2022年11月4日
Ivanti Software 株式会社

Ivanti、2022年 第2四半期～第3四半期のランサムウェアレポートを発表 ランサムウェアが 2019年以降466%増加し、現在、ランサムウェアとマルウェアが実際の戦争の前兆として利用されていることが明らかに

ほとんどの *IT* およびセキュリティ部門が、存在するすべての脆弱性を完全に把握しておらず、
最もリスクの高い脆弱性に関する脅威状況が十分に認識できていないことも判明
*124*件ランサムウェアの脆弱性が *CISA* の *KEV* カタログには未登録

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、CNA（CVE 採番機関）の Cyber Security Works、サイバーフュージョンセンター構築テクノロジープラットフォームの リーディングプロバイダーCyware とともに実施した「ランサムウェア インデックスレポート Q2-Q3 2022 」の結果を発表しました。本レポートによると、ランサムウェアは2019年から466%増加しており、ウクライナとロシアの紛争やイランとアルバニアのサイバー戦争に見られるように、実際の戦争の前兆として利用されるケースが、加速的に増大していることが明らかになりました。

ランサムウェアグループは、2022年の最初の3四半期で35の脆弱性がランサムウェアと関連づけられ、159のアクティブな悪用がトレンドとなっており、ボリュームと精巧さにおいて成長し続けています。さらに、十分なデータや脅威のコンテキストが不足しているため、組織が効果的にシステムにパッチを適用させ、脆弱性リスクの軽減を行うことがより困難になっています。

本レポートでは、新たに10種類のランサムウェアファミリー（Black Basta、Hive、BianLian、BlueSky、Play、Deadbolt、H0lyGh0st、Lorenz、Maui、NamPoHyu）が確認されたことで、合計で170種類になったことが明らかにされています。ランサムウェアの攻撃者は、101ある CVE をフィッシング対象とするため、ますますスピアフィッシング手法を利用して、無防備な感染者から悪質なペイロードを仕掛ける傾向が強まっています Pegasus の例では、単純なフィッシングメッセージが最初のバックドアアクセスの作成に使用され、iPhone の脆弱性と相まって、世界中の多く著名人への侵入や侵害が引き起こされました。

ランサムウェアには人との介入が必要であり、フィッシングだけが攻撃のベクトルであるというのは偽りです。Ivanti は、現在までに323のランサムウェアの脆弱性を分析し、MITRE ATT&CK フレームワークにマッピングすることで、組織に侵入するためのキルチェーンとして使用される正確な戦術、テクノロジ

ー、手順を特定しました。その中の57は、初期アクセスから漏洩まで、完全なシステムの乗っ取りを引き起こしていることが判明しました。

また本レポートでは、2つの新しいランサムウェアの脆弱性（CVE-2021-40539と CVE-2022-26134）が特定され、この2つは、National Vulnerability Database（NVD）に追加される前日、または同日に、AvosLocker や Cerber といった多くのランサムウェアファミリーによって悪用されていたことが分かりました。これらの統計は、組織が脆弱性へのパッチの適用を NVD の開示だけに依存していると、攻撃を受けやすくなることを意味しています。

さらに本レポートは、米国の公共部門の企業や政府機関に期限内にパッチを適用すべき脆弱性のリストを提供する CISA の Known Exploited Vulnerabilities（KEV）カタログに、124のランサムウェアの脆弱性が含まれていないことを明らかにしています。

Ivanti、最高製品責任者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。
「IT およびセキュリティ部門は、ランサムウェアやその他の脅威からの防御をより強化するために、脆弱性管理に対するリスクベースのアプローチを早急に導入しなければなりません。これには、多様なソース（ネットワークスキャナー、社内外の脆弱性データベース、侵入テストなど）からのデータを関連付け、リスクを測定し、脅威化の早期警告を行い、攻撃を予測し、修復活動の優先順位をつけることができる自動化テクノロジーの活用が含まれます。NVD やその他の公開データベースのみを活用して脆弱性の優先順位付けやパッチ適用を行うなどの従来の脆弱性管理に依存し続ける組織は、サイバー攻撃を受けるリスクは今後も高くなるでしょう。」

さらに、一般的なスキャナーが脆弱性を見逃しているという事実により、従来の脆弱性管理を超えて進化するべき必要性が強調されています。本レポートでは、ランサムウェアに関連する18の脆弱性が一般的なスキャナーで検出されないことが判明しました。

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。
「頼りにしているスキャナーが公開された脆弱性を特定できていないのであれば、それは恐ろしいことです。組織は、組織資産全体において、さらされる脆弱性を検出できる攻撃対象領域管理ソリューションを採用する必要があります。」

さらに、本レポートでは、ランサムウェアが重要インフラに与える影響を分析し、最も被害の大きかった3つの分野は、医療、エネルギー、基幹製造業であったことが報告されています。レポートでは、ランサムウェアの脆弱性の 47.4%が医療システムに、31.6%がエネルギーシステムに、21.1%が基幹製造業に影響を与えていることが明らかになっています。

Cyware 社、共同創業者兼 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。「インシデント発生後の復旧戦略は時間の経過とともに改善されていますが、「予防は治療に勝る」という古い格言は今もなお変わらない事実です。脅威のコンテキストを正しく分析し、先を見越した緩和対策の優先順位づけを効果的に行うために、セキュリティプロセスの回復力のあるオーケストレーションを通して、SecOps の脆弱性インテリジェンスを運用し、脆弱な資産の整合性を確保しなければなりません。」

また、本レポートは現在および今後のランサムウェアの動向に関するインサイトも提供しています。中でも、ランサムウェアのオペレーターは、単一のコードベースを介して複数のオペレーティングシステムを容易にターゲットにできるため、クロスプラットフォーム機能を備えたマルウェアの需要が急増しています。さらに、セキュリティソリューションやソフトウェアのコードライブラリのサードパーティのプロバイダーに対する多数の攻撃や、多くの被害者が発生する可能性が明らかになりました。Conti や DarkSide などのよく知られた攻撃グループが活動を停止したと考えられているため、今後、新しいランサムウェア集団が出現することが予期されます。新しい集団は、ソースコードを再利用または修正し、消滅したランサムウェアグループが取り入れていた手法を悪用する可能性が大いにあります。

「ランサムウェア インデックス スポットライト レポート」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、ならびに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います。レポート全文はこちらからご覧ください。

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