We bring security to life.

報道関係各位

2022/8/4
Trellix

※当資料は、米国時間2022年7月18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 1 四半期 脅威レポートを発表

ランサムウェア攻撃の第一の標的は「ビジネスサービス」、ロシアのサイバー犯罪の進化、E メールのセキュリティ等の詳細を報告

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、本日、「The Threat Report：Summer 2022」を発表しました。このレポートでは、2022 年第 1 四半期以降のサイバーセキュリティのトレンドと攻撃手法を調査分析しています。

本レポートでは、コネクテッドヘルスケアやアクセス制御システムについて Threat Research チームによる調査内容を解説しています。さらにメールのセキュリティ動向の分析、新しいマルウェアや手法がまだ観察されていないウクライナ紛争に関連するロシアの進化するサイバー犯罪の詳細も含まれています。レポートの主な調査結果は次のとおりです。

- **ビジネスサービスに対する脅威の増加**：IT、金融、その他のコンサルティングや契約サービスを提供する企業が敵対的な攻撃者の標的になるケースが頻発しており、サイバー犯罪者が 1 回の攻撃で複数の企業を狙おうとしていることを示しています。ビジネスサービスは、米国のランサムウェア検出総数の 64%を占めるとともに、セクター別でも 2022 年第 1 四半期の世界のランサムウェア検出数、マルウェア検出数、国家主導の攻撃において、通信会社に次いで 2 番目の標的となりました。

- **ランサムウェアの進化** ：1 月にランサムウェア集団 REvil のメンバーが逮捕されたことを受けて、攻撃者への身代金の支払いは減少しました。さらに、Trellix は、仮想化サービスを標的としたランサムウェアグループがロッカーを構築し、さまざまな成功を収めていることを確認しました。ウクライナ紛争は、サイバー犯罪者と国家間の境界線をさらに曖昧にし、最大の変化を引き起こしました。2022 年第 1 四半期で 2 番目に活発だったランサムウェア集団 Conti から漏出したチャットは、Conti のロシア政府への忠誠を公に表明しており、政府がサイバー犯罪者集団に指示を行なっていることを裏付けました。

- **メールセキュリティの動向**：遠隔観測分析により、メールセキュリティにおけるフィッシング URL や悪意のあるドキュメントの動向が明らかになりました。検出された悪質なメールのほとんどは、認証情報を盗んだり、マルウェアをダウンロードさせたりするために使用されるフィッシング URL を含んでいました。また、Trellix は、悪意のある文書が添付されたメールを確認したほか、情報窃取用のマルウェア（infostealer）やトロイの木馬など、悪意のある実行ファイルが添付されたメールを複数発見しています。

Trellix のリードサイエンティスト兼シニアプリンシパルエンジニアであるクリスチャーン・ビーク（Christiaan Beek）は、次のように述べています。「デジタルと物理の世界が交錯する中、サイバー攻撃は私たちの日常生活に混乱をもたらします。敵対者は自分たちが注意深く監視されていることを知っています。ウクライナ紛争の中でまったくの新しい戦術が観察されていないことは、ここで使用されているツールがうまく切り抜けていることを物語っています。世界の攻撃主体は、エスカレートした場合に備えて新しいサイバー兵器を展開できるよう準備しており、組織は引き続き警戒する必要があります。」

Media@Trellix.com

「The Threat Report：Summer 2022」では、Trellix のネットワークにおける 10 億以上のセンサー、オープンソースインテリジェンス、およびランサムウェアや国家の活動など蔓延する脅威に関する Threat Research チームの調査を基にした独自のデータを活用しています。脅威の検出に関連する遠隔観測は本レポートでの活用を目的に使用しています。検出とは、ファイル、URL、IP アドレス、その他の指標が検出され、Trellix XDR エコシステムを通して報告されることを意味します。

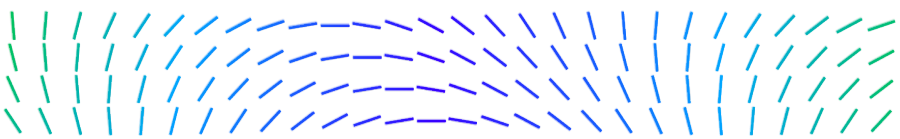
参考情報

- Trellix Threat Center（英語）
- Trellix Threat Labs Blog（英語）
- Trellix Threat Report: Summer2022

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。

＜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



Media@Trellix.com