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 2

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 1 月から 2 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。

- 法執行機関、連携してボットネット Emotet を撲滅
- フロリダの水処理施設が侵害被害
- Scan and Exploit 被害者がランサムウェア暴露サイトに公開

法執行機関、連携してボットネット Emotetを撲滅

2021 年 1 月下旬、ヨーロッパと北アメリカの法執行機関が連携し、ボットネット Emotet の撲滅に成功しました。作戦を取りまとめた欧州刑事警察機構 (ユーロポール) は Emotetを「過去10年間で最も脅威あるボットネットの 1 つ」と位置づけています。2016年以来、ボットネットは Pay-per-install (ペイパーインストール方式) で運用され、攻撃者に代わってマルウェアを拡散してきました。当社でも常に、Emotet はお客様に影響を与える最も脅威あるサイバー犯罪の 1 つとしています。

ボットネットは、今は消失しているものの組織は警戒を怠ってはならない

法執行機関がインフラを掌握したため、Emotet を運営する攻撃者グループ GOLD CRESRTWOOD はボットネット全体にアクセスできなくなりました。その結果、感染している Emotet が無害化され、悪意のあるペイロードをそれ以上拡散できなくなりましたが、感染の初期段階によっては、無害化前の Emotet により既に TrickBot や Qakbot などの二次的マルウェアが投下されている恐れがあります。

本レポートの発行時点では、Emotet によるリスクは無効化されているかもしれませんが、GOLD CRESTWOOD が活動をしばらく停止するのは珍しいことではなく、法執行機関の作戦に大きく影響を受けないホスティングプロバイダーを利用して、新しいボットネットを作成し始めている可能性もあります。GOLD GRESTWOOD は、フィッシング詐欺の電子メールを開くよう、被害者を操る能力に長けているため、今後の活動を見据えた最初の攻撃ベクターとして、引き続きフィッシング詐欺を行う可能性が高いと考えられます。

重要なポイント

Emotet のテイクダウンは成功しましたが、当社の CTU リサーチャーは、投下された二次的マルウェアが他の脅威アクターに悪用されると被害が拡大する恐れがあるため、組織での警戒を維持することを推奨しています。自組織を守るためには、フィッシング詐欺の企てを認識し、報告するといった担当者向け研修の実施を含め、この種の攻撃から防御するための階層的アプローチを適用することが重要です。

フロリダの水処理施設が侵害被害

脅威アクターの身元は曖昧だが、教訓は明らかだ

2021 年 2 月 5 日、攻撃者が、フロリダ州オールズマーにある水処理施設のコンピューターネットワークにアクセスしました。悪用されたのはリモートデスクトップソフトウェア TeamViewer だと考えられています。攻撃者はアクセス後、浄水用化学物質の濃度を有害レベルにまで上げようとしましたが、オペレーターにより直ちに検知され、元の濃度に戻されました。この攻撃はメディアから広く関心を集め、現在、連邦法執行機関が調査を実施しています。

水道関連施設に対するこの種のサイバー攻撃は今回が初めてではなく、2020 年 4 月と 6 月には、イスラエルの水道関連施設が攻撃を受けました。この攻撃の容疑者としてイランの攻撃者が疑われるなど、水道関連施設やその他の公共施設などの重要なインフラ事業体は、政府が支援する攻撃者グループの恰好の標的となっています。オールズマーの事件を報道するメディアのほとんどが敵対国の関与を疑っていますが、施設に何らかの不満を抱く内部関係者や愉快犯による攻撃の可能性もあり、捜査当局は攻撃者を特定できていません。

最初に報告された攻撃は、オペレーターのワークステーション上でカーソルの動きが見て取れ、攻撃が容易に検知できたことから、攻撃者が基本的なトレードクラフトを使用していたことを示唆しています。旧式のオペレーティングシステムの使用、ファイアウォールの欠如、TeamViewer パスワードの共有など、サイバーセキュリティの脆弱性が複数存在していたため、同施設はスキルレベルを問わずあらゆる攻撃者から侵害され得る環境にありました。

重要なポイント

優れたセキュリティハイジーンは、セキュリティ侵害により人々の命が危険にさらされる可能性のあるクリティカルなインフラ事業体にとって不可欠です。米国サイバーセキュリティインフラセキュリティ庁（CISA）は、各水処理施設に対し、一般的なセキュリティ侵害緩和に関するガイダンスやリモートコントロールソフトウェアの保護に関する推奨事項のほか、個々のインシデントに対する具体的助言を提供しています。

Scan and Exploit 被害者がランサムウェア暴露サイトに公開

ランサムウェアの攻撃者グループによる暗号化なし恐喝の試み

2020 年 12 月中旬、未知の攻撃者が、Accellion File Transfer Appliance（FTA）デバイスに対し、日和見的な Scan and Exploit（スキャンとエクスプロイト）キャンペーンを行い、2 つの新しいエクスプロイトを組み合わせて使用し、10 以上の組織から機密データを窃取しました。Accellion は対応対抗策として、直ちに脆弱性を塞ぐパッチを発行しましたが、攻撃者は別の新しいエクスプロイト 2 つの組み合わせを使用して、2021 年 1 月に 2 回目の攻撃を行いました。

Clop ランサムウェアを運営する攻撃者グループ GOLD TAHOE が、被害者名および窃取したデータを Clop 暴露サイトに公開したことで被害は大きくなりました。同サイトは、Clop ランサムウェアの被害者への Name and Shame (暴露型攻撃) とその後の身代金要求に利用されたことがありましたが、今回のキャンペーンでは Clopランサムウェアはデプロイされていませんでした。データは被害組織のネットワークからではなく、Accellion FTA ソリューション内のファイルから盗まれており、また、組織のネットワークに侵害された形跡はありませんでした。GOLD TAHOE が自らデータ窃取を試みたのか、自身の暴露サイトとその評判を利用して、その後の恐喝をあおる役割を担ったのかは不明です。

今回の活動は、二重脅迫型ランサムウェア攻撃が新たなステージに入ったことを示唆しています。攻撃者は、侵入してからランサムウェアをデプロイするという時間のかかる方法ではなく、手っ取り早い Smash and Grab (ショーウィンドウ破り) 型の攻撃でデータを窃取する方法を選ぶでしょう。その後、窃取したデータの公開をちらつかせ、被害者や影響を受ける可能性のあるその他の利害関係者に対し、データの返却や削除と引き換えに、身代金を要求します。

重要なポイント

組織はシステムへのパッチ適用によるネットワーク境界の強化、ネットワークの分離、多要素認証の導入に加え、攻撃対象領域を最低限の重要クリティカルなサービスに狭めることでランサムウェアとデータ窃盗の被害を抑えることが可能です。オンプレミス環境およびクラウド環境では、エンタープライズ検出応答 (EDR) ソリューションのデプロイ、拡張型検出対応 (XDR) プラットフォーム経由によるセキュリティテレメトリの収集により、データの盗難やランサムウェアのデプロイが発生する前に侵入を可視化、早期検出する必要があります。CISA アラート AA21-055A は、Accellion FTA ユーザに対し緩和および修復ガイダンスを提供しています。

結論

脅威の状況は絶えず変化しています。攻撃者は戦術を進化させることで、収益の最大化と投資の最小化を図っています。法執行機関からの妨害に直面することもありますが、同じ手口や新しいアプローチを利用して、悪意のある活動を再開することもあります。表面上は同じよう見えるインシデントでも、根本的原因が異なることもあります。その要素は広範囲かつ様々ですが、優れたセキュリティプラクティスが不可欠であることに変わりはありません。定期的にシステムにパッチを適用し、検出と応答のソリューションを実装し、多要素認証を採用することにより、様々な脅威から組織を保護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
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
044-556-4300
www.secureworks.jp

※ 本文書は www.secureworks.com で公開されている Threat Intelligence Executive Report 2021: vol.2 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。