2022年5月23日
Ivanti Software 株式会社

Ivanti、2022年第1四半期ランサムウェアレポートを発表
ランサムウェアに関連する脆弱性が7.6%増加
ランサムウェアグループ、「Conti」の活動急増が明らかに

ランサムウェアに関連する *APT* グループが*7.5%*、活発に悪用され集中的に狙われる
脆弱性が*6.8%*、ランサムウェアファミリー数が*2.5%*増加したことを公表

クラウドからエッジまで IT 資産の管理、検出、保護、サービスを自動化するプラットフォーム Ivanti Neurons を提供する Ivanti（本社：米国ユタ州ソルトレイクシティ、CEO：Jeff Abbott）は、本日、認証番号付与機関（CNA)である Cyber Security Works 社、次世代 Security Orchestration, Automation and Response（SOAR）、ならびに脅威インテリジェンスソリューション「Cyber Fusion」のリーディングプロバイダーである Cyware 社と共同で実施した「Ransomware Index Report Q1 2022」の結果を発表しました。本レポートでは、2022年第1四半期にランサムウェアに関連する脆弱性の数が7.6%増加し、そのほとんどをランサムウェアグループの一つである「Conti」によって悪用されていることが確認されました。レポートでは、ランサムウェアに関連する22種類の脆弱性が新たに発見され、ランサムウェアの種類が合計で310種類となったことが報告されています。また、ウクライナ侵攻後にロシア政府への支援を表明した Conti グループが、ランサムウェアを頻繁に発生させ、そのうちの19種類に関与していることが判明しました。

また、レポートでは、ランサムウェアに関連する APT グループが7.5%、活発に悪用されている脆弱性や集中的に狙われる脆弱性が6.8%、ならびにランサムウェアファミリーの数が2.5%、それぞれ増加したことも明らかになりました。この数字をさらに細かく分析すると、2022年第1四半期に新たに3つの APT グループ（Exotic Lily、APT 35、DEV-0401）がランサムウェアを使用してターゲットを攻撃し始め、新たに10のアクティブおよびトレンドの脆弱性がランサムウェアと関連付けられるようになり（これにより合計157に）、さらに4つのランサムウェアファミリー（AvosLocker、Karma、BlackCat、Night Sky）が新たに攻撃を活発化したことが明らかになりました。

さらにレポートは、ランサムウェアオペレーターがこれまで以上に迅速に脆弱性を武器化し、最大の混乱と影響をもたらすものを標的にし続けていることを報告しています。高度化・巧妙化するランサムウェアグループは、ベンダーからパッチがリリースされてから8日以内に脆弱性を悪用するようになりました。これは、サードパーティベンダーや組織のセキュリティ対策が十分でないこと、またランサムウェアグループが脆弱なネットワークに侵入するには容易であることを意味します。さらに、最も一般的なスキャナの中には、ランサムウェアの一部の重要な脆弱性を検出しないものがあります。今回の調査では、ラン

サムウェアの脆弱性の3.5%以上が見落とされており、組織を重大なリスクにさらしていることが明らかになりました。

Cyber Security Works 社、CEO であるアーロン・サンディーン(Aaron Sandeen)氏は、次のように述べています。
「重要なランサムウェアの脆弱性をスキャナが検知していないという事実は、組織にとって大きな問題です。Cyber Security Works の調査・分析の一環として、CSW の専門家がこの点について取り組み続けています。ただ、スキャナ企業がこの問題に真剣に取り組んでいるため、今期においてこの数値が下がってきていることは良い傾向と言えます。とはいえ、スキャナが検知しないランサムウェアの脆弱性は未だ11件あり、そのうちの5件は Ryuk、Petya、Locky といった悪名高いランサムウェアグループによるに関連付けられていることから、非常に重大な脆弱性と評価しています。」

さらに、セキュリティならびに IT 部門にとっては、National Vulnerability Database（NVD）、MITRE 社による共通攻撃パターン列挙・分類（CAPEC）リスト、米国土安全保障省サイバーセキュリティ・インフラセキュリティ局（CISA）による「既知の悪用された脆弱性カタログ」（KEV）にデータの齟齬が生じているという事実が問題となっています。このレポートでは、NVD では脆弱性61件、CAPEC リストでは脆弱性87件の CWE（共通脆弱性タイプ）が欠落していることが明らかとなりました。また、ランサムウェアの脆弱性は、ベンダーから開示されてから平均して1週間後に NVD に追加されます。一方、ランサムウェアに関連する169件の脆弱性は、まだ CISA の KEV リストに追加されていません。世界中のハッカーは、これらの脆弱性のうち100件を積極的にターゲットとしており、パッチが適用されていないインスタンスを1つでも発見し、悪用する目的で、組織を監視しているのです。

Ivanti、セキュリティ製品担当シニアバイスプレジデントであるスリニヴァス・ムッカマラ（Srinivas Mukkamala）は、次のように述べています。
「脅威攻撃者は、従来の脆弱性管理プロセスを含むサイバー衛生管理の欠陥を標的にした攻撃を加速しています。今日、多くのセキュリティおよび IT 部門にとって、脆弱性がもたらす現実的なリスクの特定は難しく、そのため脆弱性を修正するための優先順位付けが不適切になっています。例えば、多くの場合、パッチは新しい脆弱性や NVD で公開された脆弱性だけに適用されています。また、CVSS（共通脆弱性評価システム）のみを使って脆弱性のスコアリングと優先順位付けを行っている企業もあります。サイバー攻撃から組織をより強力に保護するために、セキュリティと IT 部門は、脆弱性管理に対してリスクベースのアプローチを採用する必要があります。そのためには、企業のエクスポージャとアクティブな脅威を特定し、脆弱性の武器化に対して早期警告を行い、攻撃を予測し、修正作業の優先順位を決めることができる AI ベースのテクノロジーが必要となります。」

また、本のレポートでは、病院や医療施設で使用されるヘルスケアアプリケーション、医療機器およびハードウェアを供給する56のベンダーを分析し、それぞれの製品特有の脆弱性624件を明らかにしました。そのうち40件の脆弱性には公開されたエクスプロイトがあり、2件の脆弱性（CVE-2020-0601

および CVE-2021-34527）は、4つのランサムウェア攻撃者（BigBossHorse、Cerber、Conti、Vice Society）に関連付けています。残念ながらこの事実は、医療業界が今後数か月のうちにランサムウェアによる攻撃に、より狙われる可能性があることを示しているのかもしれません。

Cyware 社、CEO であるアヌージ・ゴエル(Anuj Goel)氏は、次のように述べています。
「ランサムウェアは現在、世界中の組織の収益に影響を与える最もメジャーな攻撃ベクトルの1つです。第1四半期のレポートは、ランサムウェアの脆弱性やランサムウェアを使用する APT が増加していることを示す新しい数値がこの事実を明確にしています。しかし、表面化した主要な懸念事項の1つは、複数のソースから入手できる脅威情報が錯綜しているため、セキュリティ部門が脅威を完全に把握できていないことです。セキュリティ部門がランサムウェア攻撃をプロアクティブに軽減するためには、複数のソースから情報を取り込み、相関、セキュリティアクションを通じて、形を変えるランサムウェアの攻撃ベクトルを完全に可視化する一元化された脅威情報管理ワークフローとパッチや脆弱性への対応を連携させる必要があります。」

「Ransomware Index Spotlight Report」は、Ivanti と CSW の独自データ、公開されている脅威データベース、脅威研究者とペネトレーションテストチームを含む、さまざまなソースから収集されたデータに基づいて作成されたものです。レポート全文はこちらをご参照ください。

Ivanti について

Ivanti は「Everywhere Workplace（場所にとらわれない働き方）」を実現します。場所にとらわれない働き方により、従業員は多種多様なデバイスでさまざまなネットワークから IT アプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivanti Neurons 自動化プラットフォームは、業界をリードする統合エンドポイント管理、ゼロトラストセキュリティと、エンタープライズサービス管理のソリューションをつなぎ、デバイスの自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合 IT プラットフォームを提供します。Fortune 100の96社を含む40,000社以上の顧客が、クラウドからエッジまで IT 資産の管理、検出、保護、サービスのために Ivanti を選択し、従業員があらゆる場所にいても作業できる優れたユーザー体験を提供しています。
詳細については、www.ivanti.co.jp をご参照ください。

Cyware について

Cyware は、企業のサイバーセキュリティチームがプラットフォームに依存しないバーチャルサイバーフュージョンセンターを構築するための支援を行っています。Cyware は、次世代 SOAR（Security Orchestration, Automation, and Response）テクノロジーを搭載したサイバーセキュリティ業界唯一のバーチャルサイバーフュージョンセンターを提供することで、セキュリティオペレーションを変革しています。その結果、企業・組織はスピードと精度を高めながら、コストとアナリストの疲弊を低減することができます。Cyware のバーチャルサイバーフュージョンソリューションは、あらゆる規模とニーズの企業、

シェアリング・コミュニティ（ISAC/ISAO）、MSSP、政府機関にとって、安全なコラボレーション、情報共有、脅威の可視性向上を実現します。
詳細については、https://cyware.com/をご参照ください。

CSW について

CSW は、攻撃対象領域の管理とペネトレーションテストをサービスとして提供するサイバーセキュリティサービス企業です。脆弱性とエクスプロイトの調査における当社の革新的なテクノロジーにより、Oracle、D-Link、WSO2、Thembay、Zoho などの人気製品において45以上のゼロデイを検知しました。また、CVE の Numbering Authority となり、何千人ものバグバウンティハンターの活用を可能にするなど、脆弱性管理のグローバルな取り組みにおいて重要な役割を果たしています。CSW は、脆弱性の調査・分析のリーダーとして、世界中の企業が進化し続ける脅威からビジネスを保護するために、業界の最前線を走っています。
詳細については、www.cybersecurityworks.com をご参照ください。

＜報道関係に関するお問い合わせ先＞
Ivanti Software 株式会社
マーケティング部：鳥羽
Email: shoichi.toba@ivanti.com
TEL: 03-6432-4180

Ivanti 広報事務局
E-mail: ivanti@jspin.co.jp