zscaler™ | ThreatLabz

2022年版 ThreatLabz ランサムウェアレポート

目次

はじめに

ランサムウェアのニュースを耳にしない日はないと言っても過言ではありません。Zscaler ThreatLabzの調査により、2021年2月～2022年3月に発生したランサムウェア攻撃が前年比で80%増加し、攻撃の件数と被害額が過去最高になったことがわかりました。

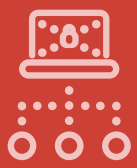
以下の3つの主なトレンドに基づき、ランサムウェアが攻撃者にとって、収益性の高い有効な攻撃手法となっていることがわかりました。

サプライチェーン攻撃

サイバー犯罪者は、信頼できるベンダ関係を悪用して組織を侵害し、複数（時には数百または数千）の被害者を同時に攻撃することで、攻撃の効果を何倍にもすることができます。

RaaS（Ransomware-as-a-Service）

アフィリエイトネットワークを使用してランサムウェアを広範囲に拡散することで、ネットワーク侵害のエキスパートであるハッカーが最も高度なランサムウェア集団と利益を共有できるようになります。



二重脅迫型攻撃

データの不正取得、DDoS（分散型サービス拒否）攻撃、顧客のコミュニケーションなどの複数の脅迫を積み重ねることで多くの身代金を手に入れようとする手法です。

これらの攻撃の被害額を合算すると、莫大な金額になります。業界の専門家は、ランサムウェアが2022年にはサードパーティの侵害やサプライチェーン攻撃で使用される最大の攻撃になり、ランサムウェア全体での被害額が今後も増加して、2024年までに420億ドルになる と予測しています。

この傾向が、さまざまな業界の組織でサイバーセキュリティにおけるランサムウェアの優先順位をさらに押し上げる結果につながりました。Aimpointの2022年版「CISOレポート」によると、ランサムウェアは他を引き離し、世界中のCISOが最も懸念する最大の脅威となっています。

最新のランサムウェア亜種を特定して防御するには、どうすればいいのでしょうか。 本レポートでは、その詳細を紹介しています。

ThreatLabzは、Zscaler Zero Trust Exchangeで処理される1日あたり2,000億以上のトランザクションと1億5,000万以上のブロックされた攻撃のデータをZscaler ThreatLabz脅威インテリジェンスと共に分析することで、最も活動的な脅威ファミリーを追跡して新たなトレンドを特定し、Zscalerのお客様の保護を強化しています。本レポートでは、2021年2月1日～ 2022年3月31日のランサムウェアデータを基に特定した最も広範囲で確認されたランサムウェアファミリーとその攻撃手法のほか、ランサムウェアからの防御に役立つ調査結果、予測、ベストプラクティスを紹介します。

主な調査結果：

ランサムウェア攻撃が前年比で80%増加： すべてのランサムウェアのペイロードがZscalerのクラウドで確認されました。

二重脅迫型ランサムウェアが117%増加： データの不正取得を戦略に採用する攻撃が増加していることがわかりました。二重脅迫型攻撃の増加率が特に大きかった業界は、医療（643%）、外食サービス（460%）、鉱業（229%）、教育（225%）、メディア（200%）、製造業（190%）などです。

最も標的にされた業界は2年連続で製造業： 二重脅迫型ランサムウェア攻撃のほぼ20%を占めました。

サプライチェーンランサムウェア攻撃の増加： サプライチェーン攻撃そのものも同様に増加しています。攻撃者は信頼できるサプライヤを悪用することで、外部攻撃に対する強力な保護機能を備えた組織も含む多数の組織を同時に攻撃できます。昨年のサプライチェーンランサムウェア攻撃としては、KaseyaとQuantaに対する大規模攻撃や、Log4jの脆弱性を悪用した多数の攻撃などが挙げられます。

RaaS（Ransomware-as-a-Service）攻撃の増加： ランサムウェアグループは、地下犯罪フォーラムでアフィリエイトを募る活動を続けています。これらのアフィリエイトは、大規模組織を攻撃し、一般的には被害者から手に入れた身代金の約80%と引き換えに、ランサムウェアグループが提供するランサムウェアを利用します。過去1年間の上位のランサムウェアファミリーの多く（11種のうち8種）が、RaaSモデルを使用して拡散しました。

法執行機関による取り締まりの強化： 昨年上位のランサムウェアファミリー、特に重要なサービスを標的にする多くのランサムウェアファミリーに世界中の法執行機関が注目し、REvil（KaseyaやJSBに対する有名な攻撃に関与）、DarkSide（コロニアルパイプラインに対する攻撃に関与）、Egregor（昨年最多だったランサムウェアファミリーであるMazeから名前を変更）はすべて、2021年に法執行機関によって資産が押収されました。

ランサムウェアファミリーは消滅するのではなく、リブランディングして活動を継続： 法執行機関による取り締まりが強化されていることから、多くのランサムウェア集団が解散し、同じ（または非常によく似た）攻撃手法を使って、新しい名前の組織として活動を再開しました。DarkSideはBlackMatterへ、DoppelPaymerはGriefへ、AvaddonはHaronとMidasへと名前を変えました。米国政府から制裁を受けたEvil Corpも名前を変えながらランサムウェア攻撃を続けています。

ロシアとウクライナの衝突による世界情勢の緊迫化： ロシアとウクライナの紛争に関連する攻撃がいくつか確認されており、HermeticWiperやPartyTicketなどの複数のワイパーを使用するものもあります。これまでのところ、この活動のほとんどがウクライナを標的にするものですが、多くの政府機関が、紛争が長引く現状で拡大する攻撃に備えるよう、組織に警告しています。

ゼロトラストは引き続き最善の防御策： 侵害の可能性や攻撃の成功によって生じる損害を最小限にするため、組織は、攻撃対象領域を削減し、最小特権によるアクセスコントロールを適用し、環境全体のデータの継続的な監視と検査を実施するなどの、多層型防御戦略を採用する必要があります。

ランサムウェアの進化

ランサムウェアは、被害者となる組織を混乱させるためにサイバー犯罪者が用いるマルウェアの一種です。ランサムウェアは組織の重要なファイルを判読不能な形に暗号化し、その復号化と引き換えに身代金の支払いを要求します。身代金要求は多くの場合、感染したシステムの数と暗号化されたデータの価値に比例し、数が多く、価値が高いほど要求額も高くなります。

攻撃者は2019年後半にランサムウェア攻撃を進化させ、一般に「二重脅迫型」ランサムウェアと呼ばれるデータを流出させる攻撃を仕掛けるようになりました。これらの攻撃では、被害者がデータの復号のための身代金の支払いを拒んで、自身でバックアップからデータを復元しようとすると、攻撃者は窃取したデータの流出を盾に脅迫します。2020年後半には、一部のランサムウェア攻撃者がDDoS戦術も追加して被害者のWebサイトやネットワークを攻撃するようになり、被害者を交渉に応じさせるためにさらなる業務妨害によって圧力をかけるようになりました。

2021年から2022年にかけて被害が最大になるランサムウェアのトレンドには、サプライチェーン攻撃が関係しており、この攻撃では、ベンダ（通常はソフトウェアやその他のテクノロジプロバイダ）の侵害をきっかけにその会社の製品に利用する組織に対する第2段階の攻撃が可能になります。サプライチェーン攻撃は2021年後半に51%も急増したと推定されます。サイバー犯罪者は、SolarWinds、Kaseya、Log4jなどの人気のソフトウェア製品のエクスプロイトによって大規模攻撃を仕掛けており、このトレンドが今後数年間にさらに増加することが予想されます。

ランサムウェアの攻撃シーケンス

今日のランサムウェア攻撃は通常、次のような段階を経て進行します。

1 **最初の侵害:** 攻撃者は、フィッシングメールやリモート /仮想プライベートネットワーク（VPN）ツールの脆弱性のエクスプロイトなどの様々な侵入ベクトルを使用してシステムへのアクセスを入手し、ブルートフォースや窃取した資格情報を使用してリモートデスクトッププロトコル（RDP）接続にアクセスします。サプライチェーン攻撃も、組織に侵入する方法の1つです。

2 **水平移動:** 最初のアクセスに成功した脅威アクターは、被害者のインフラストラクチャ情報を収集し、ネットワークシステムを水平移動します。そして、必要に応じて権限を昇格して永続化のメカニズムを確立し、重要なデータのカタログを作成して不正取得したり暗号化したり、後で実行するランサムウェアペイロードをドロップしたりします。

3 **データの流出:** 二重脅迫型攻撃の場合、攻撃者は次に機密データを不正取得して、より高額な身代金を要求するための第2の脅迫手法として使用します。そうすることで、被害者が自らの努力で回復できる可能性が低くなります。バックアップから暗号化されたデータを回復できたとしても、盗まれたデータを公開するとサイバー犯罪者に脅迫されることになります。

4 **ランサムウェアの実行:** 攻撃者は次にランサムウェアを展開して実行し、ネットワークに接続されたシステムに存在する標的のファイルを暗号化します。ランサムウェアは通常、セキュリティソフトウェアやデータベースに関連するプロセスを強制終了することで、可能な限り多くのファイルを暗号化できるようにします。ファイルをリカバリできないようにするため、シャドウコピーバックアップも多くの場合にシステムから削除されます。一部のランサムウェアファミリーは、攻撃したシステムをWindowsのセーフモードで再起動することで、ファイルを暗号化する前にセキュリティエンドポイントソフトウェアを回避します。ファイルを暗号化した後に、身代金の支払いとファイルの復号化の手順を示すメモが被害者に提示されます。

5 **DDoS:** 被害者が交渉に応じない場合、一部のハッキング集団は被害者のネットワークやWebサイトにDDoS攻撃を仕掛けて業務を混乱させることで、身代金の要求に応じる可能性を高くします。

図1に、多重脅迫型ランサムウェア攻撃の一般的な攻撃チェーンを示します。

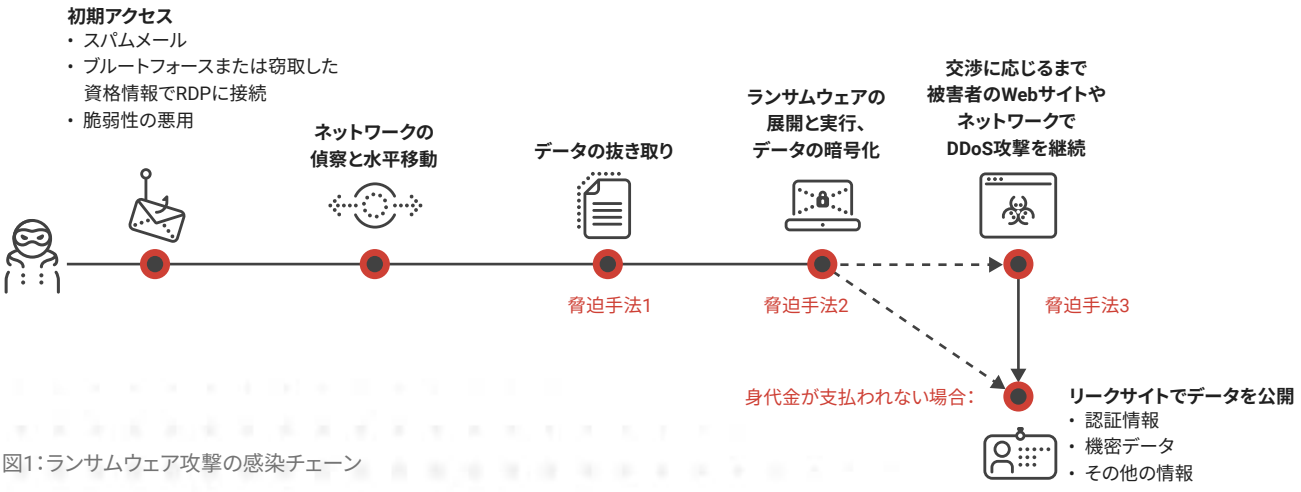


図1：ランサムウェア攻撃の感染チェーン

2021 ～ 2022 年のランサムウェア攻撃の統計

Zscaler Zero Trust Exchangeが処理する大量のトランザクションデータによって、サイバー犯罪者の手法と標的になる組織を独自の視点から捉えることができます。2021年2月～ 2022年3月に、ThreatLabzで観察されたランサムウェアペイロードが前年比で80%増加しました。 さらには、サイバー犯罪者がデータリークサイトで公開されたデータに基づき、二重脅迫型ランサムウェアの被害者となった組織が117%増加したこともわかりました。

ランサムウェアの影響を受けた業界

製造業は2020年も最も標的にされた業界であり、2019年11月～ 2021年1月の二重脅迫型ランサムウェア攻撃の12.7%を占めましたが、今年はその割合がさらに増加して19.5%になり、サービス（9.7%）、建設（8.1%）、小売（7.5%）、ハイテク（6.7%）がそれに続きました。

ランサムウェアの感染状況（業界別）

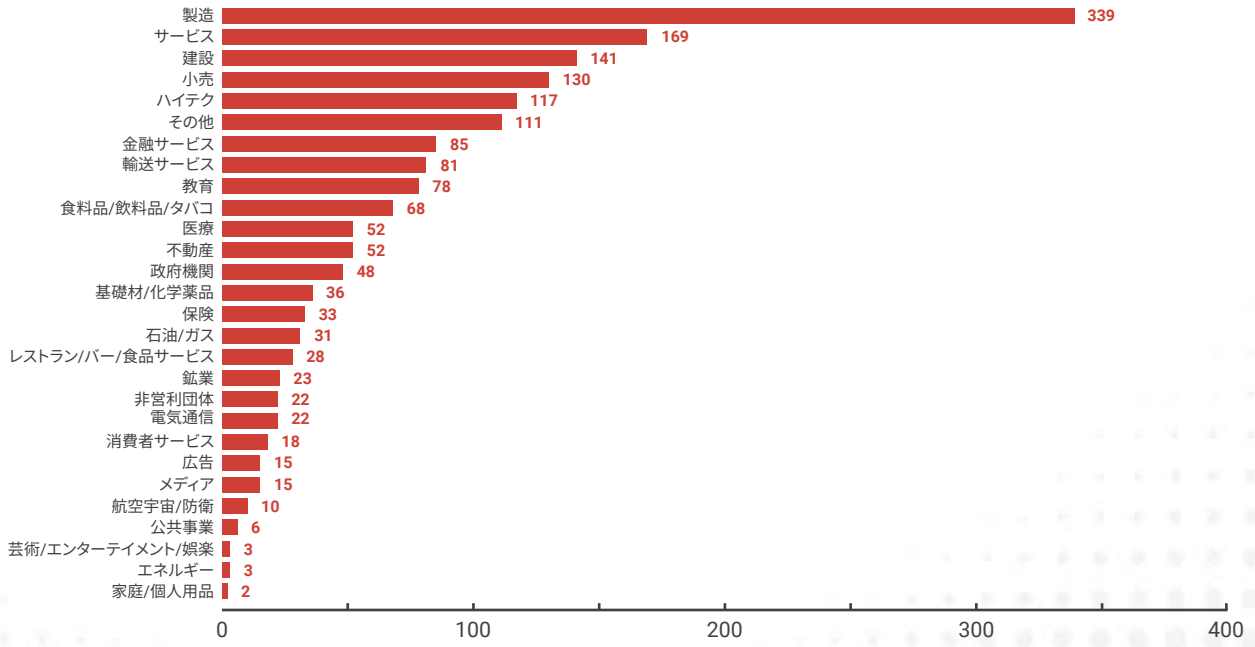


図2：ランサムウェアの感染状況（業界別）

二重脅迫型ランサムウェア攻撃の増加は業界によって大きく異なります。昨年のレポートで、法執行機関による取り締まりが強化されたこと、また、活動が活発だったいくつかのランサムウェアファミリーがCOVID-19のパンデミックが終結するまで医療機関を攻撃しないと宣言したことで、医療機関に対する攻撃が少なかったと報告しました。

今年のデータではその様相が変わりました。医療機関に対する二重脅迫型ランサムウェア攻撃が2021年に643%増加しましたが、これは、極めて攻撃が少なかった2020年からの増加率です。前年も攻撃が多かった業界でも、教育（225%）、製造（190%）、建設（161%）、金融サービス（130%）、サービス（109%）などのように攻撃が3桁の増加となった業界もあります。

二重脅迫型攻撃の変化の割合：2021年と2020年の比較

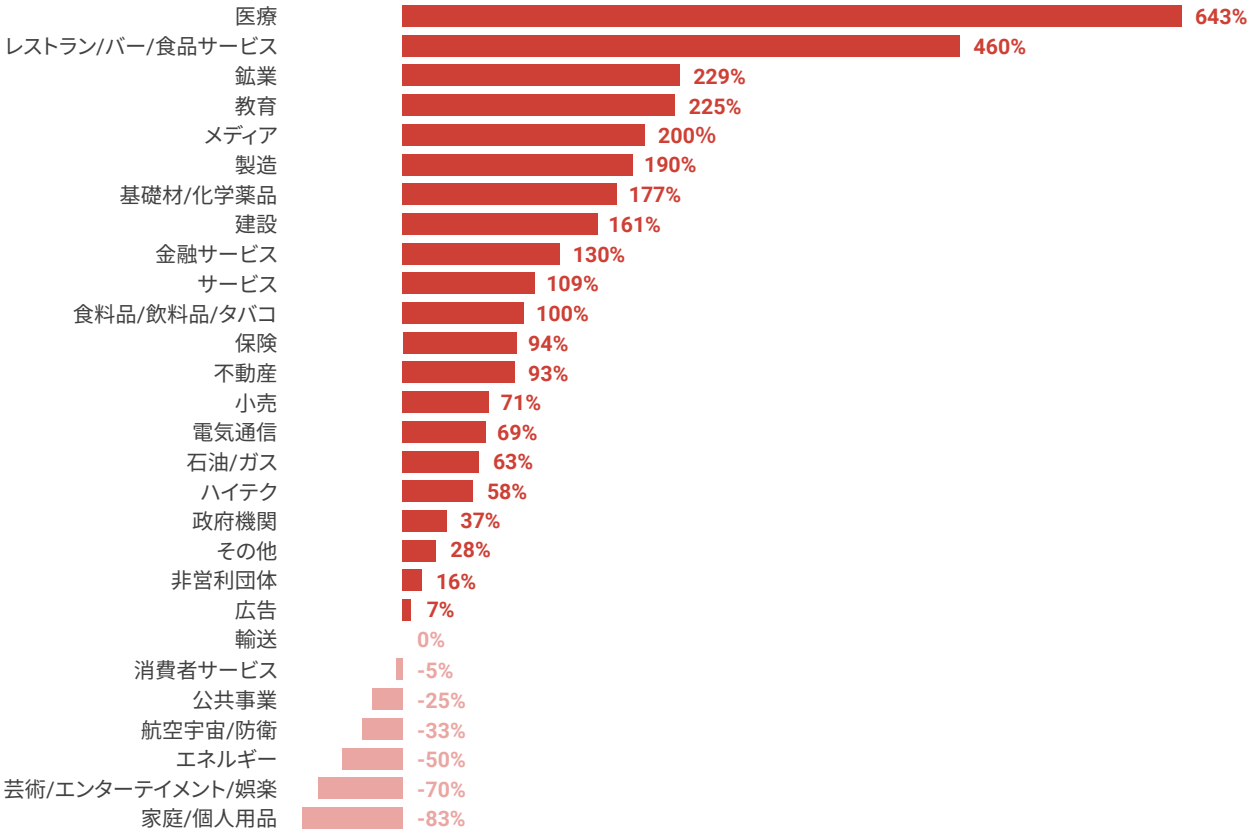


図3：二重脅迫型攻撃の変化の割合（業界別）

上位のランサムウェアファミリー

ContiとLockBitは、2021年に最も拡散した二重脅迫型ランサムウェアファミリーですが、年間を通じて新しいランサムウェアファミリーがいくつも登場しました。

図4に、この数年間に最も活発だったランサムウェアファミリーが最初に確認された時期とリークサイトやハッキングフォーラムでデータの公開を開始した時期を示します。

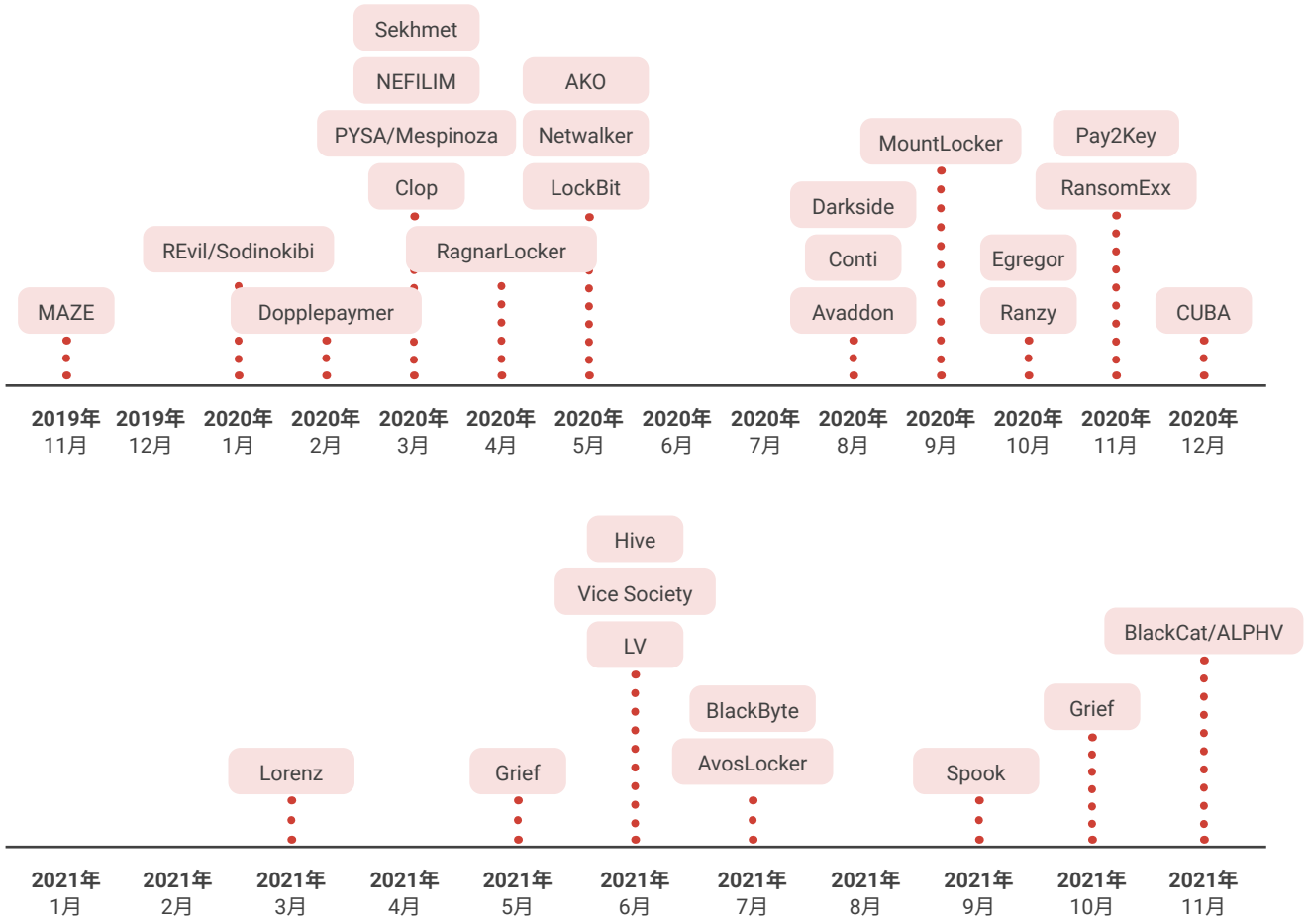


図4：データリークサイトやハッキングフォーラムでデータを公開したランサムウェアファミリー（時系列順）

2021年から2022年に活動が活発だったランサムウェアファミリーの多くは、RaaS（Ransomware-as-a-Service）モデルであり、アフィリエイトネットワーク経由で拡散します。有名ないくつかのランサムウェアファミリーが2021年にリブランディングし、例えば、DoppelPaymerがGriefへ、DarkSideがBlackMatterへと名前を変え、AvadonもHaronからさらにMidasへと名前を変えました（最後の2つはThanosランサムウェアビルダを使用するものです）。

Contiは、過去2年で最も活動が活発で、被害額が史上最多となったランサムウェア集団です。FBIは、2022年1月現在でContiランサムウェアに関連する攻撃の被害者が1,000を超え、被害総額は1億5,000万米ドル以上を超えると推定しています（関連する損害や修復の費用はこれに含まれません）。Contiの被害を受けた組織には、金融、IT、エネルギーの重要なサービスを提供する組織に加えて、アイルランドの公的医療サービスやコスタリカ政府などの公的機関も含まれます。

米国国務省は2022年5月に、このグループのリーダーに関する情報に1,000万ドルの懸賞金を提示しました。

以前はABCDランサムウェアとして知られていたLockBitは、中小規模企業を攻撃することが多いため、2021年8月のAccentureに対する攻撃を除けば、大きく注目されることはありません。LockBitは、広く使用されているRaaSで、その速さとパフォーマンスが多くの攻撃者に支持されています。

図5に、データリークサイトからの情報に基づき、2021年2月～2022年3月に二重脅迫型攻撃に使用され、攻撃の影響を受けた組織の数が最大だったランサムウェアファミリーを示します。

二重脅迫型攻撃の変化の割合：2021年と2020年の比較

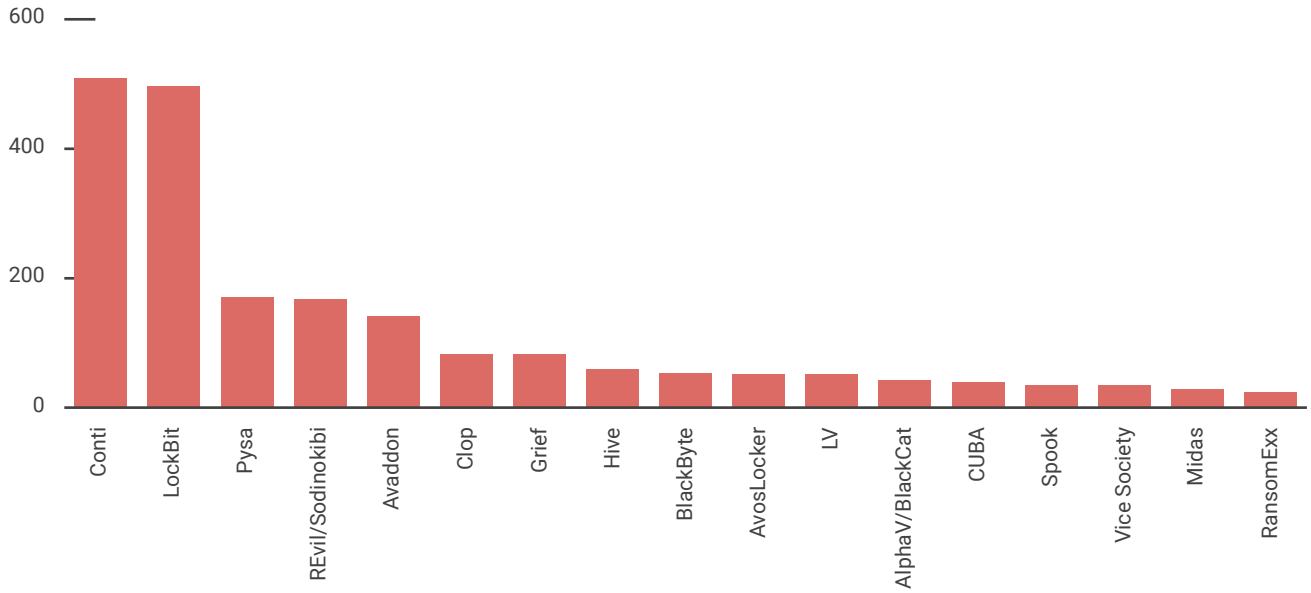


図5：ランサムウェアファミリー別の攻撃（2021年2月～2022年3月）

2022年～2023年の予測

RaaS（Ransomware-as-a-Service）は増加し続ける

RaaSはすべての関係者にとって価値があることが証明されています。新しいランサムウェア開発者とアフィリエイトは、このモデルをこれまで以上に利用して、脆弱な組織に急速に変化する攻撃を仕掛けるでしょう。

ランサムウェアモデルの変化で標的も変化する

ランサムウェアビルダも組織の情報もダークウェブで販売されているため、攻撃者は、脆弱性、利益、ランサムウェアのタイプなどを指定して企業のプロファイルをフィルタリングし、理想的な標的を特定することができます。結果として、セキュリティコントロールが十分でない中小規模企業や既知の脆弱性が存在するためにインターネットにアプリケーションが公開されてしまっている組織などの、以前にフィッシングされた資格情報を利用して簡単に攻撃できる標的に移行することが予想されます。

滞留時間が減少し続ける

攻撃者がダークウェブで販売される企業プロファイルや侵害された資格情報を容易かつ安価で入手できるようになったことで、数か月あるいは数年にわたって標的に居座り、調査してから攻撃を開始する時代は終わりを迎えようとしています。ランサムウェア攻撃者に関する多くのレポートで、滞留時間がわずか数日に短縮し、犯罪者は強力な検知手法をよく理解するようになり、攻撃の成功にとって時間が極めて重要であることを認識するようになりました。したがって、セキュリティチームは、ギャップを解消し、検知時間を数日、数時間、あるいは数分に短縮することで、2022年以降の最悪のシナリオの侵害を防止する必要があります。

犯罪者によるパートナーとサプライヤのエコシステムの侵害に伴い、サプライチェーン攻撃が増加する

世界有数の組織であれば、多くの場合に最高のセキュリティが導入されていますが、そのサプライヤやパートナー、それをサポートするネットワーク、システム、情報にアクセスするサードパーティは必ずしもそうであるわけではありません。これを実感することになったのが、ハッカー集団 Lapsus$による最近のOktaの侵害とREvilによるApple製品の有名メーカーであるQuanta Computer経由のAppleに対する脅迫です。これらの犯罪集団を始めとする多くが、サプライチェーン攻撃を使用して、最終的な標的の強力なセキュリティ対策を侵害することなく、サプライヤアクセスを使用して上流の企業の機密情報にアクセスしました。

ランサムウェアがデータを破壊するためにワイパーとして使用されたりワイパーと組み合わせて使用されたりする可能性がある

2022年初めのウクライナに対する攻撃で、HermeticWiperやPartyTicketと呼ばれるデコイランサムウェアなどの複数のタイプのワイパー攻撃が確認されました。ランサムウェアが地政学的攻撃に使用されたのはこれが初めてではなく、2017年のウクライナの組織に対する攻撃でNotPetyaやBad Rabbitが使用されたことがあります。地政学的な緊張は、正体不明のランサムウェア、ワイパー、その他の手法で、犯罪者に高レベルの匿名性ともっともらしい反証を与えることになります。

古い（そして新しい）脆弱性が損害を与え続ける

組織はこれから数年にわたり、過去1年間に確認されたいくつかの重大な脆弱性（Log4j、PrintNightmare、ProxyShell/ProxyLogonなど）への対応に追われることになるでしょう。攻撃者は今後も、パッチが適用されていない古いソフトウェアやサーバを見つけて悪用することで、セキュリティコントロールを回避し続けます。

ランサムウェアファミリーは今後もリブランディングしながら存続する

ランサムウェア集団が大規模攻撃で注目され、法執行機関から制裁を受けた後に活動を停止し、新しい名前で活動を再開するというサイクルが2021年にいくつも確認されました。法執行機関によるランサムウェアの取り締まりが引き続き強化されていることから、2022年以降もこのサイクルが継続することになるでしょう。

組織はエンドポイント保護を超えてセキュリティを強化する必要がある

ランサムウェア集団は、アンチウイルスやその他のエンドポイントセキュリティコントロールを回避する手法をこれまで以上に使用するようになるでしょう。組織は、エンドポイントセキュリティのみに頼ることなく、侵入を防止して検知する必要があるため、多層型防御に対するニーズがさらに高まると予想されます。

ランサムウェア開発者がマルウェア難読化をさらに追加する

マルウェアの開発者は、マルウェア難読化手法を実装することで、リバースエンジニアリングを妨害し、静的なシグネチャによる検知を回避しようとします。コントロールフローの平坦化、ポリモーフィック文字列の難読化、仮想マシンベースのパッカーの使用などの高度な手法により、マルウェア難読化が今後も複雑化し続けることになるでしょう。

ソースコードの流出でランサムウェアの枝分かれが進む

過去1年間にランサムウェアのソースコードの流出がいくつも発生し、ContiとBabukには2つのバージョンが存在します。Zscaler ThreatLabzは、どちらのランサムウェアファミリーもソースコードが第三者に流用され、攻撃に使用されたことをすでに確認しています。ソースコードが流出すれば、独自のランサムウェアをゼロから設計して完成させる専門知識のない犯罪集団が確実にそれを悪用することになるでしょう。

防御戦略

単純なランサムウェア攻撃、二重あるいは三重の脅迫を伴う攻撃、自己完結型の脅威ファミリー、またはアフィリエイトネットワークによって実行されるRaaS攻撃のいずれであっても、防御戦略は同じです。すなわち、ゼロトラストの原則を採用して脆弱性を制限し、攻撃の防止と検知を可能にし、成功した場合の侵害の範囲を制限します。ここでは、ランサムウェアから組織を守るために推奨されるベストプラクティスをいくつか紹介します。

1 アプリケーションをインターネットから隠す

ランサムウェアを仕掛ける犯罪者は、環境に対する偵察を実行して悪用する脆弱性を発見し、アプローチを調整することで、攻撃を開始します。インターネットに公開されるアプリケーションが多いほど、攻撃が容易になります。ゼロトラストアーキテクチャを採用して内部アプリケーションを保護し、攻撃者から見えないようにします。

2 一貫性あるセキュリティポリシーを適用して最初の侵入を防ぐ

従業員が分散している環境では、SASE（セキュアアクセスサービスエッジ）アーキテクチャを実装して、働く場所（社内、リモートワーク）に関係なく一貫性あるセキュリティポリシーの適用を可能にすることが重要です。

3 サンドボックスを使用して未知のペイロードを検知する

シグネチャベースの検知では、ランサムウェアの亜種とペイロードの急速な変化に対応できません。インラインのAIを活用したサンドボックスでファイルをパッケージングすることなく挙動を分析することで、未知の回避型の攻撃からの保護を可能にします。

4 ゼロトラストネットワークアクセス（ZTNA）アーキテクチャを実装する

ユーザ対アプリケーションやアプリケーション対アプリケーションのきめ細かいセグメンテーションを実装することで、動的な最小特権アクセスコントロールを使用したアクセスの仲介を可能にし、水平移動を排除します。これにより、暗号化や盗難が可能なデータを最小限にし、攻撃が影響する範囲を制限できます。

5 インラインの情報漏洩防止（DLP）機能を導入する

トラストベースの情報漏洩防止ツールとポリシーを活用して機密情報の抜き取りを防ぎ、二重脅迫の手口を阻止します。

6 ソフトウェアやトレーニング内容を最新の状態に保つ

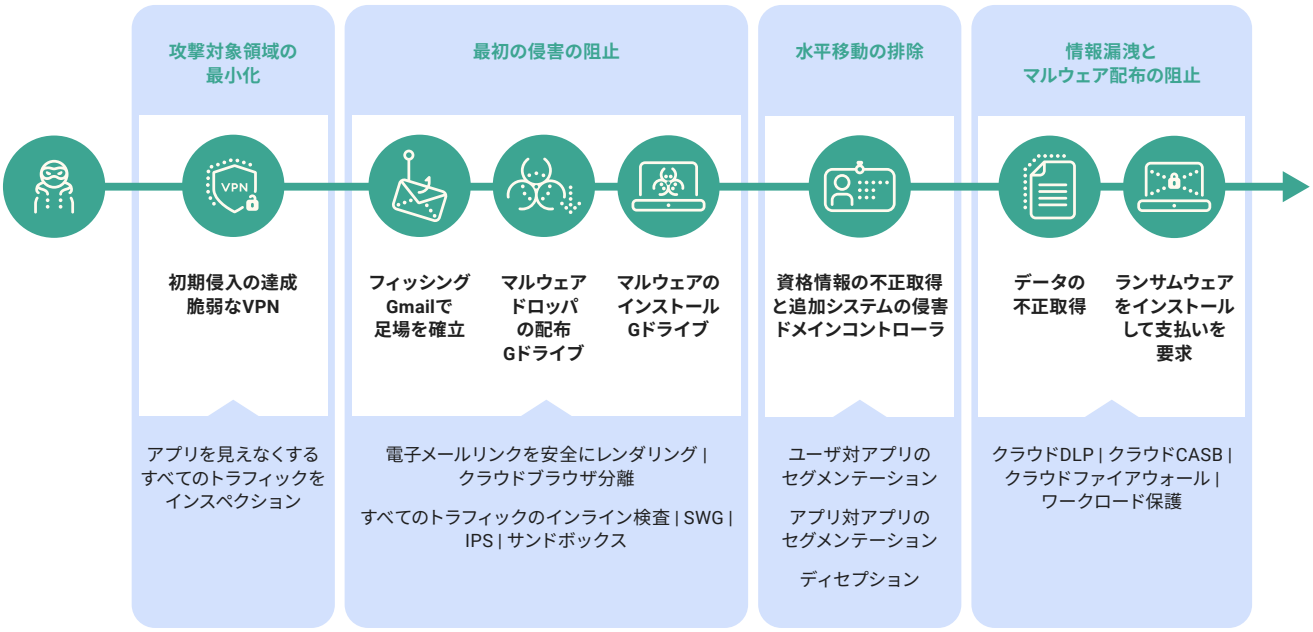
ソフトウェアにセキュリティパッチを適用し、社員向けのセキュリティトレーニングを定期的に実施することで、サイバー犯罪者に悪用される可能性のある脆弱性を減らします。

7 対応プランを策定する

全社的な事業継続、障害回復プログラムの一環として、サイバー犯罪保険の加入、データのバックアップ計画、対応プランの策定を実施して最悪の事態に備えます。

ランサムウェアに対する防御の効果を最大限にするには、多層防御を採用し、偵察から最初の侵害、水平移動、データの不正取得、ランサムウェアの実行までのそれぞれの段階で攻撃を中断できるようにする必要があります。

ゼロトラストでランサムウェアを阻止



ランサムウェアの主なトレンド

サプライチェーン攻撃

サプライチェーン攻撃とは

サプライチェーン攻撃（バリューチェーン攻撃またはサードパーティ攻撃とも呼ばれます）は、アクセスを取得する手段として実行される、組織のサプライヤに対する攻撃です。ほとんどの大規模組織は高度なセキュリティコントロールを採用していて、侵入が困難であるため、攻撃者は、サプライヤ経由でこれらの組織に侵入する方法を見つけました。

サプライチェーン攻撃は、通常のビジネス活動に存在する正当な組織間の信頼を悪用します。攻撃者は、標的が使用するとわかっている製品にバックドアを仕掛けるため、攻撃者が検知されることなく、通常は「トロイの木馬」のアップデートと呼ばれる自動化されたパッチやソフトウェアアップデートで標的のネットワークに侵入します。侵入した攻撃者は、スパイ活動、データの不正取得、他のマルウェアの埋め込み、処理の中断などを実行します。

このような攻撃には高度な計画と方法が必要であり、最初に攻撃された組織に破壊的な影響を与える可能性があります。

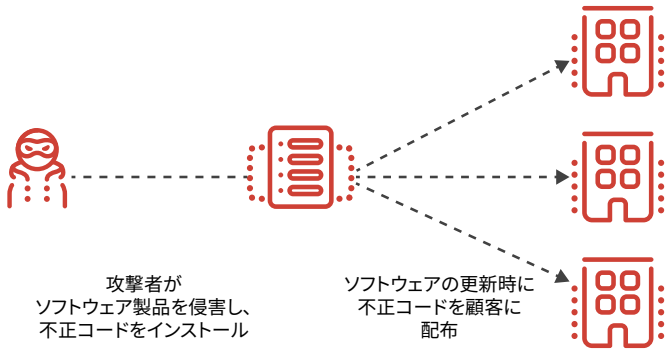


図6：サプライチェーン攻撃

Kaseyaサプライチェーンランサムウェア

IT管理ソフトウェア会社であるKaseyaが2021年7月2日に、マネージドサービスプロバイダ（MSP）によるパッチ管理、バックアップ、顧客向けクライアント監視の実行を可能にするプラットフォームであるKaseya VSAソフトウェアのオンプレミスバージョンに影響するセキュリティインシデントを発表しました。この攻撃で約70のMSPが侵害され、それを利用する下流の1,500の中小規模企業が影響を受けたとされています。

この攻撃の背後にいるサイバー犯罪者は、Kaseya VSAサーバのゼロデイ脆弱性を見つけて悪用することで、そのサーバが管理するすべてのクライアントへの不正スクリプトの送信を可能にしました。このスクリプトを使用して、影響を受けたシステムのファイルを暗号化するREvil/Sodinokibiランサムウェアスクリプトが送信されました。

Quantaコンピュータサプライチェーン

REvilが2021年4月に、世界最大規模のノートPCメーカーであり、Apple製品の有名メーカーでもあるQuanta Computerを攻撃しました。Quantaが5,000万ドルの身代金要求の支払いを拒否したため、REvilは代わりにAppleや他のQuantaの顧客を身代金の標的にしました。REvilは、MacBookの回路図のスクリーンショット21枚を公開し、AppleやQuantaが身代金を支払わなければ、Appleや他の企業のさらに多くのデータを公開すると脅迫しました。

Log4jランサムウェア

Apache Software Foundationが2021年12月に、人気のLog4jロギングライブラリに存在するリモートコード実行の脆弱性（CVE-2021-44228）に関するセキュリティ勧告を発表しました。この脆弱性により、攻撃者は意図的に作成した要求を脆弱性が存在するシステムに送信することで、不正ペイロードをダウンロードして実行できるようになります。さらには、ログメッセージやログメッセージパラメータを制御することで、Message Lookup Substitutionが有効な場合にLDAPサーバからロードした任意コードを実行できるようになります。Log4jは多くの有名なWebサイト、アプリケーション、フレームワークに組み込まれているため、その影響は広範囲に及びます。この脆弱性を悪用する次のようなランサムウェア攻撃がいくつも確認されました。

NightSkyランサムウェア

攻撃者が2021年1月4日に、VMware Horizonが動作する、インターネットに接続されているシステムに存在するLog4j脆弱性を悪用して、NightSkyランサムウェアをドロップしました。

Khonsari

WindowsシステムでLog4jエクスプロイトを使用し、Khonsariランサムウェアを展開する、複数の攻撃が確認されています。

Conti

Contiグループも、Log4jの脆弱性を悪用してランサムウェア攻撃を実行しました。このグループが脆弱なLog4j VMware vCenterバージョンを見つけて標的にし、既存のCobalt Strikeセッションから米国やヨーロッパの被害者のネットワークに水平移動していたことをAdvIntelが確認しました。

TellYouThePass

攻撃者は、Log4jの脆弱性を悪用してWindowsやLinuxのシステムにTellYouThePassランサムウェアを展開し、実行しました。

RaaS（Ransomware-as-a-Service）

ダークウェブは、脅威グループがサイバー攻撃を仕掛けようとする犯罪者に商品を販売する場所として人気を集めるようになりました。2022年のThreatLabzフィッシング現状レポートで、PaaS（Phishing-as-a-Service）の増加などの他の攻撃タイプへのこれらの市場の影響を詳しく解説しています。

RaaSは非常に人気があり、最近のランサムウェア攻撃の大部分にこのモデルで実行されています。事実、昨年の上位11種のランサムウェアファミリーのうち8つがRaaSエコシステムを利用するものでした。

RaaSモデルでは、運営者とアフィリエイトが存在する必要があります。運営者はランサムウェアを開発する脅威集団であり、アフィリエイトは被害者を標的にしてランサムウェアを実行し、要求を送り付けます。

ランサムウェアの運営者はアフィリエイトを募集し、攻撃で得られる利益の約70～80%と引き換えに、ランサムウェアとその実行に必要なツール、データリークサイトへのアクセス、交渉の支援、その他のサポートを提供します。

このモデルは両者に利益をもたらします。アフィリエイトは、非常に効果の高いランサムウェア攻撃の実行に必要なものをすべて手に入れることができ、自分で開発する必要はありません。これは、スキルのある犯罪者は開発時間とリソースを節約でき、スキルのない犯罪者は自分だけでは実行できないような攻撃が可能になることから、両者にとって魅力的なモデルと言えます。ランサムウェアの運営者は、攻撃の範囲を大幅に拡大して、結果として、大きな利益を上げることができます。

RaaSによる攻撃の件数と損害の両方が増加しました。

- **ランサムウェア攻撃の増加：**少ない時間とスキルで開発が可能になったことで、より多くのアフィリエイトがランサムウェアを実行するようになりました。
- **二重脅迫による身代金の増額：**RaaSには、攻撃者がデータを盗み、身代金が支払われない場合にデータリークサイトにそれを公開すると脅す二重脅迫のコンポーネントが含まれます。これにより、さらに多くの身代金を手に入れ、攻撃の成功率を高くすることができます。

地政学的攻撃

世界中のセキュリティリーダーが、ロシアとウクライナの紛争の結果としてランサムウェア攻撃が増加すると警戒しています。

ジョー・バイデン米大統領が2022年3月に声明を発表し、ロシアに対する経済制裁への報復として米国に対する不正サイバー活動が発生する可能性があると警告しました。大統領は声明で、公共と民間の両方の組織にサイバー防御を強化する行動を直ちに取るように呼びかけました。

2021年のランサムウェアファミリー上位11種のうち8種がRaaSエコシステムを使用したものでした。

本レポートの執筆日現在、ウクライナに対するランサムウェア攻撃や、この紛争に関連する次のようなランサムウェア攻撃がすでにいくつか確認されています。

1 **PartyTicketランサムウェア:** Goベースのこのランサムウェアと**HermeticWiperマルウェア**の組み合わせが、ウクライナの組織を標的にする攻撃で使用されています。PartyTicketはあまり精巧なランサムウェアではなく、復号化が可能な暗号化が含まれていることから、HermeticWiperに対する注目をそらすためのおとりとして開発されたものである可能性があります。

2 **Contiランサムウェア:** サイバーセキュリティインフラセキュリティ庁（CISA）、連邦捜査局（FBI）、国家安全保障局（NSA）、米国シークレットサービスが、ロシアと関連性のあるランサムウェア集団であるContiに関する勧告を再び発表しました。勧告では、「Contiのサイバー犯罪者の活動は引き続き活発であり、米国や国際的な機関に対するContiランサムウェア攻撃が1,000件以上にまで増加した」と警告しています。Contiは2月下旬に、自らのリークサイトに2つの声明を投稿し、「ロシア連邦市民に対するサイバー戦争を使用する西側の挑発とアメリカの脅威」に対抗し、ロシア政府を支援すると表明しました。

法執行機関による解体

世界中の法執行機関が、ランサムウェアファミリー、特に被害が広範囲に広がっているランサムウェアファミリーへの警戒を強めています。2021年から2022年初頭に、影響の大きかったランサムウェアファミリーの解体がいくつも成功しました。

REvilの解体

Evilは、KaseyaとJSBに対する大規模攻撃の後に報道された、過去2年間で最も悪名の高いランサムウェアファミリーの1つです。FBIはKaseya攻撃の後に、REvilサーバの解体を計画しましたが、その好機が訪れることはありませんでした。REvilは2021年7月のこの重大な攻撃の直後に、その活動を停止し、ハッカーも姿を消しましたが、Kaseyaの活動が2021年9月に再開したことから、この活動停止は短期的なものでした。

ロシア政府は2022年1月に、REvilハッキング集団を解体に追い込み、そのメンバーを米国の要請に応じて逮捕しました。ロシア連邦保安局（FSB）は25の拠点を捜索し、REvil集団のメンバー14人を拘束し、4億2,600万ルーブル、60万米ドル、50万ユーロ、20台の高級車、コンピュータ機器を押収しました。しかしながら、REvilは2022年4月に再び活動を開始し、更新されたランサムウェアバージョンで複数の組織を攻撃しました。

DarkSideの解体

DarkSideランサムウェア集団が2021年5月6日に、米国最大の石油パイプラインであるコロニアルパイプラインで注目されたランサムウェア攻撃を実行しました。米国連邦政府機関は行動を開始し、攻撃から2週間以内に、UNKNとして知られるサイバー犯罪者は、サーバにアクセスできなくなり、暗号通貨が未知のアカウントに転送されたとして、DarkSideがシャットダウンしたと発表しました。司法省は、約230万米ドルに相当する63.7ビットコインを押収したと発表しました。

Egregorの解体

Egregorランサムウェア集団（以前の名前はMaze）が2021年2月9日に、複数の法執行機関の合同作戦で解体されました。ウクライナ、フランス、米国の機関が、Egregorのリークサイトを閉鎖し、グループのメンバーを逮捕し、ランサムウェア攻撃と関連性のあるコンピュータを押収しました。Egregorは、150以上の企業から約8,000万ドルを手に入れていました。

ランサムウェアのリブランディング

多くのランサムウェア運営者が、過去1年間にランサムウェアをリブランディングしました。一般的にリブランディングするのは、法執行機関やメディアの注目をそらし、制裁を受けて身代金を収集する能力を制限されてしまうのを回避するためです。

DoppelPaymerからGriefへの名前の変更

DoppelPaymerランサムウェアの活動が2021年5月上旬に大幅に減少しました。DoppelPaymerリークサイトはまだオンラインのままですが、2021年5月6日以降に新しい被害者は投稿されておらず、6月末以降に被害者の投稿は更新されていません。このような休止状態は、2021年5月7日に発生したコロニアルパイプラインに対するランサムウェア攻撃の反動である可能性がありますが、このように活動の明らかな中断は、DoppelPaymerの背後にある脅威集団がランサムウェアの名前をGriefに変更したためです。両方のランサムウェアの亜種のマルウェアコードが共通しており、リークサイトもとてもよく似ています。Griefの身代金ポータルには、DoppelPaymerのポータルといくつかの相違点があり、例えば、身代金要求の支払方法にビットコイン（BTC）ではなくモネロ（XMR）が指定されています。暗号通貨がこのように変更されたことは、FBIがコロニアルパイプラインで支払われた身代金の一部を回収したためである可能性があります。

DarksideからBlackMatterへの名前の変更

2021年5月のDarkSideの解体後、BlackMatterという名前の新しいランサムウェアファミリーが7月下旬に登場しました。このランサムウェアで使用されている暗号化ルーチンとデータリークサイトの文言は、BlackMatterがDarkSideから名前を変えたランサムウェアであることを示しています。

BlackMatterは2021年11月に、活動を停止しました。この集団は、活動の停止のメッセージをRaaSポータルに掲載し、「当局からの圧力（最新の報道の後にチームの一部が活動に参加できなくなったこと）に関連する、いくつかの解決不能な状況により、プロジェクトを閉鎖する」と宣言しました。

Thanosベースランサムウェアのリブランディング

RaaSとしてダークウェブで宣伝されていたThanosランサムウェアは、2020年2月に最初に特定されました。Thanosビルダがリークし、その後の2年間に一連の新しい亜種が開発されました。Prometheusランサムウェアの亜種は2021年2月に登場し、9月にPrometheusからSpookへと名前が変更されました。両者は身代金メモとデータリークサイトが似ていて、どちらにもThanosの署名キー識別子が含まれています。

2021年7月に、Haronと呼ばれる別のThanosから派生したランサムウェアが確認されました。Haronランサムウェアは、Avaddonランサムウェアと非常に似ている点がいくつかあります。HaronとAvaddonの身代金メモ、交渉サイト、データリークサイトにはいくつかの共通点があります。2021年10月には、Midasと呼ばれる、Haronランサムウェアがリブランディングしたバージョンである別の亜種が発見されました。

ランサムウェアグループは、制裁を回避し、法執行機関の目をそらすために、リブランディングします。

Evil Corpの名前の変更

Evil Corp犯罪集団は、Indrik Spiderと呼ばれることもあり、さまざまな不正活動で知られています。Dridexなどの銀行トロイの木馬を作成した犯罪集団であり、後者はBitPaymerランサムウェアの配布で使用されました。

米国財務省の外国資産管理局（OFAC）が、Dridexマルウェアが40か国以上の銀行や金融機関に1億ドル以上の損害を与えたとして、Evil Corpのメンバーに制裁を課しました。これらの制裁の後に、ランサムウェアの交渉を手掛ける企業は、米国財務省からの罰金や法的措置を恐れて、Evil Corpの身代金支払の調整を拒否するようになりました。Evil Corpは、ランサムウェアの名前を変更することで制裁を回避するという、単純な抜け穴を発見しました。

Evil Corpは、2020年6月にWastedLockerランサムウェアを、2020年12月にHadesランサムウェアを、2021年3月にPhoenixランサムウェアを拡散した後に、2021年5月にランサムウェアの名前をPayloadBinに変更することで、制裁の対象にならない別のサイバー犯罪者のように偽装しました。

Rookランサムウェアの名前の変更

Babukランサムウェアから流出したソースコードに基づき、2021年11月にRookが特定されました。2021年12月にRookの亜種が名前をNight Skyに変えて、中国を拠点とする犯罪集団であるDEV-0401によって、Log4Shellの脆弱性を悪用する二重脅迫型ランサムウェア攻撃で企業ネットワークを標的にする目的で使用されたことがわかりました。2022年1月にRookとNight Skyの両方が閉鎖され、Pandoraランサムウェアが登場しましたが、コードの類似性から判断すると、PandoraもRookの名前を変えたバージョンであると考えられます。

ランサムウェア攻撃で使用される主な脆弱性

ProxyLogonの脆弱性

BlackKingdomとDearCryランサムウェアは、4つの異なるProxyLogon脆弱性エクスプロイトを組み合わせて標的のネットワークに侵入し、暗号化しました。この手法は、Microsoft Exchange Serverへのアクセス、電子メールの不正取得、その他のバックドアの展開に使用されていました。悪用されたProxyLogonの脆弱性としては、CVE-2021-26855（Exchangeのサーバ側要求偽造 [SSRF] の脆弱性）、CVE-2021-26857（ユニファイドメッセージングサービスの安全でない逆シリアル化の脆弱性）、CVE-2021-26858（Exchangeの認証後の任意ファイル書き込みの脆弱性）、CVE-2021-27065（Exchangeの認証後の任意のファイル書き込みの脆弱性）が挙げられます。Microsoftは2021年3月に、これらの脆弱性を修正するパッチを公開しました。

外部に公開されているポート443経由でのリモートコード実行を可能にする、一般的な攻撃チェーン：攻撃者は、CVE-2021-26855脆弱性を使用してMicrosoft Exchangeの認証を迂回し、ユーザを偽装します。攻撃者はさらに、ディレクトリ内のファイルを必要とない、認証なしで読み取り可能なディレクトリ内の任意のファイルに対して、自らが作成したPOST要求を送信します。攻撃者はExchangeコントロールパネル（ECP）に認証し、CVE-2021-26858またはCVE-2021-27065の脆弱性を使用して、標的システム内のすべてのファイルを上書きします。これらのエクスプロイトの後に、攻撃者がExchange ServerにあるWebシェルを使用してリモートコードを実行できるようになります。

ExchangeのProxyShellの脆弱性

Contiランサムウェアは、Microsoft Exchange Serverの脆弱性を悪用して、被害者のネットワークに侵入します。ExchangeのProxyShellの脆弱性は、CVE-2021-34473（Microsoft Exchange Serverのリモートコード実行の脆弱性）、CVE-2021-34523（Microsoft Exchange Serverの権限昇格の脆弱性）、CVE-2021-31207（Microsoft Exchange Serverのセキュリティ機能のバイパスの脆弱性）の脆弱性の組み合わせによる

ものです。Microsoftが2021年の4月～5月にこれらの脆弱性を修正しましたが、Contiはその後もパッチが適用されていないサーバを攻撃してリモートコードを実行しました。このランサムウェアの感染チェーンについては、本レポートに加えて、BlackByte、AvosLocker、およびHiveランサムウェア集団の解説でも紹介されています。LockFileランサムウェアも、これらの脆弱性を標的にしてランサムウェアを展開します。

PrintNightmare

ランサムウェアの攻撃者は、PrintNightmareの脆弱性を悪用してWindowsシステムを標的にします。PrintNightmareの脆弱性は、CVE-2021-34527とCVE-2021-34481、およびWindows印刷スプーラサービスのリモートコード実行の脆弱性の組み合わせであり、特権付きファイル処理の不正実行により、攻撃者がSYSTEM特権でリモートコードを実行できるようになります。

これは、Windowsシステムのポイントアンドプリント機能に存在する、非特権ユーザによるリモートプリンタの更新やインストールを可能にする脆弱性です。Microsoftは、2021年7月 と8月 にPrintNightmareのアップデートを発表して、この脆弱性を解決しました。

ある攻撃では、ランサムウェア集団がPrintNightmareの脆弱性を悪用し、Vice Societyランサムウェアをドロップしました。 別の攻撃では、攻撃者がPrintNightmareを悪用し、Magniberランサムウェアをドロップしました。

SonicWall SMA 100

SonicWallが2021年1月に、Secure Mobile Access SMA 100シリーズ製品にSQLインジェクションの脆弱性が存在すると発表しました。この脆弱性により、攻撃者は、認証されていない、特別に作成したクエリを使用して、ログイン資格情報とセッションにアクセスし、脆弱なアプライアンスを侵害することができます。この脆弱性は、2021年2月にSonicWallによって修正されました。

この脆弱性は、UNC2447脅威集団がこの脆弱性を悪用して標的とするネットワークを攻撃し、FIVEHANDS二重脅迫型ランサムウェアを被害者のシステムに展開した後に発見されました。攻撃者はこのゼロデイ脆弱性を使用して侵入した後に、SOMBRATバックドアに加えて、足場を確立し、偵察を実行し、データを持ち出す目的で使用する、Cobalt Strike Beacon、Adfind、BloodHound、Mimikatz、PC Hunter、Rcloneなどの追加ツールをドロップしました。UNC2447は攻撃の最後に、FIVEHANDSランサムウェアをドロップして実行し、標的システムのデータを暗号化し、ハッカーフォーラムにデータを公開すると脅迫して身代金を手に入れようとしました。

QNAP NAS デバイス

eCh0raixランサムウェアの新しい亜種が、QNAP（Quality Network Appliance Provider）のNAS（ネットワーク接続ストレージ）デバイスとSynologyのNASデバイスを攻撃しました。 攻撃者は攻撃チェーンで、QNAPのNASデバイスのCVE-2021-28799脆弱性を悪用しました。この認証不備の脆弱性は、HBS 3（ハイブリッドバックアップ同期）が動作するQNAP NASで報告されており、この脆弱性によって、攻撃者によるリモートでのデバイスへのログインが可能になります。

上位11種のランサムウェアファミリー

ここからは、11種のランサムウェアファミリーとその攻撃シーケンスの概要を紹介します。これらのランサムウェアファミリーは、その被害が2021年と2022年に最多だったことから、組織が防御しなければならないランサムウェアの現状を最もよく表すものと言えます。それぞれのランサムウェアファミリーの簡単な歴史、手法の概要（MITRE ATT&CKマッピングを含む）、標的にする業界に関するいくつかの統計を紹介します。

Conti

Contiランサムウェアは2020年2月に初めて確認されました。ContiはRaaSに分類されることもありますが、そのアフィリエイトは基本的に従業員であり、サインアップした後にポータルを使用してページを管理しますが、利益の一部を受け取ることはありません。ContiとRyukのコードが似ていることは、ContiがRyukランサムウェアの後継である可能性が高いことを示しています。Contiは、2021年に最も多く確認されたランサムウェアです。

感染チェーン：

Contiは、さまざまな攻撃でさまざまな初期アクセスのメカニズムを使用していました。

1 不正添付ファイルやリンクを含むスパムメール経由で拡散し、TrickBot、IcedID、BazarLoader、またはCobalt Strikeをダウンロードしてシステムに足場を確立します。

2 初期アクセスの取得には、Log4j、ProxyShell、あるいは弱いRDP（リモートデスクトッププロトコル）資格情報などの既知の脆弱性が悪用される場合もあります。

Contiは侵入後に、Cobalt Strike、Mimikatz、その他のエクスプロイト後のツールを使用して資格情報を不正取得し、ネットワークに足場を確立します。Contiの攻撃者は、Metasploit、Netscan、その他のレッドチームツールを使用して、ネットワークやドメインコントローラの情報を取得するとされています。攻撃者は必要な情報の取得後に、AnyDesk、PsExec、またはその他のリモートユーティリティを使用して水平移動します。Contiの攻撃者は、Rcloneやその他のツールを使用してデータを抜き取り、最後にContiランサムウェアを展開して実行することで、データを暗号化します（図7参照）。

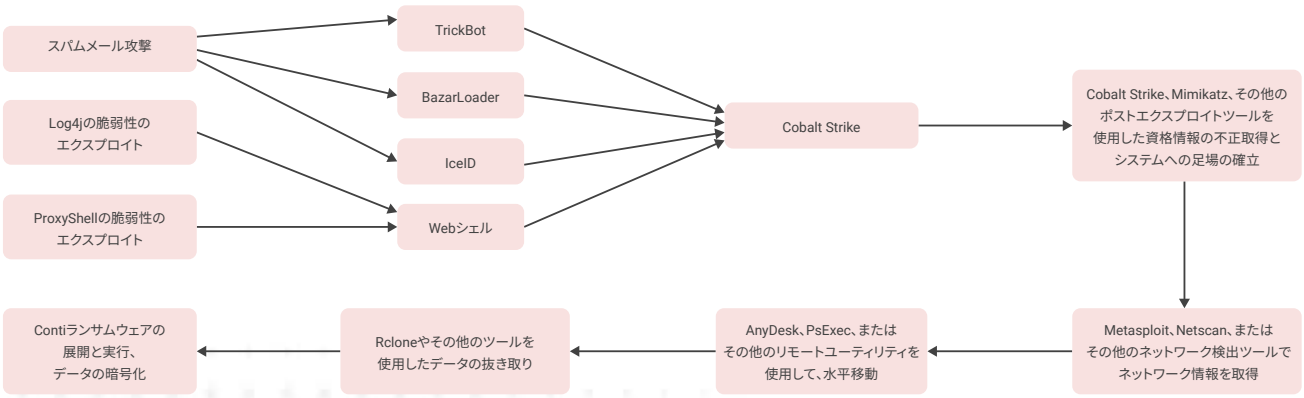


図7：Conti ランサムウェア攻撃の仕組み

Contiの最初のバージョンは、暗号化プロセスでRSAアルゴリズムとAESアルゴリズムが使用していましたが、AESは後にChaCha暗号化に置き換えられました。

ThreatLabzは2022年1月下旬に、グローバルなランサムウェア追跡活動の一環として、Contiランサムウェアの更新バージョンを特定しました。この更新バージョンは、ウクライナ侵攻後の2022年2月27日にウクライナの研究者によって公開されたContiのソースコードとチャットログの大規模リークの前に公開されたものです。新しいバージョンのContiには、ネットワーキングが有効な状態でシステムをWindowsセーフモードで再起動し、暗号化を開始するための新しいコマンドライン引数が追加されました。セーフモードで起動することで、データベースなどのビジネスアプリケーションが実行されなくなる可能性があるため、Contiができるだけ多くのファイルを暗号化できるようになります。Contiはさらに、暗号化したファイルの拡張子を変更して、大文字、小文字、数字が含まれるようにし、ファイルを暗号化した後に被害者のデスクトップに壁紙を設定します。

図8に、Contiを使用した二重脅迫型攻撃の標的となった業種を示します。

Contiの感染状況（業界別）

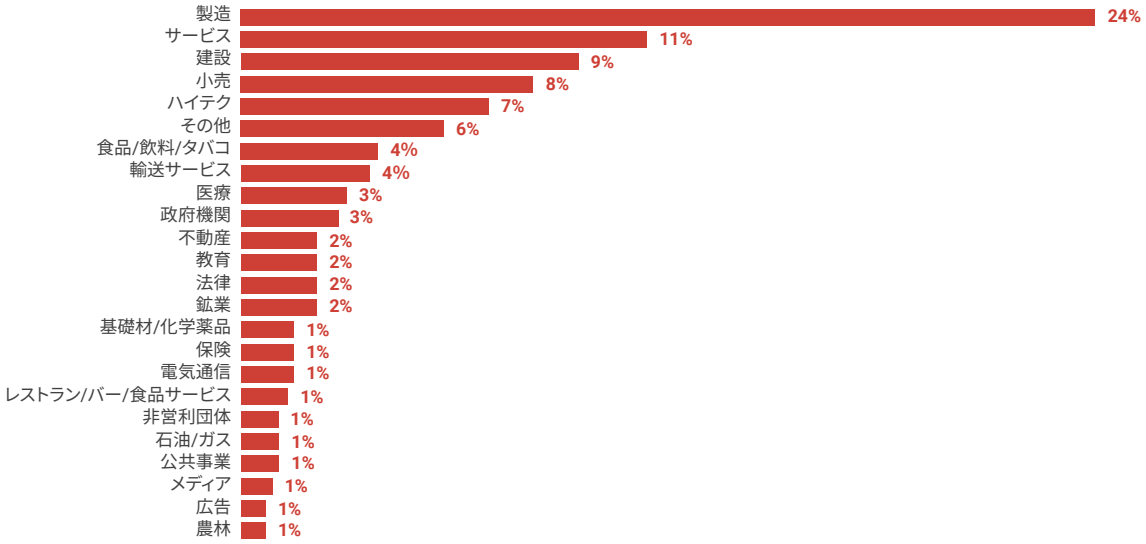


図8：Contiの感染状況（業界別）

Contiは2020年8月に独自のデータリークサイトを作成しました。要求された身代金を組織が支払わない場合、Contiは、窃取したデータを公開します。

図9：Contiのデータリークサイト

Conti：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	収集	抜き取り	影響
リンク型スピアフィッシング	コマンドラインインタフェース	ブートまたはログオンの自動起動の実行	アクセストークンの操作	ファイルや情報の難読化解除/デコード	システムネットワーク設定の探索	水平移動ツールの転送	収集したデータのアーカイブ	自動化された抜き取り	影響を与えるためのデータ暗号化
添付ファイル型スピアフィッシング	モジュールのロードによる実行		権限昇格のエクスプロイト	防御の妨害	リモートシステムの探索	リモートサービス	ローカルシステムのデータ	Webサービス経由での抜き取り	システムリカバリの阻害
外部公開されたアプリケーションへのエクスプロイト	共有モジュール			プロセスインジェクション	ファイルとディレクトリの発見				システムのシャットダウン/再起動
有効なアカウント	ユーザによる実行				セキュリティソフトウェアの発見				変造
サプライチェーンの侵害					クエリの登録				

LockBit

LockBitランサムウェアは2019年9月に、ABCDランサムウェアとして初めて登場しました。これは、「.abcd」という拡張子に由来する名前です。2020年の初めには、暗号化したファイルに拡張子「.lockbit」を追加する新しいバージョンが登場しました。LockBitは2020年に、Mazeカルテルに参加し、Mazeのデータリークサイトに被害者のデータを公開し始めましたが、Mazeが活動を停止した2020年9月から、図10に示す独自のデータリークサイトを使用するようになりました。

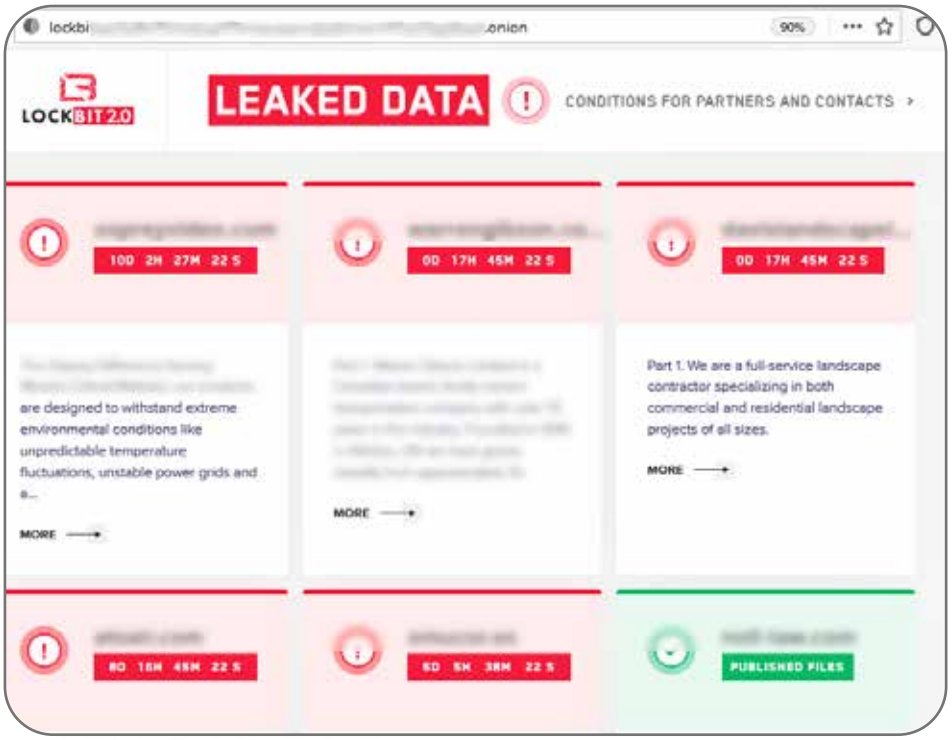


図10：LockBitのデータリークサイト

LockBitが2021年6月にLockBit 2.0という新しいバージョンを公開し、LockBit 2.0は2021年7月に、被害者である企業のデータのデータリークサイトへの公開を開始しました。LockBitはRaaSモデルを使用しており、標的とする組織で正規のネットワークアクセスを持つ従業員に接触し、不正添付ファイルやリンクを含むスパムメール攻撃を通じて拡散します。

LockBitはさらに、侵害されたRDPアカウントを使用したRDPまたはVPNの資格情報のブルートフォースにより、フォーティネット VPNのCVE-2018-13379脆弱性を悪用することでアクセスを手に入れることが確認されています。

感染チェーン:

最初に確認されたLockBit 2.0攻撃では、攻撃者はハッキングされたRDPアカウントを使用して標的システムにアクセスした後に、ネットワークスキャナを使用してネットワーク情報を手に入れ、ドメインコントローラを特定していました。攻撃者は、StealBitを使用してデータを抜き取り、Process HackerとPC Hunterを使用してデータベースに関連するプロセス、サービス、その他のツールを強制終了します。さらには、バッチファイルを使用して、セキュリティ製品をアンインストールし、WindowsイベントログとWindows Defenderの機能を無効にします。最後に、LockBitはWindowsグループポリシーを使用して、LockBit 2.0 ランサムウェアを送り込み、実行します。

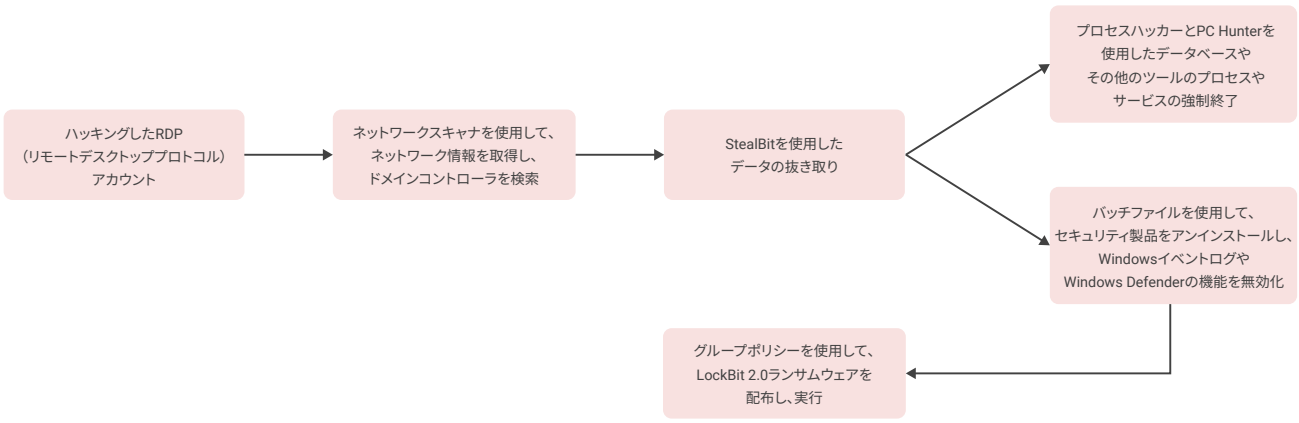


図11:LockBitランサムウェア攻撃の仕組み

LockBitは、機能が優れていることから、広く利用されています。LockBitには、マルチスレッドの暗号化アプローチを採用し、各ファイルの4 KBのデータのみを暗号化する、最速の暗号化方法が組み込まれており、RSAアルゴリズムとAESアルゴリズムの組み合わせを使用してファイルを暗号化します。LockBitは2021年10月に、LinuxとVMware ESXiの亜種を公開しましたが、この亜種は、高度暗号化標準 (AES) アルゴリズムと楕円曲線暗号化 (ECC) アルゴリズムの組み合わせを使用してデータを暗号化します。

図12に、LockBitを使用した二重脅迫型攻撃の標的となった業種を示します。

Lockbitの感染状況（業界別）

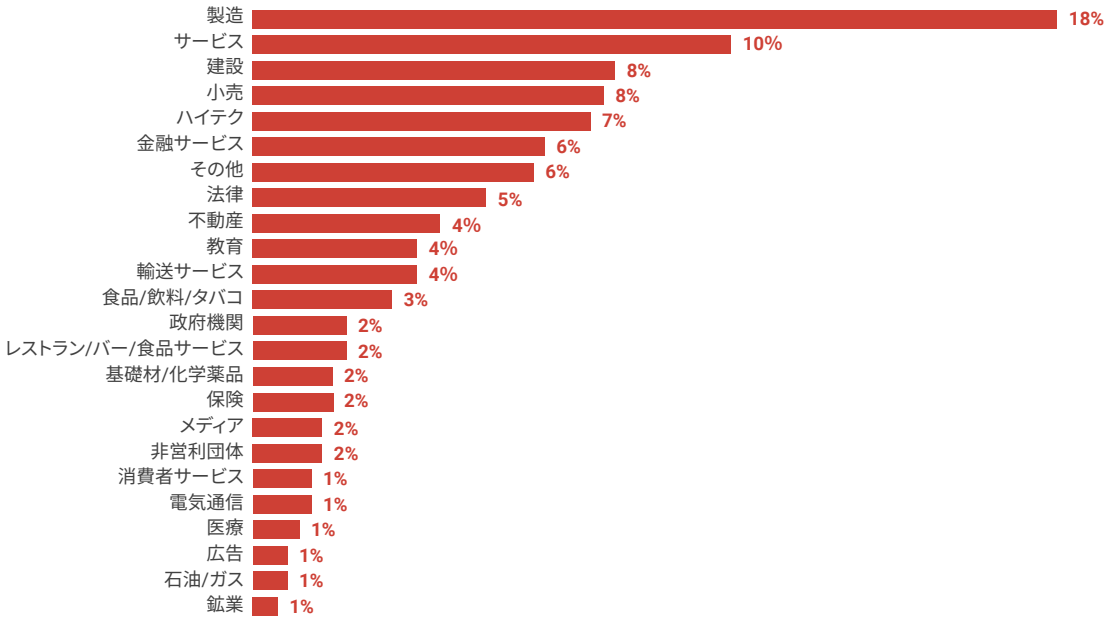


図12：LockBitの感染状況（業界別）

LockBit：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	収集	抜き取り	影響
リンク型スピアフィッシング	コマンドラインインタフェース	ブートまたはログオンの自動起動の実行	昇格コントロール侵害のメカニズム：ユーザアカウントコントロールの迂回	ファイルや情報の難読化解除 / デコード	システムネットワーク設定の探索	水平移動ツールの転送	収集したデータのアーカイブ	Webサービス経由での抜き取り	影響を与えるためのデータ暗号化
添付ファイル型スピアフィッシング				防御の妨害：ツールの無効化または変更	リモートシステムの探索	リモートサービス	ローカルシステムのデータ		システムリカバリの阻害
有効なアカウント				ホストでのインジケータの削除：Windowsイベントログの消去	ファイルとディレクトリの発見				変造
外部公開されたアプリケーションへのエクスプロイト				ドメインポリシーの変更：グループポリシーの変更	セキュリティソフトウェアの発見				
サプライチェーンの侵害									

PYSA/Mespinoza

Mespinozaとも呼ばれるPYSAランサムウェアは、2019年10月に初めて確認されました。このランサムウェアは、世界中の幅広い業種を攻撃しますが、特に、教育機関や病院などの「ソフトターゲット」を攻撃することで知られています。

感染チェーン

PYSAは、スパムメールや侵害されたRDP資格情報を使用して最初の侵害を完了した後に、ポートスキャナやFamatech Corpが開発したAdvanced IP Scannerなどのスキャンツールを使用して、ネットワーク情報を収集します。Mimikatz、PowerShell Empire、Koadic、PsExecなどのポストエクスプロイトツールを使用して、資格情報を不正取得し、水平移動します。WinSCPツールを使用して、被害者のシステムからデータを抜き取ります。さらには、PowerShellスクリプトを使用して、セキュリティソフトウェアを無効にし、シャドーコピーとシステム復元ポイントを削除することで、被害者がデータを復元できないようにします。最後に、PYSAランサムウェアを展開して実行することで、被害者のデータを暗号化します。

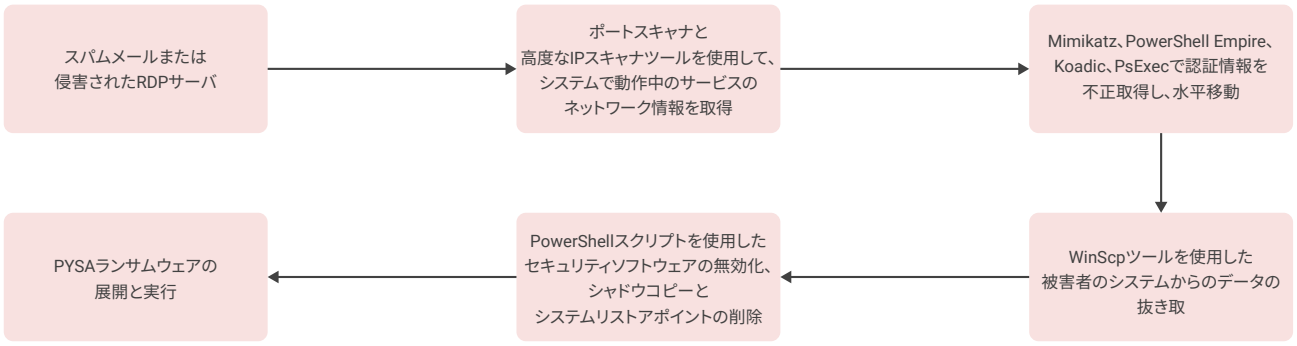


図13：PYSAランサムウェア攻撃の仕組み

PYSA攻撃の18%が教育機関を標的とするものでした。

PYSAは、RSAアルゴリズムとAES-CBCアルゴリズムを組み合わせて使用して、ファイルを暗号化します。

図14に、PYSA/Mespinozaを使用した二重脅迫型攻撃の標的となった業種を示します。

PYSA/Mespinozaの感染状況（業界別）

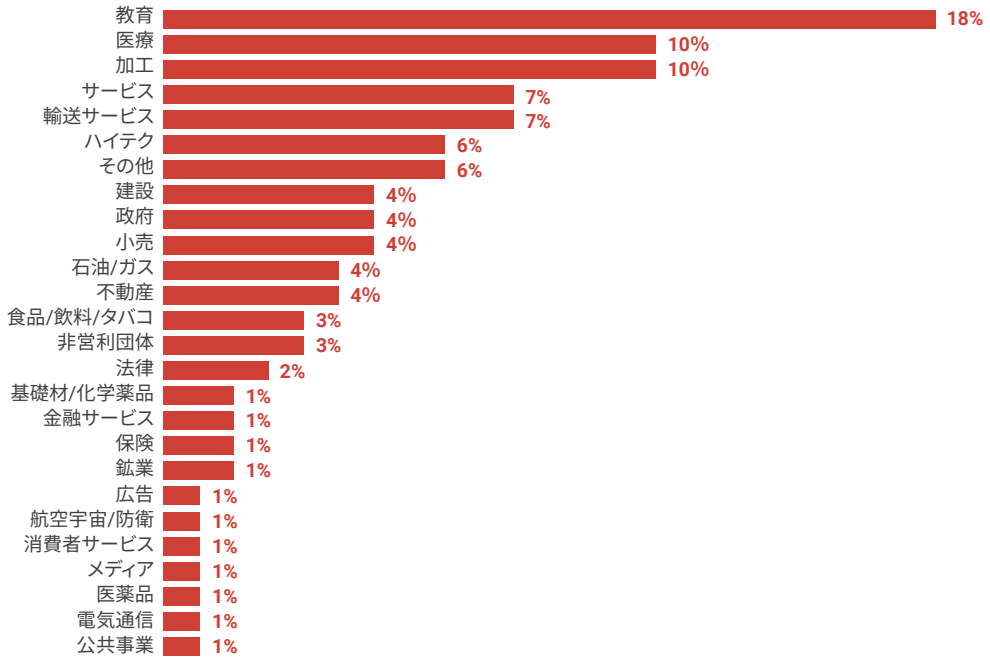


図14：PYSA/Mespinoza攻撃状況（業界別）

被害者が身代金を支払わない場合、PYSAは、盗んだデータをリークサイト（図15参照）に公開します。

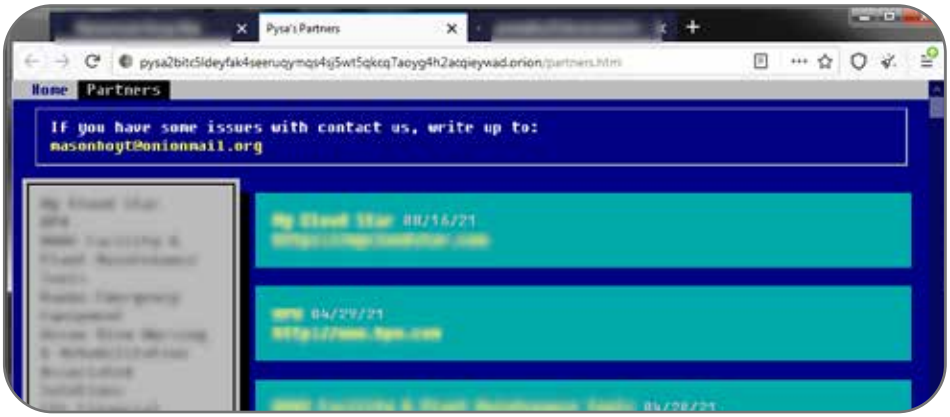


図15：PYSA/Mespinozaのデータリークサイト

PYSA/Mespinoza：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	収集	抜き取り	影響
リンク型スピアフィッシング	コマンドラインインタフェース	ブートまたはログオンの自動起動の実行	アクセストークンの操作	ファイルや情報の難読化解除/デコード	システムネットワーク設定の探索	水平移動ツールの転送	収集したデータのアーカイブ	別プロトコル経由での抜き取り	影響を与えるためのデータ暗号化
添付ファイル型スピアフィッシング	モジュールのロードによる実行	タスク/ジョブスケジューリング		防御の妨害	リモートシステムの探索		ローカルシステムのデータ	Webサービス経由での抜き取り	システムリカバリの阻害
有効なアカウント	ユーザによる実行			ドメインポリシーの変更：グループポリシーの変更	ファイルとディレクトリの発見				
					セキュリティソフトウェアの発見				
					クエリの登録				

REvil/Sodinokibi

REvilランサムウェア（別名、Sodinokibi）は、2019年4月に初めて発見された、この数年間で最も活発な脅威集団の1つです。REvilは、RaaSエコシステムも利用します。REvilは2020年1月に二重脅迫を開始し、ハッキングフォーラムで初めてデータを公開しました。Sodinokibiの攻撃者は2020年2月に、図16に示す独自のデータリークサイトを立ち上げました。

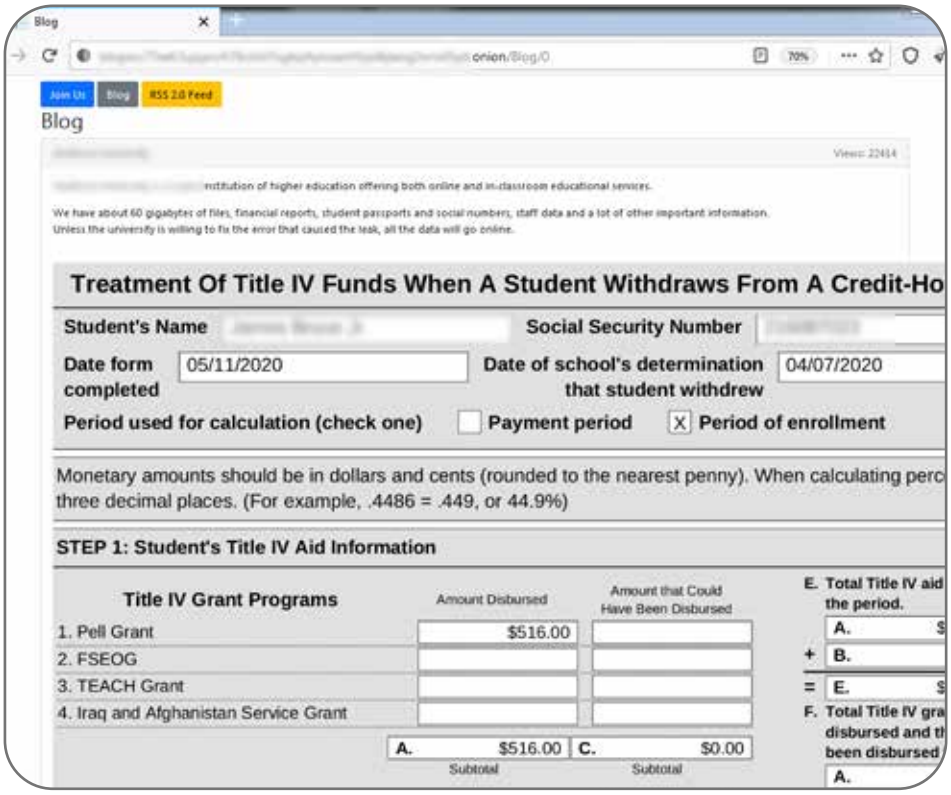


図16：REvil/Sodinokibiのデータリークサイト

さらには、リークサイトで不正取得したデータのオークションを試みましたが、最終的にこの試みは失敗しました。

REvil脅威集団は、2021年7月のKaseya VSAサーバのゼロデイ脆弱性のエクスプロイトで知られています。侵害されたKaseya VSAサーバが使用され、そのVSAサーバで管理されていたすべてのクライアントに不正スクリプトが送信されました。

前述のように、REvilのメンバーが2022年1月にロシアの法執行機関によって逮捕されたとされていますが、2022年4月にはこのランサムウェアが更新されて、インフラストラクチャもオンラインに復帰し、REvil攻撃も再開しました。

感染チェーン

REvilのアフィリエイトは、スパムメール、エクスプロイトキット、侵害されたRDPアカウント、脆弱性エクスプロイトなどの様々な初期アクセスのメカニズムを使用します。キャンペーンのある例では、不正添付ファイルを含むスパムメールから開始し、そのファイルを開くと、IcedIDなどのトロイの木馬がダウンロードされて、水平移動のピボットポイントとしての役割を果たすようになります。図17に示すように、REvilのアフィリエイトは、Cobalt Strike、SharpSploit、Mimikatz、その他のポストエクスプロイトツールなどの様々なツールを使用して資格情報を不正取得します。アフィリエイトはさらに、Netscan、BloodHound、AdFind、その他のネットワーク検出ツールを使用してネットワーク情報を収集し、PsExecまたはRDPアクセスを使用して水平移動します。データの抜き取りは、FileZilla、Rclone、MEGAsync、FreeFileSyncを使用して行われます。REvilのアフィリエイトは、PC Hunter、Process Hacker、KillAV、その他のスクリプトをランサムウェアを展開する前に使用することで、セキュリティソフトウェアに関連するプロセスやサービスを強制終了することが知られており、REvilランサムウェアを最後に展開してデータを暗号化します。

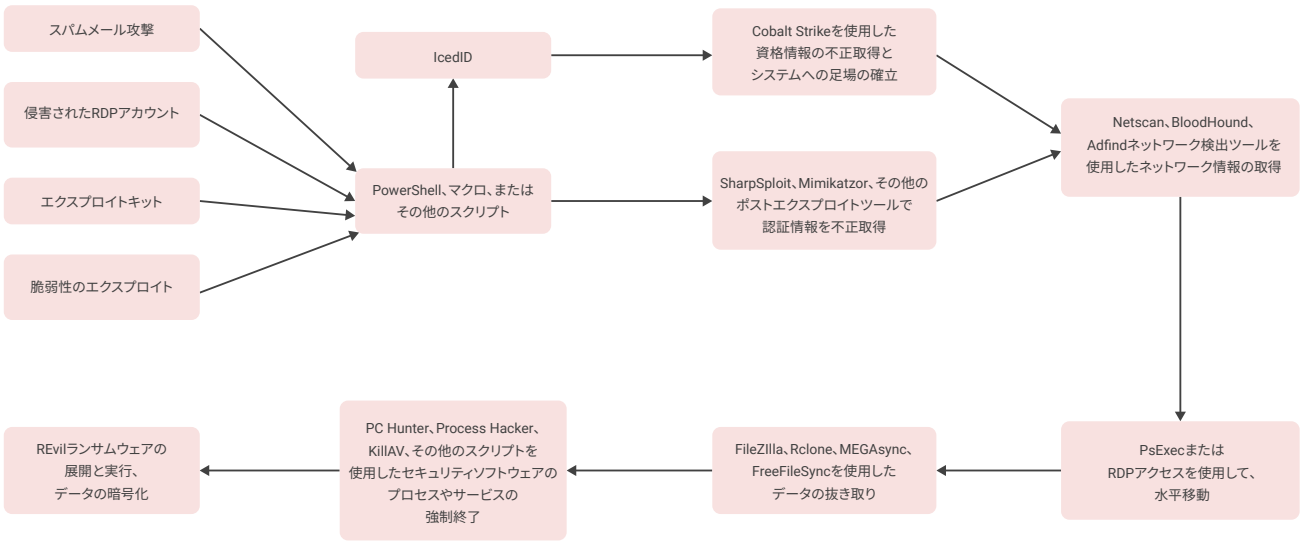


図17：REvil/Sodinokibiの攻撃チェーン

REvilは、非対称楕円曲線暗号化を使用し、Curve25519とSalsa20を組み合わせて使用してファイルを暗号化します。

図18に、REvilを使用した二重脅迫型攻撃の標的となった業種を示します。

REvil/Sodinokibiの感染状況（業界別）

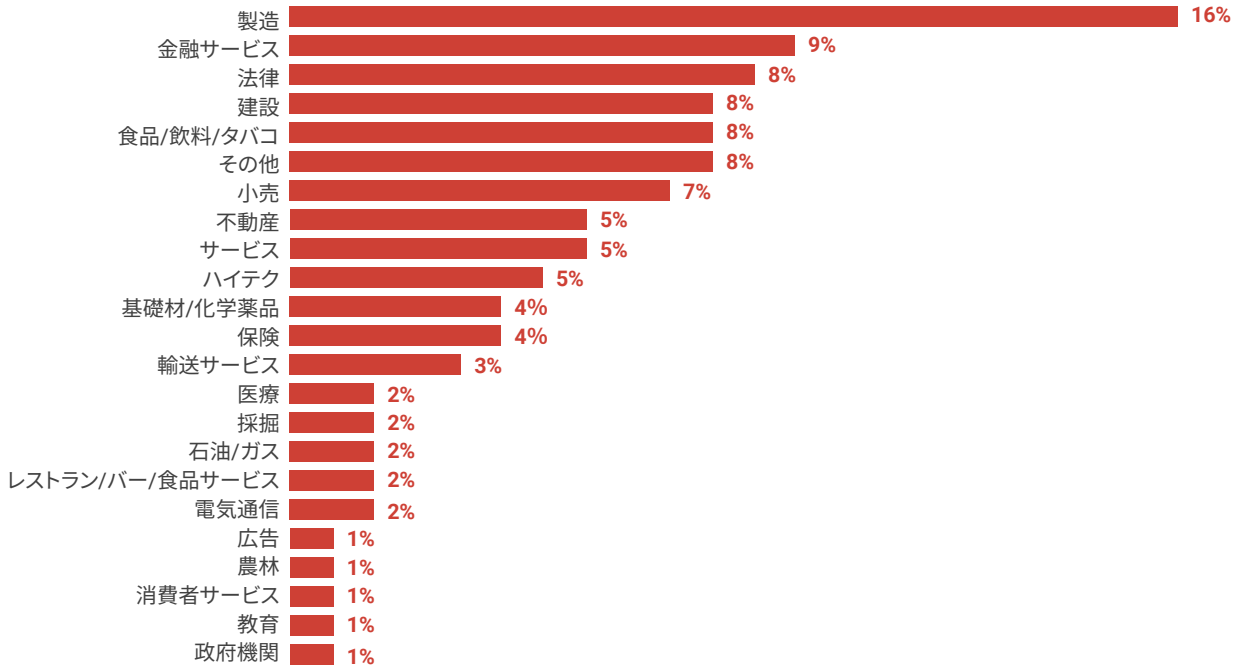


図18：REvil/Sodinokibiの感染状況（業界別）

REvil/Sodinokibi：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	収集	抜き取り	影響
リンク型スピアフィッシング	コマンドラインインタフェース	ブートまたはログオンの自動起動の実行	アクセストークンの操作	ファイルや情報の難読化解除/デコード	システムネットワーク設定の探索	水平移動ツールの転送	収集したデータのアーカイブ	自動化された抜き取り	影響を与えるためのデータ暗号化
添付ファイル型スピアフィッシング	モジュールのロードによる実行	実行フローの乗っ取り	実行フローの乗っ取り	防御の妨害	リモートシステムの探索	リモートサービス	ローカルシステムのデータ	Webサービス経由での抜き取り	システムリカバリの阻害
外部公開されたアプリケーションへのエクスプロイト	共有モジュール		権限昇格のエクスプロイト		ファイルとディレクトリの発見				システムのシャットダウン/再起動
Web閲覧による感染	ユーザによる実行				セキュリティソフトウェアの発見				変造
有効なアカウント					クエリの登録				
サプライチェーンの侵害									

Avaddon

Avaddonは、2020年6月に最初に発見された、非常に活発に活動していたランサムウェアです。AvaddonもRaaSエコシステムを使用するランサムウェアファミリーでしたが、2021年1月にDDoSが三重脅迫手法として追加されました。被害者のWebサイトかネットワークにDDoS攻撃を仕掛け、被害者が攻撃者との交渉に応じるよう誘導して、身代金の額を吊り上げます。

感染チェーン

Avadonは、様々なベクトルを悪用する異なるアフィリエイトを通じてアクセスを手に入れました。Avaddonの最も多い拡散方法はスパム攻撃やエクスプロイトキットでしたが、ブルートフォース攻撃を使用したり、RDPやVPNの資格情報を侵害してネットワークにアクセスしたりするアフィリエイトもいました。

攻撃チェーンのある例では、Avaddonが、侵害された資格情報を使用して最初に感染した初期ブローカへのアクセスを手に入れ、BlackCrowやDarkRaven Webシェルなどのカスタムマルウェアを使用して標的システムに足場を確立しました。Avaddonは、SystemBCを使用して侵害されたホストにアクセスした後に、MimikatzとSharpDumpを使用して資格情報を不正取得し、SoftPerfect Network Scanner、PowerSploit、Empireを使用してポストエクスプロイトのネットワークスキャンを実行しました。Avadonのアフィリエイトは、RDPを使用して水平移動し、Windowsスケジュールタスクを使用して永続化しました。メインのランサムウェアペイロードをドロップする前に、MEGAsyncを使用してデータを抽出し、セキュリティソフトウェアに関連するプロセスとサービスを強制終了しました。最後に、Avaddonペイロードをドロップして実行し、標的システムを暗号化しました。

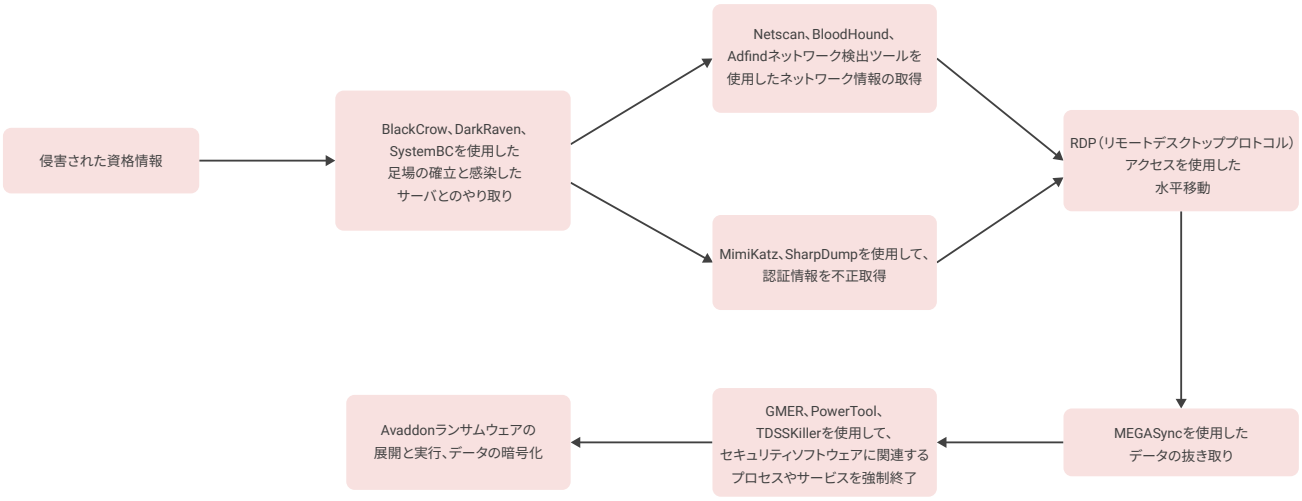


図19：Avaddonランサムウェア攻撃の仕組み

Avaddonは、RSAアルゴリズムとAESアルゴリズムを組み合わせて使用して、ファイルを暗号化しました。ある研究者が2月に、不具合が見つかった後に無料の復号化ツールを公開しましたが、その不具合はのちにAvadonによって修正されました。Avadonが2021年6月に活動を停止し、被害者の復号化キーを公開しました。これにより、EmsisoftがAvadonランサムウェアの復号化ツールを開発することができました。

前述した他のランサムウェアファミリと同様、Avaddonも2020年8月に図20に示す独自のデータリーク Webサイトを立ち上げて、トレンドに追随しました。

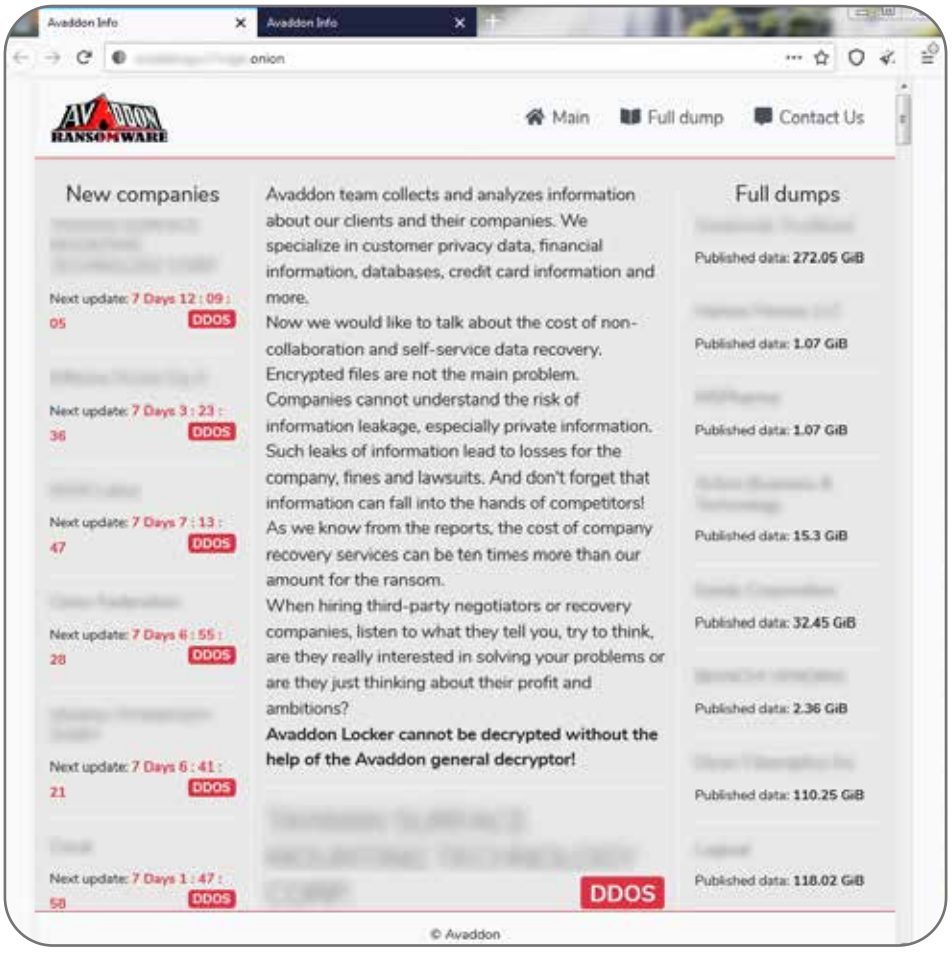


図20：Avaddonのデータリークサイト

Avaddonの脅威集団は、2021年6月に活動を停止した後に、Thanosランサムウェアビルダを使用して攻撃を再開しました。AvaddonからHaronに名前を変更し、2021年10月には再びMidasという名前に変更しました。

図21に、Avaddonを使用した二重脅迫型攻撃の標的となった業種を示します。

Avaddonの感染状況（業界別）

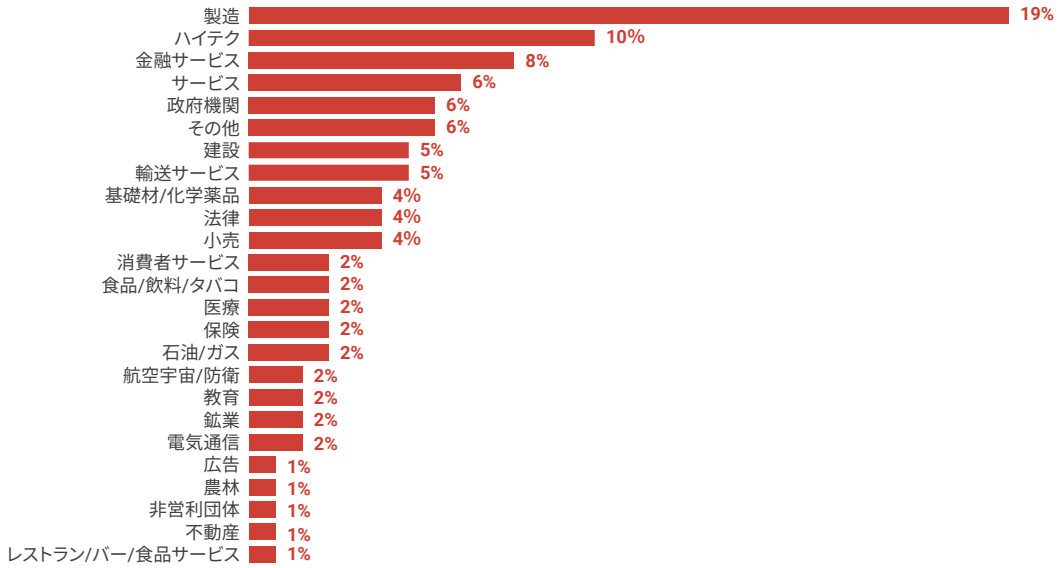


図21：Avaddonの感染状況

Avaddon：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	収集	抜き取り	影響
リンク型スピアフィッシング	コマンドラインインタフェース	ブートまたはログオンの自動起動の実行	有効なアカウント	ファイルや情報の難読化解除/デコード	システムネットワーク設定の探索	水平移動ツールの転送	収集したデータのアーカイブ	別プロトコル経由での抜き取り	影響を与えるためのデータ暗号化
添付ファイル型スピアフィッシング	タスク/ジョブスケジューリング	有効なアカウント		防御の妨害	リモートシステムの探索	リモートサービス：リモートデスクトッププロトコル	ローカルシステムのデータ		システムリカバリの阻害
外部公開されたアプリケーションへのエクスプロイト	ユーザによる実行			プロセスインジェクション	ファイルとディレクトリの発見				
Web閲覧による感染				ホストでのインジケータの削除	セキュリティソフトウェアの発見				
有効なアカウント				ホストでのインジケータの削除	セキュリティソフトウェアの発見				

Clop

Clopランサムウェアは2019年2月に初めて確認されました。Clopは2020年3月に二重脅迫の使用を開始し、身代金の支払いに応じなかった組織から盗んだデータをデータリークサイトに公開しました（図22参照）。

図22：Clopのデータリークサイト

Clopの犯罪集団は、大規模組織を重点的に攻撃します。ThreatLabzは、Clopランサムウェア集団が数千万ドルの身代金を要求し、数百万ドルの身代金の支払を受け入れない場合もあることを確認しています。

Clopランサムウェアを最初に展開したのは脅威集団のTA505とFIN11で、TA505はスパム攻撃でこのランサムウェアを広範囲に拡散しました。ThreatLabzは、特権の昇格によりリモートコード実行を可能にする、SolarWinds Serv-U CVE-2021-35211脆弱性を悪用するいくつかのClop攻撃を確認しています。FIN11も、CVE-2021-27101、CVE-2021-27102、CVE-2021-27103、CVE-2021-27104で追跡されるAccellionファイル転送アプライアンス（FTA）の複数の脆弱性を悪用したことが確認されています。FIN11は、DEWMODE Webシェルをドロップし、Clopランサムウェアをドロップして実行する前にデータを抜き取ります。

大規模組織を重点的に攻撃するClopによる被害額は2021年11月の段階で5億ドルと推定されています。

感染チェーン

TA505によるある攻撃では、HTML添付ファイルを含むスパムメールによって侵害が達成されました。その添付ファイルによってXLS文書ファイルにリダイレクトされ、そのファイルによってGet2 ローダがドロップされ、そのローダによってSdBot、FlawedAmmy、FlawedGrace、Cobalt Strikeなどのペイロードがさらにダウンロードされます。ネットワークに足場を確立してデータを不正取得した後に、Clopランサムウェアが展開されて実行されます（図23参照）。

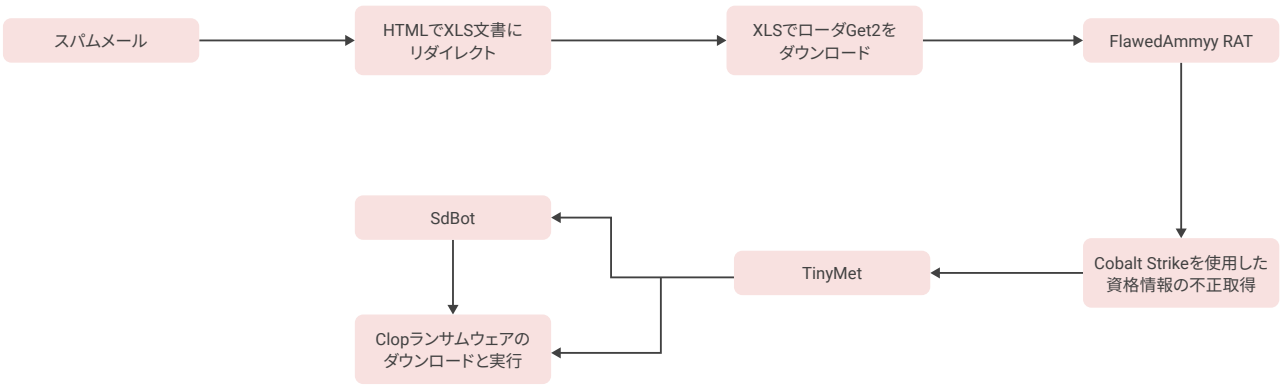


図7：Clopランサムウェア攻撃の仕組み

Clopは、RSAアルゴリズムとAESアルゴリズムを使用してファイルを暗号化します。

図24に、Clopを使用した二重脅迫型攻撃の標的となった業種を示します。

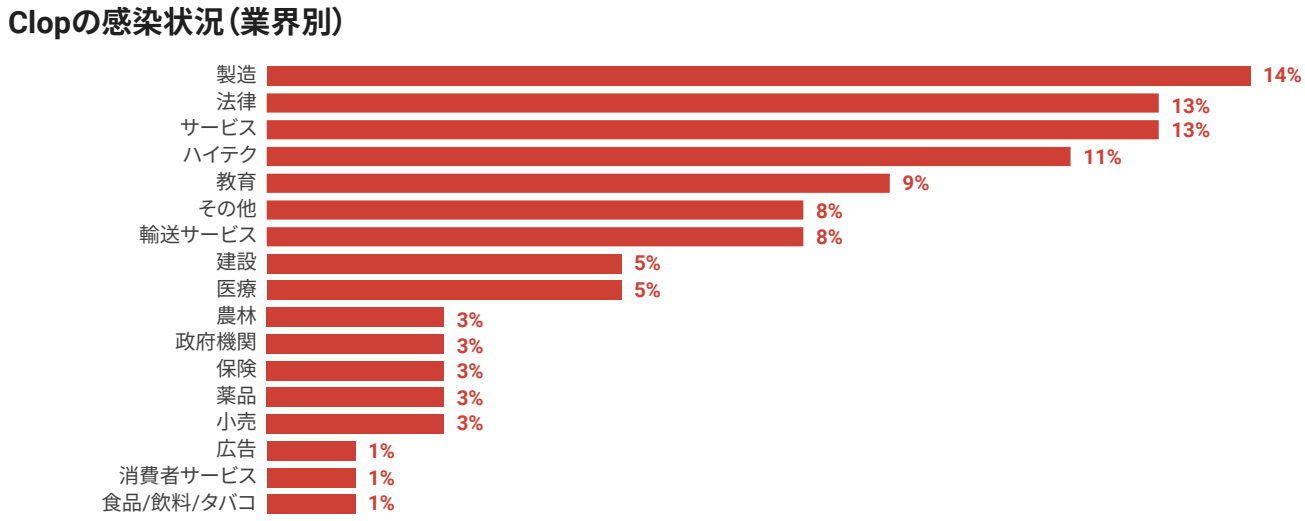


図21：Clopの感染状況（業界別）

Clop：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	抜き取り	影響
有効なアカウント	コマンドラインインタフェース	ブートまたはログオンによる自動実行	アクセストークンの操作	なりすまし：無効なコード署名	システムネットワーク設定の探索	水平移動ツールの転送	自動化された抜き取り	影響を与えるためのデータ暗号化
添付ファイル型スピアフィッシング	ユーザによる実行	システムプロセスの作成または変更：Windowsサービス	User Account Control (UAC) のバイパス	防御の妨害：ツールの無効化または変更	リモートシステムの探索	リモートサービス	Webサービス経由での抜き取り	システムリカバリの阻害
外部公開されたアプリケーションへのエクスプロイト	ネイティブAPI		権限昇格のエクスプロイト	ファイルや情報の難読化解除/デコード	ファイルとディレクトリの探索			
サプライチェーンの侵害				プロセスインジェクション：DLLインジェクション	クエリの登録			
				間接的なコマンドの実行	セキュリティソフトウェアの探索			

Grief

Griefは、コロニアルパイプライン攻撃後の2021年5月に活動が大幅に減少したDoppelPaymerから名前を変えたランサムウェアです。GriefとDoppelPaymerには、ランサムウェアコードやデータリーク Webサイトなどの多くの共通点があります。図25に、Griefのリークサイトのスクリーンショットの例を示します。

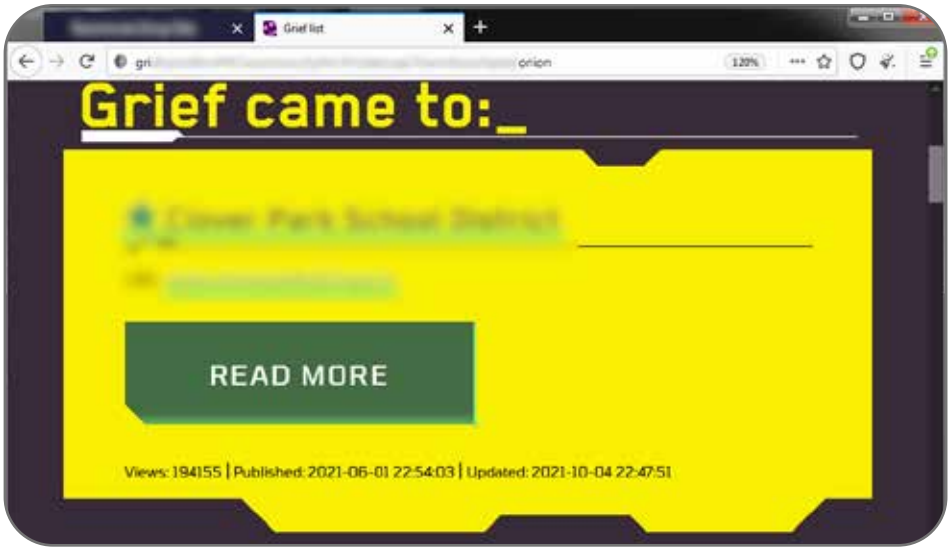


図25：Griefのデータリークサイト

Griefの身代金ポータルには、DoppelPaymerポータルといくつか相違点があり、例えば、身代金の支払にビットコインではなくモネロが指定されます。暗号通貨がこのように変更されたのは、FBIがビットコインで支払われたコロニアルパイプラインの身代金の一部を回収したためである可能性があります。

感染チェーン

Griefランサムウェアが、すでにDridexに感染しているシステムに展開されます。攻撃者はこのDridexを使用した後にCobalt Strikeを使用し、Griefランサムウェアのペイロードを展開して実行します。Griefは、2048 ビット RSAと256 ビット AESのアルゴリズムの組み合わせを使用してファイルを暗号化します。

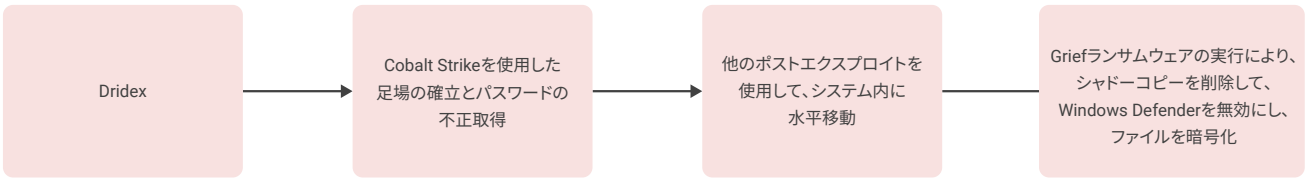


図26：Griefランサムウェア攻撃の仕組み

図27に、Griefを使用した二重脅迫型攻撃の標的となった業種を示します。

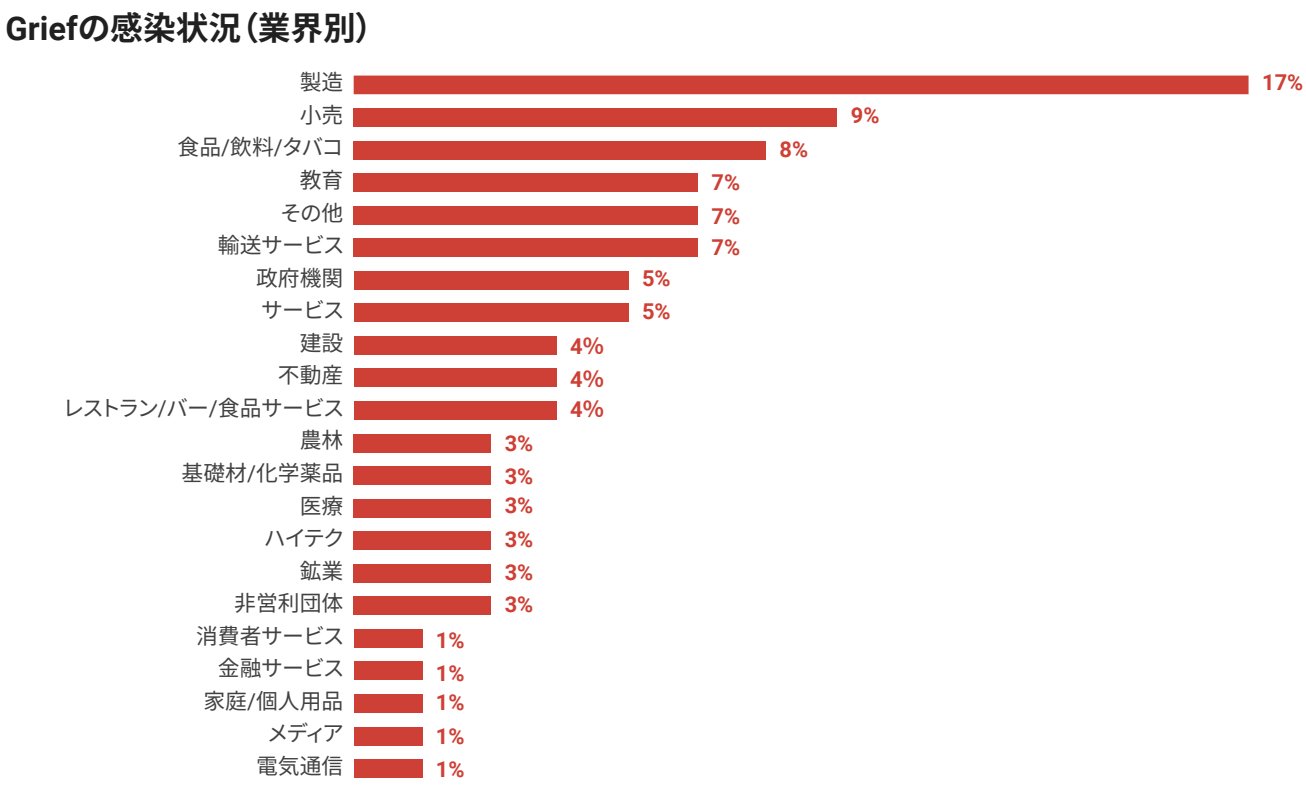


図27：Griefの感染状況（業界別）

Grief：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	抜き取り	影響
有効なアカウント	コマンドラインインタフェース	ブートまたはログオン自動開始の実行：レジストリ実行キー / スタートアップフォルダ	プロセスインジェクション	実行フローの乗っ取り：DLL検索順の乗っ取り	システムネットワーク設定の探索	水平移動ツールの転送	スケジュールされた転送	影響を与えるためのデータ暗号化
添付ファイル型スピアフィッシング	ユーザによる実行	タスク/ジョブスケジューリング		ファイルや情報の難読化解除/デコード	リモートシステムの探索			システムリカバリの阻害
	共有モジュール			防御の妨害：ツールの無効化または変更	ファイルとディレクトリの探索			システムのシャットダウン/再起動
				なりすまし：正規の名前や場所との一致	セキュリティソフトウェアの探索			

Hive

Hiveランサムウェアは、RaaSモデルを使用する攻撃という形で2021年6月に初めて確認されました。このランサムウェアは、不正スパムメール、流出したVPN資格情報、外部に公開されている資産の脆弱性のエクスプロイトなどの複数のメカニズムを使用して初期アクセスを手に入れます。最初の感染は、Microsoft Exchange Serverに存在するProxyShellの脆弱性のエクスプロイトにより開始します。Exchange Serverに存在するProxyShellの脆弱性は、CVE-2021-34473（Microsoft Exchange Serverのリモートコード実行の脆弱性）、CVE-2021-34523（Microsoft Exchange Serverの特権昇格の脆弱性）、CVE-2021-31207（Microsoft Exchange Serverのセキュリティ機能迂回の脆弱性）の組み合わせです。

感染チェーン

攻撃者は、エンコードされたWebシェルを含むファイルが添付された下書きの電子メールをメールボックス内に作成します。攻撃者は次に、メールボックス全体（作成した下書きの電子メールを含む）を拡張子がASPXのPSTファイル形式にエクスポートします。これにより、攻撃者は脆弱なサーバにWebシェルをドロップできるようになります。このWebシェルにより、エンコードされたCobaltストライクペイロードを含むPowerShellスクリプトがダウンロードされ、さらには、追加のステージャをダウンロードすることで、被害者のシステムに足場を確立します。次に、Mimikatzを使用してNTLMハッシュを不正取得し、ハッシュパス戦術を利用してドメインコントロールアカウントにアクセスします。そして、不正取得した資格情報を使用して、RDPでさらに水平移動を実行します。さらには、SoftPerfectネットワークスキャナを使用してネットワークをスキャンし、追加情報を取得します。最後に、Hiveランサムウェアを展開して実行し、データを暗号化します。

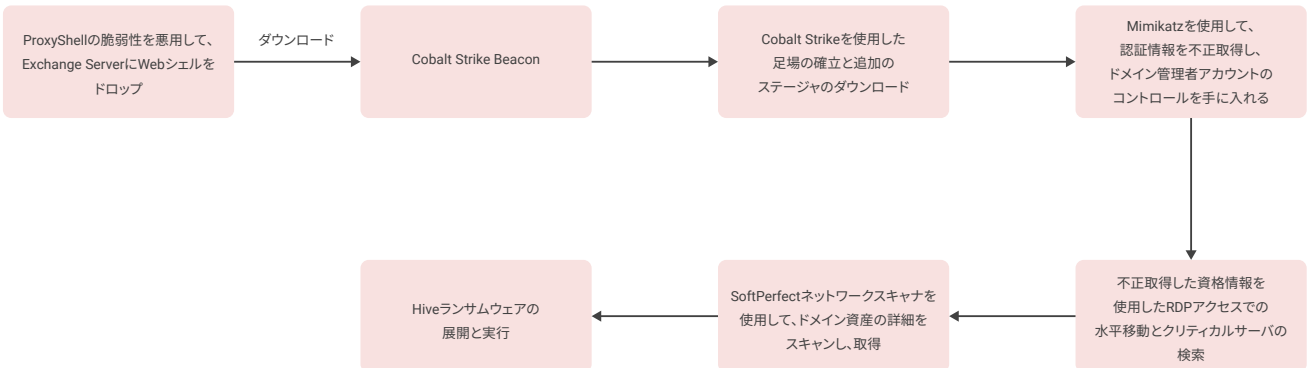


図28：Hiveの攻撃チェーン

以前のバージョンのHiveランサムウェアペイロードはGoプログラミング言語で記述され、RSAアルゴリズムとAESアルゴリズムの組み合わせを使用してファイルを暗号化していました。新しいバージョンのHiveはRustプログラミング言語で記述されており、Curve25519とChaCha20を使用してファイルを暗号化します。

Hiveのアフィリエイトは、ファイルを暗号化する前に被害者からデータを抜き取ります。図29に、Hiveのデータリークサイトのスクリーンショットを示します。

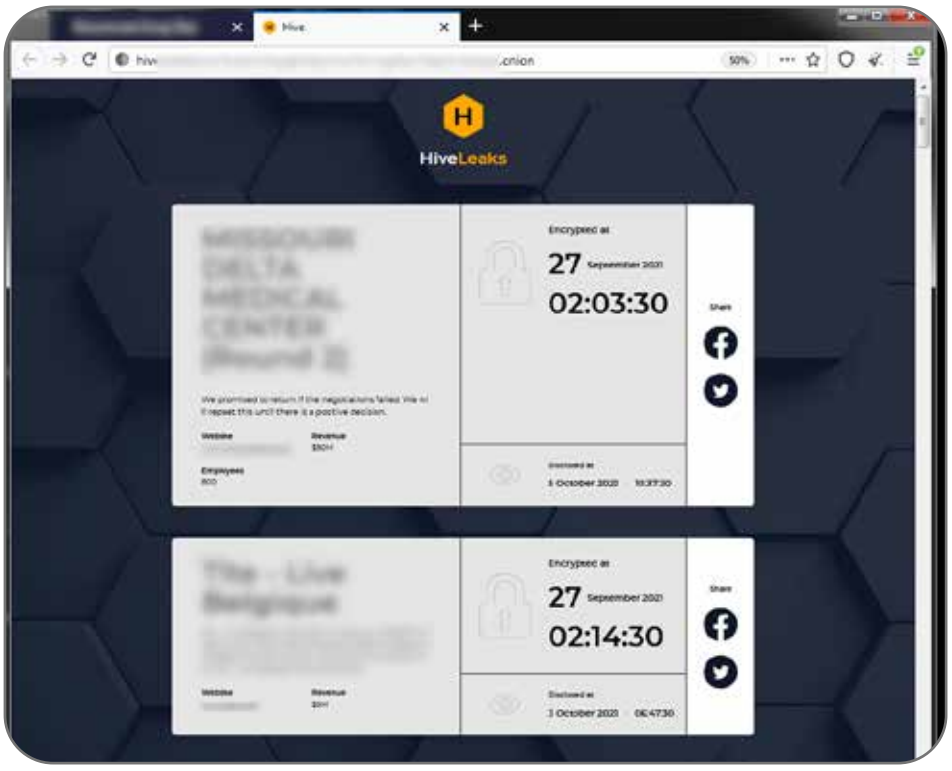


図29：Hiveのデータリークサイト

図30に、Hiveを使用した二重脅迫型攻撃の標的となった業種を示します。

Hiveの感染状況（業界別）

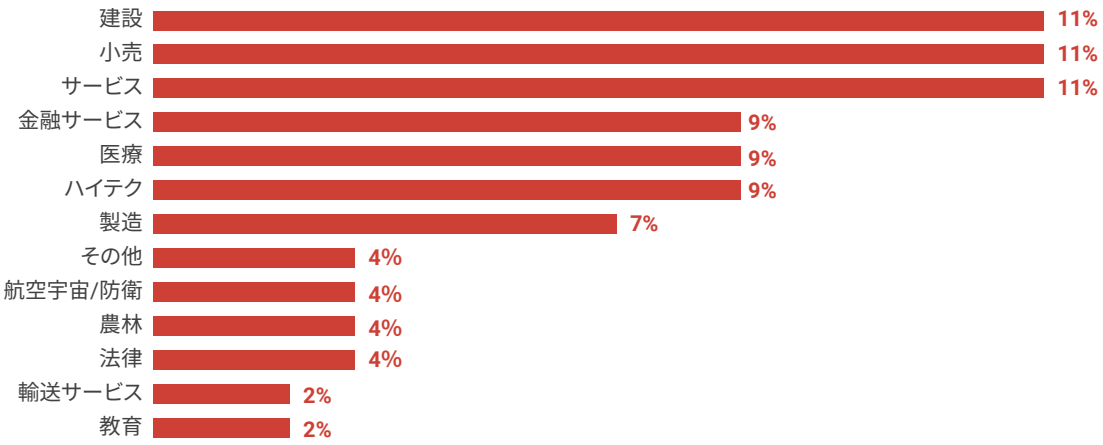


図30：Hiveの感染状況（業界別）

Hive：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	抜き取り	影響
外部のリモートサービス	コマンドラインインタフェース	有効なアカウント：ドメインアカウント	有効なアカウント	Windowsイベントログの消去	システムネットワーク設定の探索	リモートデスクトッププロトコル	スケジュールされた転送	影響を与えるためのデータ暗号化
添付ファイル型スピアフィッシング	ユーザによる実行	アカウントの作成：ドメインアカウント	ドメインアカウント	防御の妨害：ツールの無効化または変更	リモートシステムの探索	リモートサービス		システムリカバリの阻害
外部公開されたアプリケーションへのエクスプロイト			権限昇格のエクスプロイト	ファイルや情報の難読化解除/デコード	ファイルとディレクトリの探索			
					クエリの登録			
					セキュリティソフトウェアの探索			

BlackByte

BlackByteも、2021年7月に確認された、活発に活動していたRaaS集団です。最初はC#で記述されていましたが、2021年9月頃にGoプログラミング言語で記述されたバージョンが開発されました。このGoベースのバージョンは、水平方向への拡散、特権の昇格、ファイルの暗号化を実行するコマンドなどの、C#バージョンとの多くの類似点があります。

BlackByte攻撃は、Microsoft Exchange Serverに存在するProxyShellの脆弱性を悪用することで開始します。

感染チェーン

攻撃者は、電子メールの下書きをメールボックス内に作成します。その電子メールには、エンコードされたWebシェルを含むファイルが添付されます。攻撃者は次に、メールボックス全体（電子メールの下書きを含む）を拡張子がASPXのPSTファイル形式にエクスポートします。これにより、攻撃者は脆弱なサーバにWebシェルをドロップできるようになります。

次に、Webシェルを使用して、標的であるExchange ServerにCobalt Strike Beaconをドロップします。Cobalt Strikeやその他のポストエクスプロイトツールを使用して、資格情報を不正取得し、サービスアカウントにアクセスしてシステムに足場を確立します。BlackByteはさらに、AnyDesk RDPツールもインストールし、AnyDeskを使用して、水平移動と感染したドメインコントローラにCobalt Strikeをドロップします。Cobalt Strikeは最後に、BlackByteランサムウェアを展開して実行します。

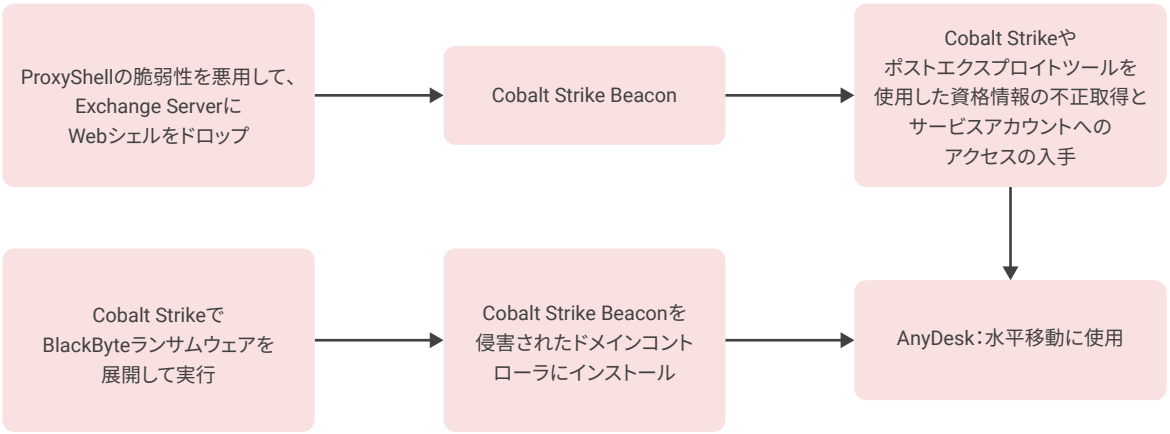


図31：BlackByteランサムウェア攻撃の仕組み

ProxyShellの脆弱性を悪用してExchange ServerにWebシェルをドロップすることで、初期アクセスを手に入れます。このWebシェルによって、Cobalt Strike Beaconがダウンロードされます。Cobalt Strikeは次に資格情報を不正取得し、AnyDesk RDPツールをインストールします。AnyDeskを使用して水平移動し、感染したドメインコントローラにCobalt Strikeをドロップし、Cobalt Strikeを使用してBlackByteランサムウェアを展開し、実行します。

BlackByteは、RSAアルゴリズムとAESアルゴリズムの組み合わせを使用してファイルを暗号化します。最新のBlackByteバージョンは、Curve25519 ECCを非対称暗号化に使用し、ChaCha20を対称ファイル暗号化に使用します。

BlackByteの攻撃者も、ファイルを暗号化する前に被害者からデータを抜き取ります。図32に、BlackByteのデータリークサイトのスクリーンショットを示します。

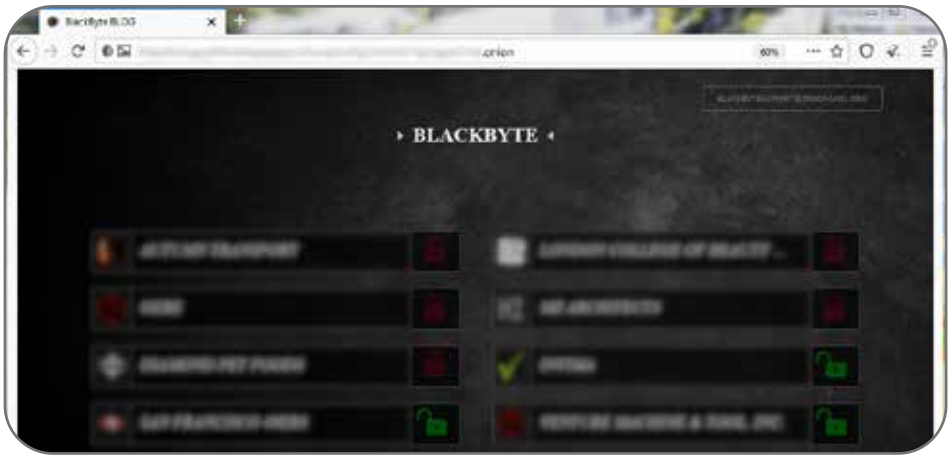


図32：BlackByteのデータリークサイト

図33に、BlackByteを使用した二重脅迫型攻撃の標的となった業種を示します。

BlackByteの感染状況（業界別）

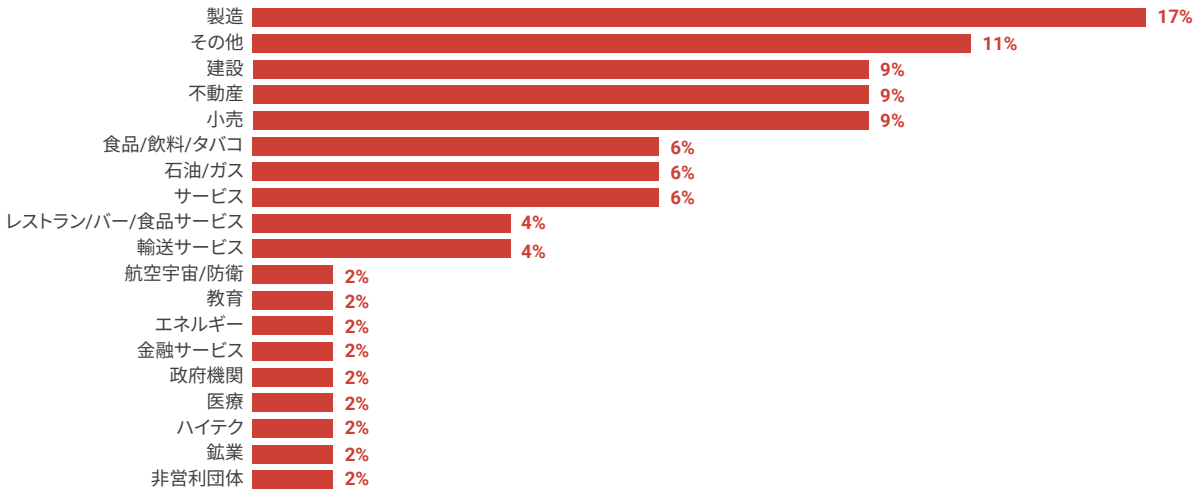


図33：BlackByteの感染状況（業界別）

BlackByte：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	抜き取り	影響
添付ファイル型スピアフィッシング	コマンドとスクリプトインタプリタ	システムプロセスの作成または変更：Windows サービス	ドメインアカウント	防御の妨害：ツールの無効化または変更	システムネットワーク設定の探索	水平移動ツールの転送	スケジュールされた転送	影響を与えるためのデータ暗号化
外部公開されたアプリケーションへのエクスプロイト	ネイティブAPI		権限昇格のエクスプロイト	ファイルや情報の難読化解除/デコード	リモートシステムの探索			システムリカバリの阻害
	ユーザによる実行			レジストリの変更	ファイルとディレクトリの探索			
					クエリの登録			
					セキュリティソフトウェアの探索			

AvosLocker

AvosLockerランサムウェアは、2021年7月に多く確認されたRaaSです。HiveやBlackByteと同様、初期感染は、Exchange Serverに存在するProxyShellの脆弱性であるCVE-2021-34473、CVE-2021-34523、CVE-2021-31207を悪用することで開始します。

感染チェーン

攻撃者は、電子メールの下書きをメールボックス内に作成します。その電子メールには、エンコードされたWebシェルを含むファイルが添付されます。攻撃者は次に、メールボックス全体（電子メールの下書きを含む）を拡張子がASPXのPSTファイル形式にエクスポートします。これにより、攻撃者は脆弱なサーバにWebシェルをドロップできるようになります。

次に、Webシェルを使用して、感染したExchange ServerにCobalt Strikeをドロップします。Cobalt StrikeとRcloneを使用して、資格情報を不正取得し、データをリモートサーバに持ち出します。

この攻撃は、AnyDesk RDPをインストールすることで、複数のシステムにアクセスし、水平移動します。いくつかのバッチスクリプトをドロップして、セキュリティソフトウェアに関連するレジストリキーを変更したり削除したりします。さらには、Windows UpdateとWindows Defenderも無効にします。

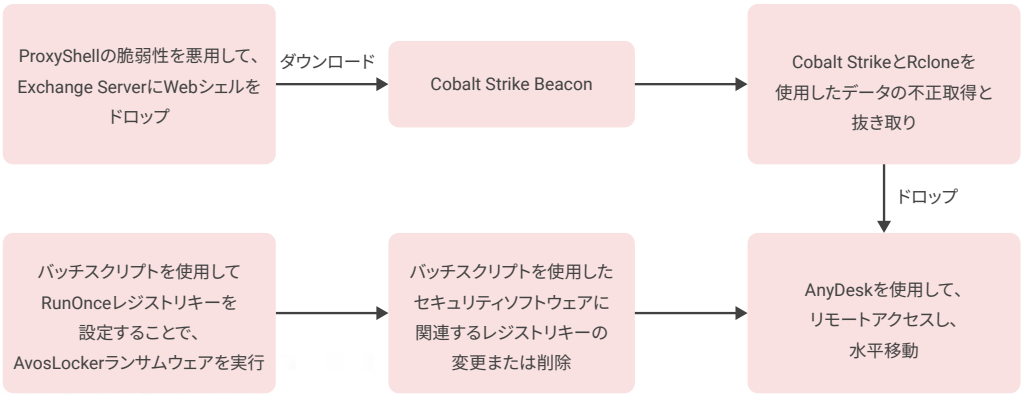


図34：AvosLockerランサムウェア攻撃の仕組み

AvosLockerは最後に、システムをWindowsセーフモードで再起動し、ファイルの暗号化を開始します。セーフモードで起動することで、できるだけ多くのファイルを暗号化できるようになります。セーフモードで起動すれば、データベースなどのビジネスアプリケーションが実行されなくなる可能性が高く、これらのアプリケーションによってファイルの暗号化の妨げとなる可能性のあるオープンファイルハンドルが開かれることがなくなります。さらには、システムがセーフモードで実行されている場合、デフォルトでは、多くのセキュリティソフトウェアアプリケーション（アンチウイルスプログラムなど）がロードされません。Windowsセーフモードでファイルを暗号化する機能は、Conti、REvil、BlackMatterなどの他のランサムウェアファミリでも確認されています。

AvosLockerは、RSAとAESのアルゴリズムの組み合わせを使用してファイルを暗号化します。AvosLockerは、VMware ESXiを標的にするランサムウェアのLinuxバージョンを作成しました。

攻撃者は攻撃後に被害者のデータをデータリークサイトに公開すると脅迫し、交渉中に被害者ネットワークに対するDDoS攻撃を実行すると脅して実際に実行する場合もあります。図35に、AvosLockerのデータリークサイトのスクリーンショットを示します。

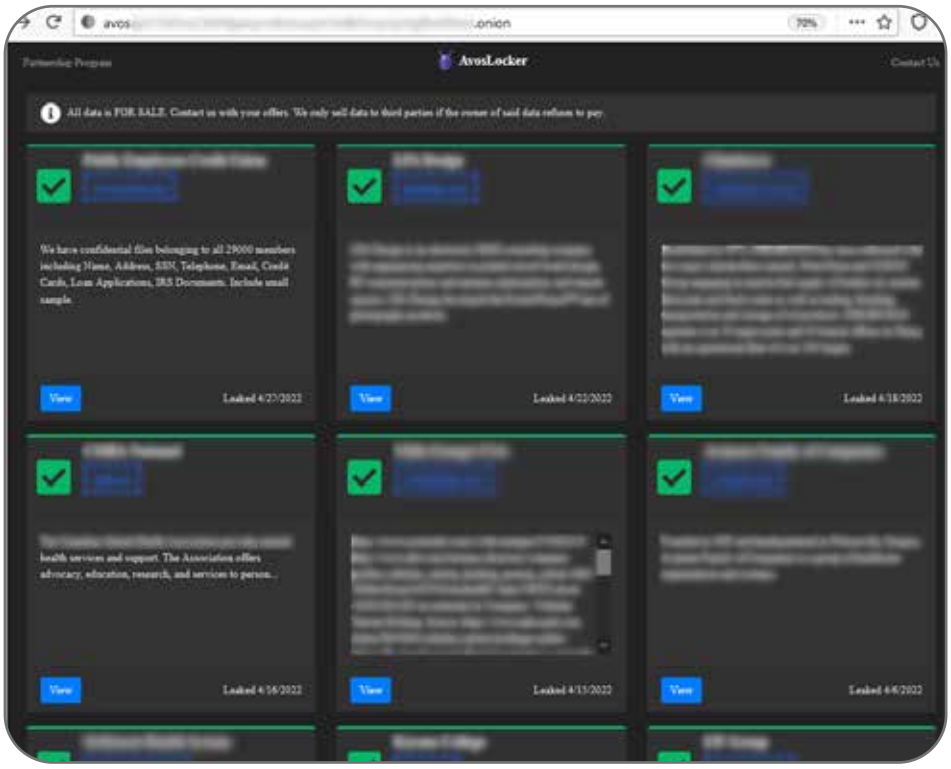


図35：AvosLockerのデータリークサイト

図36に、AvosLockerを使用した二重脅迫型攻撃の標的となった業種を示します。

AvosLockerの感染状況（業界別）

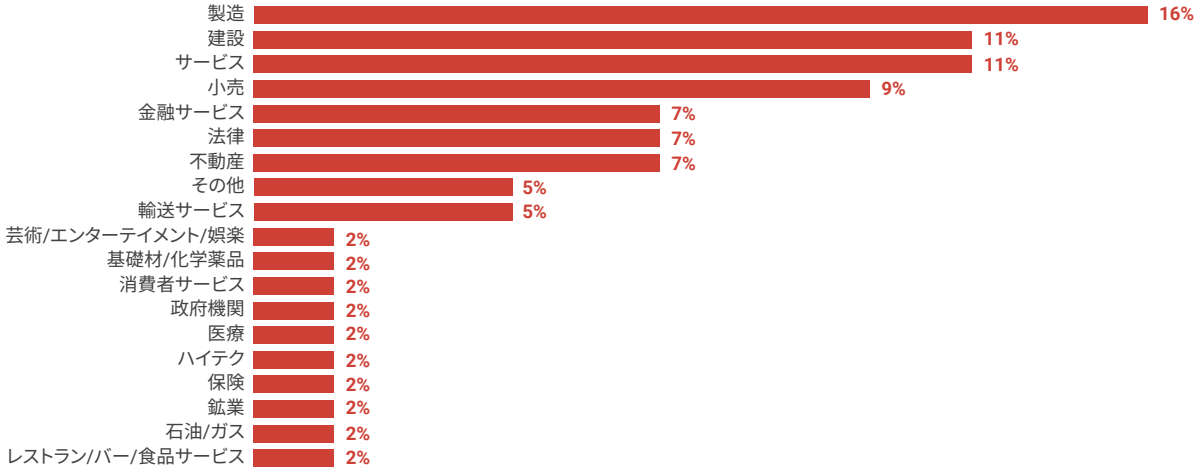


図36：AvosLockerの感染状況（業界別）

AvosLocker：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	抜き取り	影響
添付ファイル型スピアフィッシング	コマンドラインインタフェース	ブートまたはログオン自動開始の実行：レジストリ実行キー / スタートアップフォルダ	ドメインアカウント	防御の妨害：ツールの無効化または変更	システムネットワーク設定の探索	水平移動ツールの転送	スケジュールされた転送	影響を与えるためのデータ暗号化
外部公開されたアプリケーションへのエクスプロイト	ユーザによる実行	タスク/ジョブスケジューリング	権限昇格のエクスプロイト	ファイルや情報の難読化解除/デコード	リモートシステムの探索			システムリカバリの阻害
					ファイルとディレクトリの探索			システムのシャットダウン / 再起動
					セキュリティソフトウェアの探索			

BlackCat/ALPHV

BlackCat（別名 ALPHV）は、2021年11月頃に初めて発見されたRaaSです。BlackCatは、RUSTプログラミング言語を使用しており、これにより、パフォーマンスの向上と信頼性の高い同時実行処理を可能にしています。

感染チェーン

初期感染は、侵害された資格情報を使用して被害者のネットワークシステムにアクセスすることで開始します。最初にCobalt Strike、PowerShellスクリプト、バッチスクリプトを使用して、被害者のネットワークへの足場を確立します。アクセスを手に入れた後に、Active Directoryの管理者アカウントを侵害し、さらには不正 GPO（グループポリシーオブジェクト）を使用してランサムウェアを配布し、実行します。この攻撃では、Microsoft Sysinternalsやその他の管理ツールも使用されます。

図37：BlackCat/ALPHVランサムウェア攻撃の仕組み

BlackCatはDDoS戦術を作戦に追加しました。被害者のWebサイトかネットワークにDDoS攻撃を仕掛け、被害者が攻撃者との交渉に応じるよう誘導して、身代金の額を吊り上げます。図38に、BlackCatのデータリークサイトのスクリーンショットの例を示します。

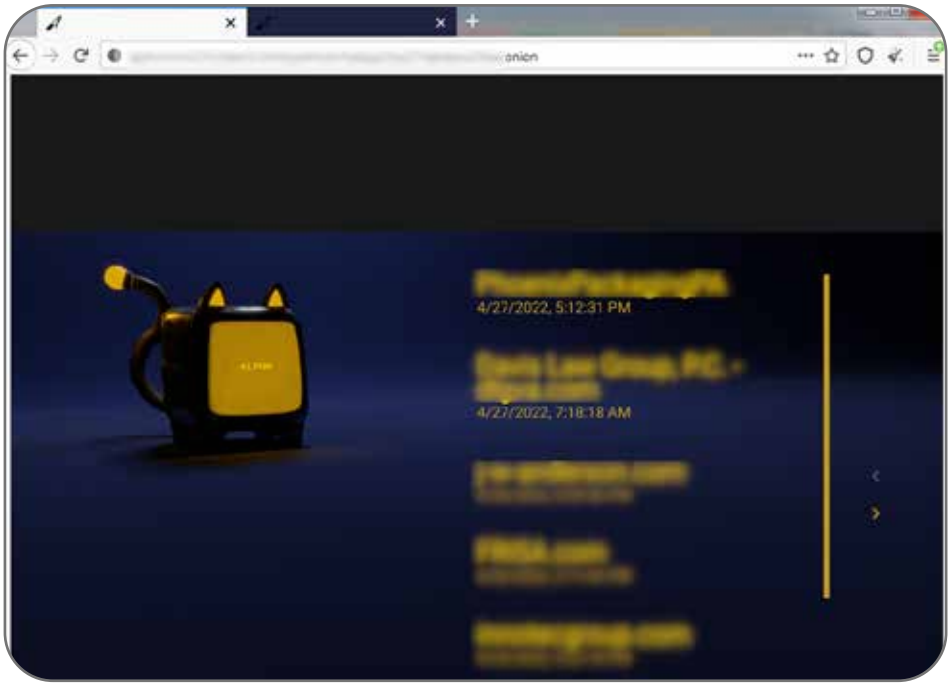


図38：BlackCat/ALPHVのデータリークサイト

図39に、BlackCat/ALPHVを使用した二重脅迫型攻撃の標的となった業種を示します。

BlackCat/ALPHVの感染状況（業界別）

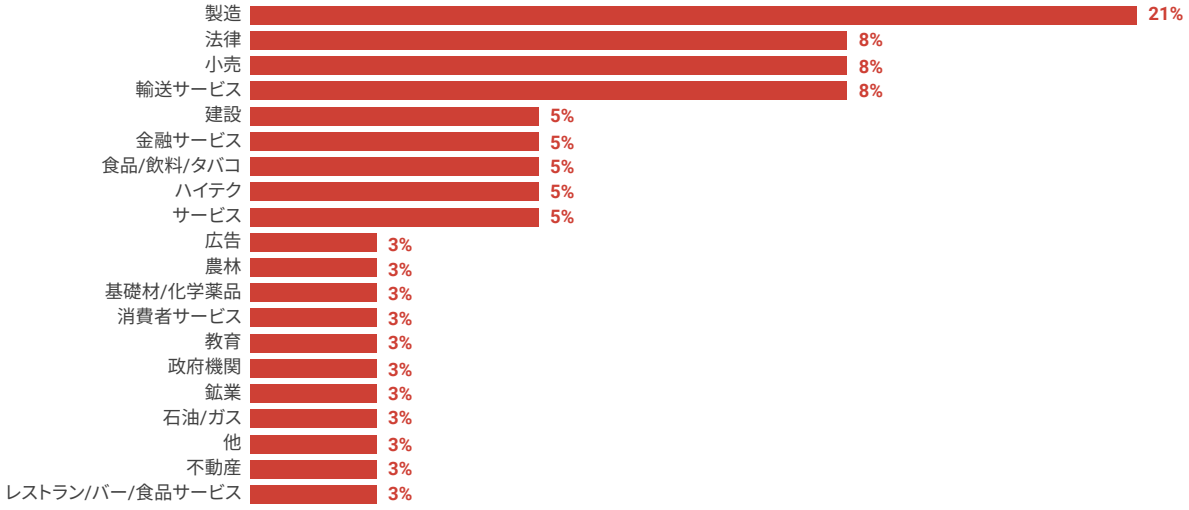


図39：BlackCat/ALPHVの感染状況（業界別）

BlackCat/ALPHV：MITRE ATT&CKによる攻撃者の戦術と手法

初期アクセス	実行	永続化	権限昇格	防衛回避	探索	水平移動	抜き取り	影響
有効なアカウント	コマンドとスクリプトインタプリタ	ブートまたはログオン自動開始の実行：レジストリ実行キー / スタートアップフォルダ	ドメインアカウント	防御の妨害：ツールの無効化または変更	システムネットワーク設定の探索	水平移動ツールの転送	スケジュールされた転送	影響を与えるためのデータ暗号化
	ユーザによる実行	タスク/ジョブスケジューリング	権限昇格のエクスプロイト	ファイルや情報の難読化解除/デコード	リモートシステムの探索			システムリカバリの阻害
				ドメインポリシーの変更：グループポリシーの変更	ファイルとディレクトリの探索			
					セキュリティソフトウェアの探索			

ThreatLabzについて

ThreatLabzは、Zscalerのセキュリティ研究部門です。世界クラスのこのチームは、新しい脅威を追跡し、世界中でゼットスケーラーのプラットフォームを使用する何千もの組織が常に保護されていることを保証する責任を担っています。マルウェアの調査と挙動分析に加え、ゼットスケーラーのプラットフォームの高度な脅威保護を実現する新しいプロトタイプモジュールの研究開発も進めており、社内のセキュリティ監査を定期的に実施することで、ゼットスケーラーの製品やインフラストラクチャがセキュリティコンプライアンス基準を満たすことを常時確認しています。ThreatLabzは、新たな脅威に関する詳細分析を定期的にポータル（research.zscaler.com）で公開しています。

Trust Issuesニュースレターのサブスクリプションにお申し込みいただくと、ThreatLabzの調査に関する最新情報をお知らせします。

Zscaler Zero Trust Exchangeは、業界をリードするセキュリティサービスエッジ（SSE）プラットフォームとしてガートナーに評価されており、ランサムウェアによる攻撃チェーンのあらゆる段階で保護を提供し、攻撃を受ける可能性を大幅に低下させるとともに潜在的な損害を軽減します。

ゼットスケーラーは、業界をリードする機能をネイティブに統合し、次のようなメリットを提供します。

攻撃対象領域の最小化

Zscalerのクラウドネイティブのプロキシベースアーキテクチャは、内部アプリケーションをインターネットから見えなくすることで攻撃対象領域を縮小し、潜在的な攻撃ベクトルを排除します。

侵入の防止

Zscaler は、暗号化されたトラフィックを含むすべてのトラフィックの完全な検査と認証を提供し、ブラウザの分離やインラインサンドボックスなどのツールを活用することで、未知の脅威や回避型の脅威からユーザを保護し、サイバー犯罪者の侵入を防止します。

水平移動の排除

Zscaler は、ユーザとエンティティをネットワークではなくアプリケーションに安全に直接接続することで水平移動の可能性を排除し、最も重要なアプリケーションを本物そっくりのデコイで囲むことで、効果的な保護を可能にします。

情報漏洩の防止

Zscaler は、クラウドアプリケーションに送信されるすべてのトラフィックを検査することで、情報漏洩を防止し、クラウドアクセスセキュリティブローカ（CASB）の機能を使用して、保存データの脆弱性を特定し、修復します。

詳細については、Zscalerのランサムウェア保護をご覧ください。

zscaler™ | Experience your world, secured.™

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタルトランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザ、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータセンタに分散された SASEベースの Zero Trust Exchange は、世界最大のインライン型クラウドセキュリティプラットフォームです。詳細は、**zscaler.jp** をご覧いただくか、Twitter で**@zscaler** をフォローしてください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp