We bring security to life.

報道関係各位

2022/12/1
Trellix

※当資料は、米国時間2022年11月16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）、2022 年第 3 四半期 脅威レポートを発表

運輸・海運業における悪意のあるサイバー活動の増加を確認

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である Trellix は、本日、世界屈指のセキュリティ研究者とインテリジェンス専門家が集結する Trellix アドバンスト リサーチ センター（Trellix Advanced Research Center）から The Threat Report: Fall 2022 を発表しました。最新のレポートでは、2022 年第 3 四半期からのサイバーセキュリティの動向を分析しています。

このレポートでは、ランサムウェアや国家が支援する高度持続的脅威（APT）の攻撃者に関連する悪意のある活動の証拠を収録しています。また、電子メールへのサイバー脅威、サードパーティー製セキュリティツールの悪用などにおけるさまざまな傾向について調査しています。主な調査結果は以下の通りです。

- **運輸・海運業におけるランサムウェアの活動量が倍増：**運輸・海運業では、ランサムウェアの活動が米国だけで、前四半期比 100%増加しました。世界的には、運輸は通信に次いで 2 番目に攻撃が多いセクターでした。また、APT 攻撃が最も検出されたのは運輸セクターでした。
- **ドイツでの検出が最高に：** 第 3 四半期、ドイツは、APT の攻撃者に関する脅威の検出数が最も多く（観察された活動の 29%）、さらに、ランサムウェアの検出数も最多でした。ドイツでの第 3 四半期のランサムウェアの検出数は第 2 四半期比で 32%増加し、全世界の活動の 27%を占めました。
- **新興の攻撃主体が規模を拡大：**中国が関与する攻撃者 Mustang Panda が、第 3 四半期に最も多く検出されました。次に活発だったのは、ロシアが関与する APT29 と、パキスタンが関与する APT36 でした。
- **進化するランサムウェア：** サイバー犯罪者にとって完全なキットとして販売されていたランサムウェア Phobos は、これまでは公の報告書では見られませんでしたが、世界的に検出された活動の 10%を占め、米国で検出されたランサムウェアの中で 2 番目に多く使用されました。また、LockBit は引き続き世界で最も多く検出されたランサムウェアで、検出数の 22%を占めました。
- **旧来の脆弱性の継続的なまん延：** 数年前の脆弱性が依然として悪用の成功要因となっています。Trellix は、第 3 四半期に顧客が受け取った悪意あるメールの中で、CVE-2017-11882、CVE-2018-0798、CVE-2018-0802 で構成されたマイクロソフト数式エディターの脆弱性が最も悪用されていたことを確認しました。
- **Cobalt Strike の悪用：**Trellix では、第 3 四半期に世界で観察されたランサムウェア活動の 33%、検出された APT 攻撃の 18%で Cobalt Strike が使用されたことを確認しました。Cobalt Strike はセキュリティ運用を向上させるために攻撃シナリオを模倣する目的で作成された正規のサードパーティーツールで、悪意をもってその機能を転用する攻撃者が好んで使うツールです。

Media@Trellix.com

Trellix の脅威インテリジェンス部門の責任者であるジョン・フォッカー（John Fokker）は、次のように述べています。「2022 年、ロシアをはじめとする国家が支援するグループは、絶え間ない活動を続けており、その規模も拡大していることを引き続き確認しています。この活動は、政治的な動機によるハクティビズムの増加や、医療や教育に対する持続的なランサムウェア攻撃によって、さらに深刻なものとなっています。サイバー脅威の攻撃主体とその手法の点検を強化する必要がかつてないほど高まっています。」

The Threat Report: Fall 2022 では、Trellix の監視ネットワークから得られた独自のデータ、オープンソースのインテリジェンス、Trellix アドバンスト リサーチセンターによるランサムウェアや国家による活動などの、広がり続ける脅威に関する調査・研究を利用しています。このレポートでは、脅威の検出に関連する遠隔観測を使用しています。なお検出とは、ファイル、URL、IP アドレス、不審なメール、ネットワークの挙動、その他の指標が検知され、Trellix XDR プラットフォームを通じて報告されることを指します。

参考情報

- The Threat Report: Fall 2022
- Trellix Advanced Research 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。

Trellix アドバンスト リサーチセンター（Trellix Advanced Research Center）について
Trellix Advanced Research Center では、セキュリティの専門家と研究者のエリートチームが、洞察に満ちた実用的なリアルタイムインテリジェンスを作成し、お客様の業績や業界全体を推進するために活動しています。業界で最も包括的な行動憲章に基づき、熟練した研究者が市場に先駆けてトレンドを検知し、お客様やパートナーが新たな脅威に対処できるよう支援します。
詳しくは、**https://www.trellix.com/en-us/threat-center.html**

＜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