Trellix

We bring security to life.

報道関係各位

2023/3/9
Trellix

※当資料は、米国時間 2023 年 2 月 22 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 4 四半期 脅威レポートを発表
ランサムウェア集団「LockBit」が、盗んだデータを最も流出させたと判明

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、Trellix Advanced Research Center（トレリックス アドバンスト リサーチセンター）による **The Threat Report：February 2023** を発表しました。最新のレポートでは、2022 年第 4 四半期のサイバーセキュリティの動向を調査しています。Trellix は、エンドポイントプロテクションの広範なネットワークと XDR 製品群から収集した遠隔観測と、オープンおよびクローズドソースのインテリジェンスレポートから収集されたデータと組み合わせて、レポートの洞察を提供します。

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。「第 4 四半期は、悪意ある攻撃者が攻撃経路の限界に挑戦していたことが確認されました。グレーゾーン紛争とハクティビズムの両方が、国家戦略としてのサイバー攻撃と攻撃主体のリークサイトでの活動を増加させました。経済情勢の変化に伴い、組織は限られたリソースの中で最も効果的なセキュリティを実現しなければなりません。」

本レポートでは、ランサムウェアや国家が支援する APT 攻撃（高度持続的脅威）の実行者に関連する悪意のある活動の状況を示し、電子メールに対する脅威、正規のセキュリティツールの悪意のある使用などを検証しています。主な調査結果は以下の通りです。

- **LockBit 3.0 は最も手荒なランサムウェア**：Trellix の遠隔観測によると、第 4 四半期では、Cuba と Hive と呼ばれるランサムウェアファミリーの検出が増え、LockBit は最も活発なランサムウェアグループではなくなりましたが、サイバー犯罪組織のリークサイトでは、最も多くの被害者が報告されています。このデータから、LockBit は被害者に対して身代金要求に応じるよう最も激しく圧力をかけていることがわかります。これらのサイバー犯罪者は、2018 年の時点で発見された脆弱性を悪用するなど、さまざまな手法でサイバー攻撃を実行しています。

- **中国が主導する国家的活動**： Mustang Panda や UNC4191 など、中国に関連する APT 攻撃グループが最も活発で、これらを合算すると検出された国家を後ろ盾とする活動の 71%を占めました。ついで、北朝鮮、ロシア、イランに関連する攻撃者でした。公開レポートにおいても、同じ 4 か国が最も活発な APT 攻撃者の拠点国として挙げられています。

- **重要インフラ分野が最大の標的に**：サイバー脅威の被害を最も受けたのは、重要インフラの各セクターでした。Trellix が検出した悪意のある活動のうち、国家を後ろ盾とする APT 攻撃の 69%が輸送・海運業を標的にし、エネルギー、石油、ガスが続きました。Trellix の遠隔観測によると、ランサムウェア攻撃者が最も標的としたセクターは金融とヘルスケアで、通信、政府、金融は悪意のある電子メールに狙われた上位のセクターでした。

- **CEO を騙ったメールによるビジネスメール侵害**：Trellix は、ビジネスメール詐欺（BEC）の 78%が、CEO が用いる常套句を使った偽の電子メールだったと判定し、2022 年第 3 四半期から第 4 四半期にかけて 64%増加したことを突き止めました。ボイスフィ

Media@Trellix.com

ッシング（ビッシング）を使い、従業員に直通の電話番号を確認するよう求めるなどの手口もありました。82%が無料の電子メールサービスを利用して送信されており、攻撃主体はサイバー攻撃を実行するために特別なインフラを必要としないことを示しています。

The Threat Report：February 2023 は、Trellix のセンサーネットワークから得られた独自データ、Trellix Advanced Research Center による国家やサイバー犯罪者の活動に関する調査、セキュリティ業界のオープンソースとクローズドソースからの情報、攻撃主体のリークサイトなどを利用しています。本レポートは、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 Trellix XDR プラットフォームによって検知され報告された、脅威の検出に関する遠隔観測に基づいて作成されています。

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 Advanced Research Center（トレリックス アドバンスト リサーチセンター）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
広報担当 戸田
Tel: 070-2680-0731
hiromi.toda@trellix.com

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