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 5

カウンター・スレット・ユニット™（CTU）
リサーチチーム

//Secure

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、企業や組織のシステム保護を支援しています。2021年 7 月から 8 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。

- 名称を変えて活動を続ける攻撃者
- ランサムウェアのエコシステムを理解する
- パッチ適用以外の修復方法について

名称を変えて活動を続ける攻撃者

ランサムウェア攻撃グループが消え去ったわけではありません。ランサムウェアは依然として、大小問わずすべての組織にとって大きな脅威であり、攻撃規模が縮小する可能性は低いでしょう。

前回のレポートでは、「2021年5月に発生した Colonial Pipeline 社への 攻撃 を受けて司法・捜査当局がランサムウェア運営組織に法的措置をとったとしてもランサムウェアエコシステムが消滅することはなく、再びかつての勢いを取り戻すだろう」と CTU リサーチャーの予測しました。7月から 8 月にかけての傾向を見ると、この予測が正しかったこと、および攻撃グループが運営面での制約をどのようにすり抜けて新たな状況に適応しているのかがわかります。

当時、ランサムウェア Darkside、Avaddon、Revil を運営する攻撃グループは活動停止の様相を呈しており、複数の闇フォーラムがランサムウェアに関するやり取りを禁止しました。しかし、新たな Name and Shame (暴露型攻撃) グループと見られるランサムウェアグループが少なくとも7つ浮上しています。また、特定されないように軽く偽装したランサムウェア関連の投稿がアンダーグラウンドフォーラムに次々に掲載されています。

新たなランサムウェアファミリーのなかには、AvosLocker、Hive、Hotarus、Vice Society のような100%新種と思われるものもありますが、既知のランサムウェアファミリーを改称 (リブランド) しただけのものもあります。米財務省外国資産管理局 (OFAC) の 制裁 リストに記載された攻撃グループとの関連性を疑われないために名前を変えている可能性もあります。

- 攻撃グループ GOLD DRAKE から枝分かれした GOLD HERON が、ランサムウェア DoppelPaymer を「Grief」という名称に変え、攻撃を再開しました。

- GOLD DRAKE による最新ランサムウェア「Payload.Bin」は、ランサムウェア運営組織 Babuk が開設した暴露サイトと同じ名前です。こうした偽装は、GOLD DRAKE (別名Evil Corp) に対する米財務省の 制裁 回避を狙ったものと思われます。
- GOLD WATERFALL は 5 月 13 日にランサムウェア Darkside の運営を停止しました。しかし、名称を「BlackMatter」に変えて存続していることが当社 CTU の調べで判明しています。外部リサーチ機関によるランサムウェアサンプルおよび暗号通貨ウォレットの分析の結果、当社の見識が正しかったことが 裏付けられています。
- 活動停止を発表したランサムウェア Avaddon の運営グループは被害企業に復号キーを配布しましたが、Avaddon に よく似た特徴をもつ ランサムウェア「Haron」が新たに出現しました。

さらに、解散したランサムウェア運営組織と協力関係にあった加盟メンバーは、別の攻撃者を探して手を組み、活動を続けている模様です。攻撃グループ GOLD MYSTIC が運営するランサムウェア LockBit に関する攻撃活動が増加している一因は、こうした加盟メンバーの移動によるものと考えられます。LockBit を使った攻撃活動は 7 月中旬から急増しており、2020 年 9 月 (暴露サイト開設時) の被害企業数はわずか 9 社でしたが、今年 8 月 27 日には 144 社に跳ね上がっています。暴露サイトには、速やかに身代金を支払わなかった企業だけが掲載されるため、実際に被害を受けた企業の数はさらに多い可能性があります。

アンダーグラウンドフォーラムでは、「加盟メンバー募集」というはっきり募集から、「侵入テスト担当者」をはじめ、職種をぼかした求人広告が掲載されるようになっています。アンダーグラウンドフォーラム運営者は 5 月にランサムウェア関連の投稿を禁止したものの、掲載内容はほとんど変わっていないように見えます。その一因は、攻撃に関する重要なやり取りの大半はすでに Telegram などの非公開チャネルを介して実施済みであること、さらに全面禁止してしまうとサイト内で発生したトランザクションで手数料を稼ぐアンダーグラウンドフォーラム運営者の収益がマイナスになってしまうためだと思われます。

たとえ攻撃者がロシアや CIS 諸国内にとどまることで司法・捜査当局の制裁を免れたとしても、サイバー犯罪に対する規制当局の措置は抑止力として期待できます。しかし、成熟化の一途をたどるランサムウェアから自社・自組織を守るには、その動向を注視し、効果的な防御態勢を維持する必要があります。

上記を踏まえ、ぜひ実行してほしいアクション：
脅威動向の進化を完全に把握できる外部組織と協力して取り組みましょう

ランサムウェアのエコシステムを理解する

ランサムウェアグループは攻撃の初期段階で得た情報をもとに、攻撃対象を慎重に選んでいる可能性がありますが、「標的」を限定するわけではありません。攻撃者は、企業ネットワークへのアクセス権をアンダーグラウンドフォーラムでランサムウェアグループや傘下の加盟メンバーに販売しているため、基本的なサイバー衛生を徹底しない限り、どのような組織であっても標的にされる恐れがあります。

ランサムウェアの運営組織と加盟メンバーの役割分担はよく知られていますが、不正アクセス仲介人 (IAB: Initial Access Broker) の役割についてはあまり知られていません。不正アクセス仲介人とは、企業の社内環境への初期アクセス権の窃取を専門とする仲介人であり、アンダーグラウンドフォーラムで数多くの不正アクセス権を販売しています。Ransomware-as-a-Service (RaaS) グループや傘下の加盟メンバーのほか、個別に活動するランサムウェアグループも不正アクセス仲介人を利用しています。

不正アクセス仲介人の役割は、防御態勢が手薄な組織を物色することです。主に、市販のスキャンツールを使って脆弱性を特定し、発見された抜け穴を無差別に攻撃します。アクセス権を入手してネットワークを侵害したら、基本的な調査を行い、身代金支払いの観点で有望なターゲットになりそうか、アクセス範囲をさらに拡大できそうかを判断します。

ランサムウェアグループが不正アクセス仲介人から企業ネットワークへのアクセス権を購入する場合、対象企業の業種や国名のほか、初期アクセスの攻撃手段 (RDP、VPNなど) の情報が買い手側に開示されるケースが一般的です。対象企業の売上高の目安が開示されることもありますが、多くのケースではアクセス権の購入が確定するまで企業名は知らされません。最近では固定価格ではなく入札形式で価格を決める不正アクセス仲介人も増えています。

ランサムウェアグループや加盟メンバーは、対象企業の売上高や、場合によっては業種を考慮したうえでアクセス権を購入するか否かを決定します。不正アクセス仲介人から取得したアクセス権を行使するか否かは、実際に購入した後に追加調査を実施したうえで判断します。つまり、この時点ではランサムウェアの標的は確定していません。境界線防御が不十分な組織は、ネットワーク侵害およびその後のランサムウェア感染リスクと常に隣り合わせの状態と言えます。

上記を踏まえ、ぜひ実行してほしいアクション：
外部に公開されているシステムすべてにパッチが適用されていることを確認しましょう

パッチ適用以外の修復方法について

リスクベースの手法を用いて脆弱性の優先順位を付けると、パッチ管理が容易になります。リスク軽減の手段として、「攻撃対象領域の縮小」を検討しましょう。

Microsoft は毎月第 2 火曜日に、業界最大規模のセキュリティアップデートを配信しています。7 月から 8 月にかけて発見された重大な脆弱性は、印刷スプーラーに影響を及ぼすPrintNightmare と、オンプレミスの Microsoft Exchange サーバーに影響を及ぼす ProxyShell の 2 種類がありました。いずれも公表後まもなく、ランサムウェア グループに悪用されたことが 報告されています。

脆弱性が世間の注目を集め、現在進行形で悪用されている事実が知れ渡ると、様々な情報が飛び交うため、対応の優先順位が迅速に決定できないことがあります。たとえば「PrintNightmare の公式パッチでは脆弱性を完全に対処できない」など、さらなる混乱を招くような 報道 もあります。ProxyShell のケースのように、攻撃が公になる前にリリースされたパッチが見過ごされることもあります。

攻撃を受けている脆弱性について当社 CTU リサーチャーからお客様に注意喚起する際は必ず「適宜、パッチを適用すること」を推奨しています。パッチがリリースされる都度、すぐに適用することが理想的です。パッチ適用は、最も効果的な防御手段のひとつであり、適用が遅れると侵害される可能性があります。

しかし現実は理想どおりにはいきません。たとえば、Microsoft Exchange に関するパッチは通常、Exchange Server ソフトウェアの最新リリース固有のパッチのため、最新版以外のソフトウェアを使っている場合は、パッチ適用の前にソフトウェアを更新する必要があります。

パッチ管理が大きな業務負担となる恐れもあります。National Vulnerability Database には、毎月 2,000 件にのぼる新たな脆弱性の報告が寄せられています。ごく普通の組織に必要なパッチは毎月わずか数百件程度かもしれませんが、リスクベースの手法を用いて対応の優先順位を付ける必要があります。たとえば、攻撃が発生中の脆弱性は優先度が高くなりますが、アクセス不可能な場所やネットワークの最深部付近に保管されている IT 資産の脆弱性であれば優先度が低くなります。組織全体でリスクを評価し、脆弱性が悪用される可能性および、その際の影響度を確認しておきましょう。

修復手段はパッチ適用以外にもあります。大きく報道されている脆弱性であっても、補完的なコントロールや緩和策が整備されている場合は優先順位を下げて構いません。攻撃対象領域の縮小および、OS の最小化・堅牢化も、パッチ関連業務の負担軽減に役立つプロアクティブな防御手段です。

組織として必要な基本タスクを定期的に実行することが、パッチ管理、リスク評価、補完的コントロールの基盤となります。以下は実行すべき基本タスクの一例です。

- 未知のデバイスにはパッチを適用しづらいこともあるため、ハード/ソフト資産の棚卸をしておく
- ハード/ソフトの脆弱性スキャンを実行し、セキュリティの更新情報や修復状況を監視する
- 優先順位の高い脆弱性にはただちにパッチを適用する
- エンドポイントに通常と異なるふるまいがないか監視する。攻撃者がパッチ未適用の脆弱性を悪用している場合、攻撃チェーンの最初の段階で検知することで、ランサムウェアの展開を阻止できる

上記を踏まえ、ぜひ実行してほしいアクション：
最後にソフト/ハード資産の棚卸を行った時期がいつだったのか確認しましょう

結論

攻撃者は状況の変化への適応性がきわめて高く、運営上の制約に合わせて素早く形態を変えて再浮上します。攻撃者に遅れを取らないためには、脅威動向の変化を常に把握し、社内システムの脆弱性やエンドポイントの不審なふるまいに目を光らせるなどの活動を含めた「監視」が有効です。

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.jp

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)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
100-8159
東京都千代田区大手町一丁目２番１号
Otemachi Oneタワー17階
03-4400-9373
www.secureworks.jp

※ 本文書は www.secureworks.com で公開されている Threat Intelligence Executive Report 2021: vol.5 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。