Secureworks®

脅威インテリジェンス エグゼクティブレポート

Volume 2021, Number 3

カウンター・スレット・ユニット™（CTU）
リサーチチーム

エグゼクティブサマリー

セキュアワークスのカウンター・スレット・ユニット（CTU™）リサーチチームは、セキュリティの脅威を分析し、組織によるシステム保護を支援しています。2021年3月から4月にかけて観測された脅威のふるまい、グローバル規模の脅威状況、セキュリティトレンドをもとに、注目すべきポイントをCTU™のリサーチャーがまとめました。

- ランサムウェアとの戦い：食い止め、阻止、準備、対応
- サプライチェーン攻撃からの防御
- リスクは明白 - パッチをあてるか、被害を受けるか

ランサムウェアとの戦い：食い止め、阻止、準備、対応

まず大事なのは、防御することです。企業や行政機関による最近のランサムウェア対策からしても、ランサムウェアがどれほど大きな問題になったのかが伺えます。
ランサムウェアオペレーターは常に攻撃の手口を進化させ、最小の手間で最大の成果を得ようとしています。しかしパッチ適用、監視、多要素認証（MFA）の実装など、基本的で効果的なセキュリティプラクティスを実施すれば攻撃者によるアクセスを未然に防ぐことができます。

The Institute for Science and Technology（IST）によるマルチセクターのランサムウェアタスクフォースは、2021年4月にランサムウェアフレームワークをリリースし、官民組み合わせた50近くの戦略を推奨し、ランサムウェアの脅威に取り組んでいます。同じく4月には米国司法省（DOJ）の内部文書でも、DOJの検事と連邦捜査局（FBI）のエージェントから構成される別のランサムウェアタスクフォースの設立概要が示されました。

ISTによる取り組みは「国内外で連携した総合的な戦略でランサムウェア攻撃を食い止め、ランサムウェアのビジネスモデルを阻止し、ランサムウェアに対する組織の準備態勢を整え、ランサムウェアに効果的に対応すること」を目標としています。DOJとFBIの取り組みでは、政府の能力を向上させ、攻撃の阻止とその背後にいる犯罪者の訴追を行うのが目的のようです。

しかし、どちらのグループも非常に大きな課題に直面しています。3月と4月にはAvaddon、Astro Team、REvil、Darkside、Babuk、DoppelPaymer、Maze、Clop、Contiといったランサムウェアの犯罪オペレーター集団が引き続き活発に活動しています。

CTU のリサーチャーが監視していたランサムウェアファミリーのうち、調査期間中最大の被害をもたらしたのはランサムウェア・アズ・ア・サービス (RaaS) の Avaddon のオペレーションで、リークサイトでの被害数は合計 44 に上りました。REvil のカスタム版である LV は、4 月に登場して以来 15 の被害が出ています。Clop と Babuk のオペレーターは暗号化なしで恐喝を行うやり方に移行し、被害者をシステムからロックアウトすることはせずにデータを盗んで身代金を要求しているようです。

CTU のリサーチャーによると、現在までにランサムウェアリークサイトで「さらし者になった」組織は 1,800 以上になるといいます。大半は身代金の支払いが遅かった、または支払わなかった組織です。すぐに身代金を支払った組織は通常、リークサイトには現れません。さらに、金銭的な利益を目指して活動する他のあらゆる団体と同じように、ランサムウェアオペレーターは常にツールや技法を進化させ、成功率を高めています。

一方で、目的を特定することが難しい場合もあります。米国財務省がロシアへの制裁に関して発表した声明では、Evil Corp としても知られるボットネット Dridex を運営している金銭目的の脅威グループ GOLD DRAKE と、ロシア連邦保安局 (FSB) との関係が明確に言及されています。財務省は、GOLD DRAKE は FSB の支援により破壊的なランサムウェア攻撃やフィッシングキャンペーンを実施したと報告しています。ランサムウェアオペレーターの多くがロシアなど旧ソ連を拠点としています。彼らは、拠点地域での被害を避ければ当該地域の警察に捜査されないという暗黙の了解のもと活動しています。ロシアがランサムウェアの犯罪グループを情勢かく乱のための便利な手段とみなし、ロシアの利害に悪影響を及ぼさない限り活動を黙認しているという可能性は少なくありません。

ランサムウェアの合計被害額はビジネスメールからの侵害には及ばないものの、今最も速く拡大・進化している脅威の 1 つです。1 回の攻撃だけでも、その被害は膨大になる場合があります。身代金の額の問題だけでなく、壊滅的に近いビジネス中断や、インシデント経験と回復に伴う損害により、最終的なコストは最初の身代金をはるかに超える可能性があります。

さらに言えば、暗号化なしでの恐喝への移行という最近の動きは、最小限の手間で最大限の利益を獲得することを狙う犯罪脅威グループのマクロトレンドを示しています。ランサムウェアでは、ツールの開発や被害者のデータの復号化という手間がかかります。暗号化せずに恐喝する場合はデータを盗み出すだけで済み、不正侵入した環境全体で検出される可能性があるマルウェアを用意する必要がなくなります。

組織にとっては、この種の脅威グループとアクティビティは攻撃ライフサイクルの早い段階で検出できるようにしなければならないということです。不正アクセス、持続メカニズム、そして水平移動を検出・防止するのは、ランサムウェアの実行を検出・防止しようとするよりもはるかに効果的な戦略です。各種タスクフォースによる活動が有益なことは間違いありませんが、パッチの適用漏れや MFA によるシステム保護を行っていないなどの基本的なセキュリティ上のミスをなくすだけでも、不正アクセスによる攻撃を未然に防げる可能性はぐっと高まります。

これだけは今すぐに：
MFA を実装してインターネット接続されたシステムへのアクセスを保護する。

サプライチェーン攻撃からの防御

自分でコントロールできないものを守ることはできません。つまりサプライチェーンのセキュリティを完璧にすることはそもそも不可能です。しかし、サプライチェーン攻撃に対抗するために、組織は以下の 3 つの対策を講じることができます。

- **特定：サプライチェーンがアクセス可能なシステムとアセットを把握する**
- **評価：特に重要なものを判断してアクセスを限定する**
- **緩和：タッチポイントを保護して影響を最小化する**

4月にはコードのレビューと監査を行う企業、Codecov が自社ソフトウェアにセキュリティ侵害があったと発表しました。Codecov は顧客 29,000 社のコードテストをサポートしコードのミスや脆弱性の検出を行っていて、顧客の多くはソフトウェアをそれぞれのクライアントに販売しています。改ざんされたCodecov Bash Uploader のスクリプトでは、コード開発環境からデータを盗み出せるようになっていて、そこにはソースコードレポジトリやその他の機密情報へのアクセスを可能にするトークンやキーも含まれている恐れがありました。Codecov への不正アクセスに成功したことで、攻撃者は他の膨大な数のサプライチェーンにも侵入できた可能性があります。

ランサムウェア攻撃によってサプライチェーンに影響が及ぶこともあります。4 月にオランダの物流会社、Bakker Logistiek が攻撃されたことで、オランダのスーパーマーケットで 全国的にチーズが不足 しました。数百、数千の組織で流通するシステムやソフトウェアを標的としたサプライチェーン攻撃は、数としてそれほど多くはありません。Codecov のソフトウェアへの攻撃のほか、2020年のSolarWinds Orionプラットフォームアップデートに対するロシアからの攻撃、2020 年末と2021年初めのAccellion File Transfer Appliances (FTA) への攻撃などがその事例です。しかしこうしたインデントは、リスクをコントロールすることが非常に難しいことを物語っています。

4 月にはまた、米国のサイバーセキュリティ・インフラセキュリティ庁 (CISA) と標準技術研究所 (NIST) が組織によるソフトウェアサプライチェーンのリスクの特定、評価、緩和をサポートするために、「Defending Against Software Supply Chain Attacks (ソフトウェアサプライチェーン攻撃からの防御)」と題する文書を発表しました。この文書ではリスクやよくある攻撃の手口について説明し、ソフトウェアベンダーやその顧客が攻撃を防御できるように推奨事項も提示しています。

サプライチェーンの安全性確保はコンプライアンスのようなものです。チェックリストを埋めるのは簡単でも、実際に効果があるのはアクセスを制限し被害の可能性を軽減することです。

これだけは今すぐに：
CISA/NIST レポートに記載されたアドバイスに従う。

リスクは明白 – パッチをあてるか、被害を受けるか

パッチを適用しなければ、セキュリティ侵害のリスクは大幅に高まります。被害の大きさと複雑さも同様に高まります。ランサムウェア実行、クレデンシャル盗難、機密データ抽出のいずれの攻撃者に対しても、パッチは最も重要な保護策の 1 つです。

2021 年 3 月と 4 月中に CTU のリサーチャーは 23 の脅威インテリジェンスレポートと 67 の脆弱性アセスメントを発表し、パッチに関するアドバイスも記載しました。
脅威インテリジェンスレポートの半数以上と、多数のメディア報道で Microsoft Exchange Server の脆弱性が指摘されています。そのうち 3 月中の 4 件は国家的な攻撃者によるエクスプロイトとの関連性が示唆されており、4 月にはリモートコード実行に伴うさらに 4 件の脆弱性が明らかになっています。

Exchange Server の脆弱性は大きな注目を集めましたが、攻撃者の標的は他にもありました。早急なパッチ適用が推奨されたその他の脆弱性には、Fortinet FortiOS、macOS、Chrome、SAP NetWeaver に影響を及ぼすものも含まれていました。SAP NetWeaver の脆弱性は 2020 年に明らかになり、共通脆弱性評価システム (CVSS) の重度スコアで最も高い 10 の評価を受けました。

米国の国家安全保障局 (NSA)、FBI、CISA も共同勧告を発し、世界中で普及する大手認証・仮想化ソフトウェアで判明している 5 つの脆弱性が、ロシアの外国諜報機関 (SVR) によって頻繁に攻撃されているとの警告がなされました。このうちいくつかは過去に複数の脅威グループに悪用されたことがあります。

NSA は、「米国や同盟国のネットワークは常にロシアの国家的サイバーアクターによるスキャニング、標的化、エクスプロイトの対象となっており」、こうした脆弱性の軽減は「非常に重要」と述べています。2020 年 11 月にも、中国の攻撃者が狙っている脆弱性について同様の文書が発表されています。

「MFA の実装」、「エンドポイントとネットワークの包括的な監視」以外に、「タイムリーなパッチ適用」もセキュアワークスのインシデント対応チームが最も頻繁に推奨する対策の1つです。組織がタイムリーなパッチ適用をしない・できないのにはいろいろな理由があり、中にはリスク上の問題もあります。しかし国家的な脅威グループから金銭目的の犯罪者に至るまで、あらゆる種類の攻撃者が、パッチ未適用でエクスプロイト可能な脆弱性を常に探しているのです。組織は MFA によってシステムへの入口を保護し、フィッシングに関する教育によってバックドアを固く閉ざすことができます。しかしこうしたセキュリティ対策をしても、窓が全部開いたままでは侵入を防ぐことはできません。

パッチはセキュリティ戦略の基本です。ネットワークにどのシステムが含まれているのかを把握し、脅威インテリジェンスを基にリスク査定をして、優先度の高いパッチを管理できるシステムを設計することが、戦略実装の重要なステップになります。パッチを適用できないシステムがある場合、代わりにエクスプロイトの防止、検出、封じ込めのためのコントロールを必ず確立しておく必要があります。しかしこういった対策はあくまでも例外です。サプライチェーンへの攻撃、ランサムウェア、その他の攻撃のいずれを警戒する場合でも、パッチはリスクを軽減できる最も効果的な手段の1つなのです。

これだけは今すぐに：
アセットインベントリの更新。何を使っているか把握していなければパッチを適用できない。

結論

脅威を取り巻く状況は進化し続けています。脅威グループは現れては消え、用いられる攻撃の種類も頻度が変化します。ただし基本的なセキュリティプラクティスの重要性は変わりありません。攻撃者に攻撃されやすい状況を作ってはなりません。ネットワークとエンドポイントの監視や検出のための報告的なソリューションを実装し、MFA を使用し、定期的かつタイムリーにパッチを適用して攻撃者によるアクセスの手がかりを防ぎましょう。

CTU リサーチチームについて

CTU のリサーチャーは、メディアでも頻繁に取り上げられ、セキュリティコミュニティ向けの技術分析を公開し、セキュリティカンファレンスでは新たな脅威について説明しています。セキュアワークスの高度なセキュリティテクノロジーと、業界でのネットワークを活用して、CTU リサーチチームは脅威アクターを追跡し、異常なアクティビティを分析して、新しい攻撃手法と脅威を追跡しています。このプロセスにより、CTUのリサーチャーは、脅威をすぐに識別し、損害が生じる前にお客様を保護する対策を開発します。

リサーチ

お客様が直面する脅威の根本を理解し、対処・保護するための対策を作成

インテリジェンス

ネットワークエッジを超えて、脅威の可視性を強化する情報を提供

統合

CTU によるリサーチとインテリジェンスを、セキュアワークスのマネージド・セキュリティ・サービスとコンサルティングに投入

Secureworks®

Secureworks® (NASDAQ: SCWX) は、サイバーセキュリティにおける世界的な先進企業です。当社ソリューションをご活用いただくことにより、お客様やパートナーは攻撃者よりも常に先手を打ち、マーケットに迅速に対応し、ビジネスニーズを満たすことができます。クラウドネイティブの SaaS セキュリティプラットフォームとインテリジェンス主導のセキュリティソリューションの独自の組み合わせにより、20 年以上の脅威インテリジェンスと分析から得た深く広い知見を提供しております。このように、長年にわたるサイバー攻撃の最前線で蓄積した実践経験に基づく知見を提供するセキュリティプラットフォームは、唯一無二のセキュアワークスだけです。

www.secureworks.com

Corporate Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
1.877.838.7947
www.secureworks.com

Europe & Middle East France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center, Unterschweinstiege
10 60549 Frankfurt am Main
Germany
069/9792-
0

United Kingdom
One Creechurch Place, 1 Creechurch
Ln London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3
5DA United
Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet
City Dubai, UAE PO Box
500111 00971 4 420 7000

Asia Pacific Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney
NSW Australia 2086
1800 737 817

日本
212-8589
川崎市幸区堀川町 580
ソリッドスクエア東館 20 階
03-6893-2317
www.secureworks.jp

※ 本文書は www.secureworks.com で公開されている Threat Intelligence Executive Report 2021: vol.3 の抄訳となります。原文 (英語) と和訳の内容に差異があった場合には、原文の記載が優先されます。