Trellix

We bring security to life.

2022年5月31日

※当資料は、米国時間2022年4月27日に米国で発表されたプレスリリースの抄訳です。

Trellix（トレリックス）、2021年第4四半期 脅威レポートを発表
地政学的な緊張の高まりから、重要インフラを標的としたサイバー攻撃が拡大

ウクライナを標的としたワイパー型マルウェアと、ロシアが支援したとみられる
攻撃者によるサイバー脅威の急増が明らかに

ニュースハイライト：

- APT（高度持続的脅威）攻撃の最大の標的となったのは、運輸・海運セクター
- 最も活動が活発だった国家主導グループは、ロシア政府機関を支援していると考えられているAPT29
- REvilランサムウェアの犯罪者グループのメンバーが逮捕された後、2021年第4四半期に最も多く検出されたのはLockbitランサムウェア
- Microsoft Excelなどのネイティブツールを悪用する環境寄生型（Living off the Land、LotL）攻撃が、政府高官や経営幹部を標的とすることに成功
- 最も多く使われた手法はマルウェアで、サイバーインシデント全体の46%
- 最も攻撃対象となったのは個人で、インシデント検出数は73%増加

XDR（eXtended Detection and Response）の未来を提供するサイバーセキュリティ企業、Trellixは、「Threat Labs Report：2022年4月版」を発表しました。本レポートでは、過去6ヶ月間のサイバー犯罪者の行動を調査しました。その結果、個人消費者が最もサイバー犯罪者の標的となったこと、これに続いて医療産業が狙われたことがわかりました。さらに、運輸、海運、製造、情報技術などの業種で脅威が急増しました。

Trellix Threat Labsのリードサイエンティスト兼プリンシパルエンジニアであるクリスチャン・ビーク（Christiaan Beek）は、次のように述べています。「私たちはサイバーセキュリティの重要な岐路に立っており、拡大し続ける攻撃対象領域における敵対的な行動の増加を観察しています。私たちの世界は根本的に変わりました。第4四半期は、サイバー犯罪者がこの2年間のパンデミックを利用して利益を得てきたことからの転換を示しています。Log4Shellの脆弱性が数億台のデバイスに影響を及ぼしたことが判明しており、2022年もサイバーの勢いは衰えず、国際的なサイバー活動が深刻化しています。」

重要インフラへの脅威

2021年第4四半期は、社会機能に不可欠な分野を標的としたサイバー活動が活発化しました。

- 運輸・海運業に対する攻撃は、敵対的でステルス性の高い攻撃者によるAPT（高度持続的脅威）が、攻撃の27%を占める
- 医療は2番目に多く標的とされ、全体の12%を占める
- 2021年第3四半期に対して、製造業への脅威が100%増加、また情報技術業界への脅威が36%増加
- Trellixの顧客では、2021年第4四半期に観察されたすべての検出の62%が運輸業を標的に

Media@Trellix.com

2022年4月、Trellixは、重要インフラ事業者がどのようにサイバー攻撃に備えているかを調査したグローバルなCyber Readiness Report（サイバーレディネスレポート）を発表しました。その結果、誰もが知るところとなった近年の侵害や情報漏洩等の攻撃被害にもかかわらず、多くの重要インフラ事業者が、サイバーセキュリティのベストプラクティスを実施していないことがわかりました。

ウクライナへの脅威

Trellix Threat Labsは、ワイパー型マルウェアなど、ウクライナを標的としたサイバー脅威を調査しました。ワイパー型は、標的とする組織内にあるデバイス操作用の重要なメモリを破壊することで、そのデバイスを使用不能にします。ウクライナ侵攻前および侵攻時に使用されたマルウェアWhispergateとHermeticWiperに関するTrellixの分析では、ウクライナ国内の通信を破壊してITシステムを不安定にするために使われたこの2つの系統の類似点と相違点を詳しく説明しています。

レポートでは、ウクライナを標的とする攻撃主体として、Actinium APT、Gamaredon APT、Nobelium APT（APT29とも呼ばれる）、UAC-0056、Shuckworm APTなどを列挙しています。2021年第4四半期にTrellixが観察したAPT活動のうち、APT29は検出数の30%を占めました。

また、これらの攻撃者が使用する戦術から積極的に自組織の環境を保護することを追求する提言を詳述します。ウクライナを標的としたサイバー活動の背景については、Trellix Threat CenterおよびThreat Labs Blogをご覧ください。

攻撃手法（Tactics, Techniques & Procedures）

Trellixでは、環境寄生型（Living off the Land、LotL）方式が引き続き使用されていることを確認しました。これは、犯罪者が既存のソフトウェアや、デバイス制御を使用して攻撃を実行するものです。2021年第4四半期に最も頻繁に使用されたNativeOSバイナリは、Windows Command Shell（CMD）（53%）とPowerShell（44%）、最も使用された管理ツールはRemote Services（36%）でした。

Trellix Threat Labsの今回の調査結果によると、韓国のAPTグループとみられるDarkHotelが実行したLotL技術は、Excelファイルを使用して高級ホテルへの侵入に成功し、仕事や会議で利用した著名人の情報を収集しました。

2022年に入ってから、政府高官や防衛産業の企業幹部を監視するため、西アジアの首相官邸に対して多段階のスパイ攻撃が行われたことをTrellix Threat Labsも確認しました。このサイバー攻撃の特徴は、MicrosoftのOneDriveをコマンドアンドコントロール（C2）サーバーとして使用し、被害者の環境にアクセスするためにExcelを使用したことです。

このほかにも、ここ数ヶ月でサイバー敵対者の間で流行している手法や技術があります。

- 2021年第4四半期にAPTグループが使用したツールの中で、Cobalt Strikeは第3四半期から95%増でトップ
- 同じく、最も観察された手法は、難読化されたファイルまたは情報で、次いでウェブブラウザからの認証情報、ファイルおよびディレクトリの発見
- 2021年第4四半期に報告されたインシデントでは、マルウェアが最も多く使用され、全体の46%を占めて2021年第3四半期から15%増加

個人に対する脅威

2021年第4四半期で注目すべきは、個人を標的としたサイバーインシデントが73%と大幅に増加し、最大の攻撃対象に位置づけられたことです。これには、ソーシャルメディアやモバイル機器など、人々がデータや認証情報を保存しているサービスを通じて実行された脅威も含まれます。例えば、2021年第4四半期には、Facebookが世界中のユーザーを標的としたスパイウェア攻撃を発見しました。別の犯罪グループはJokerマルウェアを活用して世界中のAndroidユーザーを標的としました。このような攻撃は、一般的に政治的な動機によるもので、人々の交流や接触を追跡します。

これは、Trellixと戦略国際問題研究所が2022年3月に発表したレポート　In the Crosshairs：Organizations and Nation-State Cyber Threats（照準：組織と国家のサイバー脅威）を裏付けるものです。このレポートによると、国家を後ろ盾とするサイバー攻撃の半数以上が個人の資格情報等へのアクセスをきっかけとしており、その傾向は当面継続する可能性があると考えられます。

2021年第4四半期の脅威動向

ランサムウェアファミリー：2021年第4四半期に検出されたランサムウェアファミリーは、第3四半期から21%増加したLockbit（21%）が最も多く、次いでCuba（18%）、Conti（16%）でした。

ランサムウェアの検挙：2021年第3四半期に検出されたランサムウェアファミリーのトップであるREvil/Sodinokibiは、グローバルな警察の介入により、第4四半期では顕著な検出は見られず、ランク外でした。

ランサムウェアの増加：2021年第4四半期にランサムウェア活動の大幅な増加が確認されたのは、イタリア（793%）、オランダ（318%）、スイス（173%）でした。また、インド（70%）と英国（47%）も増加が顕著でした。

マルウェアファミリー：2021年第4四半期に観察されたマルウェアファミリーのうち、RedLine Stealer（20%）、Raccoon Stealer（17%）、Remcos RAT（12%）、LokiBot（12%）、Formbook（12%）が全体のほぼ75%に相当します。

調査方法

Threat Labs Report：2022年4月版は、Trellixの10億以上のセンサーネットワークから得られた独自のデータと、ランサムウェアや国家主導の活動などの一般的な脅威に関するオープンソースの情報およびTrellix Threat Labsの調査結果を活用しています。本レポートの目的のために、脅威の検出に関連するテレメトリーを使用しています。検出とは、ファイル、URL、IPアドレス、その他の指標が検知され、Trellix XDRエコシステムを通して報告されることを指します。

参考情報

- レポート：Threat Labs Report: April 2022（英語）
- ブログ：Trellix Threat Labs レポート：地政学的な緊張の高まりから、重要インフラを標的としたサイバー攻撃が拡大
- サイト：Trellix Threat Center（英語）

Trellixについて

Trellixは、サイバーセキュリティの未来を再定義するグローバル企業です。オープンかつネイティブなTrellixのXDR（Extended Detection and Response）プラットフォームは、現在最も高度な脅威に直面するお客様が業務の保護や回復に確信を持って対応するための支えとなります。Trellixのセキュリティ専門家は、広範なパートナーエコシステムとともに、データサイエンスと自動化によりテクノロジーイノベーションを加速させ、4万を超える企業や政府機関のお客様の力となっています。

Media@Trellix.com

＜本情報のお問い合わせ＞

Trellix（McAfee Enterprise）
広報担当 戸田
Tel: 070-2680-0731
hiromi.toda@trellix.com

Trellix（McAfee Enterprise）広報担当
LaCreta 担当：野澤 / 近藤
Tel: 050-4560-2425
trellixjpn@lacreta.jp