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 4

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 5 月から 6 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。

- Colonial Pipeline 社への攻撃をきっかけに、ランサムウェアを取り巻く状況は様変わりしたのか？
- 攻撃戦術は変われど、依然として汎用ツールを使った攻撃が主流
- 脅威アクターに最も狙われやすい「セキュリティ統制の抜け穴」

Colonial Pipeline 社への攻撃をきっかけに、ランサムウェアを取り巻く状況は様変わりしたのか？

この攻撃では、司法・捜査当局がランサムウェアオペレーターに勝利したものの、ネットワーク防御担当者は警戒を緩めてはなりません。適切なセキュリティプラクティスを常に心掛けない限り、ランサムウェア攻撃と防御のイタチごっこは続きます。

2021 年 5 月 7 日、ランサムウェアを運営する Darkside のアフィリエイトが Colonial Pipeline 社に 攻撃 を仕掛けました。これにより米国東海岸一帯での石油・ガスの輸送が被害を受け、ガソリンなどの価格が急騰し、同社は市民はもとより、米国政府や司法・捜査当局からも非難を浴びました。

このインシデントから数日後、Darkside を運営するサイバー攻撃グループ GOLD WATERFALL が「おそらく捜査当局の手によって、我々の外部通信用インフラへのアクセスが遮断された」という声明を出し、「5 月 13 日付でランサムウェア・アズ・ア・サービス (RaaS) プログラムの運営を終了する」と発表しています。同グループはさらに、被害企業すべてに復号ツールを配布することを約束しましたが、実際に配布したという証拠はほぼ皆無です。6月7日に米国司法省 (DoJ) は、63.7 ビットコイン (230 万ドル相当) を回収したことを発表しました。この金額は、ランサムウェア攻撃を受けた Colonial Pipeline 社が支払った身代金のうち、Darkside のアフィリエイトが関与した部分に相当するものと見られます。

他のランサムウェア攻撃グループもこれに反応しました。ランサムウェアオペレーターである Avaddon は「アフィリエイトによる公共機関への攻撃が禁止され、標的企業のシステムに侵入することができなくなった」と発表し、ほどなくして 6 月に入るとランサムウェアの運営を全面停止しました。また、ランサムウェア REvil を運営する攻撃グループ GOLD SOUTHFIELD は、RaaS の展開を停止しました。XSS や RaidForums などの闇フォーラムは、ランサムウェア関連の投稿を禁止しました。

これらとは別に 6 月 16 日、さらなるランサムウェア撃退のニュースが捜査当局から発表されました。ウクライナ警察が、ランサムウェア Clop を運営する GOLD TAHOE のメンバー 6 人を 逮捕したというニュースです。

こうした動きから「ランサムウェアの脅威に対するセキュリティ対策全般の潮目が変わった」と考えられるでしょうか？実際の件数を見ると、そうではないことがわかります。Colonial Pipeline 社への攻撃の数日前の時点で、当社 CTU リサーチャーが監視する Name and Shame (暴露型攻撃) のサイトに新たに情報を暴露された企業の 4 月度総数は 229 社でした。5 月にはさらに増加し、当社が 2019 年に月次統計を開始して以来 3 番目に高い 235 社となりました。

さらに、暴露サイトに公開されている数は被害企業のほんの一部であると思われます。たとえばAvaddonは、その活動期間を通じて182社を暴露サイトに公開していますが、運営を停止する際、被害企業に対する復号キーとして 2,934個の個別キー をリリースしています。

また、GOLD TAHOE メンバーが逮捕されて数日後、同グループの暴露サイトに Clop 攻撃の被害企業名がさらに追加されました。ランサムウェア Babuk のオペレーターは 2021 年 4 月下旬に「データ窃取や恐喝目的のランサムウェアの展開を中止した」という声明を出したものの、新たな暴露サイトに被害企業の名前を次々と追加し、「我々はランサムウェアの新バージョンを開発した」とうそぶいています。それだけでなく、ランサムウェア Babuk を他の攻撃グループにも広めるために、Babuk ビルダー (旧バージョンの開発ツール) を公開しています。

ランサムウェア攻撃グループの活動レベルには波があり、個々のグループが淘汰されることもあります。しかし、別のランサムウェアから 派生する ランサムウェアファミリーの新種や亜種が続々と出現しています。ネットワークを守るには、防御の手を緩めてはなりません。

上記を踏まえ、ぜひ実行してほしいアクション：
ランサムウェア侵入の兆候を早期に特定できるよう、エンドポイントおよびネットワークトラフィックを監視しましょう。

攻撃戦術は変われど、依然として汎用ツールを使った攻撃が主流

高いスキルをもつ国家ぐるみの脅威アクターは、攻撃の戦術、手法、手順 (TTP: tactics, techniques, procedures) を標的に合わせて柔軟に適応させています。しかし、攻撃の目的を遂行するために用いられる主な手段は、汎用的なペイロードなどです。攻撃ツールとしてよく使われる Cobalt Strike などの使用状況を監視することが、サイバー犯罪や国家ぐるみの攻撃者から自組織を保護するための一助となります。

Microsoftは 2021 年 5 月と 6 月に、ロシア政府を後ろ盾とする IRON RITUAL (別名 NOBELIUM) による新たな攻撃キャンペーンが仕掛けられたとの情報を公開しました。IRON RITUAL は、SolarWinds のサプライチェーン侵害を実行した高度標的型攻撃 (APT) グループで、ロシアの対外情報庁 (SVR) とのつながりをもつ集団です。

最初の攻撃キャンペーンでは、スピアフィッシング攻撃のメールが 350 以上の政府機関や政府間組織 (IGO)、非政府組織 (NGO) に送りつけられました。被害に合った組織には、ウクライナでの汚職撲滅運動や紛争調停、欧州連合域内における偽情報の監視、米国政府による対外援助の分配などを担当する団体が含まれていました。2 回目の攻撃キャンペーンでは米国やイギリス、ドイツ、カナダ、その他 32 カ国の IT 企業、政府機関、NGO、シンクタンク、金融機関が狙われました。

これらの攻撃キャンペーンで使用された TTP は、SolarWinds 攻撃で使われた TTP とは対照的です。標的組織の属性はどちらも似ていますが、SolarWinds 攻撃の際は、ごく小数の高額ターゲットのシステムに IRON RITUAL が秘密裡に侵入し、手の込んだサプライチェーン侵害を引き起こしました。一方、5 月に報告されたスピアフィッシング攻撃は配信されたメールの数が多く、大々的に展開されました。また、ユーザーに対していくつものアクションを実行させてから、侵害されたシステムへの永続アクセスを確立するマルウェアがインストールされるという内容でした。2 回目の攻撃キャンペーンでは、ログイン認証情報を推測するために攻撃グループから大量のパスワードが送信されました。この手法は検知しやすく、比較的簡単に防御できます。

最初の攻撃キャンペーンでは、市販ソフトウェアツールの Cobalt Strike も使われました。このツールはセキュリティテストの認定機関で広く採用されていますが、違法版が APT 攻撃グループやサイバー犯罪者によって頻繁に悪用されています。IRON RITUAL も例に漏れず、SolarWinds 攻撃の際にこのツールを使いました。こうした汎用ツールを使って初期アクセスを確立した脅威アクターは、手の内を明かすことなく標的組織に侵入し、足場を固めることができます。また攻撃者がこうした汎用ツールを使っているという事実だけでは、単なるサイバー犯罪者なのか、国家ぐるみの脅威アクターなのかをネットワーク防御側で識別できないため、攻撃元の特定がより困難になります。

IRON RITUAL および、他の APT 攻撃グループが使った TTP に関する詳細情報は、米サイバーセキュリティ・インフラセキュリティ庁 (CISA)、英国家サイバーセキュリティセンター (NCSC)、米連邦捜査局 (FBI)、米国家安全保障局 (NSA) が 5 月上旬にリリースした共同アドバイザリーに掲載されています。CISA と FBI は 5 月下旬に追加のアラートを公表しています。

上記を踏まえ、ぜひ実行してほしいアクション：
侵入の早期兆候を見極めるためのエンドポイントやネットワークトラフィックの監視時に、Cobalt Strikeなどの汎用的な攻撃ツールが使われた痕跡がないかチェックしてください。

攻撃者に最も狙われやすい「統制の抜け穴」

ネットワーク防御は決して簡単ではありませんが、攻撃者の大半は高度な手腕を持ち合わせていません。主な攻撃ベクトルは広く周知されているため、その使用を未然に防ぐことができます。攻撃者が活動しにくい状況を整備することで、攻撃リスクを低減できます。

当社の CTU リサーチャーは、様々な動機をもつ攻撃グループの動向を幅広く追跡しています。金銭目的の集団もあれば、NGO の監視、反体制派の動向把握、選挙の妨害などを中心に活動する集団もあります。これらすべてに共通する属性は、「標的ネットワークにたやすくアクセスできる方法が好まれる」ということです。たとえば、強度が低い/改ざんされた認証情報、パッチ未適用の脆弱性、保護されていないリモートサービス、単一要素認証、監視の不備などが狙われます。

CTU リサーチャーがまとめた脅威インテリジェンスのトレンドレポート (5 月・6 月版) では、これらの実例 (攻撃者に侵入されやすい状況) をいくつかご紹介しています。

- 攻撃グループのGOLD ULRICKは、長年使用され、検知方法も確立されているツールを使って2021年はじめにランサムウェア Ryuk による攻撃を実行しました。
- 別の攻撃者は、Office 365メールアカウントの認証情報を不正利用し (よくあるパスワードの試行など)、標的組織のネットワークを侵害しました。この組織では、侵害された Office 365 アカウントに多要素認証を実装していなかったため、攻撃者による受信ボックスへの侵入を許してしまいました。
- セキュアワークスのインシデント対応サービスでネットワーク侵入事案を調査した結果、マルウェア感染した Zoom インストーラーファイルを外部ウェブサイトからダウンロードしたことが原因だったという事例もありました。

- さらに、ある利用者が悪質なウェブサイトからメッセージングアプリをダウンロードしたことで発生したインシデントもありました。
- 既知の脆弱性が存在し、パッチが提供されているにもかかわらずパッチ未適用のシステムも攻撃者に狙われます。こうした攻撃が複数報告されています。

金融業界には何層にも重なるサイバーセキュリティ要件の準拠が義務付けられており、これまでの経験からセキュリティおよび適切な統制の重要性が充分理解されています。そのため必然的にランサムウェアの被害を受けにくい体質になっており、個々の金融機関が日常的に攻撃の阻止や侵入の早期検知・阻止に取り組んでいます。こうした組織は多要素認証を実装し、インターネット接続デバイスのセキュリティ強化、強力なパスワードおよびインターネットのダウンロードに関するポリシーの整備、迅速なパッチ適用を徹底しているだけでなく、既知の侵害痕跡を追跡するための包括的な監視ソリューションも導入しています。セキュリティに関するイベント (事象) が何も発生しないと脅威インテリジェンスの教訓事例として取り上げられにくいものの、「些細な見落としが攻撃者につけ込まれる」ということが改めてわかります。

上記を踏まえ、ぜひ実行してほしいアクション：
攻撃者の標的にならないために、基本的なセキュリティ統制を整備しましょう。

結論

実証済みのセキュリティ対策を展開することで、多くの攻撃を早い段階で防止/阻止できます。自社のエンドポイントやネットワークトラフィック全体に包括的な監視・対応システムを採用し、脅威に関する既知の指標をもとにアラートを発信する仕組みを構築しましょう。その際は、汎用ツールによる攻撃活動も監視してください。適切なセキュリティプラクティスと脅威インテリジェンスを組み合わせることで、脅威アクターが活動しづらい状況を作り、たやすく侵入できない環境を確立することができます。

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

United States
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 93218Saint 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 5DAUnited
Kingdom
+44(0)131260 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.4 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。