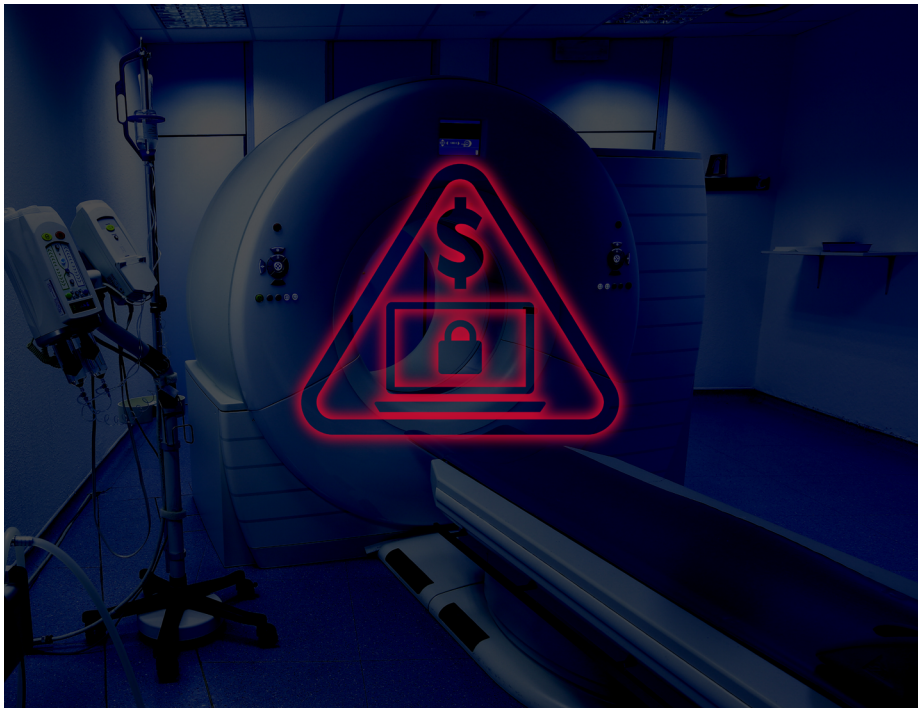
ホワイトペーパー

Symantec
A Division of Broadcom

ランサムウェアの脅威

脅威調査（Threat Hunting）チーム著

目次



はじめに

ランサムウェアは、企業や他の大規模組織にとって大きな脅威であり続けており、特に標的型ランサムウェア攻撃はサイバー犯罪者にとって大きな利益をもたらすものとなっています。数百万ドルの身代金を要求する大規模なランサムウェア攻撃に魅力を感じてこの分野に参入する悪質なアクターがますます増えています。

この 1 年間、ランサムウェア攻撃者はますます野心的になり、大損害を引き起こす派手な攻撃をいくつも実施してきました。2021 年 5 月に起きた米国の大手パイプライン運営会社 Colonial Pipeline に対する攻撃は、大きな混乱を引き起こし、国の燃料供給に関する懸念をもたらしました。それと同じ月に、アイルランドの国営医療サービスである Health Service Executive が攻撃を受け、数千件の予約をキャンセルする事態に陥りました。世界的なパンデミックの最中、ネットワークが復旧するまでコンピュータがオフラインになったため、スタッフは紙の記録を作成しなければなりませんでした。

これらの攻撃はランサムウェア集団が平然と活動している実態をよく表していますが、これらの攻撃が引き起こした混乱は政治的な影響を与え、米国のジョー・バイデン大統領がロシアのウラジミール・プーチン大統領にランサムウェア攻撃者の取締りを要請しましたが、これらの攻撃者の多くがロシアを拠点としていると考えられています。

このように注目を集めた攻撃とその後の法執行機関による取り締まりが話題になったことで、2021 年には Darkside、Sodinokibi（別名 REvil）、Egregor など、積極的に活動したランサムウェアの脅威が消滅したと考えられます。

脅威が去ることは喜ばしい展開ではありますが、ランサムウェア活動が減少すると考えるべきではありません。往々にして、いったん姿を消した攻撃者が新たなツールセットを携えて再登場したり、姿を消した攻撃者が占めていた市場を奪おうと新たな攻撃者が現れたりするものです。脅威の状況が変化するということは、ネットワーク防御者が、誰が主要な攻撃者となるのか、どのような戦術を使うのかわからない不確実な時期があるということです。

特に懸念されるのが 2 つの傾向です。サービスとしてのランサムウェア（RaaS）という現象は目新しいものではありませんが、主要なランサムウェア開発者の多くが RaaS を作戦の一部として取り入れるようになったことで、標的型ランサムウェアによる攻撃が急増しています。RaaS は攻撃の増加を招いているだけでなく、ランサムウェアを配信するために採用されているツール、戦術、手順（TTP）の数を増やしています。各ランサムウェアの脅威は、複数の異なる脅威アクターのいずれかによって配信される可能性があり、その多くが異なる TTP を使用しています。また、RaaS により、スキルの低いアクターの参入障壁が低くなり、攻撃者の数が増加しています。

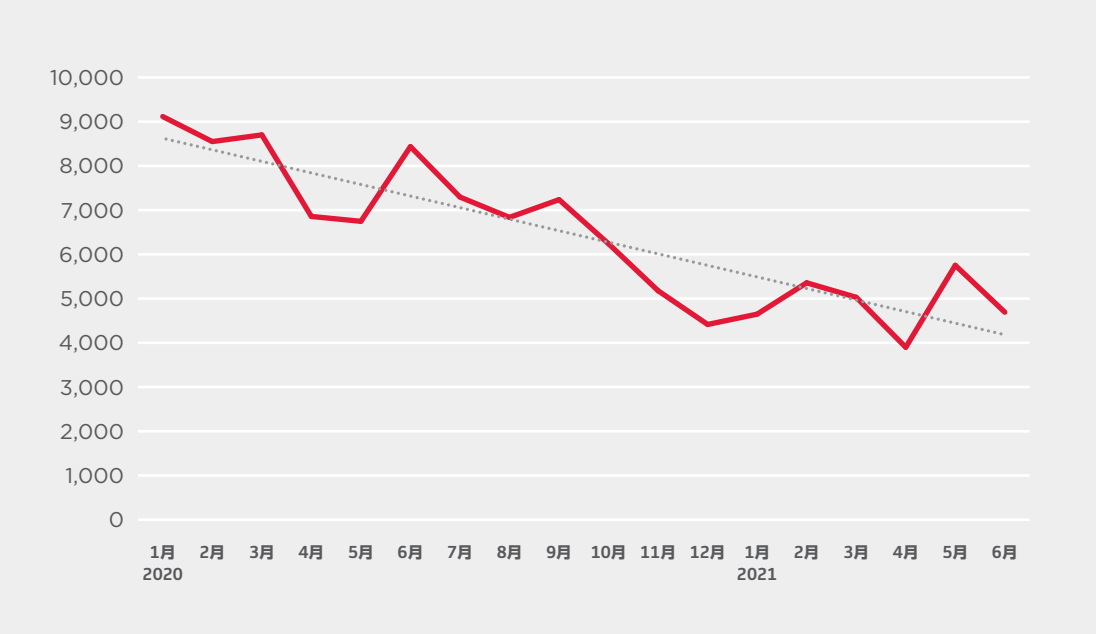
第 2 に、ラランサムウェアオペレーターの中には、他のマルウェア開発者、特に金融詐欺ボットネットと協力して被害者にアクセスする者が増えています。主要なボットネットは、広範囲に渡って活動していることが多く、被害者候補がひしめく大きな釣り堀をランサムウェア集団に提供できる可能性があります。

現在のランサムウェアグループは洗練された脅威アクターとなっており、他の攻撃者と関係を構築して攻撃の範囲を広げたり、進化したツールや戦術を採用して攻撃を効果的に行うことができます。現在、ランサムウェアの攻撃をうまく防御するには、組織の深層部の防御と、これらの攻撃がどのように展開するかについての深い理解が必要です。

ランサムウェアの動向

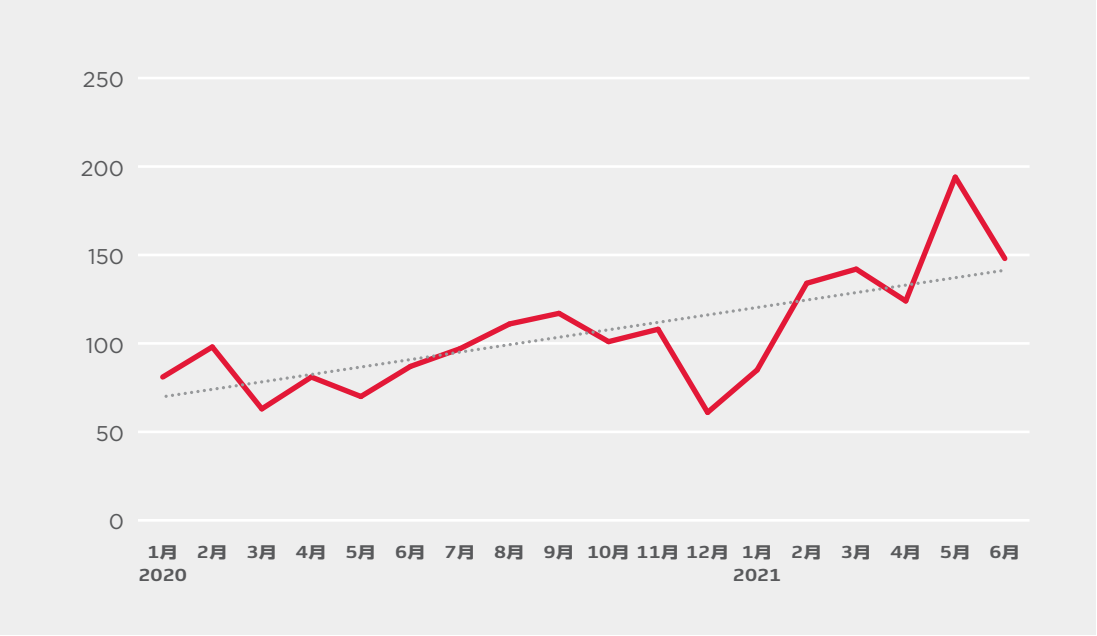
過去数年にわたり、ランサムウェアの脅威の状況には顕著な変化が見られ、その傾向は最近も続いています。過去 18 カ月間で、シマンテックが検知･ブロックしたランサムウェア攻撃の総数は、2020 年 1 月の 9,116 件から 2021 年 6 月の 4,692 件へとほぼ半減しています。

図 1: すべてのランサムウェアの検出数 -2020 年 1 月から 2021 年 6 月



ランサムウェアの活動が減少していることは歓迎すべきことですが、全体的な数の減少は、比較的単純で無差別な攻撃が継続的に減少していることに起因しています。現在では、標的型ランサムウェア攻撃に注力する脅威アクターが増えています。この攻撃では、一度に 1 つの組織が攻撃され、攻撃者はネットワーク上の可能な限り多くのコンピュータを暗号化して、高額な身代金を引き出そうとします。このような攻撃は、比較的数は少ないものの、通常は少数のコンピュータにしか被害が及ばない無差別攻撃よりも、はるかに組織へのダメージが大きくなります。

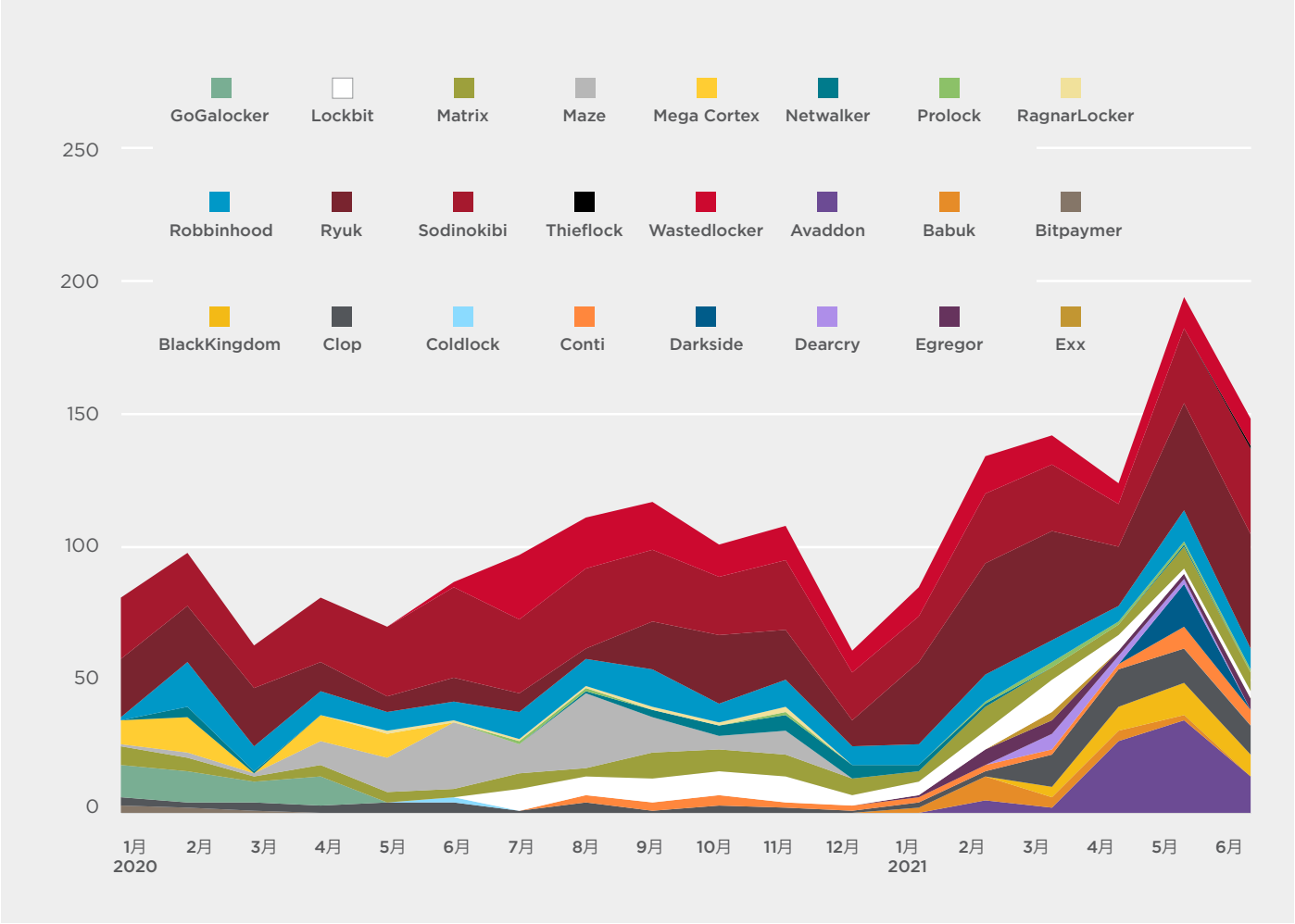
図 2: 標的型ランサムウェア攻撃の影響を受けた組織の数 -2020 年 1 月から 2021 年 6 月



標的型攻撃の統計は、ランサムウェア攻撃全体の統計とは異なる傾向を見せており、標的型ランサムウェア攻撃を受けた組織の数は、2020 年 1 月の 81 件から 2021 年 6 月の 148 件へと、過去 18 カ月間で 83%増加しています。標的型ランサムウェア攻撃の実際の件数は、これをはるかに上回ると考えられます。ランサムウェアのファミリーの中には、標的型攻撃に使われるだけでなく、スパムキャンペーンによって展開されるものもあります。これらの脅威の被害者のうち、どれだけの数が標的型攻撃で感染し、どれだけの数が他の手段で感染したのかを確定する方法がないため、標的型攻撃の中に数えることはできません。

これに加えて、既知の標的型ランサムウェアのファミリーからであると確認された攻撃は、これらの脅威を含む攻撃の全体数の代表的なサンプルに過ぎないと考えられます。標的型ランサムウェアの攻撃の多くは、ペイロードが展開される前に停止するため、ランサムウェアとして認識されない可能性があります。さらに、標的型ランサムウェアオペレーターの多くは、新しい攻撃を行うたびにランサムウェアを再コンパイルしています。つまり、攻撃に使用されたランサムウェアの亜種は、そのランサムウェアファミリーに関連した検知ではなく、一般的な検知シグネチャや機械学習で生成された検知シグネチャでブロックされる可能性があるのです。

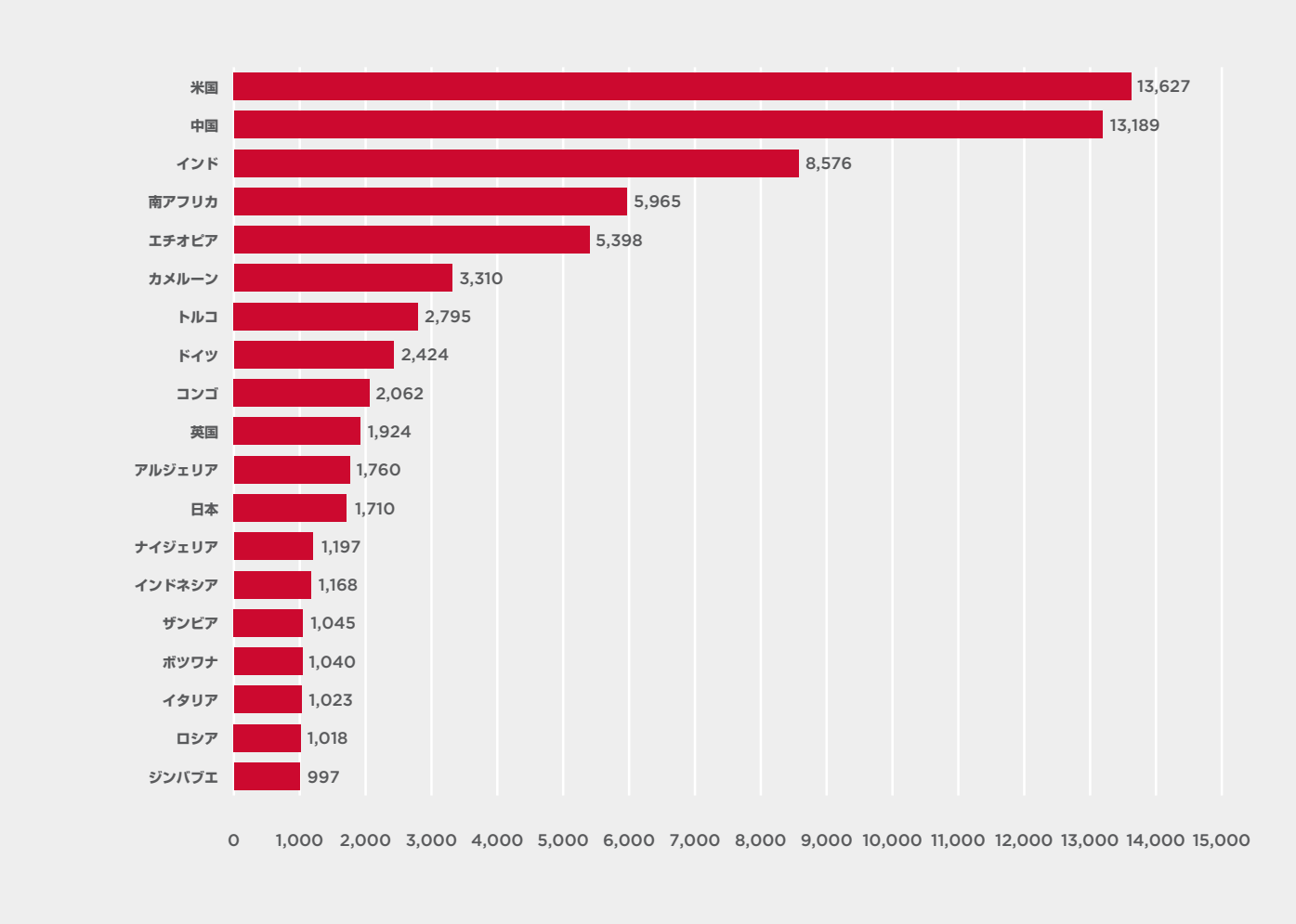
図 3: 標的型ランサムウェア攻撃のファミリー別被害組織数 -2020 年 1 月から 2021 年 6 月



標的型攻撃をランサムウェアの種類別に分類すると、2 つの傾向が明らかになります。第 1 に、新たな脅威の大量発生が続いており、それが全体的な攻撃の増加につながっています。分析した 24 グループのうち、2020 年 1 月には 9 グループが活動していましたが、2021 年 6 月には 13 グループが活動していました。第 2 に、Ryuk、Sodinokibi、そして最近では Avaddon などの少数の多作な脅威アクターが、攻撃の大きな割合を占めています。

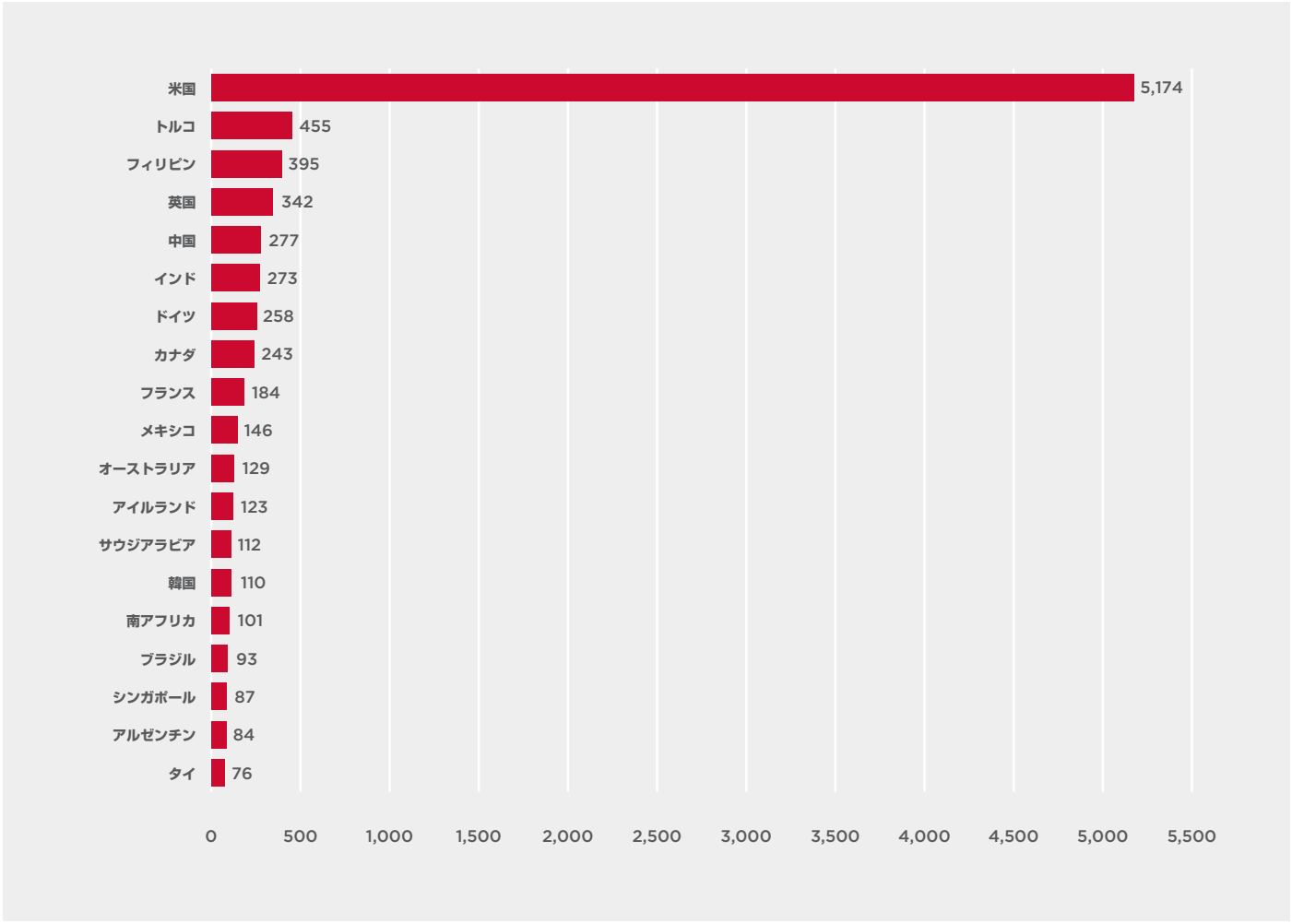
繰り返しになりますが、これらの統計は、シマンテックによってブロックされた攻撃の代表的なサンプルとして扱われるべきであることを強調しておきます。大半の攻撃は、ランサムウェアが展開される前の段階で、あるいは特定のランサムウェアのファミリーに関連づけられる前にブロックされている可能性が高いのです。

図 4: 国別ランサムウェア検出数の推移 -2020 年 1 月から 2021 年 6 月



また、ランサムウェアの被害者の地域を調べると、もう一つの重要な傾向が見えてきます。最も多くの被害を受けているのは米国ですが、ランサムウェアによる攻撃は一般的に世界各地で行われており、過去 18 カ月の間に上位 20 位以内にアフリカの国が数多くランクインしています。アフリカが上位にランクインしているのは、スパムメールキャンペーンや既知の脆弱性の悪用など、無差別にランサムウェア攻撃をしかける攻撃者が特に多いことが主な理由です。

図 5: 国別の標的型ランサムウェアの検出数 -2020 年 1 月から 2021 年 6 月



標的型ランサムウェア攻撃だけを分析すると、まったく異なる様相を呈します。最も被害を受けているのは米国であり、過去 18 カ月間に受けた攻撃の件数は、2 番目に攻撃を受けている国（トルコ）の 11 倍以上に上ります。

被害者が米国に集中していることは驚くに当たりません。ビジネス分野が高度に発達した豊かな大国である米国は、当然、標的型ランサムウェア攻撃の格好の標的となります。いくつかのランサムウェア集団は、米国内の組織を標的にしていると公言していますが、それだけではありません。

トルコとフィリピンが上位にランクインしているのは意外かもしれませんが、これは前年の統計と一致しており、両者ともトップ 5 にランクインしています。

なお、前述の標的型ランサムウェアの統計では、組織の数をカウントしていましたが、今回の統計では、標的型ランサムウェアのファミリーが検出されたコンピュータの数をカウントしていることに注意してください。標的型ランサムウェアの被害者の多くが複数の国で活動しているため、攻撃を地域別に分析する場合は、別の方法を採用する必要があります。

脅威の増大：サービスとしてのランサムウェア（RaaS）

ランサムウェアの脅威を増大させた主な要因は、RaaS（サービスとしてのランサムウェア）の登場です。標的型ランサムウェア攻撃は、成功すると驚くほど効果的な攻撃になり得ますが、その一方で、攻撃者にとっては非常に多くの労力を要するという欠点があります。典型的な標的型ランサムウェア攻撃には、資格情報の窃取、特権昇格、ラテラルムーブメント（水平移動）、データの抽出、バックアップの削除、ペイロードの展開など、さまざまなステップを踏むため、多くの場合、攻撃者側が積極的に関わる必要があります。したがって、ランサムウェアアクターが実行できる攻撃の数は、攻撃に参加できる人員の数によって制限されます。

成功したランサムウェアの作者は、アフィリエイトと呼ばれる他の攻撃者を募り、身代金の支払いの一部と引き換えに自家製ツールへのアクセスを提供することで、収益を上げることができることに気づきました。このビジネスモデルは現在、高度に発達しており、話題の標的型ランサムウェア開発者のほとんどが、何らかの RaaS プログラムを運営しています。

入手可能な証拠によると、アフィリエイトの関係は様々なタイプがあるようですが、現在の基本的なテンプレートは、ランサムウェアの作者が、ランサムウェア自体へのアクセス、侵害されたデータのホスティング、身代金の交渉の処理を提供するというものです。場合によっては、ランサムウェアの開発者がアフィリエイトのためにすべてのプレイブックを提供していることも報告されています。しかし、多くの場合、アフィリエイトは独自の TTP を使用します。シマンテックでは、アクターが同じ TTP を使用しているにもかかわらず、時間の経過とともに異なるペイロードを使用しているケースを頻繁に確認しています。また、アクターが同時に複数のランサムウェア開発者の傘下にある証拠もいくつかあります（下記の「ケーススタディ：アフィリエイト間での忠誠心の変化」を参照）。

ランサムウェア開発者の中には、RaaS のビジネスモデルのみで活動している者もいるようですが、より実践的で、自ら攻撃を仕掛け続ける者もいます。また、アフィリエイトに要求される内容も様々です。「アクセスブローカー」という広告を出している企業が確認されていますが、これは、被害者となりうるネットワークへのアクセス手段を探しているだけで、それ以外の攻撃は自分たちで行うということを示唆しています。

各ランサムウェアの脅威は、複数の異なる脅威アクターのいずれかによって提供される可能性があり、その多くが異なる TTP を使用しているため、アフィリエイトの出現は、ネットワーク防御者にとってランサムウェアの脅威の状況をより複雑なものにしています。

ケーススタディ：アフィリエイト間での忠誠心の変化

ほとんどのランサムウェアアフィリエイトは、単一のランサムウェア開発者と排他的に結び付いているようには見えません。ランサムウェア開発者がオフラインになったり引退した場合、そのアフィリエイトの多くは別の RaaS オペレーターへと移っていきます。

たとえば、Leafroller（別名 REvil）グループが 2021 年 7 月初旬に Sodinokibi ランサムウェアの運営を突然停止した際、そのアフィリエイトの一部がライバルの運営会社に移ったと思われます。Sodinokibi の消滅後、LockBit を利用した攻撃が顕著に増加しており、シマンテックは、少なくとも 1 つの元 Sodinokibi のアフィリエイトが LockBit を利用している証拠を発見しました。この攻撃者は、2021 年 7 月まで一貫した TTP を使用して Sodinokibi を被害者に配信していましたが、その時点でペイロードを LockBit に切り替えていました。

このアクターの攻撃は mimi.exe という名前のファイルから始まります。このファイルは、多数のパスワードダンプツールをドロップするインストーラーです。ランサムウェアが起動する直前には、さまざまなサービスを無効にしたり、RDP（リモートデスクトッププロトコル）へのアクセスをブロックしたり、シャドーコピーを削除したりするための大量のコマンドが実行されます。このアクターは、ランサムウェアのペイロードを一貫して「svhost.exe」と命名しており、この習慣は LockBit への移行後も維持されています。

ランサムウェアの脅威アクター

Miner

別名： Wizard Spider

ランサムウェアファミリー： Ryuk、Conti、GoGalocker（活動休止中）、MegaCortex（活動休止中）

活動開始時期：2014 年

Miner は、少なくとも 2014 年 6 月から活動していると考えられており、金融詐欺キャンペーンでバンキング型トロイの木馬 Dyre の使用を開始しました。Dyre は 2015 年 11 月に活動を停止しましたが、2016 年 9 月に Trickbot と呼ばれる新しい金融トロイの木馬が登場しました。その後、Trickbot と Dyre が共通のオーサーシップを持つように見えたことから、Miner グループとの関連が指摘されました。

Trickbot はもともと、被害者がオンラインバンキングアプリケーションを使用しているときにオンライン取引を傍受するための MitB（Man-in-the-Browser）攻撃を実行できる金融トロイの木馬として開発されました。その後、資格情報の窃取や他のマルウェアの配信チャネルとして再利用されています。

Miner はまた、2020 年 4 月に BazarLoader と BazarBackdoor という新しいマルウェアを導入しました Trickbot と同様、BazarLoader はスパムメールキャンペーンで拡散され、第 2 段階の BazarBackdoor ペイロードを配信することができます。Trickbot とは異なり、Bazar ファミリーは主にマルウェアの配布を目的として開発されたようです。

2018 年には、Ryuk ランサムウェアを使用して、標的型ランサムウェアにも手を広げました。Ryuk は、古い Hermes ランサムウェアファミリーをベースにしており、オリジナルの開発者から入手したと思われます。

Ryuk の攻撃では、感染経路として Trickbot や Emotet といったボットネットが頻繁に使用されています。その後、Cobalt Strike や Metasploit などの一般に公開されているマルウェアを使用して、ネットワークを列挙し、ラテラルムーブメント（水平移動）や権限の増加を図ります。このステップが完了すると、攻撃者はドメインコントローラの管理者権限を獲得します。その後、攻撃者は PsExec を介して導入されたバッチファイルを使用して、環境全体のバックアップ / 復元機能とセキュリティサービスを無効化および削除します。

2019 年、Miner は、GoGalocker（別名：LockerGoga）と MegaCortex という 2 つの新しいランサムウェアファミリーを使い始めました。どちらも Ryuk とコードを共有しており、シマンテックによる分析では、3 つのランサムウェアファミリーが使用するコマンド & コントロール（C&C）インフラストラクチャに重複が見られました。GoGalocker と MegaCortex による攻撃は、2020 年初頭に停止しました。

その後、Miner は、2019 年 12 月に初めて登場した Conti ランサムウェアとつながりました。Conti は、RaaS モデルの下でアフィリエイトが使用するために特別に作成されたという憶測もありますが、これはまだ確認されていません。

Ryuk も Conti も、非常に似た TTP を使って配布されています。2021 年 5 月にシマンテックが行った調査では、両者の配信に使用されたツールに大きな重複が見られました。この攻撃では、Cobalt Strike の亜種が多用されていました。いくつかのケースでは、感染経路は IcedID マルウェアを経由しているようで、Longlist として知られるマルウェアを配信し、それが Cobalt Strike のインストールに使用されています。

ケーススタディ : BazarLoader 攻撃におけるソーシャルエンジニアリング要素

Miner グループの BazarLoader マルウェアを利用した最近の攻撃キャンペーンでは、攻撃者が被害者のネットワークにマルウェアを送り込むために、ある程度のソーシャルエンジニアリングを採用していました。このキャンペーンは、2021 年 7 月に複数の大規模組織を対象に行われ、被害者のネットワーク上の 1 台のコンピュータに悪意のある Excel ファイルが出現したことから始まりました。

すべてのケースで最初の感染経路は確認されていませんが、ある組織では、従業員にスピアフィッシングメールが送信されたことが攻撃の始まりでした。このメールでは、受信者が最近交通事故に遭い、自動車保険に請求があったとされていました。メールには、詳細情報を問い合わせるための電話番号が記載されていました。メールの内容に納得した従業員は、その番号に電話をかけました。電話した従業員はある URL へと誘導されました。この URL から悪意のある Excel ファイルがダウンロードされました。

標的に疑わしいファイルをダウンロードさせるために電話連絡を使う戦術は、検知を逃れるための工夫です。知らない送信者から届いた電子メールに不審な添付ファイルやリンクがあると、セキュリティソフトで自動的にブロックされたり、受信者に疑われたりする可能性があります。一方、エンドユーザーが手動で入力した URL は、それほど警戒されない可能性があります。

攻撃者は、侵入したコンピュータに新しいディレクトリを作成し、そこに新しい名前で Certutil をコピーしました。

CSIDL_COMMON_APPDATA\epvv2e\epvv2e.exe

この偽装テクニックは以前に Kaseya の攻撃で使用されており、Certutil の悪意ある使用を隠すことを目的としています。

Certutil は、悪意のある DLL ファイルをダウンロードするために使用されます。これは、BazarLoader と同定されました。シマンテックは、攻撃者がペイロードの導入に成功したことを確認していません。しかし、これらの TTP が過去のランサムウェア攻撃と関連していることから、初期段階のランサムウェア活動である可能性が高く、Ryuk が関与している可能性が高いと考えられます。

Leafroller

別名 : REvil

ランサムウェアファミリー : Sodinokibi（活動休止中）、Gandcrab（活動休止中）

活動開始時期 : 2018 年

Leafroller は、2019 年 4 月から 2021 年 7 月にかけて、Sodinokibi ランサムウェアを使用した標的型ランサムウェア攻撃を実行しました。このグループは、RaaS モデルを用いて、アフィリエイトと連携していることが知られています。多くのランサムウェアグループと同様に、Leafroller とそのアフィリエイトは、暗号化する前の被害者のデータを日常的に盗み、そのサンプルを一般公開の Web サイトに掲載しています。そして、身代金を支払わなければ機密情報を掲載すると脅して、被害者にさらなる圧力をかけて恐喝しようとします。

Sodinokibi を作成する前には、古いタイプの Gandcrab ランサムウェアのソースコードを開発者から入手して、その攻撃に関与していました。また、Gandcrab を共有していたアフィリエイトの一部は、Sodinokibi に移行した後も継続していました。

Leafroller は、身代金の額を最大化するために、知名度の高い組織を狙うことで知られています。代表的な被害者としては、2020 年 1 月に攻撃を受けた外貨両替サービス会社 Travelex が挙げられ、ランサムウェア集団に 230 万ドルの身代金をもたらしました。

また、Leafroller は、新しい TTP を頻繁に試すことでも知られています。2020 年には、被害者のネットワークをスキャンして、クレジットカードや POS（販売時点情報管理）のソフトウェアを探す様子が観察されました。 攻撃者がこのソフトウェアを暗号化やデータ窃取の対象としていたかどうかは明らかではありませんでした。2021 年 7 月、Sodinokibi は、Kaseya ソフトウェアを含む斬新なランサムウェア・サプライチェーン攻撃に使用されました（「ケーススタディ : ランサムウェアサプライチェーン攻撃」を参照）。

Kaseya 攻撃から 2 週間も経たないうちに、Leafroller に属するインフラストラクチャと Web サイトがオフラインになりました。このグループに関連するダークネットとクリアネットの両方のインフラストラクチャが影響を受け、身代金交渉サイト、データ侵害サイト、C&C サーバーなどが含まれます。同グループが姿を消した理由はまだ不明です。しかし、本稿執筆時点では、Sodinokibi の新たな活動を示す証拠はありません。

Hispid

別名 : EvilCorp、Indrik Spider、TA505

ランサムウェアファミリー : BitPaymer（廃止）、DoppelPaymer、WastedLocker、Hades、Phoenix Locker

活動開始時期 : 2011 年

Hispid は、2011 年頃から活動しているベテランのサイバー犯罪者集団です。このグループは、もともと金融詐欺を働いており、バンキング型トロイの木馬 Dridex を使用していました。Dridex は、その最盛期には、数百万のメールアドレスを対象とした大規模なスパムで配布され、最も多くのサイバー犯罪の脅威の 1 つとなりました。

2017 年頃、同グループは標的型ランサムウェアに重点を移し、BitPaymer ランサムウェアファミリーを導入しました。その後、DoppelPaymer と呼ばれる 2 つ目のランサムウェアファミリーを導入しました。このランサムウェアは、いくつかの細かい違いはあるものの、同じコードをベースにしています。DoppelPaymer は、アフィリエイトが使用するために開発されたと報告されていますが、シマンテックはこれを確認できていません。

Miner が Trickbot を使い続けたのと同様に、Hispid はランサムウェアに移行した後もしばらくの間 Dridex を使い続け、ランサムウェア攻撃の前駆ツールとして使用するためにマルウェアを再利用していました。

2019 年 12 月には、2 人のロシア人が、同グループの活動に関連する複数の容疑で起訴されました。彼らの逮捕または有罪判決につながる情報に対して、500 万ドルの報奨金が提供されました。

2020 年 5 月、Hispid はツールを一新し、新たなランサムウェアファミリー WastedLocker を導入しました。攻撃は、ソフトウェアの更新を装った SocGholish と呼ばれる悪質な JavaScript ベースのフレームワークから始まりました。2020 年 6 月にシマンテックが行った調査では、米国の新聞社の Web サイト数十件を含む 150 以上の侵害された Web サイトで SocGholish が発見されました。

攻撃者が被害者のネットワークに足場を築くと、PowerShell を使ってローダーをダウンロードして実行しました。このローダーには、.NET インジェクターと Cobalt Strike Beacon のローダーが含まれていました。

Cobalt Strike Beacon は、コマンドの実行、他のプロセスの注入、現在のプロセスの昇格、他のプロセスへのなりすまし、ファイルのアップロードとダウンロードなどに使用できます。PowerView の Get-NetComputer コマンドは、攻撃者によってランダムな名前に変更されていました。そしてこのコマンドは、Active Directory データベース内のすべてのコンピュータオブジェクトを検索しました。

特権の昇格は、Windows オペレーティングシステムのアクティベーションと更新を行う Windows コマンドラインユーティリティである Software Licensing User Interface ツール（slui.exe）を含む、一般に文書化された手法を用いて行われました。

攻撃者は、Windows Management Instrumentation（WMI）コマンドラインユーティリティ（wmic.exe）を使用してリモートコンピュータ上でコマンドを実行し、新しいユーザーを追加したり、追加でダウンロードした PowerShell スクリプトを実行したりしました。Cobalt Strike は、ProcDump を使ったクレデンシャルダンピングの実行や、ログファイルを空にするためにも使用されました。

ランサムウェアを展開するために、攻撃者は Windows Sysinternals ツールの PsExec を使用して、Windows Defender を管理するための正規のコマンドラインツール（mpcmdrun.exe）を起動し、ダウンロードしたすべてのファイルや添付ファイルのスキャンを無効にしたり、インストールされているすべての定義ファイルを削除したり、場合によってはリアルタイム監視を無効にしたりしていました。

その後、PsExec を使用して PowerShell を起動し、win32_service WMI クラスを使用してサービスを取得し、net stop コマンドを使用してこれらのサービスを停止しました。Windows Defender が無効化され、組織全体のサービスが停止された後、PsExec を使って WastedLocker ランサムウェア自体が起動され、データの暗号化とシャドウボリュームの削除が開始されました。

2021 年 3 月、同グループはランサムウェアの新たな亜種 Hades を導入しましたが、そのコードのかなりの部分は WastedLocker と重複していました。Hispid が Hades ランサムウェアを開発したのは、2019 年に米財務省外国資産管理局（OFAC）が課した、被害者が脅威グループに支払いを行うことを禁止する制裁措置に対応するためであると考えられます。

本稿執筆時点で、同グループは、米国の制裁に違反しないように被害者が支払いをしないことを恐れて、定期的にランサムウェアの名前を変更していると報じられています。Hades はその後 Phoenix Locker に改名され、2021 年 6 月時点では、すでに Babuk グループに関連している PayloadBin という名前を使用していたと言われており、被害者に別のアクターから感染したと思わせるためだと推定されます。

Thysanura

別名 : Avaddon

ランサムウェアファミリー : Avaddon

活動開始時期 : 2019 年

少なくとも 2019 年から活動している Thysanura は、大規模な組織に対して標的型ランサムウェアキャンペーンをしかけることで知られています。このグループは、RDP や仮想プライベートネットワーク（VPN）などのリモートアクセスのログイン資格情報を使用して、被害者を頻繁に侵害します。

Thysanura は、RaaS モデルで運営されており、ロシア語のサイバー犯罪フォーラムで宣伝されています。このグループは複数の恐喝戦術を使って被害者に支払いを迫ります。

ファイルを暗号化するだけでなく、被害者から盗んだ情報を流出させると脅し、2021 年 1 月には、身代金を支払わない被害者に対して、DDoS（分散型サービス拒否）攻撃を行うと言い始めました。今までのところ、このグループがこの脅迫を実行したかどうかはまだ確認されていません。

攻撃者は、被害者のネットワークにアクセスした後、ネットワークのマッピングを行い、削除や暗号化の対象となるバックアップを特定します。Avaddon を使用する攻撃者は、被害者を侵害するために以下のツールを利用します。

- PowerShell
- WMIC.exe（WMI -Windows Management Instrumentation）
- Svchost.exe（サービスホストシステムプロセス）
- Taskhost.exe（ホストプロトコル）

2021 年 6 月 11 日に、このグループは活動をやめて被害者に復号化キーを渡したと発表しました。この集団はをニュースサイト Bleeping Computer に 3000 近い復号キー送り、それを受けてセキュリティ会社 Emsisoft が無料で公開する復号ツールを制作しました。本稿執筆時点では、このグループが永久に消滅したかどうかは不明なままです。

Syrphid

別名 : LockBit

ランサムウェアファミリー : Lockbit

活動開始時期 : 2019 年

LockBit ランサムウェアが初めて登場したのは 2019 年 9 月で、当初は暗号化されたファイルに使用していたファイル拡張子にちなんで ABCD と呼ばれていました。2020 年 1 月には、アフィリエイトプログラムを作成して RaaS ビジネスモデルに移行することで、その活動を拡大しました。

LockBit を使用する攻撃者は、古い VPN サービスを実行している Web サーバーに対して総当たり攻撃によって組織を侵害することで知られています。また、大量の脆弱性スキャン、フィッシング、クレデンシャルスタッフィングなどを媒介とすることも報告されています。さらに、侵害済みのサーバーへのアクセスをアンダーグラウンドフォーラムで購入しているとも言われています。

場合によっては、ネットワーク内で自由に活動するために総当たり攻撃で管理者の資格情報を取得することもあります。また、侵入後（post-exploitation）のフレームワークを使用して、特権昇格やラテラルムーブメントを行うことも知られています。

Syrphid はファイルを暗号化する前に、標的のネットワーク上の機密データを特定し、外部のホスティングサービスにエクスポートしようと試みます。アフィリエイトは、被害組織ごとにランサムウェアを独自に構築して使用します。

Lockbit を利用した攻撃は 2021 年 7 月に顕著に増加しており、Syrphid が Sodinokibi の元アフィリエイトを勧誘しようとしていたことを示唆する証拠もあります（「ケーススタディ : アフィリエイト間での忠誠心の変化」を参照）。

Snakefly

別名 : Clop

ランサムウェアファミリー : Clop

活動開始時期 : 2019 年

Snakefly は、Clop ランサムウェアを開発したことで知られており、Hispid（別名 Evil Corp）が所有する配信チャネルを頻繁に活用しています。このグループは、2019 年のマーストリヒト大学への攻撃など、いくつかの注目を集める事件に関連しています。

同グループの攻撃は一般的に、より説得力を持たせるために、以前に侵害されたアカウントから送信される悪意のある電子メールから始まります。このメールには、危険なウェブサイトにリダイレクトする HTML 添付ファイルが含まれており、その後、Get2 ローダーをドロップする悪意のあるマクロを含む文書が配信されます。これにより、SDBot マルウェアやその他のリモートアクセスツール（RAT）がダウンロードされ、攻撃者がネットワーク上を水平移動（ラテラルムーブメント）したり、データを流出させたり、Clop ランサムウェアをダウンロードしたりするのを支援します。

ランサムウェアのペイロードの中には署名入りの証明書が付随しているものがあり、正規のプログラムのように誤認されやすく、セキュリティ対策を回避できる可能性があります。Clop は、実行されるとセキュリティ製品を探し出して削除しようとします。Malwarebytes、ESET、および Microsoft のセキュリティ製品を Clop が削除したり停止させたりすることが、第三者によって確認されています。このランサムウェアは、ファイルを暗号化し、感染したファイルに .clop という拡張子を付けた上で、身代金を要求するメッセージをマシンに表示します。

このランサムウェアは、暗号化の前に被害者のデータを盗み出し、身代金を支払わないとデータを公開すると脅すことでも知られています。最近の多くのランサムウェアグループと同様に、このグループも身代金の支払いを拒否した被害者から盗んだデータを公開する Clop データリークサイトを運営しています。

Coreid

別名 : Darkside

ランサムウェアファミリー : Darkside、BlackMatter（未確認）

活動開始時期 : 2020 年

Coreid は、一時的に最も多くの標的型ランサムウェアの脅威の一つとなり、2021 年 5 月に米国東海岸への燃料供給を停止させた Colonial Pipeline 社への攻撃を筆頭に、数々の野心的な攻撃に使用されました。

Coreid は、RaaS モデルで運営されており、アフィリエイトと協力してランサムウェア攻撃を行い、利益の分配を受けていました。多くのランサムウェアアクターと同様に、Coreid に関連する攻撃は被害者のデータを盗み、それを公開すると脅して被害者に身代金の支払いを迫ります。

Darkside を利用する攻撃者は、被害者のネットワークに侵入すると、通常、データ、資格情報、その他の機密情報の流出を開始します。また、攻撃者はネットワーク上を横方向に移動（ラテラルムーブメント）し、ドメインコントローラ（DC）へのアクセスを試みます。DC に到達すると、機密情報を流出させ、さらに PowerShell を使用して DarkSide バイナリをダウンロードします。

この攻撃者は、DC 自体に企業名を使用した共有フォルダを作成し、そこに Darkside バイナリをコピーすることが知られています。その後、攻撃者は BITSAdmin を使用して、共有フォルダからネットワーク上の他のコンピュータにランサムウェアのバイナリを配信します。

Coreid のアフィリエイトは、被害者とのコミュニケーションやランサムウェアの管理に TOR を使用しています。Coreid は、身代金の支払いを暗号通貨モネロ（Monero）で要求するようアフィリエイトに勧めていると言われています。おそらく、暗号通貨の高い匿名性が理由であると考えられます。

Coreid は、Colonial 社への攻撃の後、同グループのインフラストラクチャの一部がオフラインになった後で、活動を停止したようです。

2021 年 7 月下旬、メディアの報道によると、Coreid は BlackMatter という名前の新たなランサムウェアの脅威に関連しています。このランサムウェアは、Darkside が使用していたものと同じ暗号化ルーチンを使用していると考えられています。Recorded Future 社とのインタビューで、BlackMatter の開発者はそのつながりを否定し、「Darkside チームとは過去に一緒に仕事をしたことがあるので知っていますが、私たちは Darkside ではありません。彼らのアイデアはよく使わせてもらっていますが」と述べています。しかし、ブロックチェーン分析企業の Chainalysis は、2 つの脅威の間に金銭的なつながりがあることも発見し、BlackMatter は Coreid が作成したものであると結論づけています。シマンテックの評価では、BlackMatter に関する決定的な帰属を決めるのはまだ早すぎるとしています。

Hornworm

別名 : RagnarLocker、Viking Spider

ランサムウェアファミリー : RagnarLocker

活動開始時期 : 2020 年

Hornworm は、RagnarLocker ランサムウェアと関係しています。RagnarLocker は 2020 年初頭に初めて登場し、2020 年 11 月には FBI のフラッシュアラート（警戒速報）の対象となりました。FBI の報告によると、RagnarLocker は大企業のネットワーク上のコンピュータを暗号化し、1,100 万ドルの身代金を要求し、身代金が支払われなければ盗んだ 10TB のデータを公開すると脅しました。その後、米国内の他のさまざまな組織に対してランサムウェア攻撃をしかけています。

RagnarLocker は検知を逃れるために、感染したコンピュータ上に完全な仮想マシンとして導入されていることが報告されています。一部のケースでは、MSI パッケージに紛れ込ませたペイロードが配信されていました。このパッケージには、古い Oracle VirtualBox（Sun xVM VirtualBox バージョン 3.0.4）の作業用インストールと、micro.vdi という名前の仮想ディスクイメージファイル（VDI）が含まれています。micro.vdi は、MicroXP v0.82 と呼ばれる、Windows XP SP3 オペレーティングシステムのストリップダウンバージョンのイメージです。このイメージには、49 kB のランサムウェアのペイロードが含まれています。Hornworm がこの手口の先駆けだったかもしれませんが、その後シマンテックは、他のペイロードを使用する攻撃者が、Hornworm のようにペイロードを仮想マシンから実行しようと試みるケースを確認しています。

RagnarLocker は、暗号化されたファイルに .RGNR_<ID> という拡張子を付けます。<ID> には当該コンピュータの NETBIOS 名が入ります。RAGNAR_LOCKER と名乗る攻撃者は、コンピュータに .txt 形式の身代金メモを残し、身代金の支払い方法や復号化キーの受け取り方法などを説明します。このグループは、難読化の手法を頻繁に変更することで知られており、VMProtect、UPX、および独自のパッキングアルゴリズムを持っています。

Hornworm は暗号化の前に被害組織のデータを盗み出し、身代金を支払わないとそのデータを公表すると脅すことが報告されています。その目的のために、Tor 上でホストされたデータリーク専用の Web サイトを使用しています。

ケーススタディ : Hornworm と FIN8 の提携

Hornworm はサイバー犯罪集団 FIN8 と関係を築いている可能性があります。2021 年初頭には、FIN8 が米国の金融サービス企業で感染させたマシンに RagnarLocker ランサムウェアを導入しているのが目撃されており、これはシマンテックが FIN8 が感染させたマシンにランサムウェアを導入しているのを確認した初めてのケースでした。

FIN8 グループが使用することが知られている BADHATCH マルウェアは、2021 年 1 月に PowerShell を介して同組織のコンピュータで起動されました。これも FIN8 が使用していることで知られる悪用された正規の sslip[.]io サービスから、複数の PowerShell スクリプトがダウンロードされました。また、WMI オブジェクトから未知のコンテンツをダウンロードするためにも PowerShell が使用されました。FIN8 は PowerShell を使って被害者のマシンに悪意のあるツールを導入します。

さらに、キーロガーも導入されて実行されました。2021 年 2 月、ネットワーク上で不審な動きが初めて確認されてから 3 週間半後、オープンソースツール Rclone がデータの流出に使用されました。その後 1 カ月も経たない 3 月半ばには、Safebitsloader と呼ばれる別のツールによって RagnarLocker ランサムウェアがネットワーク内にドロップされました。

このネットワーク上での FIN8 と RagnarLocker の活動は、2 つの異なるアクターによって別々に行われた可能性がありますが、そうではないことをいくつかの事実が示しています。これには、BADHATCH と Rclone の両方が同じ IP アドレスからダウンロードされたこと、ランサムウェアと PowerShell スクリプトの両方が感染したコンピュータの同じディレクトリ（%WINDIR%\temp）にダウンロードされたことが含まれます。

Leaftier

別名 : Babuk

ランサムウェアファミリー : Babuk

活動開始時期 : 2021 年

2021 年の初頭に初めて世間の関心を集めた Leaftier は、データ侵害の脅迫に重点を置いている点が特徴です。当初は RaaS というビジネスモデルで活動しており、被害者からデータを盗むだけでなく、ファイルを暗号化するという二重脅迫戦術で被害者を脅していました。しかし、その後、暗号化を行わず、データの窃取のみで被害者から金銭を搾取することを発表しました。

Babuk は、Vasa Locker という別のランサムウェアの脅威と高い類似性があることが判明しました。McAfee が分析した Vasa のサンプルは、Babuk と同じコードベースを約 86%共有しており、Babuk の最初のリリースの 1 カ月前にコンパイルされていました。これらの事実から、Babuk と Vasa Locker の背後にいるアクターは同一であるか、または互いに強いつながりがあると考えられます。

2021 年 4 月下旬、Leaftier は、アフィリエイトプログラムを終了し、被害者のコンピュータの暗号化に頼らない脅迫モデルに移行することを発表しました。このグループは、その代わりに、被害者から盗んだ情報の身代金を要求することに注力するとしています。

2021 年 5 月、Leaftier は、他のアクターが利用できるデータリークサイトとなる「独立リーク」のためのプラットフォームの開発を発表しました。同時に同グループはリブランディングを行い、新しいリークサイト（Payload.bin）の名前を Babuk から Payload Bin に変更しました。

2021 年 7 月初旬、Leaftier が企業ネットワークを標的としたランサムウェアの使用に戻ったと思われることが報告されました。この集団は Babuk ランサムウェアの新バージョン（Babuk v.2.0）の使用を開始し、新たなデータリークサイトに移行しました。

Leaffolder

別名 : Maze、Egregor

ランサムウェアファミリー : Maze、Egregor

活動開始時期 : 2019 年

Leaffolder の活動を示す最初の証拠は、2019 年 5 月、Maze ランサムウェアの登場にあります。Leaffolder は、暗号化の前に被害組織からデータを流出させ、身代金を支払わないとこのデータを公開すると脅す戦術の先駆者として知られています。この手口は、すぐに他のさまざまな標的型ランサムウェアグループによって模倣されました。

Maze の主な配信チャネルは、エクスプロイトキットの Fallout と Spelevo で、被害者はスパムメールキャンペーンを介してこれらのキットに誘導されました。攻撃者は、ネットワーク上の 1 台のコンピュータにアクセスすると、ネットワークを水平移動（ラテラルムーブメント）してマシンを列挙するために、コモディティマルウェア Cobalt Strike と Metasploit Framework をダウンロードします。

2020 年 10 月、Leaffolder は、ランサムウェア Maze の運用を停止することを発表しました。同グループはその後、Maze が引退した直後に登場した Egregor と呼ばれる新しいランサムウェアの運用と関連していました。Maze を利用していた多くのアフィリエイトが Egregor の利用に移行しました。

Egregor のアフィリエイトは、2021 年 2 月に法執行機関による取り締まりの対象になりました。Egregor は、この取り締まりの後、活動を停止していると考えられます。

Canthroid

別名 : UNC2447

ランサムウェア : Thieflock

活動開始時期 : 2021 年

Canthroid が初めて登場したのは 2021 年初頭で、Thieflock を使った標的型ランサムウェア攻撃を行うようになりました。また、RaaS プログラムを運営しています。

現在までに、Sonicwall VPN のゼロデイ脆弱性（CVE-2021-20016）を悪用して被害者を危険にさらしたことで知られています。この脆弱性は 2021 年 2 月にパッチが適用されましたが、Canthroid はパッチが適用されていないバージョンのソフトウェアを使用する組織を攻撃し続けています。エクスプロイトによる侵害が成功すると、攻撃者は自分の資格情報を作成し、標的のネットワークに参加することができます。

ネットワークに侵入すると、ホスト名やネットワークサービスの発見に使用される一般に公開されているツールである SoftPerfect Network Scanner を使用することが確認されています。また、カスタムリモートアクセスツールである SombRAT の使用も確認されています。このツールを使用することで、攻撃者はさらなるツールをダウンロードしたり、C&C サーバーとの通信を維持したりすることができます。

暗号化する前に、標的のネットワークからデータを流出させることが知られています。この攻撃者は、暗号化機能を備えたクラウドストレージサービスである pCloud を使用していると報告されています。

ツール、戦術、手順（TTP）

ほとんどのランサムウェア攻撃は複数の段階を経て行われますが、特に標的型ランサムウェア攻撃では、通常、多くの段階を経て、攻撃者の側でかなりのレベルのやり取りが行われます。被害者のネットワークに侵入し、資格情報を盗み、権限を昇格させ、ネットワーク内を水平移動し、複数のコンピュータにランサムウェアのペイロードを導入するために、さまざまなツール、戦術、手順（TTP）が用いられます。

ランサムウェア攻撃者が使用する TTP を知ることで、ネットワーク防御者は、組織がどのように侵害される可能性があるかをより深く理解することができ、防御策の優先順位を決める際の指針となります。たとえば、PsExec などの Windows ツールは攻撃者に頻繁に悪用されるため、管理者権限を持つアカウントの数を減らしたり、管理者アカウントの保護を強化したりすることで、攻撃成功のリスクを軽減することができます。

表 1: ランサムウェア攻撃で最もよく観測された TTP-2021 年 4 月から 2021 年 6 月

TTP	ランサムウェア調査の割合
Cobalt Strike	41%
PsExec	33%
Netscan	15%
Mimikatz	15%
Adfind	15%
Weirdloop	11%
IcedID	11%
SystemBC	7%
ProcDump	7%
Nsudo	7%
Defender を無効化	7%
シャドーコピーを削除	7%
WMI	4%
rclone	4%
Qakbot	4%
BITSAdmin	4%

シマンテックでは、最近のランサムウェアの調査結果から、前駆ツールが発見された場合、ランサムウェア攻撃で最もよく使用されている TTP を把握することができました。最も頻繁に使用されたツールは、コモディティマルウェアの Cobalt Strike（全調査の 41% で観測された）でしたが、PsExec や WMI など、自由に利用できるデュアルユースのツールやオペレーティングシステムの機能がリストの大部分を占めていました。

- **Cobalt Strike:** コマンドの実行、他のプロセスの注入、現在のプロセスの昇格、他のプロセスへのなりすまし、ファイルのアップロードとダウンロードなどに使用できる市販ツールです。このツールには表向きにはペネトレーションテストツールとしての正当な用途がありますが、常に悪意のあるアクターに利用されています。
- **PsExec:** 他のシステム上でプロセスを実行する Microsoft Sysinternals ツールです。このツールは主に攻撃者が攻撃対象のネットワーク上で水平移動するために使用されます。
- **Netscan:** SoftPerfect Network Scanner は、ホスト名とネットワークサービスの検出に使用される公開ツールです。
- **Mimikatz:** 権限の変更やセキュリティ証明書のエクスポート、Windows パスワードの平文テキストでの復元（構成による）ができる、無償で入手できるツールです。
- **Adfind:** Active Directory に対するクエリに利用できる無償ツールです。
- **Weirdloop:** Weirdloop は、2021 年に Ryuk が関与した一部の攻撃で使用された Cobalt Strike HTTPS ステージャーのローダーです。
- **IcedID:** もともと金融トロイの木馬として開発されましたが、現在ではランサムウェアの攻撃者と共同で活動することが多いボットネットマルウェアです。
- **SystemBC:** 感染したコンピュータ上にバックドアを開いて、SOCKS5 プロキシプロトコルを使って C&C サーバーと通信できるコモディティマルウェアです。
- **ProcDump:** Microsoft Sysinternals のツールで、アプリケーションの CPU スパイクを監視したり、クラッシュダンプを生成したりしますが、一般的なプロセスダンプユーティリティとしても使用できます。
- **Nsudo:** オープンソースのシステム管理ツールですが、特権の昇格に悪用できます。
- **Windows Management Instrumentation（WMI）（wmic.exe）:** Microsoft のコマンドラインツールで、リモートコンピュータ上でコマンドを実行するために使用できます。
- **Qakbot:** もともとは金融トロイの木馬として開発されたボットネットマルウェアです。
- **BITSAdmin:** Microsoft のコマンドラインツールで、ダウンロードやアップロードのジョブを作成し、その進捗状況を監視するために使用されます。

ケーススタディ：ランサムウェアサプライチェーン攻撃

標的型ランサムウェア攻撃が攻撃者にとってきわめて高収益であることは証明済みですが、それでも攻撃者は継続的に戦術を洗練させることを止めませんでした。2020 年の大きな革新は、ネットワーク上のコンピュータを暗号化する前にデータを盗み、身代金を払わないとこのデータを公開すると脅すという手法でした。データ侵害の脅威は、被害者である組織への支払い圧力を高めます。また、暗号化されたシステムをバックアップから復元できる被害者に対しても、この脅迫は有効です。

2021 年 7 月には、Sodinokibi ランサムウェアを使った攻撃者が、サプライチェーン攻撃によってランサムウェアを配信するという新たな戦術を試みました。この攻撃では Kaseya VSA ソフトウェアのゼロデイ脆弱性（CVE-2021-30116）が悪用され、このソフトウェアを使用する複数のマネージドサービスプロバイダ（MSP）を介して被害者の組織を危険にさらしました。

このランサムウェアは、世界中で少なくとも 1,500 の組織に感染したと考えられます。このプロセスの多くは自動化されており、ランサムウェアは複数の組織で同時に作動し、被害者に攻撃の予兆を与えないようにしていたと思われます。米国では 7 月 4 日の週末が祝日と重なったため、多くの組織で従業員の配置が手薄になると見込み、そのタイミングを狙って攻撃が行われた可能性があります。

攻撃者はこのエクスプロイトを利用して、悪意のあるスクリプトと agent.crt という名前の ASCII PEM を Kaseya VSA クライアントに配信しました。ドロッパーは、ASCII PEM ファイルの中に隠れており、Microsoft Defender を無効にしようとした後、Certutil を使って解読されました。ドロッパーは 2 つのリソースを投下しました。Windows Defender（MsMpEng.exe）の古い正規バージョンのコピーと、悪意のあるカスタムローダーです。ドロッパーは 2 つのファイルをディスクに書き込み、MsMpEng.exe を実行し、カスタムローダーのエクスポート（mpsvc.dll）をサイドロードして実行しました。

今回の攻撃が新たなトレンドの始まりとなるかどうかは、まだわかりません。この攻撃の性質上、「従来の」標的型ランサムウェア攻撃と比較して、効果がやや低い可能性があります。攻撃が自動化されているため、攻撃者はデータの流出やバックアップの削除など、このような攻撃で行われる標準的な手順の一部を省略する必要がありました。

Sodinokibi の背後にある Leafroller グループは、攻撃から 2 週間も経たないうちにオフラインになりました。姿を消した理由は不明のままで、それが単なる偶然なのか、それとも Kaseya の攻撃に何らかの形で関連しているのかは不明です。

攻撃から数週間後、Kaseya 社はランサムウェア用の汎用復号化ツールを入手したと発表しました。 同社は、 「信頼できる第三者」 から復号化ツールを入手し、 現在、 影響を受けたお客様と共有していると述べています。

この攻撃後、攻撃者は、汎用復号化ツールに 7,000 万ドル、各 MSP 用の復号化ツールに 500 万ドル、あるいは暗号化されたコンピュータ 1 台につき 4 万ドルを要求したと報告しています。Kaseya 社は、復号化ツールを入手するために身代金を支払ったかどうかについては確認も否定もできないと述べています。

感染ベクトル

標的型ランサムウェアのグループは、多様な配布方法を用いています。標的型ランサムウェア攻撃は比較的件数が少ないため、感染経路の確立が困難な場合があります。標的型ランサムウェア犯行グループはスパイ活動グループから得た情報を利用して、攻撃対象ネットワークに足場を築くことが多いようです。

二次感染

二次感染は、過去 12 カ月の間に、ランサムウェアグループの最も一般的なアクセス手段の一つとなりました。一般的には、ランサムウェアグループが潜在的な被害者を大量に獲得できることから、大量メール送信型ボットネットを利用して配布されるマルウェアが対象となります。Trickbot のように、かつては金融詐欺に利用されていたトロイの木馬も、最近では主にランサムウェアをはじめとする他のマルウェアの配信チャネルとして利用されています。

また、ランサムウェアの攻撃者が、Trickbot ボットネットを所有する Miner グループのように、すでにボットネットを制御しているケースもあります。Trickbot は、Miner に帰属する Ryuk による攻撃の前駆ツールあると考えられています。Hispid も同様に、もともと金融機関への攻撃を目的として構築された独自のボットネット Dridex を活用して、組織にランサムウェアを配信する手段として活用しています。

その後、この攻撃パターンを再現しようと、既存のボットネットオペレーターとの協力関係を模索しているアクターもいます。その中でも最も注目すべきは、ランサムウェア Conti の少なくとも 1 つのアフィリエイトオペレーターが IcedID を使用していることです（「ケーススタディ：IcedID と Conti の提携」を参照）。

ケーススタディ：IcedID と Conti の提携

Conti ランサムウェアを含む攻撃についてシマンテックが最近行った調査では、複数の攻撃で一貫した攻撃チェーンが確認されており、Conti を利用する少なくとも 1 人の攻撃者が IcedID ボットネットとの連携を開始していたことが示唆されています。

標的となった組織での悪意ある活動の最初の証拠は、標的のネットワーク上に IcedID が存在していることでした。その後、IcedID は Longlist と呼ばれるマルウェアの配信に使用され、そのマルウェアは Cobalt Strike のインストールに使用されます。また、この攻撃には、一般に公開されているクレデンシャルダンプツールの LaZagne や、Active Directory のクエリに使用できる無償のデュアルユースツールの Adfind などが使用されました。

IcedID は広く配布されているマルウェアですが、これらの他のツールと一緒に存在していることから、ランサムウェア攻撃が準備されていると考えられます。

フィッシング

フィッシングは、最も広く利用されている感染経路の 1 つであり、業務上の連絡事項（請求書、配送確認書など）を装って従業員にメールを送信します。フィッシングキャンペーンの中には、関心のある標的を広範囲に探し出す無差別なものもあります。また、攻撃者が事前に標的を選び、組織内の特定の従業員にスピアフィッシングメールを送信する場合もあります。

スピアフィッシングキャンペーンは、組織の業務に関連したテーマを用いて、標的に合わせて行われることがあります。受信者がだまされて悪意のある添付ファイルを開いたり、悪意のあるリンクをクリックしたりすると、被害者のマシンにマルウェアがダウンロードされ、攻撃者は被害者のネットワーク上を移動し始めることになります。

マルバタイジング

これまでランサムウェアの感染経路としては知られていませんでしたが、2020 年に WastedLocker のオペレーターが利用したのはマルバタイジングでしたこのグループは、メディアのウェブサイトを侵害して、ソフトウェアの更新を装った SocGholish と呼ばれる JavaScript ベースのフレームワークを含む悪意のある広告を提供することが確認されています。

脆弱性の悪用

組織のネットワークに侵入するもう一つのルートは、公開されているサーバー上で動作する脆弱なソフトウェアを悪用することです。これまでのほとんどのケースではゼロデイ脆弱性は利用されておらず、攻撃者は JBoss や Apache Web サーバーなどのパッチが適用されていないソフトウェアの既知の脆弱性を利用していました。この戦術の主な利用者の 1 つは、今は亡き SamSam グループで、2019 年 11 月に活動を停止しました。最近では、Canthroid グループが Sonicwall VPN のゼロデイ脆弱性（CVE-2021-20016）を悪用して被害者を危険にさらしたことで知られており、Proxylogon Exchange Server の脆弱性も複数のアクターがランサムウェア攻撃を行うために活用していました。

セキュリティ対策に不備のあるサービス

もう 1 つの感染経路として、セキュリティが不十分なサービスを侵害することです。Crysis（別名 Dharma）は、漏洩した資格情報や脆弱な資格情報を利用して、セキュリティが不十分な RDP サービスを介して組織を攻撃することが繰り返し確認されています。今は亡き GandCrab グループは、インターネット上で公開されている MySQL データベースをスキャンして、マルウェアに感染させることが確認されています。

保護

シマンテックの支援策
シマンテックエンタープライズビジネスは、今日のセキュリティの課題に対処し、データとデジタルインフラストラクチャを多面的な脅威から保護するためのセキュリティソリューションの包括的なポートフォリオを提供しています。これらのソリューションには、高度な攻撃を防止し、検知するために設計されたコア機能が含まれます。

Symantec Endpoint Security Complete
Symantec Endpoint Security Complete（SESC）は、高度な攻撃からの防御を支援するために特別に開発されました。多くのベンダーが侵入を発見するための EDR を提供していますが、シマンテックと同じように、弱点があります。この弱点をシマンテックは盲点と呼んでいますが、SESC にはこの盲点をなくすための技術があります。
詳細はこちら

Privileged Access Management（PAM）
PAM ではセキュリティの侵害を防止するために、機密性の高い管理者クレデンシャルの保護、特権ユーザーアクセスの制御、セキュリティポリシーのプロアクティブな適用、特権ユーザーの活動の監視と記録が行えます。
詳細はこちら

Symantec Web Isolation
Symantec Web Isolation は、エージェンシーのエンタープライズシステムと Web 上のコンテンツサービスの間にリモート実行環境を構築することで、Web 上の脅威を排除し、未知の、分類されていない、潜在的にリスクのある Web サイトへのアクセスを提供するという難しい課題を解決します。
詳細はこちら

Symantec Secure Web Gateway（SWG）
SWG は、高性能なオンプレミスまたはクラウドのセキュア Web ゲートウェイを提供し、企業が未知の、分類されていない、またはリスクの高い Web サイトへのアクセスを制御またはブロックするために活用できます。
詳細はこちら

Symantec Intelligence Services
Symantec Intelligence Services はシマンテックの Global Intelligence Network を活用し、Symantec Secure Web Gateway、Symantec Content Analysis、Symantec Security Analytics などの複数のシマンテックネットワークセキュリティソリューションにリアルタイムの脅威インテリジェンスを提供します。
詳細はこちら

高度なサンドボックス機能を備えた Symantec Content Analysis
Symantec Content Analysis プラットフォームではゼロデイ脅威が自動的にエスカレーションされ、動的なサンドボックス機能を備えた Symantec Malware Analysis に仲介され、潜在的な APT ファイルやツールキットの詳細な検査とふるまい分析が行われます。
詳細はこちら

Symantec Security Analytics
Symantec Security Analytics は、充実したフルパケットキャプチャによるネットワークトラフィックの完全分析、高度なネットワークフォレンジック、異常検知、すべてのネットワークトラフィックのリアルタイムコンテンツ検査を提供し、インシデント対応者の迅速な解決を支援します。
詳細はこちら

軽減

企業を標的型攻撃から守るため、次のベストプラクティスを推奨します。

ローカル環境：

- ネットワーク内でのデュアルユースツールの使用を監視します。
- PowerShell が最新のバージョンであることと、ロギングが有効になっていることを確認します。
- RDP サービスへのアクセスを制限します。指定された既知の IP アドレスからの RDP のみを許可し、多要素認証（MFA）を使用していることを確認します。
- 管理者アカウントの利用について適切な監査と管理を実施します。また、管理者資格の盗難や悪用を防ぐために、管理業務用のワンタイムクレデンシャルを導入することもできます。
- 管理ツールの使用状況のプロファイルを作成します。これらのツールの多くは、攻撃者がネットワーク内を検知されずに水平移動するために使用されます。
- 可能であれば、アプリケーションのホワイトリストを使用します。
- PowerShell をロックダウンすることで、制約のある言語モードなどで、セキュリティを向上させることができます。
- たとえば Windows 10 で資格情報ガードを有効にしたり、SeDebugPrivilege を無効にしたりして、クレデンシャルダンピングを困難にします。
- 多要素認証は、漏洩した資格情報の有用性を制限するのに役立ちます。
- **社外関係者の通知を検討する計画を作成します。**FBI やその他の法執行機関など、必要な組織に正しく通知するために、確認のための計画を必ず立ててください。
- **重要な管理情報のハードコピーとアーカイブしたソフトコピーを入れた「ジャンプバッグ（救急バッグ）」を作成します。**これらの重要情報の利用が阻害されたときのために、トラブルシューティングに必要なハードウェアとソフトウェアもジャンプバッグに入れておきます。ネットワーク上のファイルが暗号化される可能性があるため、これらの情報をネットワーク上に保存しておくのでは意味がありません。

電子メール：

- 多要素認証を有効にすることで、フィッシング攻撃による資格情報の漏洩を防ぐことができます。
- 電子メールシステム関連のセキュリティアーキテクチャを強化し、エンドユーザーの受信箱に到達するスパムの量を最小限に抑え、SPF の使用やフィッシング攻撃に対するその他の防御策など、メールシステムのベストプラクティスに従っていることを確認します。

バックアップ：

- **バックアップコピーをオフサイトのストレージに保管します。**週次のフルバックアップと日次の増分バックアップを少なくとも 4 週間分オフサイトで保管します。
- **オンサイトにオフラインのバックアップを作成します。**ネットワークに接続していない場所でバックアップを保持し、ランサムウェアによる暗号化を回避します。
- **サーバーレベルのバックアップソリューションを検証およびテストします。**これはディザスタリカバリプロセスに含める必要があります。
- バックアップおよびバックアップデータベースに対する**ファイルレベルのアクセス権を設定**して、バックアップを暗号化されないようにします。
- **復元機能をテストします。**復元機能がビジネスのニーズに対応できるかを確認します。

Symantec™
A Division of Broadcom

製品情報とディストリビュータの完全なリストについては、弊社の Web サイト（broadcom.com）をご覧ください。

SES-TRT-WP109-JPN 2021 年 8 月 15 日