを把握し、(2) この視点に立って将来的なサイバー攻撃を予測、防止、防御する機能を向上させる上で役に立つ有意義なインサイトを抽出し、確認して検証します。

用途：本レポートの情報の使用方法

業界をリードする評価チームとプロセスには、バイアスの影響を把握して認識し、可能であれば緩和することが欠かせません。バイアスとは、事実とその意味を受け入れるか、拒否するか、操作するかを左右する傾向のことであり、自然な場合も、仕組まれた場合も、目に見えない場合もあります。コンテンツの消費者についても同じことが当てはまります。

高度に構造化された制御ベースの数学のテストや実験とは違い、本レポートは本質的に便宜的なサンプルです。つまり医療やヘルスケア、心理学、社会学のテストでよく用いられるもので、入手とアクセスが可能なデータを利用した非確率的なタイプの調査ということです。

目次

序文

まえがき

はじめに：サイバー脅威レポート：2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論：データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス：LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い：サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途：本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

- つまり、本レポートの調査結果は、私たちが観察できたことに基づいており、検出、報告、データ収集を回避した脅威、攻撃、戦術のエビデンスは含まれていません。
- 「完全な」情報や「完璧な」可視性がない以上、これは本レポートの目的に最も適したタイプの調査です。本レポートの目的は、サイバー セキュリティの脅威に関する重要なデータについて既知の情報ソースを明らかにし、このデータの合理的、専門的、倫理的な解釈を展開して、サイバー防衛のベストプラクティスにつながる情報を届けることです。

本レポートで分析を理解する方法

本レポートでインサイトとデータを理解するために、以下のガイドラインを簡単にご確認ください。

- **時間上のスナップショット**：インターネットに接続されているシステムすべてのログにアクセスできるわけではありませんし、あらゆるセキュリティ インシデントが報告されているわけでもありません。被害者のすべてが侵害を受けてリーク サイトに掲載されることもありません。しかし、追跡できるものを追跡することで、各種の脅威について理解を深めることができ、分析と調査の盲点も減らすことができます。
- **誤検知と非検知**：データを収集するための Trellix の特別な追跡システムとテレメトリ システムの高性能な技術的特性の一部として、誤検知および非検知の結果を緩和・除去するメカニズム、フィルター、戦術があります。これにより、分析レベルと調査結果の質を向上させることができます。
- **感染ではなく検出**：テレメトリを話題にするとき、感染ではなく、検出がその焦点になります。検出は、ファイル、URL、IP アドレス、その他の指標を弊社のいずれかの製品が検出し、弊社に報告したときに記録されます。
- **データのキャプチャは不均等**：なかには、慎重な解釈が必要なデータ セットもあります。たとえば、通信データには、他の多くの産業やセクターで運営されている ISP クライアントからのテレメトリが含まれています。
- **国家の関与**：同様に、国家が関与するハッカーやサイバー犯罪者が互いになりすましたり、悪意のある活動を信頼できるソースからのものとして偽装したりする一般的な現状をふまえると、さまざまなサイバー攻撃や脅威に関する国家の責任を判断するのも、極めて難しい場合があります。

目次

序文

まえがき

はじめに：サイバー脅威レポート：2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論：データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス：LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い：サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途：本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

リソース

脅威レポートのアーカイブ

The Mind of the CISO (CISO の考え方)

TRELLIX ARC を X でフォロー

Trellix ARC

脅威レポートのアーカイブを見る

Trellix Advanced Research Center

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

- Trellix Advanced Research Center について
- Trellix について

TRELLIX ADVANCED RESEARCH CENTER について

Trellix Advanced Research Center は、サイバー脅威を取り巻く環境全体の中で、サイバー攻撃者が用いる新たな手法、トレンド、ツールに関する調査の最前線に立っています。この優秀な研究者チームは、全世界の CISO、シニア セキュリティ リーダー、セキュリティ オペレーション チームにとって不可欠なパートナーとして活動しています。Trellix Advanced Research Center は、最先端のコンテンツを通じて実用および戦略に関する脅威インテリジェンスをセキュリティ アナリストに提供し、業界有数の AI を活用した XDR プラットフォームをサポートし、世界中のお客様にインテリジェンス製品やサービスを提供します。 詳細については、https://www.trellix.com/ja-jp/advanced-research-center.html をご覧ください。

TRELLIX について

Trellix は、サイバー セキュリティの将来と気持ちのこもった業務を再定義するグローバル企業です。 今日の最も高度な脅威に直面している組織は、弊社のオープンでネイティブの eXtended Detection and Response (XDR) プラットフォームを使用することにより、業務の保護と耐久性に自信をもつことができます。 Trellix は、広範なパートナー エコシステムと共に、AI、自動化、分析を通じて技術革新を加速させ、生きたセキュリティによって 40,000 以上の企業や政府機関のお客様を支援しています。 詳細については、https://trellix.com をご覧ください。

この文書とそこに続く情報は、教育上の目的および Trellix 顧客の利便性のみを目的としたコンピューター セキュリティ リサーチについて記述したものです。Trellix は脆弱性の適切な開示に関するポリシー | Trellix に従ってリサーチを進めています。記載されている行為の一部または全部を再現する試みは、ユーザーの責任において行われるものとし、Trellix およびその関連会社はいかなる責任も負わないものとします。

Trellix は、Musarubra US LLC または米国その他の国における関連会社の商標または登録商標です。その他の名前およびブランドは、他社の所有物である場合があります。

目次

序文

まえがき

はじめに : サイバー脅威レポート : 2024 年 6 月

- サイバー分野に影響する地政学的事象
- ハイライト概要
- 方法論 : データの収集および分析方法について

レポート分析、インサイト、データ

- 国家と APT (Advanced Persistent Threat)
  - 活発な国家と APT グループ
  - APT グループと拠点国
  - 標的とされる国と地域
  - 悪意のあるツール
  - 悪意のないツール
  - まとめ
- Volt Typhoon: 中国が関与する国家支援型 APT 脅威
  - 概要
  - 攻撃活動のタイムライン
  - 戦術、手法、手順 (TTP)
- 進化するランサムウェア状況
  - オペレーション クロノス : LockBit を阻止する法執行機関活動
  - ランサムウェアの総合的考察
- EDR キラーの登場と回避ツール
  - Spyboy の EDR Terminator ツールを用いた 1 月のキャンペーン
  - 確認される EDR キラーの増加
- メールは依然として攻撃者が盛んに用いる手段
  - 選挙資金寄付詐欺
  - 税金関連のフィッシング
- 生成 AI のせめぎ合い : サイバー犯罪者の地下活動に関する所見
  - ロシアの APT グループによる使用が疑われる「ChatGPT in Jabber」プロジェクト
  - インフォスティーラーに導入される生成 AI
  - 「Telegram Pro Poster」ボット プロジェクト

最後に

方法論

- 用途 : 本レポートの情報の使用方法
- 本レポートで分析を理解する方法

リソース

Trellix Advanced Research Center について

Trellix について

Copyright © 2024 Musarubra US LLC