SOPHOS
Cybersecurity delivered.

複数の攻撃者:
今そこにある危機

クリプトマイナーや RAT の間では激しい競争が繰り広げられていますが、ランサムウェアはその流れに逆らっています。

ソフォスの MDR (Managed Detection and Response) チームと RR (Rapid Response) チームは、その設立以来、何百件ものランサムウェアインシデントの調査を依頼されてきました。時には、まだ標的ネットワーク上で活発に行われている攻撃に介入することもあります。

ここ数か月の間、ソフォスは攻撃を複数回受ける組織が増えていることに気付きました。複数の攻撃が同時に行われることもあれば、数日、数週間、数か月の間隔をおいて行われることもあります。また、異なる種類のマルウェアが使われているケースや、同じ種類のマルウェアに 2 重、3 重に感染しているケースもあります。

何度も攻撃を受けると、壊滅的な被害となる可能性があります。修復や事業継続計画に支障をきたすだけでなく、経済、風評、および心理の面での影響も計り知れません。今回の調査結果から、同じ組織が複数回攻撃を受けた場合、攻撃の間隔は通常 6 週間であると考えられます。

ソフォスでは、特定の標的に対して複数回攻撃が実行される方法 (および理由) を調査することにしました。MDR チームと RR チームによる最近のケーススタディでは、こうした攻撃が**どのように**行われるかが説明されています。また、攻撃者間の協力と競争に目を向けることで、その**理由**は明らかになります。本書では、この分析に基づき、複数回攻撃を防止するための 8 つのアドバイスを提供します。

執筆者 : Matt Wixey (Sophos X-Ops)

目次

はじめに

サイバー攻撃の確率について、業界では次のフレーズがよく使われます。「『もし』ではなく、『いつ』の問題」。しかし、ソフォスの MDR (Managed Detection and Response) チームや RR (Rapid Response) チームが最近調査したインシデントの中には、業界にこの考え方の変更を迫るものがあります。問題は、「もし」でも「いつ」でもなく、「何回」かということです。

組織が複数回攻撃を受けるケースが急増しています。[1] 攻撃は同時に行われることもあれば、数日、数週間、数ヶ月の間隔をおいて行われることもあります。また、異なる種類のマルウェアが使われているケースや、同じ種類のマルウェアに 2 重、3 重に感染しているケースもあります。

根底にある原因はさまざまで、深刻な脆弱性や設定ミス、あるいは、攻撃者が次々に参入する脅威環境の中でリソースと支配権の奪い合いが発生していると考えられます。

根本原因が何であれ、複数回の攻撃は壊滅的な被害をもたらす可能性があります。修復や事業継続計画に支障をきたすだけでなく、経済、風評、および心理の面での影響も計り知れません。「ついに最悪の事態が起きてしまった」と思い、本当に「もし」ではなく「いつ」の問題であったことを確信した次の瞬間、別の攻撃に見舞われることになるのです。今回の調査結果から、同じ組織が複数回攻撃を受けた場合、攻撃の間隔は通常 6 週間であると考えられます。

ソフォスでは、特定の標的に対して複数回攻撃が実行される方法 (および理由) を調査することにしました。MDR チームと RR チームによる最近のケーススタディでは、こうした攻撃がどのように行われるかが説明されています。また、攻撃者間の協力と競争に目を向けることで、その理由は明らかになります。本書では、この分析に基づき、複数回攻撃を防止するための 8 つのアドバイスを提供します。

不幸な出来事の積み重ね

多くの複数回攻撃の根本原因は、次の2点に集約されます。1つは、攻撃対象がソフトウェアまたはハードウェアの重大な脆弱性に対処していないこと、もう1つは、攻撃後に被害者が、先の攻撃者が残していった悪意のあるツールやハードウェア/ソフトウェアの設定ミスに対処していないことです。

しかし、それ以上に複雑な問題があります。以下に紹介するケースからもわかるように、まず「炭鉱のカナリア」にあたるクリプトマイナーが侵入し、その後にワーム型ボットネット (Mirai など) 、IAB (Initial Access Broker: 初期アクセスブローカー) にデータを供給するマルウェア配信システム (Web シェルや RAT)、そして最後にランサムウェア、というように、多くの攻撃は特定の順序で実行されます。

これら攻撃者の一部は相互依存関係にあります (たとえば、IAB のおかげで一部のランサムウェア攻撃は可能になっています)。また、共存しているものもあります。たとえば、クリプトマイナーとランサムウェアは目的が異なるため、互いに直接干渉する理由がありません[2] (ただし、ランサムウェアはクリプトマイナーの設定ファイルや Web シェルなどの他の攻撃のアーティファクトを暗号化し、これらの攻撃を不活性化させる可能性があります)。

複数のランサムウェア攻撃を受けた組織も確認されていますが、これは攻撃者がそれまでの感染を知らなかったり、単に意に介さないだけであったりするためです。以下のケーススタディの 1 つでは、ランサムウェアに *3 回*感染し、一部のファイルが 3 種類のランサムウェアによって暗号化されています。このケースでは、3 番目の攻撃者が自身の攻撃の痕跡だけでなく、前の 2 つの攻撃の痕跡も消去してしまったため、調査が困難になりました。

その一方で、攻撃者の中には協力し合うことなく、他の感染や脅威を積極的に妨害するものもあります。たとえば、CPU リソースには限りがあり、同時感染で得られる収益は少ないため、クリプトマイナーは他のクリプトマイナーのプロセスを終了させようとします。もちろん、例外もあります。Outlaw などのクリプトマイナーは、多くのライバルとは異なる標的 (ブルートフォース SSH 攻撃による IoT デバイスや Linux サーバーへの攻撃) に焦点を当てているため、競合については無関心です。そのようなクリプトマイナーにも「キルスクリプト」があるかもしれませんが、使用する必要はほとんどありません。[3]

攻撃者間の関係については以下で詳しく説明しますが、その前に、大きな脆弱性が複数回攻撃につながる例をいくつか見ておきましょう。

大きな脆弱性

ProxyLogon (CVE-2021-26855[4]) の脆弱性は 2021 年 3 月、ProxyShell (CVE-2021-34473[5]、 CVE-2021-34523[6]、CVE-2021-31207[7]) の脆弱性は 2021 年 8 月に初めて公開されました。当時、ProxyLogon と ProxyShell の両方を大々的に取り上げましたが[8、 9]、その後の調査で、Lemon Duck[10] や Tor2Mine[11] などのクリプトマイナーがいち早く悪用していたことが判明しました。Tor2Mine は、他のクリプトマイナー、RAT、クリッパー (ユーザーのクリップボード上の暗号通貨ウォレットのアドレスをスワップするマルウェア) など、70 以上の競争相手に関連するプロセスを強制終了するように設計された、高度に難読化された 116 行の専用 PowerShell スクリプトまでも装備しています。マルウェア配信ボットネット「Squirrelwaffle」も、2021 年に ProxyShell を悪用しています。[12]

そして、ランサムウェアの登場です。ProxyLogon と ProxyShell を悪用する初期の亜種は、パッチが適用される前に脆弱なホストを悪用するように開発されたためか、比較的粗雑なものであったようです。そうした初期の亜種には、2021 年 3 月に企業・組織を攻撃対象とした DearCry[13] や Black Kingdom ランサムウェア[14] などがあります。

8月には新種のランサムウェア「LockFile」[15] が発見され、2021 年 9 月には Conti アフィリエイトの攻撃がありました。2022 年 2 月には、Conti と Karma ランサムウェアのアフィリエイトが同時にある医療機関を攻撃しているのを確認しました[16] (この件に関しては、この 2 つのグループの間に興味深い動きが見られたため、後ほど詳しく説明します)。

ProxyLogon/ProxyShell を悪用する攻撃者は、多くの場合、侵入先のサーバーに Web シェルをドロップしていきます。セキュリティ侵害を受けているにもかかわらず、パッチ適用後にクリーンアップを行わなかった組織では、パッチ適用済みの Exchange サーバー上にこれらのバックドアや攻撃者が作成したメールアカウントが多数存在しており、今後攻撃者によって使用または販売される可能性があります。

2021 年 12 月に公開された Log4Shell (CVE-2021-44228[17]) も、同様の経緯をたどりました。PoC (概念実証) が公開されてからの数日間は、予想されたほどの攻撃は発生しなかったものの、かなりの量のスキャン活動[18] が観測されました。この小康状態は続かず、すぐにクリプトマイナーが登場しました[19] (その直後、IAB によって Web シェルやバックドアが展開されました)。また、前述した通り、その多くが他のクリプトマイナーを強制終了させる機能を搭載していました。

興味深いことに、上記リンク先のレポートで調査されているクリプトマイナーの「Jin」は、Log4Shell に対して脆弱な Tomcat サービスを終了させ、他の攻撃者がこの感染経路を利用することを防止しているようです。侵入した後に攻撃者がドアに鍵をかけることは、それほど一般的ではありませんが、実際に起きています。この点については後ほど詳しく説明します。

Atlassian で最近発見されたリモートコード実行の脆弱性[20] (CVE-2022-26134[21]) の悪用は、今のところ同じパターンで実行されています。以前お伝えしたように、Atlassian の脆弱性を悪用した攻撃者は、さまざまなペイロード (クリプトマイナーや Web シェルなど) を配信し、その後しばらくしてからランサムウェアを試みているのが確認されています。

要点 1: あらゆるものにアップデートを

簡単なことだと思われるでしょうが、すべてをアップデートすることが重要です。今回の調査での主な発見の 1 つは、脆弱性が公表されて最初に登場するのがクリプトマイナー、そして、IAB によって展開される Web シェルやバックドアであることが多く、後者は通常、ステルス的に動作しようとする、ということです。そのため、攻撃を回避していたつもりでも、実際はすでにマルウェアに感染していた、という事態が発生します。このような場合、その後のランサムウェア攻撃によって、事態がさらに深刻化する可能性があります。早期にパッチを適用することは、将来的に被害を受けないようにするための最善の方法ですが、だからといって、パッチを適用した時点でまだ攻撃を受けていないとは限りません。パッチを適用する前には必ず、まだ侵入されていないことを調査することが重要です。

要点 2: 最も深刻な脆弱性を最優先する

では、どうすればパッチを迅速に適用できるのでしょうか。また、適用すべきパッチをどのように判断すればよいのでしょうか。脆弱性の公開件数の多さ (2021 年は 18,429 件[22] で 1 日平均 50 件以上となり、過去最大の年間報告件数) を考えると、優先順位の決定は大きな課題です。そこで、1) 特定のソフトウェアスタックに影響を及ぼす重大な脆弱性、2) 自社のテクノロジーに影響を及ぼす可能性のある注目度の高い脆弱性、という 2 つの重要な要素に焦点を合わせます。脆弱性情報を有料で提供するサービスもありますが、特定の製品に関してカスタムアラートを設定できる無料のツールもあります。Bug Alert[23] は、影響力の大きい脆弱性を早期に警告する非営利のサービスです。また、注目すべき脆弱性が、最初にリリースされたときに議論される場である「infosec Twitter」をモニタリングすることも推奨されます。あるいは、複数のサイトからデータを収集し、最も話題になっている脆弱性を表示する CVE Trends[24] も活用してください。

開けっ放しのドア

リモートアクセスの設定ミス (たとえば、インターネットに公開され、セキュリティ対策が施されていない RDP サーバーや、RDWeb、AnyDesk などのアプリケーション) は、インシデント対応担当者が最初のインシデント発生後にその設定ミスに対処できていなければ、複数の攻撃を招く主な要因にもなります。次のケーススタディでは、最初の攻撃者は RDP を使用してアクセスに成功しました。そして、この問題が修正されなかったため、2 回目の攻撃につながりました。

ケーススタディ : 外部に公開されている RDP アプリケーションにより、5 週間で 2 件の攻撃が発生

2022 年 4 月 8 日: セキュリティ対策が施されていない RDP サーバーを介して、攻撃者が社内ネットワークにアクセスする。

4 月 12 日: Advanced IP Scanner[25] をインストールし、ネットワーク上の他のデバイスに関する情報を収集する。

4 月 13 日: さらに RDP 接続を確立して、管理者権限を持つ新規ユーザーを追加し、Mimikatz を実行する。[26]

4 月 19 日: キーロガーとリモートコマンド実行に関連する複数の PowerShell マルウェアステージャーをダウンロードする。

4 月 20 日: 企業側が脅威を除去。ソフォスの MDR チームが企業に対し、複数のホストについてインターネットからの RDP アクセスを無効にすること、感染したユーザーのパスワードをリセットすること、ドメイン全体の認証情報をリセットすることなど、いくつかの助言を行う。いくつかの助言は実行されず。

5 月 13 日: 第 2 の攻撃者が、前回の攻撃後にセキュリティ対策を講じるようソフォスが推奨したホストの 1 つに対し、RDP で認証を行う。Cobalt Strike[27] の活動が観察される。

5 月 27 日: 攻撃者 RDP で認証を行う。

5 月 29 日: 攻撃者は、ドメイン上で偵察を行い、アカウントの認証情報を改ざんし、レジストリハイブの保存を試みる。これに失敗すると、偵察を続け、別のホストに移動し、Active Directory 情報 (すべてのドメインユーザーのパスワードハッシュなど) のデータベースである **ntds.dit** ファイルをダンプする。攻撃者に人気のファイル共有サービスである **anonfiles[.]com** と **fex[.]net** に対する DNS リクエストが確認される。攻撃者は、少量のデータのアップロードに成功し、数分後に攻撃が停止する。

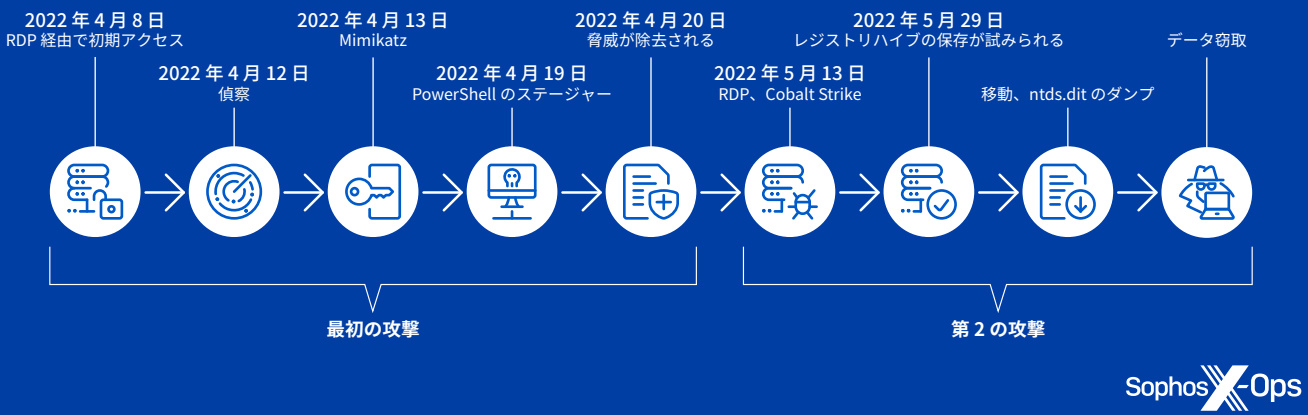

図 1: 時系列で見た攻撃

要点 3: 設定に注意する

設定ミスの存在や、攻撃を受けた後も設定ミスを修正できないことが、複数回攻撃が発生する主な原因です。クリプトマイナーのオペレーター、IAB、およびランサムウェアのアフィリエイトは、公開されている RDP ポートや VPN ポートを常に探しており、そうしたポートは多くの犯罪者向けマーケットプレイスで最も人気の高い商品の 1 つとなっています。インターネット経由のリモートアクセスや管理が必要な場合には、社内ネットワークとインターネットの間に VPN や、ログイン手順に MFA が組み込まれている ZTNA (ゼロトラストネットワークアクセス) ソリューションを設置してください。

最高金額での入札者にネットワークへのアクセスを販売する

注目を集めている脆弱性や設定ミスは、セキュリティ侵害につながる可能性があります。当然ですが、攻撃を受けた後に根本の問題を解決しなければ、別の攻撃者に悪用される可能性があります。実際、攻撃者が大規模にスキャンを行うことを考えると、その可能性は極めて高いと言えます。

しかし、複数回攻撃を引き起こす原因は、他にいくつもあります。クリプトマイナーとランサムウェアの優先順位の違いについては先ほど簡単に説明しましたが、ここでは、犯罪エコシステムのどのような特徴が複数回攻撃に関係しているかを詳しく見ていきましょう。

犯罪者は、犯罪者向けマーケットプレイスでネットワークへのアクセス権を IAB から購入します (これは、Access-as-a-Service (AaaS) とも呼ばれます[28])。IAB は、セキュリティ侵害が発生したことを被害者に気付かせたくないため、通常は商品リストから企業名や識別情報を削除しますが、買い手を引き付けるために業種、収益、ネットワークの規模、提供されるアクセスの種類などの詳細は表示します。最高額を入札した者に AaaS が競り落とされるケースもあります。また、売り手と個人的に交渉することもできます (通常は闇フォーラムとは別の Jabber や Tox などのチャットプラットフォームが使用されます)。

以下は、ロシア語の闇フォーラムに出品された典型的な AaaS の例です。

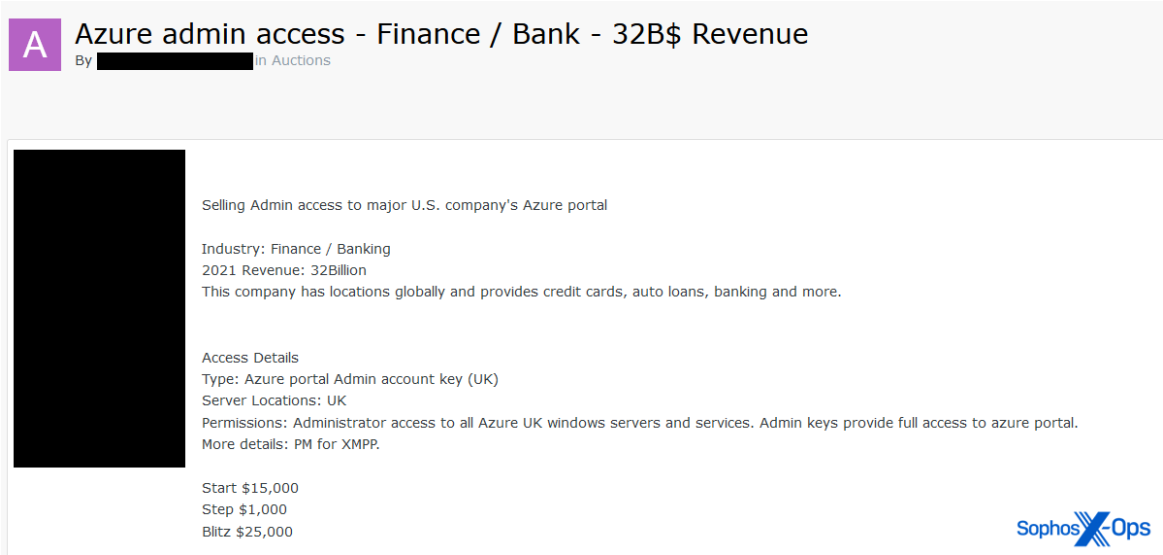

図 2: 犯罪者向けマーケットプレイスに出品された AaaS。このリストはオークションに出品されており、開始、ステップ、ブリッツ (即時落札) の各価格が提示されている

お気付きかもしれませんが、独占権についての言及がありません。このフォーラムの規約を見てみると、興味深いことがわかります。規約の 1 つを大まかに訳すと、次のような指示が書かれています。「商品が 1 回限りの使用である場合、または独占権が失われる場合には、その旨を一番上に明記するか、第一購入者と調整すること」つまり、出品者は、出品が独占的であるかどうかを明示することが求められています。

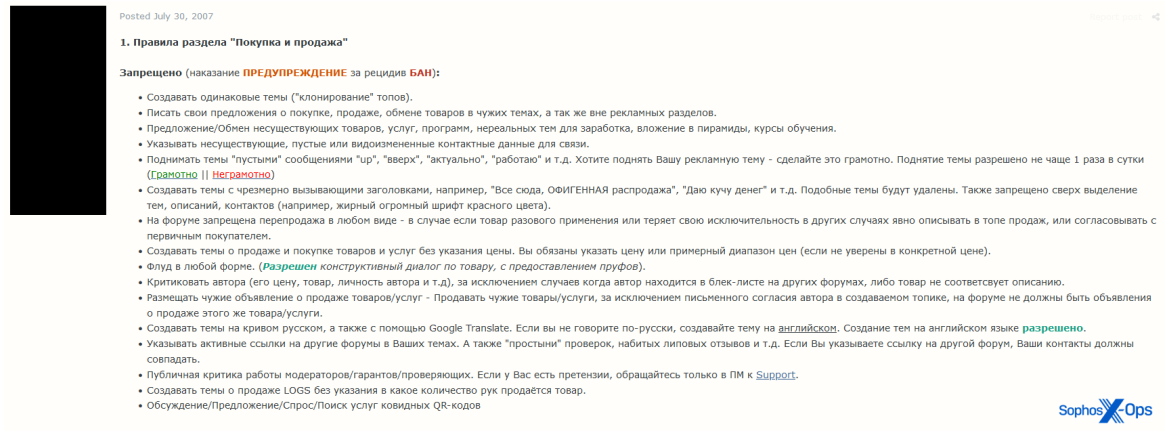

図 3: 売買に関するフォーラムの規約

以下は、「独占販売」と明記し、独占権を明示的に約束している例です。

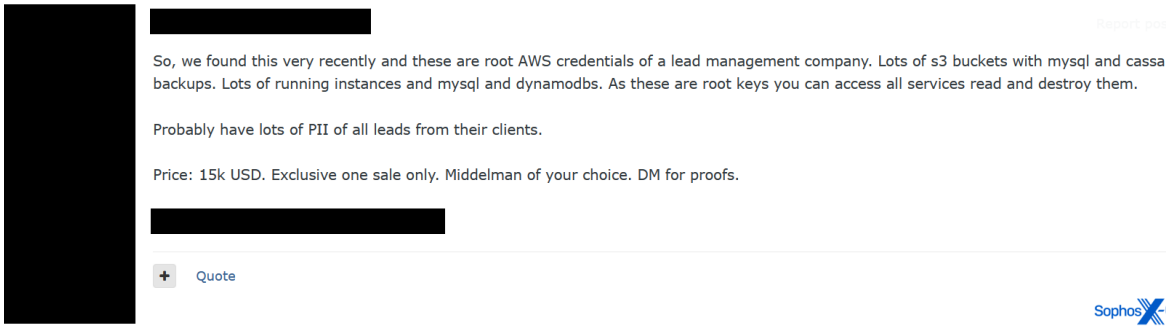

図 4: 犯罪者向けマーケットプレイスにおける独占販売

これはこのフォーラムに限ったことではありません。別の有名な犯罪サイトでは、出品者が次のように書いています。「通報を避けるため、**会社名は最終的な落札者にのみ開示します**。アクセスは独占的です。利益分配はありません。」[太字は原文ママ]

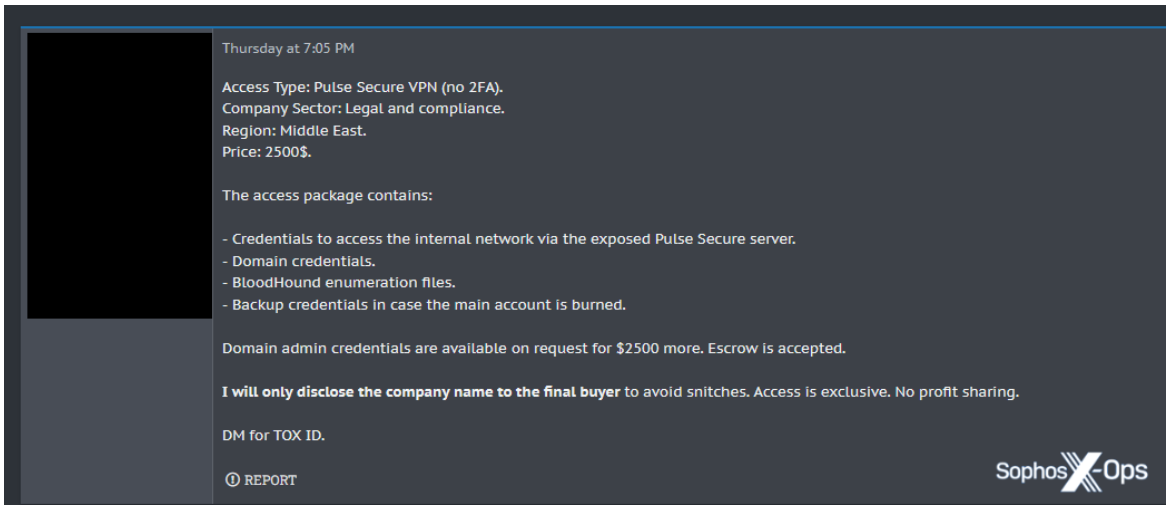

図 5: 別の犯罪者向けマーケットプレイスに掲載されている出品 (中東の組織への独占的 VPN アクセスを提供)

しかし、これらは例外であり、多くの商品には独占権に関する記載が全くありません。また、フォーラムでは一般的に転売が禁止されていますが、多くの AaaS は非独占的であり、需要の高まりに乗じて複数の購入者に販売されるため、結果として複数回攻撃が行われている可能性があります。実際、Genesis のようなマーケットプレイスでは、独占権を手に入れるには追加料金が必要な場合もあります。

興味深いことに、ランサムウェアのアフィリエイトメンバーもまた独占権を得られるとは限らず、複数のプログラムに所属している攻撃者もいるようです。たとえば、最近ソフォスが調査したケースでは、Hive と Conti というランサムウェアの亜種が戦略、コミュニケーションの方法、オペレーションセキュリティのレベルで顕著な違いがあるにもかかわらず、同じインフラストラクチャを共有していました。[29]

ケーススタディ : Hive と Conti の両方を使用するランサムウェアのアフィリエイト

2022 年 3 月、ソフォスの MDR チームは Conti ランサムウェアのインシデントに対応しました。攻撃者は MSBuild.exe[3] を悪用して **Cobalt Strike** を実行し、**edgecloud[.]ink** にビーコンを送信していました。

数日後、MDR チームは Hive ランサムウェアが関与している別のインシデントに対応しました。ここで攻撃者は再び **MSBuild.exe** を悪用して **Cobalt Strike** を実行し、同じドメインにビーコンを発信しました。

MDR チームはその後、インフラストラクチャが重複する複数の Hive ランサムウェアインシデントに対応していることから、この活動は同一のランサムウェアアフィリエイトによるものである可能性が高いと考えられます。

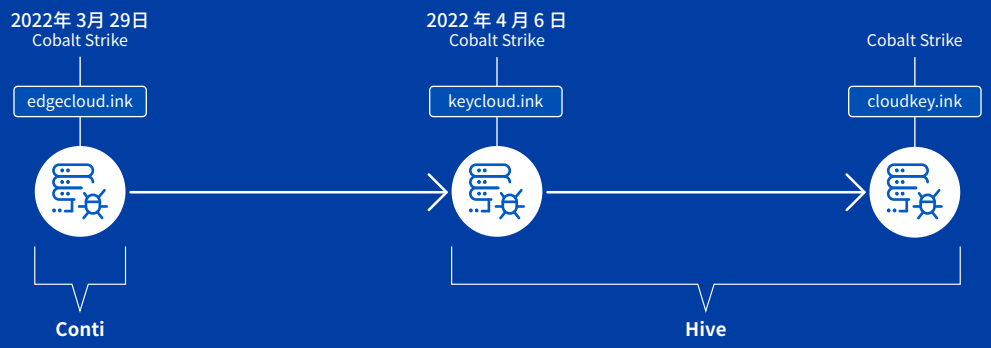

図 6: 2022 年 3 月と 4 月に発生した Hive および Conti ランサムウェア攻撃で観測された共有インフラストラクチャ

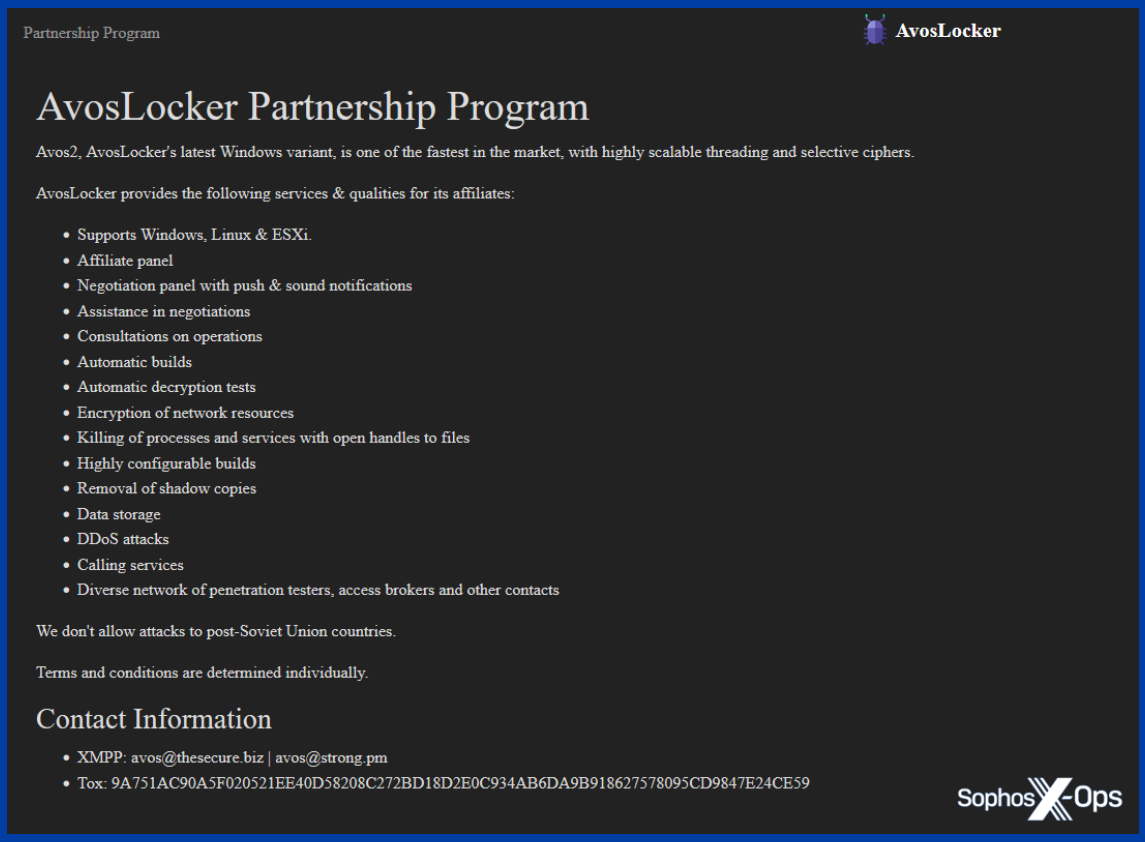

図 7: AvosLocker のアフィリエイトスキームの詳細

一方、Lockbit のアフィリエイト規約には、競合との連携は「禁止事項ではいないが...必ず報告し、連携する理由を説明すること」と明記されています。

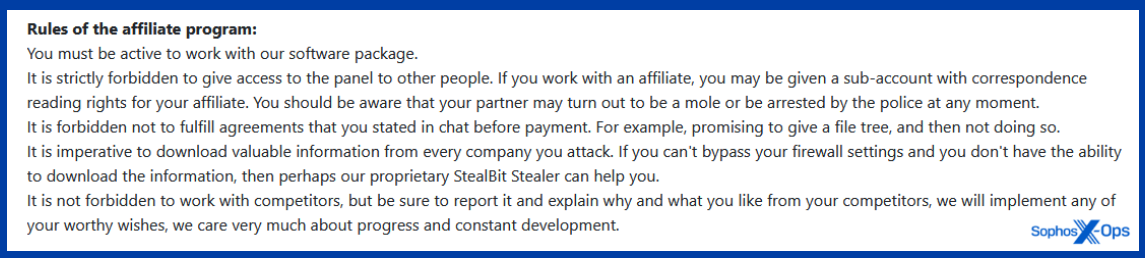

図 8: 競合との連携に言及している Lockbit のアフィリエイトスキームの詳細

また、次のケーススタディで紹介するように、ランサムウェア攻撃者は、別の攻撃者の活動の恩恵を受けることもあり、競争を過度に意識しているようには見えません。

また、攻撃が複数回行われる理由として、リーク (情報漏洩) サイトの存在が考えられます。ランサムウェアグループは、被害者に関する情報を、時には盗み出したデータとともに公開します (新しい Lockbit 3.0 のサイトでは、他の攻撃者によるデータへの即時アクセスや破壊を可能にしているため、被害者に対する身代金支払いへのプレッシャーはますます高まります)。

セキュリティ研究者の Kevin Beaumont 氏が指摘[31] するように、一般的な意見とは異なり、リークサイトで情報が公開されている被害者の大半を占めているのは、身代金要求に応じない被害者です。

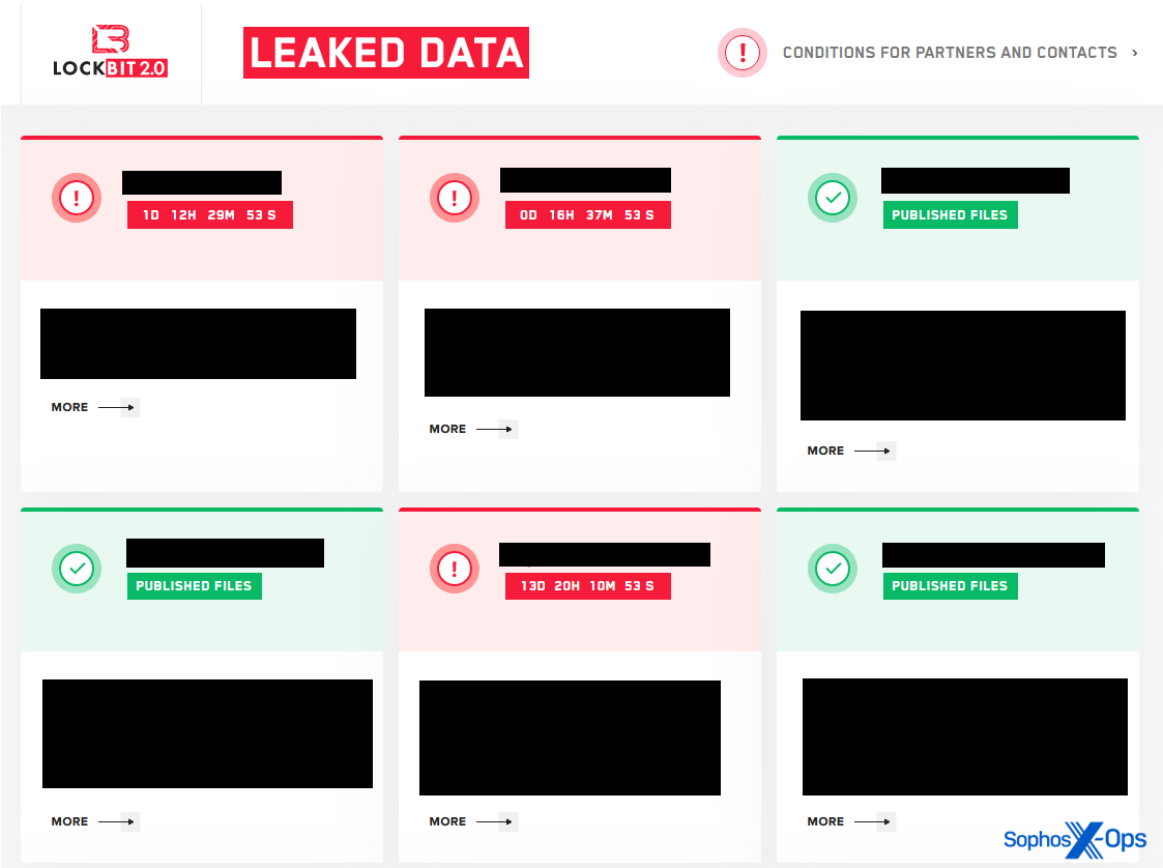

図 9: Lockbit 2.0 のリークサイト。現在および過去の被害者の情報が表示されている (編集済み)。

図 10: Lockbit 3.0 のリークサイト。誰でもお金を支払えば、タイマーの延長、企業データの破壊 / ダウンロードが可能なオークションが開催されている。証拠として、侵入先のネットワークのスクリーンショットがギャラリーが掲載されている

それがなぜ、複数回攻撃につながるのでしょうか。リークサイトは公開されています。便乗型で低レベルのランサムウェア攻撃者は、被害者が身代金要求にまだ応えていない場合、感染経路にも対処していないと判断するでしょう。攻撃者は、失うものは何もないのです。出品されている AaaS を購入するのとは異なり、リークサイトに掲載されている組織を狙うのにコストはかかりません。

また、最初のランサムウェア攻撃で暗号化できなかったファイルがあったのかもしれません。第 2 の攻撃者がさらにファイルを暗号化すれば、身代金を支払うよう、さらなるプレッシャーをかけることができます。複数回攻撃がランサムウェアグループにもたらすのがメリットなのかデメリットなのかについては、次のセクションで説明します。

ランサムウェア以外の攻撃者もまた、個人情報やパスワードなど、リークサイトに公開されたデータを入手し、さらなる攻撃を実行する可能性があります。ランサムウェアグループの中には、この状況を後押ししているグループもあります。たとえば、ALPHV/BlackCat は最近[32]、「サイバー犯罪者コミュニティにとって公開データがより使いやすくなるように」自分たちのリーク情報を検索できるようにした、と発表しています。

2022-07-05

Support ALPHV	Hi	02:40:38
	We have something new and very cool today.	02:41:33
	Dear Adverts!	02:41:58
	We bring to your attention a new view on corporate leaks, and with it a tool for breech-surfing - ALPHV Collections. Resources with leaks posted in our secure repository are now indexed and searchable by wildcard(*). Search by filename as well as by content, e.g. you can find text in PDF, DOCX, even JPG,PNG, etc! What is the purpose of this? We want to make the published data more usable for the cybercriminal community. We want to make it easier to find documents, confidential information about companies or employees during OSINT, passwords for dictionaries, etc. By doing so, we will make companies reconsider their attitude towards leaks, separating leaks "on paper" from real leaks. In the very near future, ALL the published companies will be placed on the same resource with a clear net pass-through. Translated with www.DeepL.com/Translator (free version)	
	http://vqifktlreqpudvulhbzmc5qocbeawl67uvs2pttswemdorbnhaddohyd.onion/search?text=password http://vqifktlreqpudvulhbzmc5qocbeawl67uvs2pttswemdorbnhaddohyd.onion/search?text=John%20Hannan http://vqifktlreqpudvulhbzmc5qocbeawl67uvs2pttswemdorbnhaddohyd.onion/search?text=net%20income%20	02:42:11

図 11: ランサムウェアグループ「ALPHV/BlackCat」がアフィリエイトに向けて発信したメッセージ。(画像出典 : @vxunderground[33])

図 12: ランサムウェア「Black Basta」のリークサイト (組織名は編集済み)

要点 4: 他の攻撃者も脆弱性をすでに発見していると考える

攻撃者は単独では行動しません。IAB は商品を再販または再出品する可能性があり、アフィリエイトは複数のランサムウェアを使用する可能性があります。したがって、1 つの脆弱性や設定ミスが、ネットワークを悪用しようとする複数の攻撃者を呼び込みかねません。

要点 5: 進行中の攻撃への対処を遅らせるべからず

リークサイトに掲載されていると、便乗型の他の攻撃者を引き寄せる可能性があります。不幸にもランサムウェア攻撃を受けてしまった場合には、セキュリティチームやインシデント対応プロバイダーと連携し、修復計画の一環として最初のエントリポイントを塞ぎ、どのデータが流出したかを判断するなど、直ちに行動を起こす必要があります。

攻撃者はなぜ、共存できなかったのか？

では、攻撃者たちはこの状況どう考えているのでしょうか。攻撃者はスペースを共有するのが好きなのか、必要悪だと考えているのか、それとも少しでもチャンスがあれば感染先のシステムから相手を追い出そうとするのでしょうか。

マルウェアの歴史[34] を振り返ると、かつては協力 (あるいは、少なくとも平和的共存) という概念は、多くの攻撃者にとって受け入れられないものでした。同盟関係も希薄で、些細なことで敵意をむき出しにすることも少なくありませんでした。マルウェアの作成者は、ホスト、得意げに話す権利、技術力、ボットネットの数などをめぐって常に争っていました。

2000 年代半ばの「ワーム戦争」最盛期には、競合するワームを駆除するための特定のルーチンが組み込まれているワームや、駆除されないための保護機能を搭載したワームがよく見られました。このような争いは、クリプトマイナー間で現在繰り広げられている戦いと同じように熾烈なものでした。Netsky、Bagle、Mydoom の開発者は、ソースコードの中で侮辱し合っていたほどで、当時ソフォスのシニアテクノロジーコンサルタントだった Graham Cluley は、次のようにコメントしています。「彼らがコードの中ではなく、掲示板で罵り合っている方がはるかにましです。」[35]

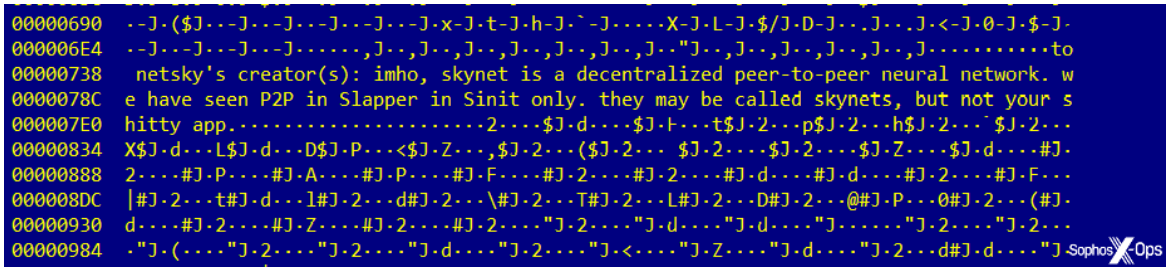

図 13: 2004 年 3 月、Mydoom の作成者と Netsky の開発者が「挨拶」を交わしている様子

ワーム同様、クリプトマイナーも、理由は異なるもののボットネットモデルを採用することがよくあります。クリプトマイニング (暗号通貨マイニング) 攻撃は、大規模な割に利益の少ないビジネスモデルであるため、十分な見返りを得るためには大量の感染が必要であり、感染したすべてのホストの CPU リソースを最大限に悪用する必要があります。当初からクリプトマイナーにライバルを強制終了させるルーチンが含まれているのはそのためです。ソフォスがある闇フォーラムのアーカイブを詳細に調査したところ、購入希望者に「kill other Miner」[原文ママ] 機能を提供する 2014 年のクリプトマイナーの仕様書を発見しました。

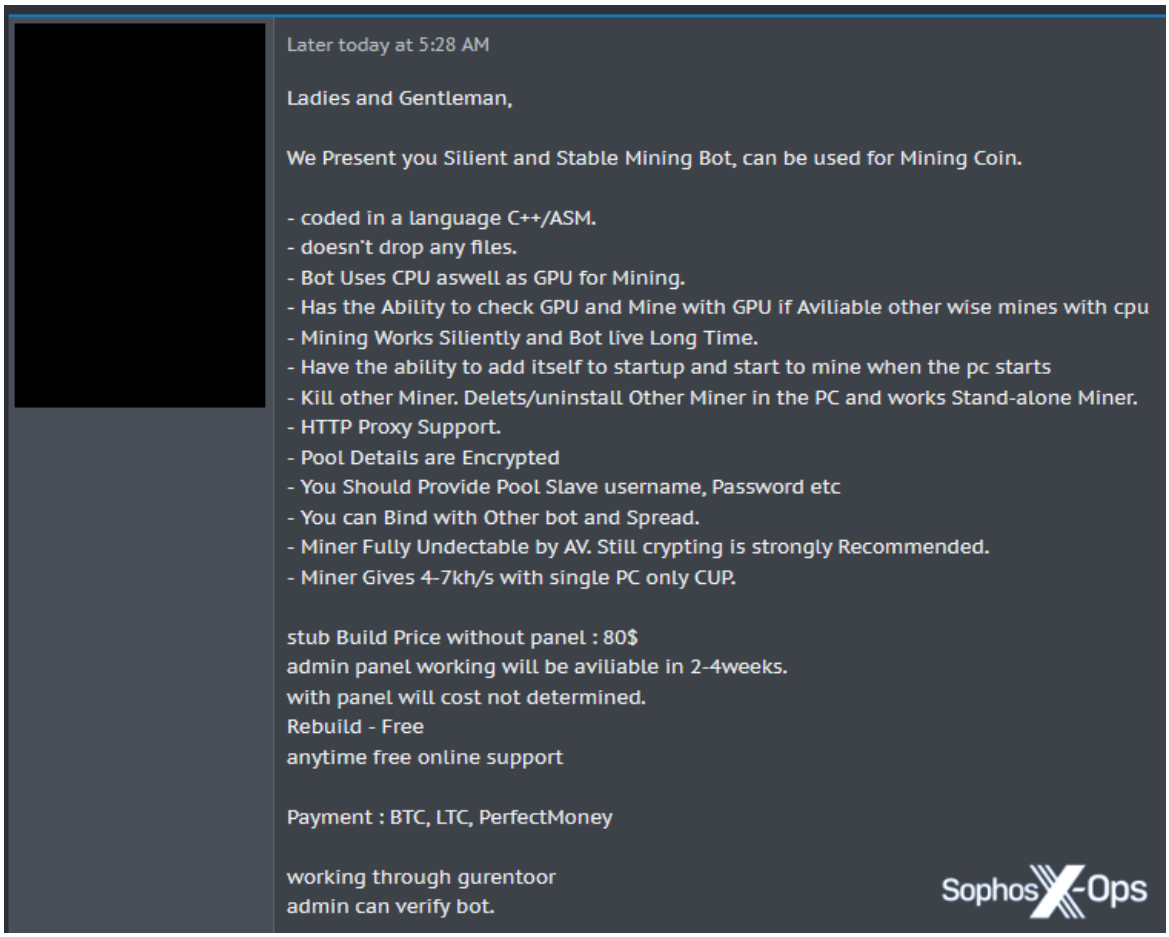

図 14: 2014 年に闇フォーラムに投稿されたクリプトマイナーの広告

当然ながら、敵対行為はワームやクリプトマイナーに限ったことではありません。2010年代初頭、クライムウェアキットSpyEye[36] には、ライバルの 1 つである Zeus[38] の感染をハイジャックまたは削除するための機能[37] がありました (ただし、この2つはhave 後に統合された[39] 可能性があります)。そして 2013 年、Omega Bot と呼ばれるマルウェアパッケージは、Zeus と SpyEye だけでなく、他の数多くの競合も削除できると主張しました。

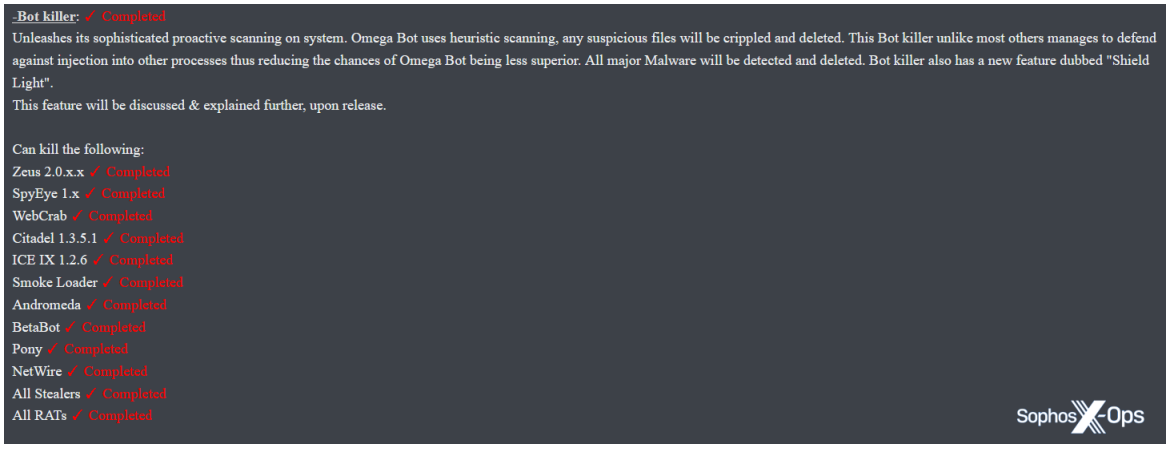

図 15: 2013 年に闇フォーラムで売りに出された Omega Bot

これは現在に至るまで続いており、最近の RAT は**ボットを強制終了**する機能をセールスポイントにしています。2022 年 6 月に売り出された Spectre RAT の仕様書には、次のように記されています。

図 16: 闇フォーラムに掲載された Spectre RAT の最新版の広告

また、最近 Follina の脆弱性[42] (CVE-2022-30190[43]) を悪用していることが研究者によって観測[41] された AsyncRAT[40] のバージョンは、2021 年 12 月の次の広告の中で、ボーナス機能として「ボットキラー」を提供しています。

図 17: 2021 年に闇フォーラムに掲載された　AsyncRAT の広告

しかし、RAT に限らず、一部の攻撃者はライバルを攻撃・妨害するために、これまで以上に想像力を駆使した手段を講じています。たとえば、2022 年 2 月、npm リポジトリ内の悪意のあるパッケージを利用する攻撃キャンペーン[44] が研究者たちによって発見されました。これには、他のマルウェア作成者を攻撃するために設計されたものも含まれます。

先ほど触れたように、攻撃者は自分がアクセスするために利用した脆弱性を修正または削除して、他の攻撃者が侵入できないようにすることがあります。2003 年にこれを実際に行い、名を知られるようになったのが Welchia ワームです。[45] このワームは、Blaster ワーム[46] と同じ脆弱性を悪用していますが、ホストに侵入すると Microsoft からパッチをダウンロードしてその脆弱性を修正し、Blaster ワームによる感染の除去を試みます。なお、その際には (意図的に) 悪意のある活動を行うことはありません。Welchia は、いわゆる「役に立つ」ワームの一例で、「アンチワーム」や「nematode (線虫)」[47] とも呼ばれます。ただし、大半のアンチワームと同様に、法的・倫理的に重大なリスクをはらんでいます。また、Welchia は (破壊的ではないものの) 意図せず被害を引き起こすため、大量のネットワークトラフィックが生成された結果、サービス拒否 (DoS) 状態が発生しました。

また最近では、ソフォスが Kingminer クリプトマイナーボットネットを調査 したところ、このクリプトマイナーは、Windows のバージョン番号とインストールされているホットフィックスを列挙し、感染したシステムが Bluekeep エクスプロイトに対して脆弱であるかどうかをチェックすることが判明しました。ホットフィックスが見つからない場合には、他のマルウェアがこの脆弱性を悪用してアクセスするのを阻止するため、RDP 接続を無効にします (ただし、当時は Bluekeep が他のクリプトマイナーによって悪用されることはほとんどありませんでした)。[48]

しかし、ランサムウェアがセキュリティのあり方を一変させたマルウェアであるということは、その攻撃方法は他のマルウェアとは異なるということです。ランサムウェアのグループがいつも仲が良いというわけではなく、闇フォーラムで仲間割れしたり[49]、 and 互いのコードを盗み合ったり[50] することもあります。下図のように、「有名なランサムウェアグループ」の個人情報を販売しようとする攻撃者もいます。

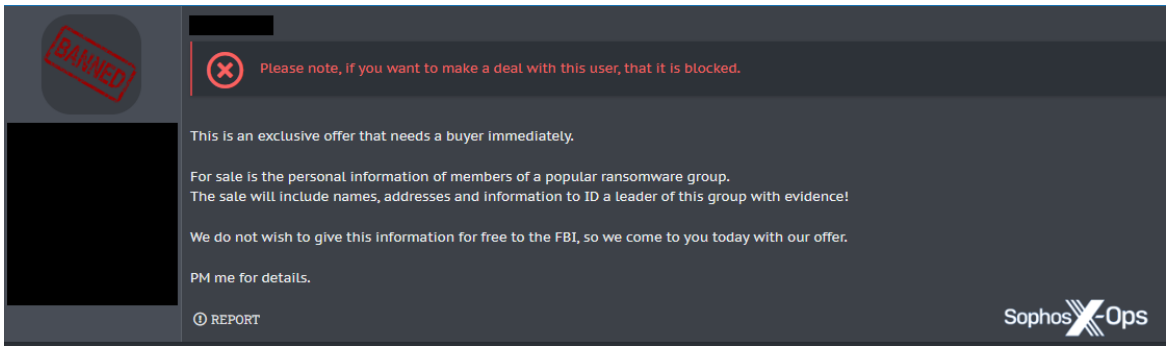

図 18: 2020 年、闇フォーラムでランサムウェアグループの個人情報を売りに出す (凍結済みの) ユーザー

しかし、攻撃に関しては、攻撃対象を共有することに概ね満足しているようです。攻撃者は　CPU　リソースやボットネットの規模を競っているわけではないため、ライバルのランサムウェアプロセスを終了させたり、他のマルウェアを排除したりしません。また、長期的に検知されずにアクセスする必要もありません。つまり、「競合をキルする」必要性がないのです。

実際、Maze ランサムウェアグループ[51] が、身代金の支払いに応じた被害者にはセキュリティホールを教えると申し出たところ、あるユーザーが闇フォーラムで次のように尋ねていました。「これは、競争の激しい状況とは言えませんよね?」

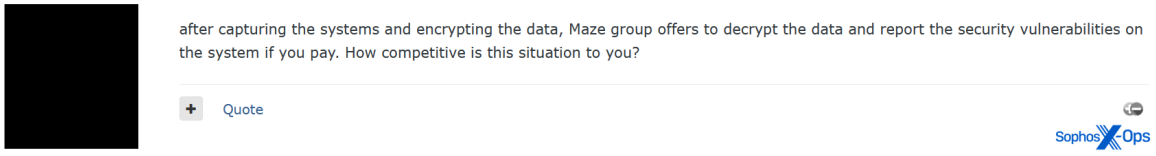

図 19: 身代金を支払った被害者にはネットワークの脆弱性を通知するというランサムウェアグループ「Maze」の提案について意見を募ったユーザー

重複する攻撃がランサムウェアグループに利益をもたらすか、不利益をもたらすかは別の問題です。一方、身代金を支払うようにプレッシャーを与えることができれば、攻撃者としては望ましい結果であると言えます。ランサムウェアグループがプレッシャーをかけようとする方法はさまざまで、とりわけ不快なものもあります[52] が、複数のランサムウェアに感染することによって、(協調戦略とは言えないまでも) 同様の効果が得られる可能性があります。

一方、複数回感染していると、ランサムウェア攻撃者は通常の戦術を実行することが困難になり (たとえば、他のグループによって暗号化されているため、データを漏洩すると脅迫できなくなる[53])、2 倍、3 倍の額の身代金を要求された被害者は支払うことをより嫌がるか、単に支払えなくなる可能性があります。ランサムウェアグループは、最初に暗号化した者が身代金を受け取れる可能性が高いと判断し、複数のランサムウェアに感染したシステムで 1 つのグループが暗号化を開始すると、他のグループもそれに続くかもしれません。これが、暗号化の所要時間を自慢するランサムウェアグループ[54] が存在する理由の 1 つであると考えられます。

ケーススタディ : 3 度も暗号化されたファイル

2021 年 12 月 2 日: 攻撃者 (おそらく IAB) が、ある組織のドメインコントローラーに RDP セッションを確立する。セッションは 52 分間継続。

2022 年 4 月 20 日: Lockbit のアフィリエイトが、断定はできないが (この点については後ほど説明します) おそらくは公開されている RDP インスタンスを通じて企業ネットワークにアクセスし、4 つのシステムから盗み出したデータを **Mega** (攻撃者がよく利用するクラウドストレージサービス) にデータを流出させる。

4 月 28 日: 攻撃者はラテラルムーブメントと **Mimikatz** の実行によって、パスワードを抽出。

5 月 1 日: 攻撃者は、正規のツールである PsExec[55] を介して、ネットワーク上にランサムウェアのバイナリを配布するためのバッチスクリプトを 2 つ作成する。10 分後、19 台のホストでバイナリが実行されてデータが暗号化され、感染した各マシンにランサムノート (身代金要求文書) がドロップされる。

それから 2 時間弱: Hive ランサムウェアのアフィリエイトは、(初期アクセスにはおそらく RDP を使用し、) 正規のツール PDQ Deploy[56] を使用して、ランサムウェアバイナリをネットワーク上に配布。使用したコマンドは、**C:\Windows\AdminArsenal\PDQDeployRunner\service-1\exec\windows_x32_encrypt.exe**。約 45 分後、このバイナリが実行され、16 台のホストのデータが暗号化される。

5 月 15 日: ALPHV/BlackCat[57] ランサムウェアのアフィリエイトがネットワークにアクセスし、漏洩した認証情報を使用して横方向に移動し、2 つのランサムウェアバイナリをドロップする。このバイナリをネットワーク上に配布する際には、PsExec を使用。約 30 分後、バイナリが 6 台のホストで実行され、再びデータが暗号化される。

それから 2 時間弱: ALPHV/BlackCat の攻撃者は、**cmd.exe /c for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1"** というコマンドを実行して、Windows イベントログをクリア。このアクションが原因で、また、調査前の修復アクションやこの企業のネットワーク構成の特殊性と相まり、インシデントレスポンス活動が著しく困難になる。BlackCat の攻撃者は、自身の活動に関するログだけでなく、Lockbit および Hive の攻撃者のログも消去するため、初期アクセス、ラテラルムーブメント、およびその他のイベントに用いられた方法を特定することが困難になる。

5 月 15 日: Sophos Rapid Response チームが支援に入り、3 つのランサムノートと、2 重、3 重に暗号化されたファイルを確認する。

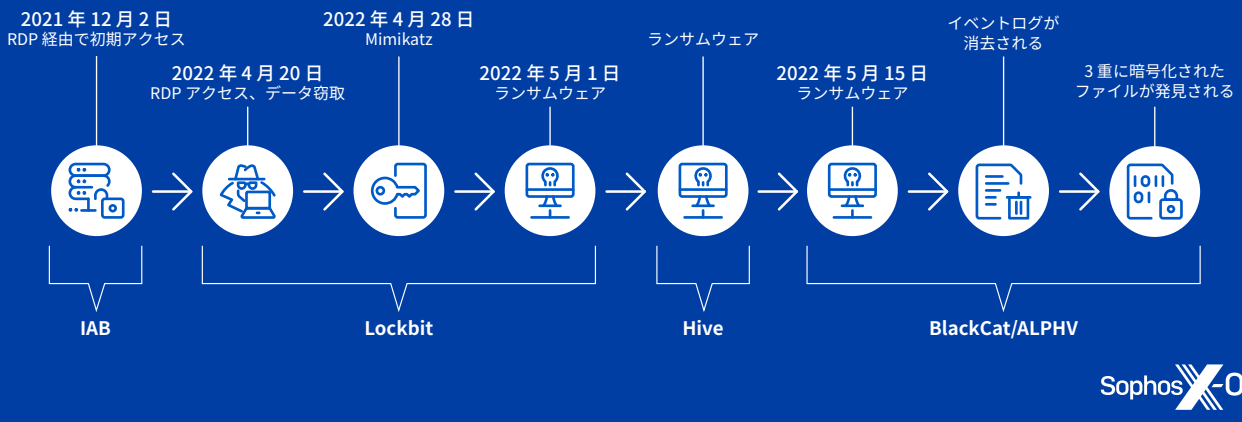

図 20: 時系列で見た攻撃

たとえば、同時感染が発生した場合、あるランサムウェアグループは暗号化し、別のグループは暗号化を行わずにデータを流出させるといったように、ランサムウェアグループのトップレベルが相互に有益な取り決めを行っている可能性もあります。

実際、2021 年 12 月の事例[58] では、事前に調整されていたかどうかは分かりませんが、まさにこのような行動が確認されています。

最初に ProxyShell 経由で Karma ランサムウェアに感染しましたが、データは暗号化されずに窃取されただけでした (ランサムノートには、被害者が医療機関であるためと書かれていますが、他のランサムウェアグループは、特定の種類の医療機関は一切標的にしないと明言しています (下図参照))。その後、Karma のランサムノートがドロップされている最中に、同じ脆弱性を悪用する Conti が登場し、ファイルを暗号化していきました。

図 22: ランサムウェアグループ「Babuk」の規約。病院を含むさまざまなカテゴリーの組織を攻撃することをアフィリエイトに禁じている

ランサムウェアグループ同士が連携しているかどうかは別として、複数回攻撃は彼らにとって大きな問題ではないようです。新規参入者が多く、コモディティ化した市場において活動する以上、仕方のないことだと受け入れているのかもしれません。

とはいえ、ランサムウェアグループが同じ組織を攻撃する際に、互いの活動によって利益がもたらされることがあります。私たちが知る限り、これは意図的なものではありません (少なくとも、今のところは)。しかし、複数の感染への対応は、被害者だけでなく、対応や調査の担当者にとっても、複雑なものになる可能性を示しています。次のインシデントでは、ある攻撃者がインストールしたバックドアが、4 か月後に別の攻撃を受けたという事例です。

ケーススタディ：別の攻撃を呼び込むバックドア

2022 年 1 月 6 日: ある組織のネットワークで、ProxyShell を悪用しようとする複数の試みが発見される。初期アクセスの後、攻撃者は **Advanced IP Scanner** を実行。

1 月 19 日: 攻撃者は、漏洩したアカウントへの RDP 接続を確立する。1 月から 2 月にかけて、この攻撃者は複数の RDP 接続を行い、RealVNC をダウンロード。[59]

2 月 23 日: ネットワーク上の 2 つのデバイスが DNS を介して C2 サーバーと通信する。攻撃者は 1 テラバイトを超えるデータを **Mega** に流出させる。その後、攻撃者は数日間にわたり、SFTP/FTP クライアントの WinScp[60]、クラウドストレージファイルマネージャーの Rclone[61]、圧縮ユーティリティの 7-zip[62]、SSH および Telnet クライアントのPutty[63]、リモートデスクトップアプリケーションの AnyDesk[64]など、複数の正規ツールをダウンロードおよびインストールする。さらに RDP 接続を確立。

3 月 12 日: 攻撃者は **AnyDesk** を実行し、AdFind.exe[65] (Active Directory クエリーツール)、SharpShares[66] (ネットワーク共有情報をリストアップするバイナリ)、**lsass_dumper.exe**、NanoDump[67] (LSASS プロセスのミニダンプを作成) などのツールを引き続きダウンロードおよびインストール。同日、攻撃者は **Cobalt Strike** ビーコンをサービスとしてインストールし、Base64 エンコードされた PowerShell スクリプトを実行して、Active Directory における攻撃可能な経路を特定するための正規の侵入テストツール BloodHound[68] をダウンロード・実行。

3 月 17 日: 攻撃者は、ランサムウェアのバイナリ Lockbit をダウンロードし、実行。

3 月 25 日: Lockbit のリークサイトにこの組織のデータが掲載される。

4 月 28 日: 2 番目の攻撃者が、一般公開されている RDWeb ポータルを介して企業環境に侵入。**rundll32 107s32.dll**、**StartW**、**Cobalt Strike** DLL でよく使用されるコマンドを実行し、**Cobalt Strike** のステージングサーバーに複数の外部接続を確立する。この攻撃者は **BloodHound** のダウンロードと実行も試みるが、このアクティビティはブロックされる。

6 月 2 日: 第 3 の攻撃者は、すでにインストールされている **AnyDesk** インスタンスを悪用してネットワークにアクセスし、認証情報を収集・窃取する。標的組織のデータの一部を、ファイル共有サービスである **dropmefiles[.]com** にアップロードする。この攻撃は、最初の侵入からデータ窃取までを 15 分未満で完了させている。

6 月 8 日: 「Karakurt チーム」から身代金要求の連絡が入る。Karakurt (トルコ語で「黒い狼」、東ヨーロッパとシベリアに生息するクモを指す) は通常、データを暗号化せず、身代金を支払わないとデータを盗んで公開すると脅す。[69] 研究者は以前から Karakurt と Conti ランサムウェアグループとの関係を指摘している)。[70]

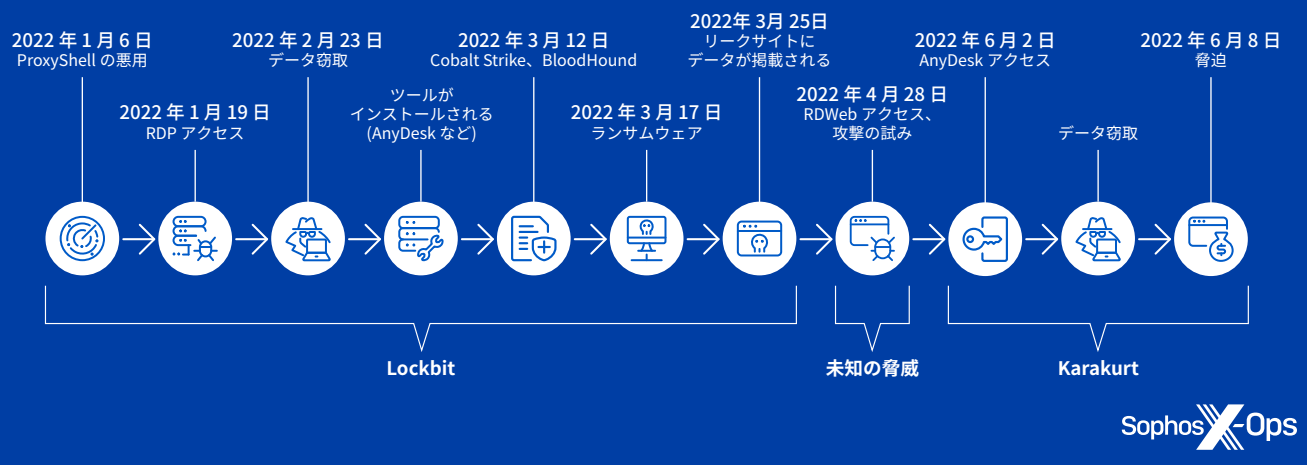

図 23: 時系列で見た攻撃

要点 6: 他のランサムウェアとの共存

多くの攻撃者は、感染先のシステムでライバルを追い出すほど対抗意識が強く、クリプトマイナーや一部の RAT に関しては、現在もその傾向が見られます。しかし、ランサムウェアにはこの傾向は当てはまらないようで、他のランサムウェアグループが同じネットワーク上にいてもファイルの暗号化を続行したり、一方のグループがデータを窃取し、他方は暗号化するというように、相互に利益をもたらす動きを見せることがあります。

要点 7: 新たに開かれるバックドア

攻撃者の中には、アクセスした後に別の脆弱性を悪用したり、意図的に、もしくは意図せずにバックドアを作成したり (正規ソフトウェアのインストールを含む) するため、後続の攻撃者がそれらを悪用する可能性があります。したがって、最初の感染経路を遮断することが極めて重要である一方、a) アクセスに利用される可能性のある他の脆弱性や設定ミス、b) 新たに出現した侵入口についても検討することが重要です。

要点 8: より悪質な攻撃者

すべてのランサムウェアが同じというわけではありません。ランサムウェアの中には、対応や調査を困難にする機能や特徴を持つものもあります。このことからも、複数回攻撃を受けないようにすることが重要です。

ガイダンス

複数回攻撃は以前よりも頻繁に発生しているのでしょうか。統計的に確信を持って言うのは難しいのですが、事例を見る限り、その答えは「イエス」です。ソフォスのインシデントレスポンス担当ディレクターである Peter Mackenzie は、次のように指摘しています。この傾向は、多くの組織で見られるようになっています。これは、ますます多くの攻撃者が市場に参入していることと、RaaS (ランサムウェア・アズ・ア・サービス) がより専門化し、参入へのハードルが下がっていることが原因だと思われます。

ランサムウェアのアフィリエイトプログラムが採用と拡大を続け、クリプトマイナーが新たな脆弱性の悪用を続ける中、攻撃者の数は増加し、攻撃の機会も多くなっています。

一般的に、複数回攻撃の原因は、被害者が最初の攻撃の根本原因に対処していないことにあります。複数回攻撃を引き起こすその他の要因として、犯罪エコシステムの特徴が挙げられますが、そもそも犯罪エコシステムに組み込まれないようにするために組織ができることがあります。

本記事で紹介した 8 つの要点に加え、ランサムウェアや関連するサイバー攻撃から身を守るために、以下の標準的ベストプラクティスが推奨されます。

1. **パッチの適用と調査を行う。**Windows やその他のソフトウェアを常に最新の状態に保ちましょう (脆弱性アラートの設定や、新しい脆弱性に関するニュースをいち早く知るための情報源もモニタリングしてください)。これは、パッチが正しくインストールされ、インターネットに接続するマシンやドメインコントローラーなどの重要なシステムにパッチが適用されていることを再確認することも意味します。ただし、単にパッチを迅速に適用すればよいというものではありません。攻撃者は、意図的であるかどうかにかかわらず、バックドア (正規のソフトウェアのインストールを含む) を残していったり、新しい脆弱性を導入したりすることがあるので、防御する側は調査を行い、第 2 の攻撃の可能性を低くする必要があります。
2. **アラートを監視して対応する。**環境内に見られる脅威を監視し、調査し、対応できるよう、適切なツール、プロセス、およびリソース (人員) が利用可能でることを確認しておきます。ランサムウェアの攻撃者は、監視するスタッフがほぼ不在であると考えて、オフピークの時間帯、週末、または休日に攻撃を仕掛ける可能性があります。
3. **外部からアクセス可能なサービスをロックダウンする。**外部から自社ネットワークをスキャンし、VNC、RDP、また他のリモートアクセスツールで頻繁に使用されるポートを特定してロックダウンしましょう。リモート管理ツールを使用してマシンにアクセスする必要がある場合は、VPN の内側でツールを使用するか、ログイン時に MFA を使用するゼロトラストネットワークアクセスのソリューションを使用しましょう。
4. **セグメンテーションとゼロトラストを導入する。**重要なサーバーは異なる VLAN に配置し、サーバー間およびサーバーとワークステーション間を分離して、ゼロトラストネットワークモデルを確立しましょう。
5. **強固なパスワード、および多要素認証 (MFA) を設定・適用する。**強度の高いパスワードは、攻撃に対する最初の防衛線となります。パスワードは一意、もしくは複雑なものを使用し、絶対に使い回しをしないでください。認証情報を保存できるパスワードマネージャーを使用することで、複雑なパスワードを簡単に管理できます。しかし、強固なパスワードであっても侵害される恐れがあります。電子メール、リモート管理ツール、ネットワーク資産などの重要なリソースへのアクセスを保護するためには、なんらかの多要素認証を導入してください。
6. **資産とアカウントのインベントリを作成する。**ネットワーク上の保護されていないデバイスや、パッチが適用されていないデバイスは、リスクを高め、悪意のあるアクティビティを検出できずに見逃してしまう要因になります。接続されているすべてのコンピュータと IoT デバイスの最新のインベントリを作成することが極めて重要です。ネットワークスキャンと物理的な調査を併用してデバイスの場所を特定し、記録しておきましょう。
7. **できるだけ多くのポイントで攻撃者を阻止できるよう、多層防御を導入する。**ネットワークに接続可能なすべてのエンドポイントに多層防御を導入しましょう。
8. **製品を正しく構成し、定期的に構成を確認する。**保護が不十分なシステムやデバイスも、攻撃に対して脆弱です。セキュリティソリューションが適切に構成されていることを確認し、セキュリティポリシーを定期的にチェックして (必要に応じて) 更新することが重要です。新しいセキュリティ機能が自動的に有効になるとは限りません。

謝辞

Sophos X-Ops は、本記事に貢献してくれたソフォスの Managed Detection and Response チームの Hilary Wood と Colin Cowie、Rapid Response チームの Syed Shahram Ahmed と Mauricio Valdivieso、および SophosLabs の Andrew Ludgate と Gabor Szappanos に謝意を表します。

参考文献

1 https://news.sophos.com/ja-jp/2022/06/07/active-adversary-playbook-2022-jp/
2 https://news.sophos.com/ja-jp/2021/10/11/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack-jp/
3 https://documents.trendmicro.com/assets/white_papers/wp-navigating-the-landscape-of-cloud-based-cryptocurrency-mining.pdf
4 https://nvd.nist.gov/vuln/detail/CVE-2021-26855
5 https://nvd.nist.gov/vuln/detail/CVE-2021-34473
6 https://nvd.nist.gov/vuln/detail/CVE-2021-34523
7 https://nvd.nist.gov/vuln/detail/cve-2021-31207
8 https://news.sophos.com/ja-jp/2021/03/29/mtr-in-real-time-exchange-proxylogon-edition-jp/
9 https://news.sophos.com/ja-jp/2021/09/06/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do-jp/
10 https://news.sophos.com/ja-jp/2021/05/18/new-lemon-duck-variants-exploiting-microsoft-exchange-server-jp/
11 https://news.sophos.com/ja-jp/2021/12/02/two-flavors-of-tor2mine-miner-dig-deep-into-networks-with-powershell-vbscript-jp/
12 https://news.sophos.com/ja-jp/2022/02/15/vulnerable-exchange-server-hit-by-squirrelwaffle-and-financial-fraud-jp/
13 https://news.sophos.com/ja-jp/2021/03/23/dearcry-ransomware-attacks-exploit-exchange-server-vulnerabilities-jp/
14 https://news.sophos.com/en-us/2021/03/23/black-kingdom/
15 https://news.sophos.com/ja-jp/2021/09/06/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion-jp/
16 https://news.sophos.com/ja-jp/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits-jp/
17 https://nvd.nist.gov/vuln/detail/CVE-2021-44228
18 https://news.sophos.com/ja-jp/2022/01/14/log4shell-no-mass-abuse-but-no-respite-what-happened-jp/
19 https://news.sophos.com/en-us/2022/03/29/horde-of-miner-bots-and-backdoors-leveraged-log4j-to-attack-vmware-horizon-servers/
20 https://news.sophos.com/ja-jp/2022/06/16/confluence-exploits-used-to-drop-ransomware-on-vulnerable-servers-jp/
21 https://nvd.nist.gov/vuln/detail/CVE-2022-26134
22 https://www.computerweekly.com/news/252510662/2021-another-record-breaker-for-vulnerability-disclosure
23 https://bugalert.org/
24 https://cvetrends.com/
25 https://www.advanced-ip-scanner.com/
26 https://github.com/gentilkiwi/mimikatz
27 https://www.cobaltstrike.com/
28 https://ke-la.com/access-as-a-service-remote-access-markets-in-the-cybercrime-underground/
29 https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf
30 https://learn.microsoft.com/ja-jp/visualstudio/msbuild/msbuild?view=vs-2022
31 https://twitter.com/GossiTheDog/status/1541688001620754436
32 https://twitter.com/vxunderground/status/1544306201600598016
33 https://twitter.com/vxunderground/status/1544306201600598016
34 https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-cyberthreats-20-year-retrospective-wp.pdf
35 http://news.bbc.co.uk/1/hi/technology/3532009.stm
36 https://nakedsecurity.sophos.com/2012/01/05/spyeye-bank-trojan-hides-its-fraud-footprint/
37 https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=6aa65e05-2a44-4dd3-be3d-6dbb06cc94ad&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
38 https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/Sophos-what-is-zeus-tp.pdf
39 https://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/
40 https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp
41 https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/follina-msdt-exploit-malware
42 https://news.sophos.com/ja-jp/2022/05/30/malicious-word-doc-taps-previously-unknown-microsoft-office-vulnerability-jp/
43 https://nvd.nist.gov/vuln/detail/CVE-2022-30190
44 https://jfrog.com/blog/malware-civil-war-malicious-npm-packages-targeting-malware-authors/
45 https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-cyberthreats-20-year-retrospective-wp.pdf
46 https://learn.microsoft.com/ja-jp/troubleshoot/windows-server/security-and-malware/blaster-worm-virus-alert
47 https://www.youtube.com/watch?v=SrVeLNGcbBE
48 https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-labs-kingminer-botnet-report.pdf
49 https://www.techtarget.com/searchsecurity/news/252512902/Distrust-feuds-building-among-ransomware-groups
50 https://www.secureworks.com/research/lv-ransomware
51 https://nakedsecurity.sophos.com/2020/05/12/maze-ransomware-one-year-on-a-sophoslabs-report/
52 https://www.documentcloud.org/documents/20428892-doppelpaymer-fbi-pin-on-dec-10-2020
53 https://news.sophos.com/ja-jp/2021/08/11/ransomware-mishaps-adversaries-have-their-off-days-too-jp/
54 https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
55 https://learn.microsoft.com/ja-jp/sysinternals/downloads/psexec
56 https://www.pdq.com/deploy/
57 https://news.sophos.com/ja-jp/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck-jp/
58 https://news.sophos.com/ja-jp/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits-jp/
59 https://www.realvnc.com/en/
60 https://winscp.net/eng/index.php
61 https://rclone.org/
62 https://www.7-zip.org/
63 https://www.putty.org/
64 https://anydesk.com/
65 http://www.joeware.net/freetools/tools/adfind/index.htm
66 https://github.com/djhohnstein/SharpShares
67 https://github.com/helpsystems/nanodump
68 https://github.com/BloodHoundAD/BloodHound
69 https://www.cisa.gov/uscert/ncas/alerts/aa22-152a
70 https://www.infinitumit.com.tr/conti-ransomware-group-behind-the-karakurt-ha

ソフォス株式会社営業部
sales@sophos.co.jp

2022-08-01 JA (DD)