UNIT 42™

ランサムウェア脅威レポート

2022年

paloalto NETWORKS®

目次

序文 3

要旨 4

01
ランサムウェア入門 6

02
ランサムウェアの情勢 8

03
ランサムウェアグループの行動 13

04
ランサムウェア リーク サイトからの知見 23

05
クラウド環境内のランサムウェア 29

06
ランサムウェアのコスト 31

07
結論と推奨事項 32

ランサムウェア攻撃に対して準備を整えるには 37

調査方法 38

パロアルトネットワークスについて 39

Unit 42について 39

序文

2021年のランサムウェア攻撃は世界中で大々的に報道され、その勢いは衰える気配がありませんでした。実際、サイバー犯罪者はランサムウェアにくわえ、被害者を脅迫する手段を見つけて利益を倍増させています。その手段が二重脅迫です。二重脅迫は2020年に初めて出現し、ダーク ウェブ上にはリーク サイトが登場しました。こうしたリーク サイトは、サイバー犯罪者たちがランサムウェア被害者を名指ししてそれら企業の機微データを公開すると脅すために使われています。2021年、ランサムウェア ギャングはこうした戦術を新たなレベルに引き上げ、多重脅迫手法が一般的となって、脅威への対応にかかるコストや緊急度が高まりました。たとえば、身代金の支払いに応じさせようと従業員と顧客に脅迫電話をかけたり、サービス拒否(DoS)攻撃を仕掛けて被害組織のWebサイトをダウンさせたりする攻撃者が確認されています。

2021年には、サービスとしてのランサムウェア(RaaS)のオペレータが増加していることも確認されました。RaaSオペレータは使いやすいツールやサービスを多数提供していて、ランサムウェア攻撃をオンライン オークション サイトの使用と同じくらい簡単にしています。こうしたオペレータは、ビジネスの最適化に向け、これまで数年にわたり投資を行ってきました。マルウェアの完成度を高め、アフィリエイトを増やすマーケティング戦略を定め、さらには身代金の支払い後に被害者の復旧を支援するテクニカル サポート体制も整えたのです。

こうしたイノベーションがすべてあわさって組織のランサムウェア防御がますます困難になり、本レポートで説明するように多額の身代金を支払わざるを得なくなる組織が出てきました。昨年Unit 42コンサルタントが算出した各事例の平均身代金要求額は144%増加して220万ドルに達し、平均支払額は78%上昇して54万1,010ドルになりました。

ランサムウェア ギャングとRaaSオペレータは技術障壁を乗り越えて身代金を増やす新たな手口をつぎつぎ見い出してくることから、2022年も引き続きランサムウェアがあらゆる規模の組織で課題となるでしょう。ランサムウェアはサイバーセキュリティにおける最上位の脅威の1つとなっていることから、パロアルトネットワークスでもこの領域に注力しています。本レポートでは、既存および新興のランサムウェア グループ、支払いのトレンド、セキュリティ上のベストプラクティスに関する最新の知見を示します。本レポートで示した知見が組織の皆さまの脅威への理解を深め、その管理態勢の改善につながれば幸いです。

Ryan Olson

Ryan Olson
脅威インテリジェンス担当VP
パロアルトネットワークス Unit 42

要旨

ランサムウェアは2021年に大々的に報道され、注目度の高い一連の攻撃が世界中の企業、政府、学校に被害を及ぼしました。ランサムウェア攻撃は、わたしたちが当たり前とみなしている日々の活動の多くを妨げます(医師の診療、ガソリンの補給、食料品の購入、テレビでのローカル ニュース視聴、請求書の支払い、旅行の予約、さらには救急支援の要請など)。

Unit 42は、すべてのランサムウェア活動をわかりやすく整理し、ランサムウェアの情勢や今後の方向性について理解が深まるよう、2022年ランサムウェア脅威レポートをまとめました。**本レポートの作成にあたり、弊社リサーチャー、セキュリティ コンサルタントは、以下の2つの情報源からデータを入手しました。**

1. Unit 42が対応した事例。これらから活動している多様な脅威アクターに関する実践的な見解を得ました。
2. リークサイトと一般的なアンダーグラウンド フォーラムの分析結果。リークサイトにはランサムウェア オペレータが盗んだ情報の一部を公開しています。こうした公開は「ネーム・アンド・シェイム」と呼ばれる被害者を名指しで晒しものにする(多重脅迫)戦術の一環として行われていて、被害者に身代金支払いを強要することが目的です。また、アンダーグラウンド フォーラムではサイバー犯罪者が攻撃用ツールについて議論しています。

重要なポイントの1つは、身代金が要求額と支払額の両方で上昇し続けていることです。2021年のインシデント レスポンス事例(主に米国)の身代金要求額は平均約220万ドルでした。弊社コンサルタントが2020年に担当した事例の要求額は平均90万ドルでしたので約144%増加していることになります。また、Unit 42コンサルタントが担当した事例の支払額は平均54万1,010ドルに達し、前年から78%増加しました。

144%

平均要求額
(2021年)

78%

平均支払額
(2021年)

要旨

サイバー犯罪者の採る戦術はランサムウェア情勢のさらなる洗練と成熟を示すものです。**2021年は、以下のような事例の観測が増えました。**

被害者にすみやかに身代金を支払わせるため、組織のファイルを暗号化するだけでなく、被害者を名指しで晒しものにしたり、追加の攻撃(例: DDoSと呼ばれる分散型サービス拒否)を実行すると脅したりする多重脅迫の手口。2021年には被害を受けた2,566組織の名前や侵害の証拠がランサムウェアのリーク サイトに公開され、これは2020年から85%増加しています。

サービスとしてのランサムウェア(RaaS)ビジネス モデルが急速に普及しました。サイバー犯罪志願者に「スタートアップ キット」と「サポート サービス」を提供することで技術参入障壁を大幅に下げ、攻撃の着手・拡散スピードが加速しています。

脆弱性の迅速な兵器化。たとえば、主要なランサムウェア ギャングは、Log4Shellと一般に呼ばれるCVE-2021-44228をすぐさま悪用しました。組織が既知の重大な脆弱性にパッチを適用しない限り、攻撃者がその脆弱性を悪用する可能性は高くなります。

ランサムウェア攻撃を免れうる組織は存在しないようで、2021年にはほとんどすべての国と業界の組織が標的となりました。弊社のランサムウェア リーク サイト分析からは、南北アメリカ地域が最も被害を受けていることが判明しました。公開された被害者の所在地の60%がこの南北アメリカ地域で、31%がヨーロッパ、中東、アフリカ(EMEA)、9%がアジア太平洋地域でした。専門・法的サービスと建設がとくに標的とされたセクターで、それぞれ1,100社と600社の被害者がリーク サイトに記載されていました。

とくに標的となった地域

60%	31%	9%
南北アメリカ	ヨーロッパ、中東、アフリカ	アジア太平洋地域

とくに標的となったセクター

1,100	600
専門・法的サービス	建設

ランサムウェア攻撃の長期的影響は甚大になりがちです。身代金の実際のコストだけでなく、ダウンタイム、復旧、事業中断に関連し、多くの付随コストが生じることがあります。

弊社がランサムウェア グループの戦術・手法・手順(TTP)を明らかにすることで、ランサムウェア ギャングに対する防御側の形勢を逆転し、流れを変えていければと願っています。これを念頭に、本レポートはランサムウェア問題への対応に使える実用的知見を提供します。本レポートの最終目標は、組織がランサムウェア情勢を理解し、防御力を強化し、たとえ(いつか)ランサムウェア攻撃を喫しても最適な行動方針を決定できるようにすることです。

01
ランサムウェア入門

ランサムウェアは多種多様

仕掛ける攻撃のタイプ(使用するファイル、方法、戦術、身代金要求メモ)、追求する標的が異なるさまざまなランサムウェア グループが知られています。最近は、ContiやREvilなどのランサムウェア ギャングによる攻撃の報道がとくに目立ちます。これらのグループは、攻撃実行者であるアフィリエイト(サイバー犯罪者)を積極的に採用しています。ランサムウェア グループのなかには、アフィリエイトの採用効率や全体的な成功率をあげるため、リーク サイトや「サポート」サイト、ソーシャル メディア プロファイルなど、オンライン上での存在感を維持しているところもあります。

ランサムウェアは、金銭的利益のためにサイバー犯罪者によって使用されるマルウェアの一種です。被害システムへの侵入のしかたは、ほかの種類のマルウェアと同じです。たとえば攻撃者は、組織への攻撃実行に使える足がかりを得るため、既知の脆弱性を悪用し、すでに侵害されているシステムを利用し、フィッシング メールなどのソーシャル エンジニアリング手法を使用します(フィッシング メールとは、ユーザーを騙して、感染ファイルをダウンロードさせたり、悪意のあるリンクをクリックさせようとしたりする手法です)。

侵入に成功すると、ランサムウェアは、被害者のファイルやシステムを乗っ取り、重要な情報を暗号化して組織が使用できないようにします。
攻撃者は、復号キーと引き換えに身代金の支払いを要求します。この支払いにより、ファイルが元の状態に復元される、ということになっています。

一般に、ファイル/システムの暗号化と同時に、被害者のシステムに身代金要求メモがインストールされます。この身代金要求メモには、ランサムウェア ギャングの要求に関する情報が記載されます。つまり、要求する身代金の金額、支払期限(早期の支払いに対する割引の提案が含まれることもあります)、身代金を要求しているグループに連絡し、支払いを行う方法に関する指示が詳述され、被害者が取引を完了するために必要な暗号通貨ウォレットなどの連絡情報に関する詳細が提供されます。被害組織のセキュリティ態勢に対する批判や、有料で被害者の今後のセキュリティを支援する提案など、グループの身代金要求メモには、さらに多様な情報が含まれることがあります。

また、特定のファイルで復号キーをテストする方法を被害者に示し、攻撃が本物で危険であることについてのなんらかの証拠を提供するグループも存在します(ランサムウェア ギャングのリーク サイト上にあるデータのサンプルの公開など)。近年はランサムウェアの定義が拡大され、被害者のデータを人質にするだけでなく、追加の脅威と戦術を組み合わせる二重脅迫攻撃や多重脅迫攻撃が含まれるようになりました。

こうした戦術のせいで、被害組織は身代金を全額ただちに支払うよう迫られ、オフライン バックアップも対策としては不十分になります。これまでは組織がオフライン バックアップを取って(かつテストして)いれば、ランサムウェア攻撃からの復旧には十分でした。ところがこの多重脅迫により、オフライン バックアップでは、ランサムウェア グループのもたらしうる負の影響をすべて阻止することができなくなりました。

二重脅迫は、被害者を脅して身代金を支払わせるため、ランサムウェア攻撃中にデータを漏出させる行為を指します。この行為は「被害者は(一般にダーク ウェブでホストされる)リーク サイトに情報が公開されたり、違法なフォーラムで販売されたりすることを望まない、だからできる限り早くインシデントを解決しようとするだろう」という考えに基づいています。多重脅迫は、分散型サービス拒否(DDoS)攻撃を仕掛けて標的組織の公開Webサイトをダウンさせるなど、さらにプレッシャーを与える戦術を含むものです。

02
ランサムウェアの情勢

2021年のランサムウェア活動を分析し、過去数年間の活動と比較すると、ランサムウェア情勢を形づくる新たなトレンドに加え、攻撃者が繰り返し利用する手法や戦術が複数確認されました。以下は防御力向上戦略の策定時に考慮すべき(新旧の)所見を示します。

ランサムウェア アクターの行動様式

攻撃者は手っ取り早い方法を使う

多くのランサムウェア ギャングが初期アクセス ブローカーを標準で使うようになってきています。こうしたブローカーは侵害した企業ネットワークへのアクセスを売っていて、料金さえ支払えばだれにでも利用させてくれます。サイバー犯罪界隈では多くの攻撃者がこの種のアクセスを求めていますが、とくにランサムウェア オペレータは関心を持っています。これでアフィリエイトの労力と時間を大幅に節約できるからです。この協力関係は、ランサムウェア オペレータ、アクセス ブローカーの双方にとって非常に有益です。また、ひそかにネットワークに侵入する方法を見つけられないスキルの低い未熟な脅威アクターでも、すでに侵害された環境にランサムウェアを投下するだけで、簡単に攻撃を実行できるようになります。組織は警戒を怠らず、環境内に潜む攻撃者の検出にむけて最善を尽くさねばなりません。そのためにはラテラルムーブを探したり、攻撃の足がかりである可能性のある休眠状態の実行可能ファイルを探したりする必要があります。

攻撃者は使えるものはなんでも使う

攻撃者による匿名サービスの使用が増えています。匿名サービスを利用すると、セキュリティ リサーチャーや法執行機関によるアクティビティの追跡や、ネットワークの防御に使えるセキュリティ侵害の兆候(IoC)の特定がさらに困難になります。Tor(The Onion Router)をはじめとする匿名サービスはランサムウェア グループに非常に人気があります。攻撃への防御をできる限り困難にするために、今後も攻撃の重要要素になると見込まれます。

攻撃者はあれこれ工夫する

ランサムウェア脅威アクターは、独自ツールに投資しつづけることで、被害組織の侵害をつづけられるようにしています。そのためにランサムウェア亜種の新たな開発や更新を行い、それらをスタンドアロン マルウェアとして使ったり、商用マルウェアと一緒に使ったりします。LinuxのようなWindows以外のオペレーティングシステムを標的とする亜種を開発するランサムウェア グループ (HelloKittyなど)や、Rustのようにカスタマイズ性の高いプログラミング言語で攻撃コードを作りやすくしているランサムウェア グループ(BlackCatなど)も増えています。攻撃者たちが今後も新たな亜種を開発し、あらゆる種類のシステムを標的とするために機能を高めていくことは明らかで、その過程で攻撃を受けうる被害者の範囲は広がっていくことでしょう。対する組織側も同様に防御機能を高め、機能の改良・追加で攻撃対象領域を最小化していく必要があります。

知っておくべき2022年の3つのランサムウェア トレンド

1 被害者を晒し者にする「ネーム・アンド・シェイム」が増加

要求した身代金の支払いを被害組織に強要するために、多重脅迫手法を使用するランサムウェア ギャングが増えています。攻撃者は、すみやかな支払いを促すために、組織のファイルを暗号化するだけでなく、リーク サイトを利用し、さらなる攻撃(DDoSなど)を実行すると脅します。被害者から窃取/漏えいしたデータのサンプルをダークウェブやギャングのリーク サイトで公開するのは、攻撃者が実際に情報を持っていて、脅威が深刻であることを証明することで、被害者を名指しで晒しものにし、身代金を支払わせるためです。また、攻撃者は、手持ちデータの総量に関する詳細を公開することもあります。こうした戦術のせいで、オフライン バックアップでは、ランサムウェア攻撃のもたらしうる負の影響をすべて阻止することができなくなっています。

2020年初頭の時点では生まれてからまだ1年も経っていなかった多重脅迫手法は2021年に急増しました。2021年には、Black Matter、Hive、Griefなど、少なくとも35の新しいランサムウェア ギャングが出現し、データを公開すると脅したり、リーク サイトを利用したりしました。Suncryptと新たな攻撃者BlackCatは、三重脅迫攻撃を実行し始めました。この攻撃では、ランサムウェア展開前に被害者のデータを盗み出して情報を公開すると脅し、身代金が支払われなかった場合はDDoS攻撃を仕掛けます。2021年には、2,566の被害組織名と侵害の証拠がランサムウェア リーク サイトに公開されましたが、これは2020年から85%の増加でした。2022年以降には、多重脅迫攻撃戦術がさらに増加すると予想されます。

35
2021年の
新興ランサムウェア
ギャング数

2,566
2021年にリーク サイトに
公開された被害組織数

85%
2020年と比較した
被害組織数の増加率

2 サービスとしてのランサムウェアが急速に技術障壁を下げている

ランサムウェアは、サイバー犯罪者が利益・知名度の両面で成果を挙げるのに有効なメカニズムであることが実証されてきました。このため、参入したいサイバー犯罪者の増加に乗じて「企業家精神」を持つ脅威アクターが出現し、ランサムウェアの状況が発展しました。このような企業家は、RaaSの提供を始めています。これは犯罪者による犯罪者のためのビジネスで、しばしば月額料金または支払われた身代金の一定の割合と引き換えに、実際のランサムウェアを提供する条件を定める契約が締結されます。RaaSによって、攻撃実行がはるかに容易になり、参入障壁が低下し、ランサムウェアの感染規模が拡大しています。弊社は少なくとも56グループの活動中のRaaSグループを積極的に追跡していますが、その一部は2020年から活動しています。RaaSグループが成功を収めているため、このタイプの活動は増加し続けると予想されます。

3 攻撃者によるゼロデイの悪用が増加している

ランサムウェア攻撃では最初の攻撃経路としてさまざまな脆弱性が利用されることがよくあります。2021年には、ランサムウェア オペレータが複数のテクノロジにまたがる少なくとも42種類の脆弱性を悪用していることが確認されました。

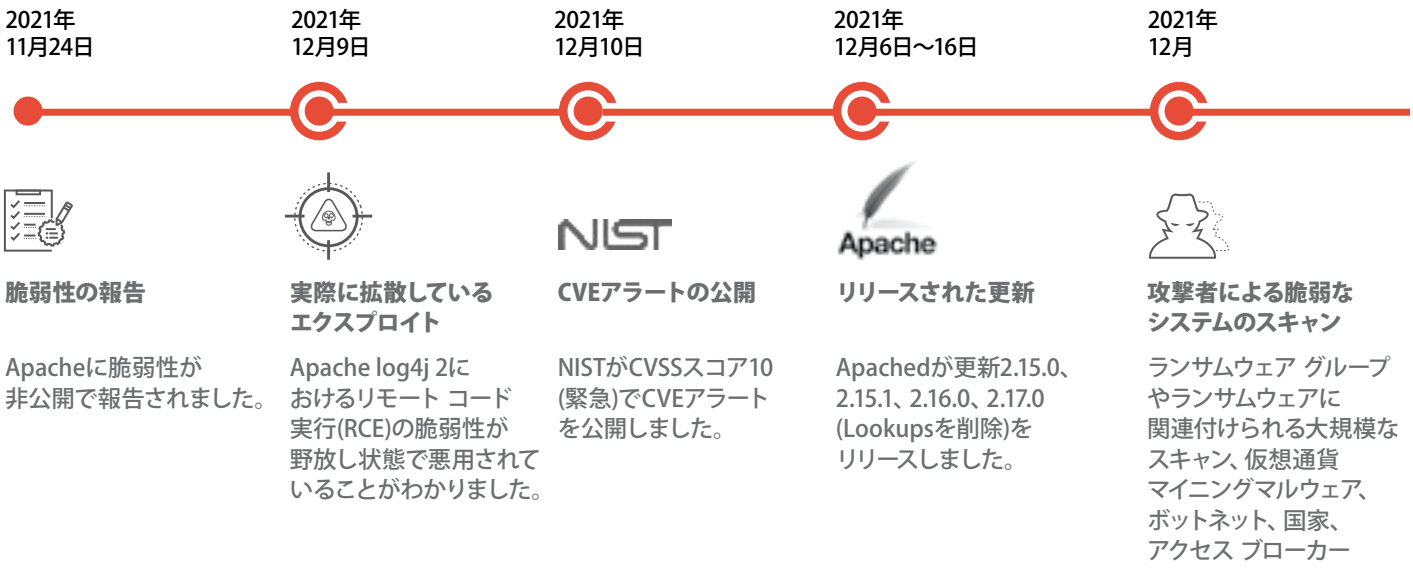
図1: 2021年にランサムウェア アフィリエイトによる悪用が確認された脆弱性

Pulse Secure VPN • CVE-2021-22893 • CVE-2020-8260 • CVE-2020-8234 • CVE-2019-11510 • CVE-2019-11510	**Citrix** • CVE-2020-8196 • CVE-2020-8195 • CVE-2019-11634 • CVE-2021-22941	**Microsoft Exchange** • CVE-2021-34523 • CVE-2021-34473 • CVE-2021-31207 • CVE-2021-26855
Fortinet • CVE-2020-12812 • CVE-2019-5591 • CVE-2018-13379	**Sonicwall** • CVE-2021-20016 • CVE-2020-5135 • CVE-2019-7481	**F5** • CVE-2021-22986 • CVE-202-5902
QNAP • CVE-2021-28799 • CVE-2020-36198	**Sophos** • CVE-2020-12271	**Sharepoint** • CVE-2019-0604
Log4J • CVE-2021-45046	**Microsoft Windows** • CVE-2019-0708 • CVE-2020-1472 • CVE-2021-31166 • CVE-2021-36942	**Microsoft Office** • CVE-2017-0199 • CVE-2017-11882 • CVE-2021-40444
vCenter • CVE-2021-2198	**Accellion (主にCl0pが利用)** • CVE-2021-2701 • CVE-2021-27104 • CVE-2021-27102 • CVE-2021-27103	**FileZen** • CVE-2021-20655
Atlassian • CVE-2021-26084	**Zoho Corp** • CVE-2021-40539	**Microsoft Azure** • CVE-2021-38647

図2: Microsoft Exchange Serverの脆弱性のタイムライン

比較的古い、未修正の脆弱性も多少は利用されていますが、目立った脆弱性をつねに把握し、それを組織への最初の足がかりを得るのに悪用するアクターは増えているようです。脆弱性発見から悪用までの期間はどんどん短くなっています。脆弱性そのものと、その悪用で得られるアクセスが重大であれば、脆弱性公開とほぼ同時に攻撃が発生することがあります。そのことは、Microsoft Exchange Serverの脆弱性(CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065)に対するHafniumのAPT攻撃からも確認できます。この攻撃では複数の脅威グループがさまざまな攻撃を仕掛けて脆弱なシステムを悪用していました。

図3: Log4jのタイムライン



もう1つは9月のはじめにContiがCVE-2021-34473、CVE-2021-34523、CVE-2021-31207(ProxyShell)をランサムウェア攻撃に利用し、12月にはLog4Shellと呼ばれる最近の脆弱性CVE-2021-44228を悪用しはじめて、被害者のシステムに侵入して内部デバイス間のラテラルムーブを行いました。

脆弱性が利用できる状態(パッチ未適用)であるかぎり、攻撃者は、それらを目的達成に悪用します。攻撃者はサードパーティ ソフトウェアの脆弱性悪用や、サプライ チェーン コンポーネントへの攻撃も行いますので、そこから多くの組織にとってのリスクが生じうることも念頭に置くべきです。そのことは、REvilによるKaseyaの攻撃でも確認されています。

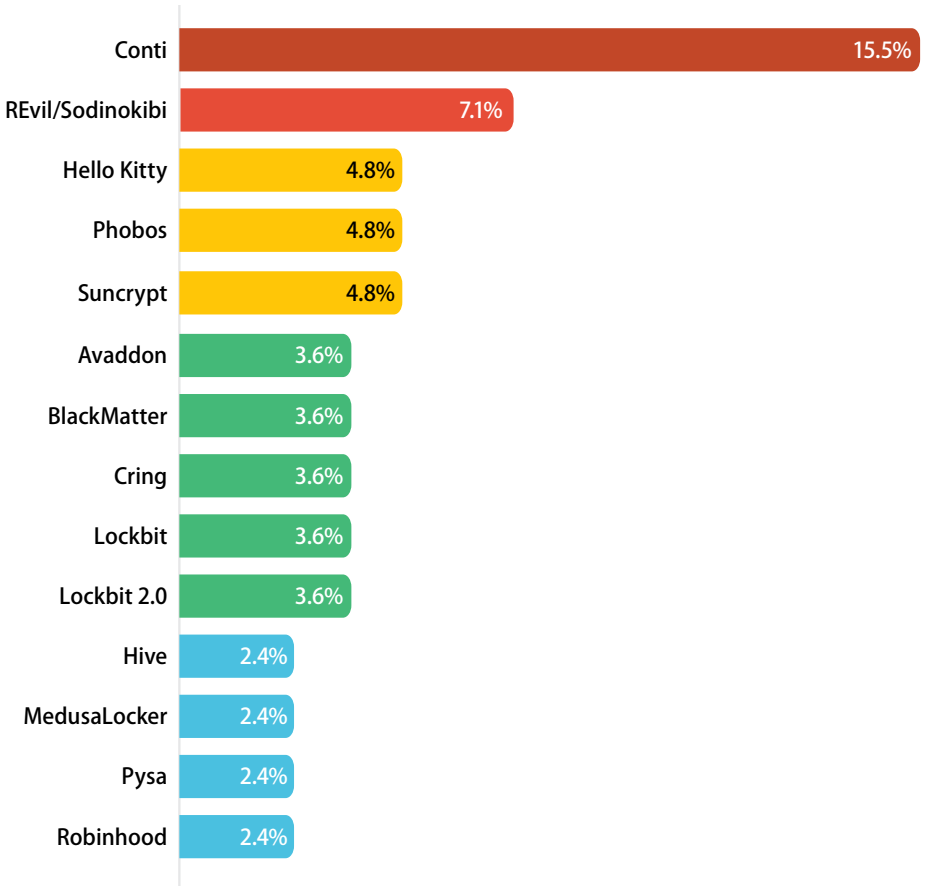
組織によっては、習慣的に脆弱性公開からパッチの適用までに時間をかけている場合があります。パッチに相応の注意を払うことはいまでも大切ですが、インターネットをスキャンして脆弱なシステムを探す攻撃者の能力は高まっているので、パッチ適用までの時間をいかに短縮するかがこれまで以上に重要になっています。こうした既知のセキュリティギャップをできるかぎりすみやかに解消するには、組織のパッチ管理やオーケストレーションの改善が必要です。

03

ランサムウェア グループの行動

2021年には、多くの新しいランサムウェア ギャングの出現と、長期間活動していなかった多数の既存グループの再出現が確認されました。ほとんどのランサムウェア グループが非常に活発化しており、身代金の支払いの可能性を高めるために多重脅迫の手法を採ることが増えています。

図4: 2021年に最も活発だったランサムウェア亜種 – Unit 42インシデント レスポンス データに基づく



とくに活発なランサムウェアグループ

Contiは、2021年 にUnit 42が対応したインシデント レスポンス事例のなかで圧倒的に最も活発なランサムウェア グループで、ランサムウェア活動の15.5%を占めていました。2位のREvil/Sodinokibiは7.1%、それに続くHello KittyとPhobosはそれぞれ4.8%を占めました。

15.5%
CONTI

7.1%
REVIL/SODINOKIBI

4.8%
PHOBOS

4.8%
HELLO KITTY

Conti

上述したように、Contiは、2021年にUnit 42が対応したインシデントのなかで最も活発なランサムウェア グループでした。このグループは、大規模な組織に被害を及ぼし、非常に高額な身代金を要求しました。3月にこのグループの最初の事例に対応したとき、初回の身代金額は50,000ドルでした。これは、このグループについて2021年に報告されたなかで最も低い要求額です。Contiは、要求額を急速かつ大幅に高め、この年の平均額は約178万ドル、初回の最高支払要求額は300万ドルでした。このグループによる2020年の(確認できている範囲では)初回の身代金要求額が187,114ドルだったことを考えると、このグループは、その攻撃数や自信を急速に高めているとみなせるでしょう。

Contiは、2020年の出現以降、冷酷無比のランサムウェア ギャングとして注目されています。このグループの活動にはなんの「行動規範」もありません。脅威アクターのなかには、被害者の生命にかかわる場合や、きわだって弱い立場の者を標的とするかどうかについて「行動規範」を遵守すると主張する場合がありますが、Contiにはそれがありません。Contiは、被害者を晒し者にして身代金を支払わせるために、二重脅迫手法を使用して病院、救急サービス、法執行機関に対する攻撃を実行します。弊社のインシデント レスポンス チームが対応した被害者以外を含むリーク サイトのデータからは、Contiが2020年以降に600を超える組織の情報を漏えいさせたことが判明しました。

600以上

2020年以降に被害を受けた組織数

病院 **救急サービス** **法執行機関**

また、Contiは、最初の攻撃経路として日和見的に既知の脆弱性を悪用します。2021年、このグループはCVE-2021-34473、CVE-2021-34523、CVE-2021-31207(ProxyShell)をランサムウェア攻撃に利用し、12月にはLog4Shellと呼ばれるCVE-2021-44228の脆弱性をうまく悪用して、内部デバイス間のラテラルムーブを行いました。

2022年2月には、社内チャット メッセージ、スクリーンショット、生データ ファイルなど、Conti関連の大量のデータが漏えいしました。その情報の多くが元はロシア語でした。以下に、漏えいした一部のデータを翻訳したスクリーンショットを示し、Contiが被害者とどのように対話しているかを示します。

Contiは、2020年の出現以降、極めて容赦のないランサムウェア ギャングとして注目されている

118,114ドル

2020年の初回の身代金要求額(確認された事例のみ)

5万ドル

2021年3月の初回の身代金要求額

178万ドル

2021年の身代金要求額の平均

300万ドル

2021年の最高要求額

```
{ "ts": "2021-11-06T11:27:44.059579",
"from": "tramp@q3mcco35auwcstmt.onion",
"to": "bio@q3mcco35auwcstmt.onion",
"body": "hi"
}
{
{ "ts": "2021-11-06T11:27:51.064723",
"from": "tramp@q3mcco35auwcstmt.onion",
"to": "bio@q3mcco35auwcstmt.onion",
"body": "are you there ?"
}
{
{ "ts": "2021-11-06T11:28:02.267373",
"from": "tramp@q3mcco35auwcstmt.onion",
"to": "skippy@q3mcco35auwcstmt.onion",
"body": "I did not mean to step on your toes seems I did not get my message over
to you. We do understand the consequences of the situation. That is why we want to
negotiate a solution with you! All I was trying to deliver is the message that we
are in a tough economic situation and simply cannot pay your demand. I have spoken
to my management. They understand the situation and are willing to pay. The money
we can afford is 500,000.00 USD. This is a huge amount for us. Please let us fix a
deal."
}
{
{ "ts": "2021-11-06T11:28:19.202666",
"from": "tramp@q3mcco35auwcstmt.onion",
"to": "skippy@q3mcco35auwcstmt.onion",
"Here are the guys you wrote the bigger letter to yesterday."
}
{
{ "ts": "2021-11-06T11:28:40.724324",
"from": "tramp@q3mcco35auwcstmt.onion",
"to": "skippy@q3mcco35auwcstmt.onion",
"body": "he Price to unlock is
$2,000,000."
}
{
{ "ts": "2021-11-06T11:29:02.278040",
"from": "tramp@q3mcco35auwcstmt.onion",
"to": "skippy@q3mcco35auwcstmt.onion",
"body": "we need to raise their price to 1.5kk at least"
}
```


図5: 2021年11月のContilによる通信(英語への翻訳)


```
{
{ "ts": "2022-02-23T12:50:43.214428",
"from": "pumba@q3mcco35auwcstmt.onion",
"to": "skippy@q3mcco35auwcstmt.onion",
"body": "We are very upset that you don't believe in the fulfillment of our
conditions. First of all, we appreciate and value our reputation (about us and
on the fulfillment of our agreements you can find a lot of information in the
Internet). This is the main thing. But you will understand this when we make the
deal. The second one, we will explain you a little bit deeper about amount: The
Conti has a big legal department and it checks all the possible data and sources to
establish an appropriate amount. We check your annual income, the value of
materials (you have a lot of SENSETIVE and PRIVATE files, Military bufget and so
on), etc.
Also, please don't forget about the decryption software and our expenses.
Therefore, basing on all the info, we set a 5% amount for a payment. FYI, every our
client is asked to pay this sum, you are not unique. But considering your situation
we can give you very big disount - 20%. Now our price for you is $8kk."
}
```


図6: 2022年2月のContilによる通信(英語への翻訳)

Revil (別名Sodinokibi)

REvil/Sodinokibiは、2021年に2番目に活発だったランサムウェア グループで、最も活発だった2020年から活動がやや低下しました。弊社の2021年インシデント レスポンス データによると、このグループの初回の平均身代金要求額は約220万ドルでした。これは、2020年に確認されたこのグループの488,928.52ドルの平均身代金要求額よりもはるかに高額でした。2020年、このグループの初回の最高身代金要求額は300万ドルで、2021年の最高要求額は540万ドルでした。

このランサムウェアの背後にいるオペレータ、PINCHY SPIDERは、2019年半ばにGandCrabオペレーションをREvil/Sodinokibiに切り替えました。その理由は、約7,000件の感染に対する関与が疑われたアフィリエイトの最近の逮捕であると思われます。しかし、この切り替えによって、このグループの存在感は一切低下しませんでした。実際、Kaseya VSAやその他の大々的に報道された攻撃によって、このグループは世界で最大級に悪名高いランサムウェア オペレータとなっています。

2020	48万9,000ドル 初回身代金要求額の平均	300万ドル 最高要求額
2021	220万ドル 初回身代金要求額の平均	540万ドル 最高要求額

また、REvil/Sodinokibiは、とくに注目されているRaaSプロバイダの1つで、交渉された身代金額の一定の割合を手数料として受け取っています。具体的な身代金額は、組織規模と窃取されたデータの種類しだいです。また、被害者がBitcoinで期限内に支払わなかった場合、要求額を倍増させることがよくあります。被害者が身代金を支払わないか交渉に応じない場合は、最終的に盗んだデータをリーク サイトに公開します。

BlackCat

BlackCat(別名ALPHV)は急速に成長しており注目に値します。同グループは2021年11月の出現からわずか1か月で、Unit 42の追跡するランサムウェア グループのなかで7番目に多い被害者をリーク サイトに公表しました。RaaSビジネス モデルを運営しているBlackCatは、既知のサイバー犯罪フォーラムでアフィリエイトを勧誘していることが確認されています。BlackCatは、アフィリエイトにランサムウェアの利用を許可し、アフィリエイトは支払われた身代金の80 ～ 90%を受け取って、残りの10 ～ 20%をBlackCatの作成者に支払うことを提案していました。このグループによるこれまでの被害者のほとんどは米国の組織ですが、BlackCatとそのアフィリエイトは、欧州、フィリピン、その他の地域の組織も攻撃しています。被害者には、建設およびエンジニアリング、小売、輸送、商業サービス、保険、機械、専門サービス、通信、自動車部品、製薬の各セクターの組織が含まれます。

80-90%

アフィリエイトへの
身代金の支払い

10-20%

BlackCatの作成者に対する
身代金の支払い

**BLACKCATの被害組織には
以下のセクターが含まれる**

+ 建設/エンジニアリング
+ 小売
+ 輸送
+ 保険
+ 商業サービス
+ 専門サービス
+ 機械
+ 通信
+ 自動車部品
+ 製薬

BlackCatは、(最初ではないとしても)初期にRustプログラミング言語でコーディングされたランサムウェアの1つです(他のマルウェアでRustが使用された例はあります)。Rustはネイティブ オプションを多数備え、高度なカスタマイズが可能です。このため、マルウェア作成者の攻撃方針変更やカスタマイズが容易です。同プログラミング言語では、さまざまなオペレーティング システム アーキテクチャ向けにランサムウェア攻撃を容易にコンパイルできます。これでBlackCatの急伸に説明がつきます。

AvosLocker

AvosLockerは、6月末に活動を開始したRaaSです。このグループは、被害者との連絡と新しいアフィリエイトの採用を目的とした「プレス リリース」で自己を識別するために青いカブトムシのロゴを使用しています。AvosLockerは、ダーク ウェブのディスカッション フォーラムやその他のフォーラムでRaaSプログラムを宣伝し、アフィリエイトを探していることが確認されています。多くの競合グループと同様に、AvosLockerは、暗号化ソフトウェアで攻撃を受けた後に被害者の復旧を支援するためのテクニカル サポートを提供しています。この暗号化ソフトウェアについて、このグループは「失敗がなく」、検出率が低く、大きいファイルを扱うことができると主張しています。このランサムウェアには脅迫サイトもあり、米国、英国、アラブ首長国連邦、ベルギー、スペイン、レバノンの6つの組織に被害を与えたと主張しています。

Hiveランサムウェア

Hiveランサムウェアは6月に活動を開始した二重脅迫型ランサムウェアです。それ以降、Hiveは、現在このグループの脅迫サイトに公開されている66の組織に被害を及ぼしました。これには、欧州の航空会社と米国を本拠とする3つの組織が含まれています。Hiveは、最初の侵害日の公開、カウントダウン、リーク サイトで実際に公開された日付など、脅迫ツールセットで利用できるすべてのツールを使用して、被害者にプレッシャーを与えます。さらに、リーク サイトへの訪問者に、公開されたリークをソーシャル メディアで共有するオプションも提供しています。

HelloKitty

HelloKittyは新しいランサムウェア グループではありません。主にWindowsシステムを標的としていた2020年まで遡ることができます。しかし、7月に、クラウドとオンプレミスのデータ センターで広く採用されているVMwareのESXiハイパーバイザを標的とするHelloKittyのLinux亜種が確認されました。また、活動の2つのクラスタも確認されました。確認されたサンプルでは、電子メールを使用して被害者と連絡を取ることを好む脅威アクターもいれば、ピアツーピアの匿名インスタント メッセージ サービスであるTorChatsを使用している脅威アクターもいました。確認された亜種は、イタリア、オーストラリア、ドイツ、オランダ、米国の5つの組織に被害を及ぼしました。

LockBit 2.0

LockBit 2.0(旧称ABCDランサムウェア)は、2021年7月に名称をLockBitに変更し、新しいアフィリエイトを募る巧妙なマーケティング活動を開始しました。3年前に活動を開始したこのRaaSオペレータは、2021年に複数の業界にわたって注目度の高い数件の攻撃に関与したとみられ、このマーケティング活動は成功したようです。この成功を受けて連邦捜査局(FBI)は2022年のはじめにLockBitに関する警告を発しました。**このグループは、ランサムウェア市場で最速の暗号化を提供すると主張しています**。今日までに、このグループのリーク サイトには406の被害者が公開されています。これには、米国、メキシコ、ベルギー、アルゼンチン、マレーシア、オーストラリア、ブラジル、スイス、ドイツ、イタリア、オーストリア、ルーマニア、英国の組織が含まれています。

Mespinoza

Mespinozaは、不動産、製造、教育セクターの組織を標的としていることが確認されています。調査と分析を通じて、Unit 42リサーチャーは、Mespinozaが大規模かつグローバルに展開しており、米国、カナダ、南米、欧州、南アフリカ、オーストラリアに被害者が生じていると判断しました。**Mespinozaは、最初の攻撃経路としてリモート デスクトップ プロトコルを使用し、リーク サイトで公開するためにファイルを盗み出しています**。

eCh0raix

eCh0raixは、約1年間にわたって活発に活動し、小規模オフィスやホーム オフィス(SOHO)で使用されるSynologyのNAS(Network-Attached Storage)とQNAP(Quality Network Appliance Provider)のNASデバイスを標的としています。今日までに、攻撃によってささやかな額の身代金が支払われました。**SOHOユーザーは、一般にIT専門家やセキュリティ専門家を採用せず、ランサムウェア攻撃に対する対策が比較的不十分なのでランサムウェア オペレータには魅力的です**。攻撃者が企業に対するサプライチェーン攻撃の足がかりとしてSOHO NASデバイスを利用できる場合、eCh0raixは、より大規模な企業に侵入する可能性もあります。

初回の身代金要求額と支払額の比較

多くのランサムウェア ファミリは多額の身代金を要求しますが、ほとんどの場合、弊社が対応したインシデント レスポンス事例における実際の支払いは、それより下がる傾向があります。BlackCatが初回の900万ドルの要求に非常に近い850万ドルの支払いを受けているように、なにごとにも外れ値はありますが、ほとんどの支払額は初回の要求額よりも大幅に下がります。

たとえば、ある事例でSuncryptは20万ドルの最終的な支払いを受け取りました。これは、1,200万ドルの初回要求額の1.67%です。弊社の計算では、被害者は1事例あたり初回身代金額の平均42.87%を支払っていました。図8に、ランサムウェア ギャングが300万ドル以上を要求し、被害者が身代金の支払いを選択したインシデントについて、実際の身代金の支払額と初回の身代金要求額の差を示します。1つの例外を除き、このグラフのすべての支払額は要求額の50%以下です。このことは、被害者が攻撃を受けた場合に、どの程度の交渉の余地があるかを示しています。

初回身代金要求額に対する実際の支払額の割合

42.87%

(弊社の計算による最終平均値)

図7: 2020年と2021年のランサムウェアの身代金と支払額の比較
(Unit 42のインシデント レスポンス データに基づく)

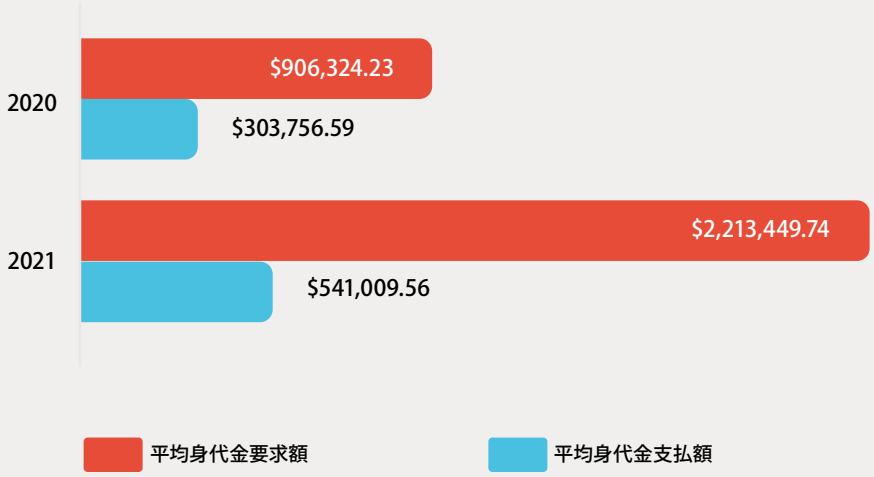
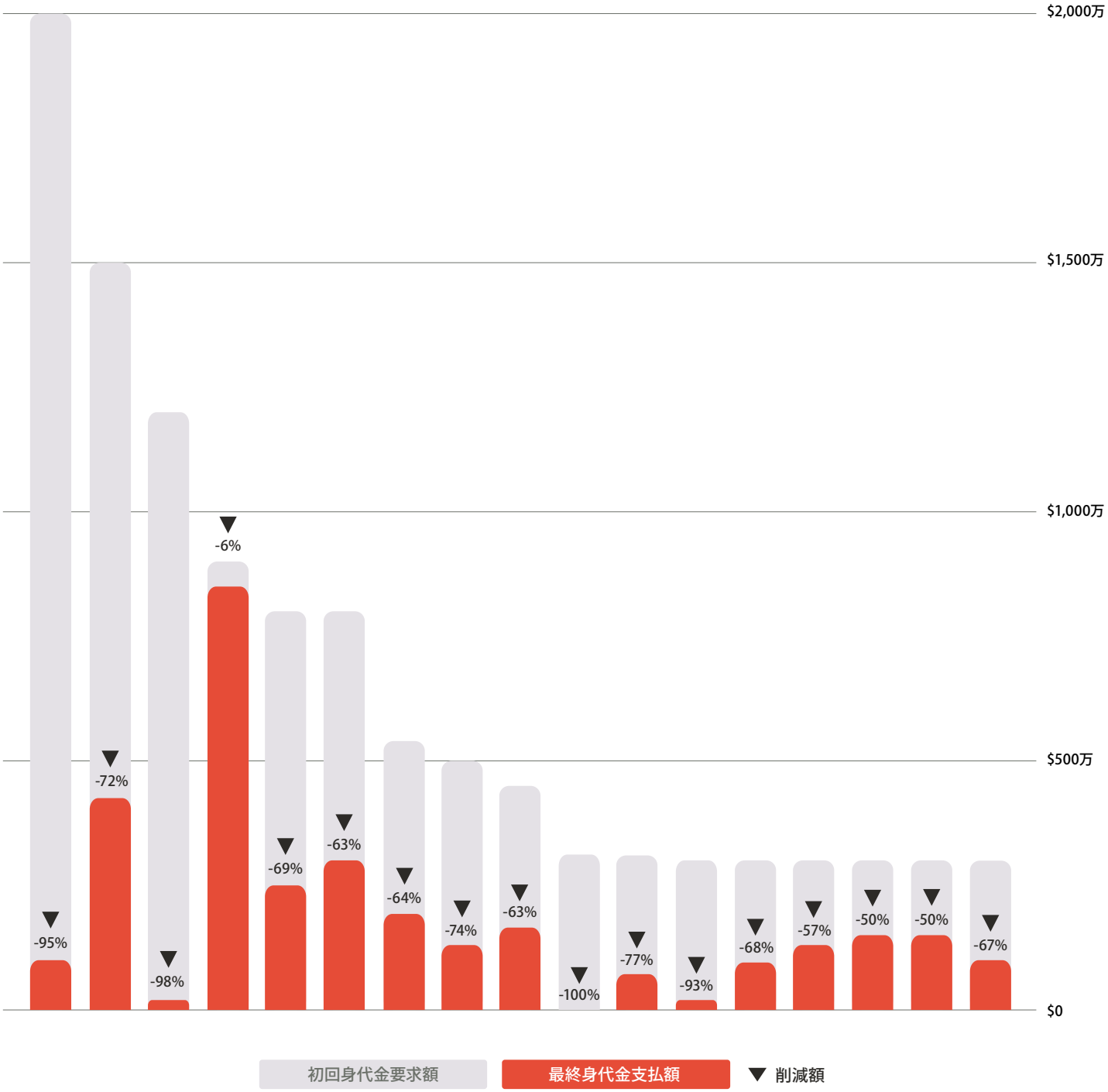


図8: 被害者が身代金の支払いを選択した事例で、
2021年の300万ドルを超える初回の身代金要求額に対する最終的な身代金支払額
(Unit 42のインシデント レスポンス データに基づく)



二重(多重)脅迫手法の増加

2019年にMazeが二重脅迫戦術の人気を高め、今後のランサムウェア オペレータへの道筋を示しました。多重脅迫手法では、身代金を要求後、すみやかに全額を支払わせることをねらい、身代金が支払われない場合は盗んだデータを公開すると被害者に伝えます。2021年には、同じ脅迫モデルを使う35の新興グループが確認されました。

三重脅迫手法を適用するランサムウェア グループも発生し始めています。2019年10月に初めて確認されたSuncryptは、BlackCatとならび、三重脅迫戦術を適用した初期のランサムウェアです。つまり、データ暗号化や窃盗に加えて、ギャングとそのアフィリエイトは、身代金要求交渉が決裂した場合、組織のインフラストラクチャまたはネットワークにDDoS攻撃を仕掛けると伝えることによって、被害者をさらに脅迫します。交渉がうまく進まない場合、攻撃者は、被害者が交渉の再開のために連絡してくることを期待して、被害者のデータを公開するだけでなく、被害者の事業を停止させるためにDDoS攻撃を開始します。

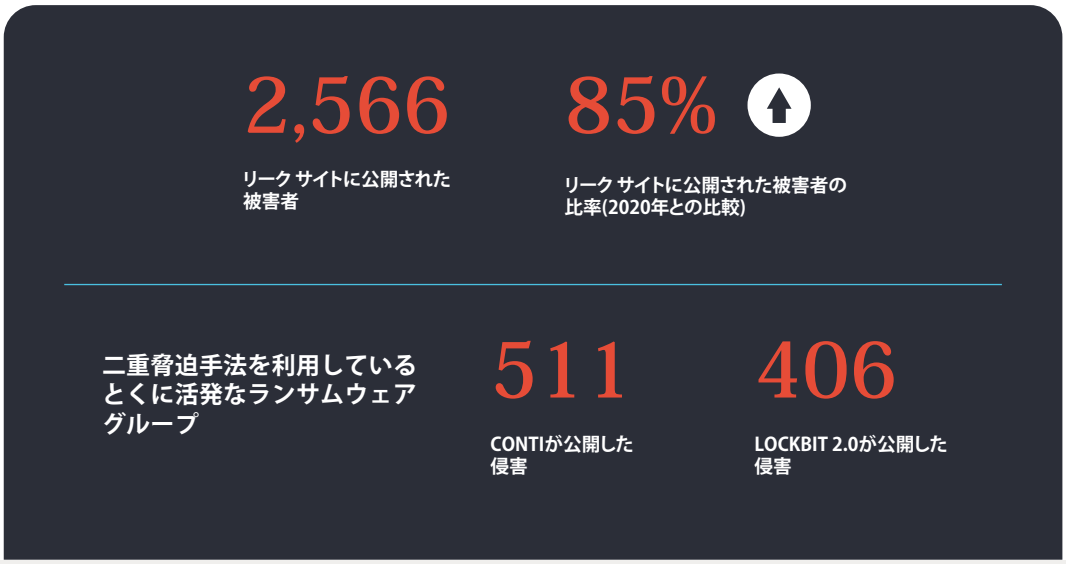
Suncryptは、三重脅迫がうまく行かない場合に、(最初ではないとしても)初期に多重脅迫を利用したランサムウェア グループの1つでもあります。多重脅迫には、従業員、ステークホルダー、メディアに侵害の事実を公開すると脅すなど、さらに戦術をエスカレートさせることが含まれます。Suncryptオペレータは、要求に抗う気力を奪うため、被害組織の従業員にボイスメールを送ることまでやっていました。

図9: 2020年と2021年に出現した、二重脅迫の手口を用いるランサムウェア ファミリの比較 (ランサムウェア グループのリーク サイトの分析に基づく)

04

ランサムウェア リーク サイトからの知見

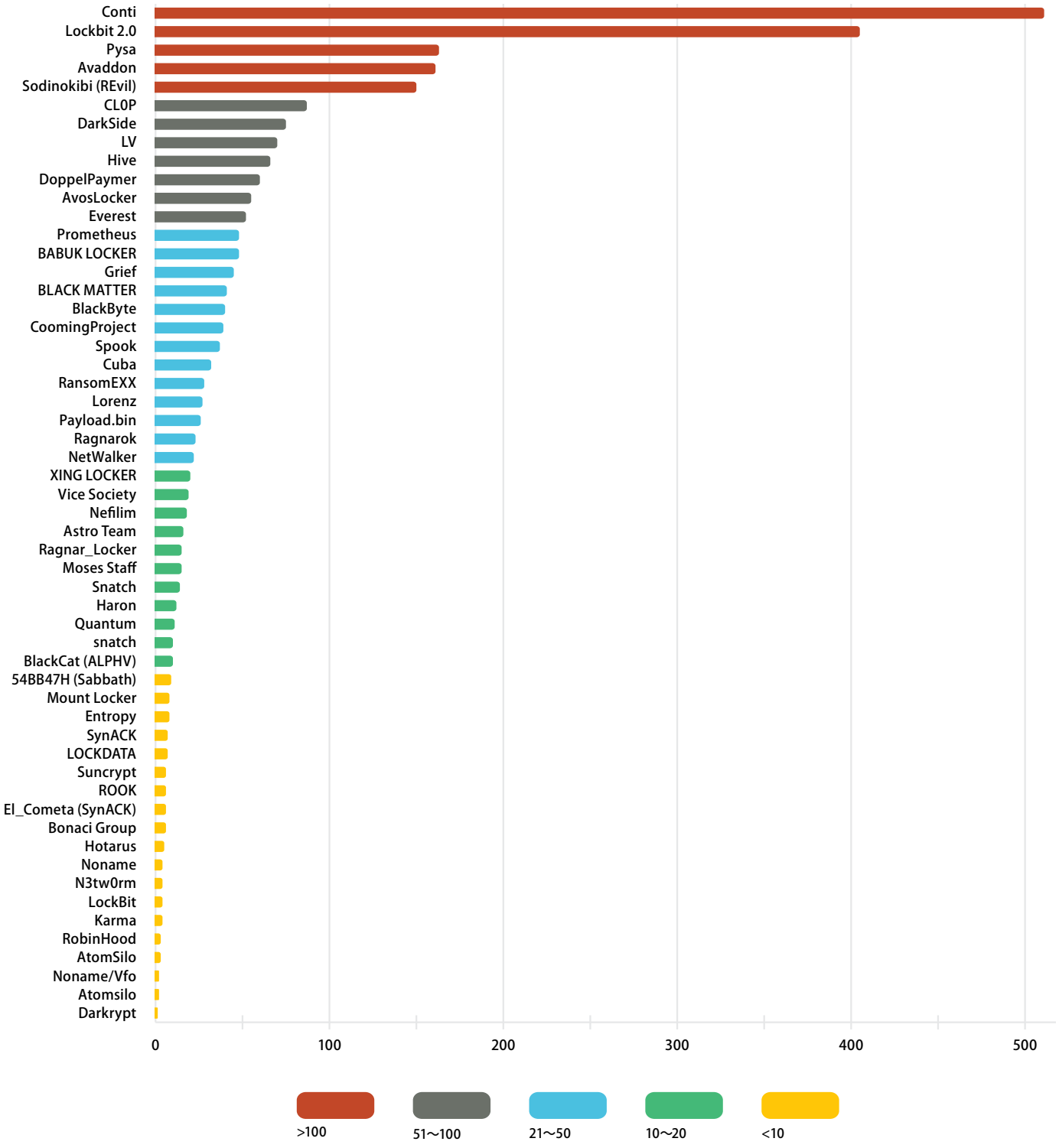
2021年は、被害を受けた2,566組織の名前や侵害の証拠がランサムウェアのリーク サイトに公開されましたが、これは2020年から85%の増加でした。以下に、リーク サイト上の情報の照合、分析、エンリッチ化によって収集した重要な知見をいくつか示します。



リーク サイトで最も活発なのはConti

リーク サイトの分析からは、ContiとLockBit 2.0が多重脅迫戦術を利用しているとくに活発なランサムウェア グループであることが判明しました。Contiは、2021年に最も多くの侵害(511件)を公開したランサムウェア ファミリです。LockBit 2.0が僅差でこれに続き(406件)、2021年7月に名称を変更して以来、積極的にデータを公開しています。

図10: 2021年のランサムウェア ファミリ別の被害者数



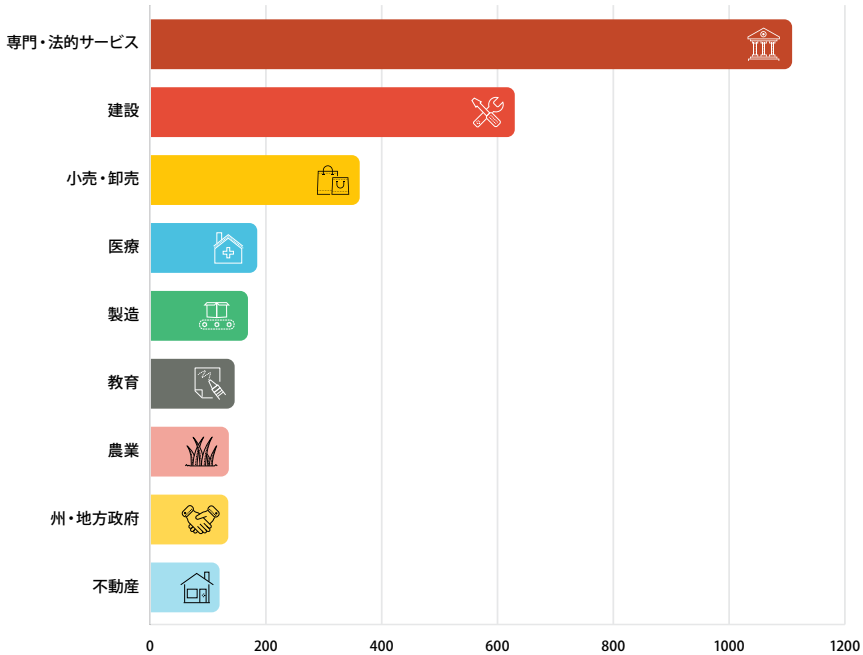
とくに標的となっているセクターと業界

ランサムウェア リーク サイトのデータによると、2021年に最もランサムウェア攻撃の標的となっていたのは専門・法的サービス業界で、1,100を超える被害者がさまざまなサイトに公開されました。このセクターに続いて標的となったのは建設業界で、その被害者数は600を超えます。

建設業界の組織は、パッチを簡単に適用できない、ないし定期的な更新/パッチ適用ができない古いソフトウェアを稼働するシステムで運営されていることが多く、サイバー攻撃を受けやすくなっている可能性があります。ランサムウェア オペレータはこうした古い脆弱性を起点に攻撃できます。また、IoTの急速な普及も、攻撃者がランサムウェア(WannaCryなど)を展開できる攻撃対象領域を急速に拡大させています。

これらの業界が標的となりやすいもう1つの理由は、事業の中断により被害者が製品やサービスを提供できなくなることを攻撃者が認識していることです。上記セクターの組織の多くは独自のテクノロジでサービスを提供しています。このためランサムウェア攻撃の被害を受けると生産停止やプロセススピードの低下でビジネスが影響を受け、多額のコストや損害が発生するおそれがあります。こうした組織は成果物の期日内生産というプレッシャー下にあり、できる限り早い復旧と事業再開のために全額をすみやかに支払いたくなるだろうとランサムウェア グループは期待しています。

図11: とくにランサムウェアの標的となっているセクターと業界(リーク サイトのデータ)



とくに標的となっている地域と国

リーク サイトのデータは、2021年にランサムウェア攻撃により最も大きな被害を受けたのは南北アメリカ地域で、EMEAとアジア太平洋地域がこれに続くことを示しています。

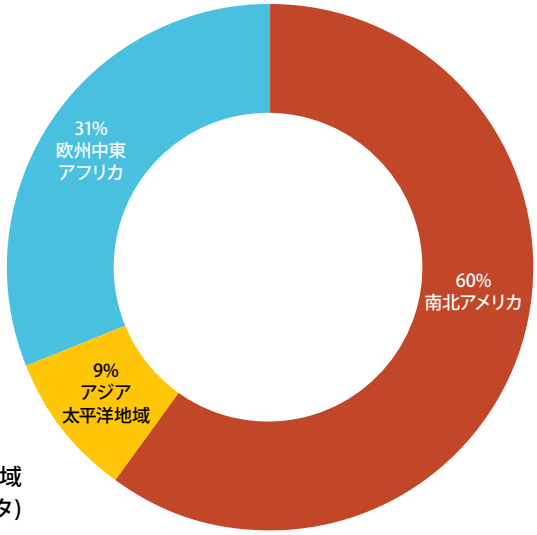
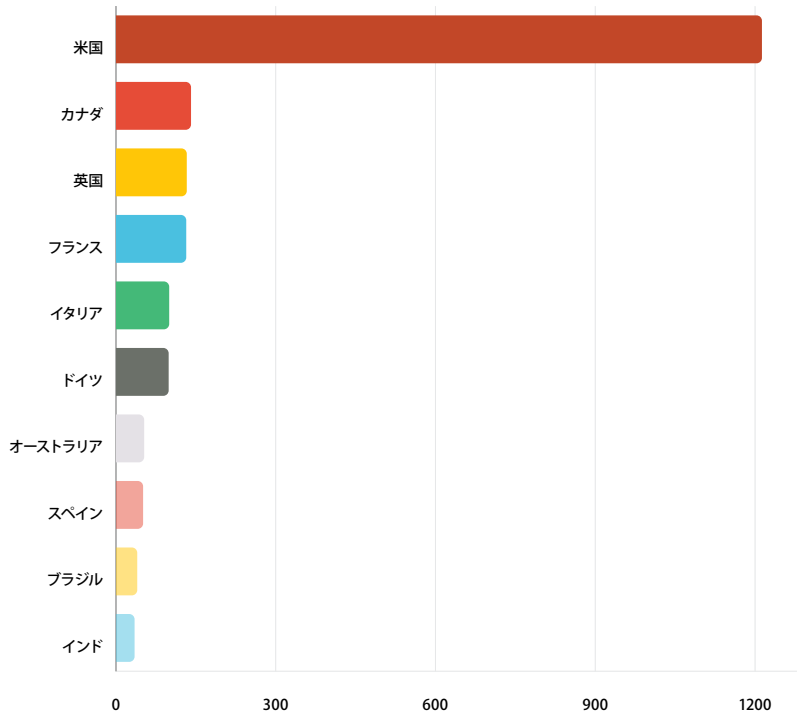


図12: 2021年にランサムウェアの被害を受けた地域
(リーク サイトのデータ)

図13: 最もランサムウェア被害の多かった国々
(各国内で被害を受けた組織数に基づく)



地域ではなく国ごとにトレンドを調査すると、データ侵害によって最も大きな被害を受けたのは米国で、米国組織はリーク サイトのデータの49%を占めています。これに続いて、カナダと米国がそれぞれ5%を占めています。多くのランサムウェア脅威アクターは、高い金銭的利益を求めて、収益の多い米国の組織に重点を置く傾向があります。とはいえランサムウェアはグローバルで問題となっていて、90か国を超えるさまざまな国で少なくとも1つは被害を受けた組織が存在することが確認されています。

49%
米国

5%
カナダ

5%
英国

ランサムウェア ギャングの活動の変動

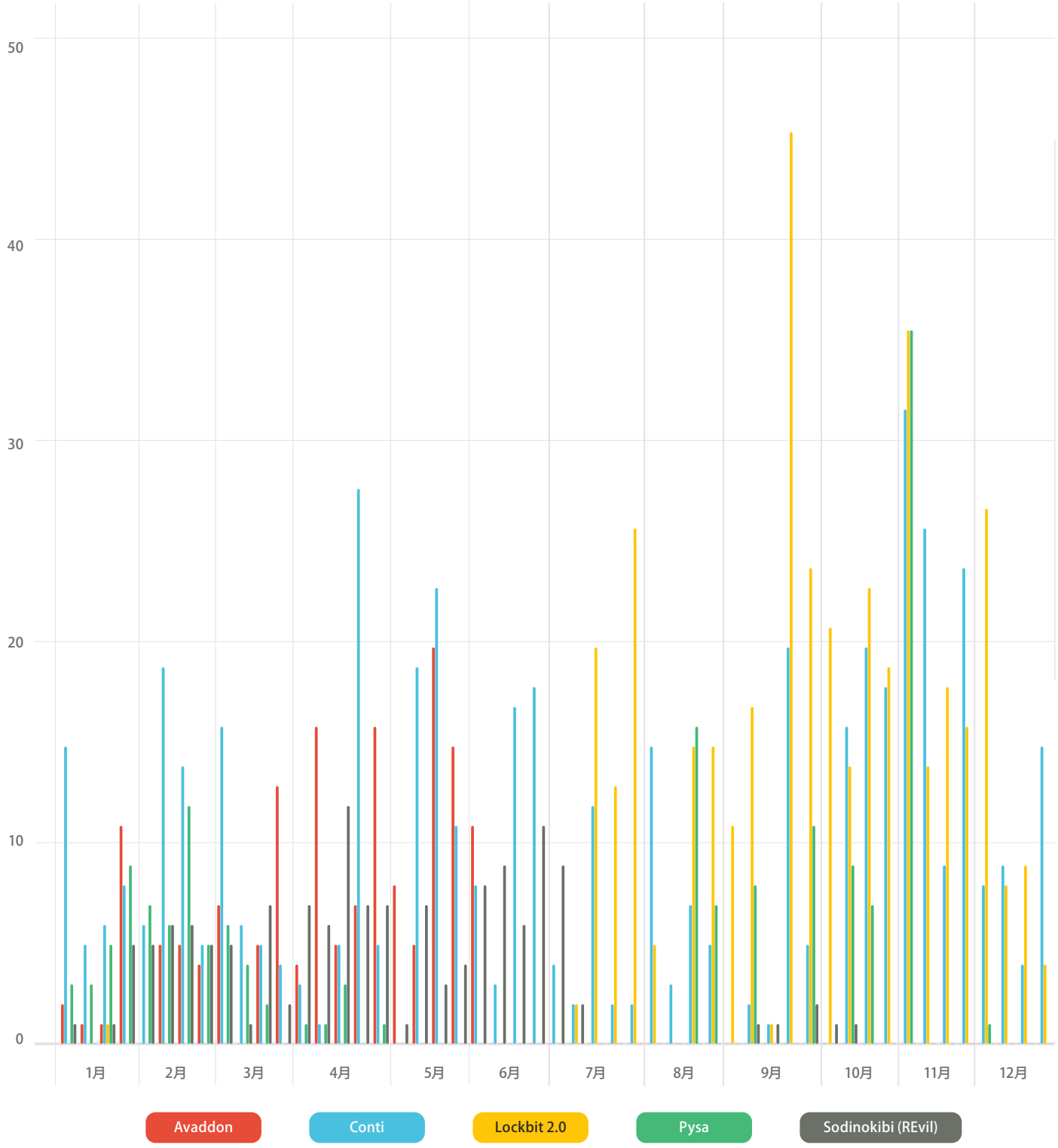
個々のランサムウェア グループの活動には波があります。つまり、ある月に活発で目立っていたグループが、翌月にはまったく姿を消したように見えることがあります。これらのランサムウェア グループは、さまざまな理由から活動を停止ないし休止します。この理由には、たとえば法執行機関からの圧力や捜査、(オペレータとアフィリエイト間の)内輪もめの調整、競合グループへの対応(たとえば、新しいRaaSが有利な料率でアフィリエイトに乗り換えを促した)などがあります。

また、グループは単にランサムウェアの名称を変更したり、再ローンチしたりすることもあります。オペレータは、ランサムウェアを使用したい人々 (アフィリエイト)を必要とするため、ランサムウェアを販売できなければ、改善や名称の変更を試みることがあります。1つの興味深い事例は、**EmsisoftのリサーチャーがDarkSideとBlackMatterに見つけた重大な欠陥**です。この欠陥のために、被害者は身代金を支払わずにファイルを復号・復旧可能でした。これらのランサムウェア グループは数百万ドルの身代金を受け取りそこねたので、これが活動休止の理由に関係していると思われます。これらのグループは、改善バージョンに取り組むために活動を休止したと推定されています(2021年11月に突然現れて波乱を起こしたBlackCatグループが彼らなのではないかと疑われていますが、Unit 42リサーチャーは現時点ではこれを確認していません)。

2021年にランサムウェア グループの活動の変動が確認された例

- **LockBit**は昨年、LockBit 2.0の公開で名称変更に成功しました。 2021年7月の出現以来同グループは数か月にわたり非常に安定したペースで被害者を増やし、2021年9月にピークに達しました。
- **Avaddon**は、6月のはじめにサイトへの投稿を減らし、6月半ばに活動をすべて停止しました。その際に、2,934の被害者すべてに復号キーを提供しました。(この活動が、ランサムウェア攻撃の調査の困難さを示していることは注目に値します。このグループのサイトには、約180の被害者しか公開されていませんでした)。
- **REvil/Sodinokibi**の活動は年間を通じて目立っていましたが、Kaseyaに対する攻撃が原因で、2021年7月以降に被害者の投稿を停止しました。このグループは、図14が示すように9月に再び現れましたが、恐らくこのグループに対する法執行活動の結果として、この年の残りの期間にわたって再び活動を休止しました。
- **Pysa**は、2021年の夏の活動停止後、年末に再び現れ、活発に活動しました。
- **Conti**、**LockBit 2.0**、**Pysa**は、11月に非常に活発で、それぞれのリーク サイトで30を超える投稿を行いました。

図14: 2021年のランサムウェア ファミリについてリーク サイト活動の変動を示す図



05

クラウド環境内のランサムウェア

弊社はクラウド セキュリティのベストプラクティスに従っているパブリック クラウドの方が、オンプレミス環境よりも、ランサムウェアに対するレジリエンス(回復力)が高い場合が多いと考えています。責任共有モデルは、インフラストラクチャやプラットフォーム、ソフトウェアを個々の組織で保護するさいの負担を大幅に軽減してくれます。API駆動型クラウド サービスは、モニタリング、自動化、一元的なアクセス制御を簡素化し、クラウド ネイティブのバックアップ サービスは、クラウド リソース復旧の信頼性の高い手段となります。ただし、クラウド ワークロードのセキュアな設定、運用、モニタリングは各組織の責任です。

ITインフラストラクチャはビジネスの成長とともに大きくなることから、マルチクラウド環境とハイブリッド クラウド環境内の数千の動的ワークロードの保護は困難になることがあります。しかし、DevOpsのセキュリティ自動化を実践すれば、ITチームとセキュリティ チームは、非常に動的な環境でセキュリティを維持できます。

クラウドに存在する重要データの量を考えれば、ランサムウェア グループがクラウド環境を標的とするのは時間の問題です。クラウド環境でランサムウェア攻撃を仕掛けるにあたって脅威アクターは新しいTTPを利用する可能性が高いので、対する組織側も防御アプローチの調整を準備しておく必要があります。

イメージのダウンロード段階からのクラウド ワークロードのハードニング

Log4J脆弱性は、優れた脆弱性管理プログラムと、更新が不可能な場合は代替コントロールが必要であることを明確に示しています。クラウド ワークロード上のほとんどの攻撃は、既知の脆弱性を対象としています。このため、必ず脆弱性にパッチを適用し、特権コンテナなどの設定ミスを実行前および実行中に修正することが不可欠です。ゼロデイ攻撃や、パッチを適用できないワークロードに対しては、仮想パッチの適用、異常なプロセス、ネットワーク、ファイル アクセスなどの代替コントロールを導入する必要があります。緊密に管理されるIAMポリシーを通じたクラウド リソースのセグメンテーションも、ワークロードが侵害された場合に、単一または少なくとも少数のワークロード内に感染を確実に封じ込めるのに役立ちます。

IAMのベストプラクティスを通じたクラウドAPIの保護

クラウドにランサムウェアを展開する場合、単純にクラウド内でたくさんホストを見つけて感染させてファイルを暗号化する、というわけにはいきません。クラウドの場合、脅威アクターはクラウドAPIを使ってデータにアクセス・暗号化します。このため組織はクラウドAPIへのアクセスを保護する必要があります。

これがクラウド セキュリティのベストプラクティス遵守が重要である理由の1つです。すべてのAPI通信は、ユーザーが操作しようとしているクラウド リソースに対し、IDおよびアクセス管理(IAM)用のアクセス キーと十分な権限を求めます。クラウドAPIの悪用をもくろむ脅威アクターは、アクセス キーを盗んで権限をテストする必要があります。このため、組織はIAM権限を綿密にモニタリングすることで、このタイプの攻撃を防御できます。組織ははじめにIAMアクセスに設定ミス、権限の範囲が広すぎないか、その他に弱い部分がないかをチェックする必要があります。次に、公開されているIAMアクセス キーを特定し、クラウド リソースに対するIAMアクセス キーの継続的モニタリング手順に着手する必要があります。

脅威アクターはクラウドの障壁に阻まれている組織の準備はいま時間に余裕のあるうちに

さまざまな障壁があることから、当面はクラウド経由で組織の攻撃をねらう脅威アクターは阻めると予想されます。クラウド サービスごとにサポートされるAPIは異なり、各クラウド サービス プロバイダは多様なデータ ストレージ サービスを提供しています。しかし、組織がクラウド内でランサムウェアの攻撃を受けることはない、と思い込んではなりません。脅威アクターがクラウド経由のランサムウェア展開に重点を置く前に保護対策を講じるため、とくにIDおよびアクセス管理に関して、今すぐベストプラクティスに着手する必要があります。

このベストプラクティスには、適切なコンプライアンス フレームワークの着実な導入、クラウド環境における有効な資産管理実施に役立つクラウド セキュリティ態勢管理(CSPM)の利用などが含まれます。クラウド インフラストラクチャ権限管理ツール(CIEM)は、IAMセキュリティ モニタリングに役立ちます。クラウド コード セキュリティ (CCS)やクラウド ワークロード保護(CWP)などの他のツールは、クラウドの規模に合わせてセキュリティ チームを拡大できるよう、自動的に設定できます。

06
ランサムウェアのコスト

ランサムウェア ギャングが大胆になるにつれて、標的となる組織の被害が増大しています。一般には身代金を支払わないことが推奨されますが、業務停止の長期的な影響により、組織がそれ以外の選択肢を検討して業務復旧をはからざるを得ない場合があります。

ランサムウェア攻撃の長期的影響は、組織の大きな課題となることがあります。カナダの調査において、ランサムウェア攻撃を受けた企業のうち、IT部門の意思決定者のほとんど(58%)は、組織が身代金を支払ったと回答し、14%は複数回身代金を支払ったと回答しました。

身代金に加えて(組織による支払いのいかんは問わない)、攻撃によって生じる損害には、以下のような他の付随的コストを含める必要があります。

- ビジネスのダウンタイムまたは中断に関連するコスト
- 企業ブランドの評判に対する侵害の影響
- ITスタッフがインシデントへの対応と復旧に費やした時間
- 規制およびコンプライアンス上の考慮事項に対応するために負担した法的費用
- 最も注目すべき、データの損失とそこから生じるさまざまな影響

カナダの調査により、ランサムウェア攻撃を受けた企業の41%は1か月未満で復旧できましたが、58%は復旧までに1か月を超えたことが判明しました。一部の企業は、さらに長い期間にわたって復旧に取り組んでいました。ランサムウェア攻撃を受けた調査対象企業の29%は復旧に3か月以上かかり、9%は通常の業務に戻るまでに5 ～ 6か月以上かかったと回答しました。

攻撃成功による影響を最小限に抑える、ないし完全に防御するには準備が重要です。これには復旧期間短縮のためにバックアップ システムと予防的防御の両方を導入することが含まれます。

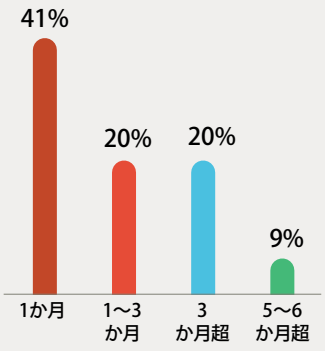
58%

身代金を支払った組織の割合

14%

複数回身代金を支払った組織の割合

ランサムウェア攻撃からの復旧に要した期間



07

結論と推奨事項

ランサムウェアアクターの活動は世界中で増加し続けているため、その攻撃を阻止するには準備が重要です。新興ランサムウェア ファミリは二重脅迫とリーク サイトを新たな標準としており、その分賭け金も吊り上がっています。ここで失う危険に晒されているのはデータへのアクセスだけではありません。被害組織の評判や組織に対するお客様の信用も失われかねないのです。優れたサイバー衛生の維持やセキュリティ意識の啓発教育導入から始めるのが基本ですが、同時にUnit 42からはランサムウェアに対する回復力を高める以下の推奨事項を提案します。

1 進化する脅威情勢の最新情報を入手する

ランサムウェアの脅威情勢が今後も進化し続けることはまちがいありません。脅威アクターは手を変え品を変え事業妨害を図ってくるからです。ランサムウェア脅威の最新状況、ビジネスへの潜在的影響、組織が攻撃阻止のために取れる措置について、セキュリティ チームと主要な役員レベルの関係者につねに最新情報を提供しましょう。つまり、ビジネスのことばを使い、脅威情報を活用して戦略的にリスク プロファイルやセキュリティ戦略を伝えることにより、鍵となる経営幹部関係者と取締役会に情報を提供する、ということです。攻撃経路、戦術・技術・手順(TTP)、身代金要求、攻撃を防ぐ最善の防衛対策など、最新のランサムウェアの脅威に関し、技術セキュリティ チームへの教育も必要です。

2 重要データの損失によるビジネス インパクトを分析する

重要データへのアクセス喪失による影響を理解するには、はじめに組織の全資産を把握し、重要データの格納場所、アクセス方法、組織全体での利用形態を理解しておく必要があります。秘密情報へのアクセスが「最小限の関係者のみが知るべき」という原則に基づいて確実に行われるように、データ マッピングの演習を行っておくことをお勧めします。次に、データへのアクセス喪失に関連するリスクを十分に理解するため、上流・下流の両観点からビジネス インパクト分析を行います。たとえば小売組織の場合、POSシステムがダウンして手動処理ができない場合、本社、店舗、サプライ チェーンでどの程度のダウンタイムが生じるかを分析します。

3 内部および外部の準備状況を評価する

セキュリティ態勢をつねに評価していなければ、要求額の高いランサムウェア攻撃の成功によるリスクは増大します。自社特有の人員、プロセス、テクノロジ、ガバナンス機能の状況を考慮し、自組織が直面している最も重大なランサムウェア リスクを評価しましょう。さらに業務全体を見渡して、リスクをもたらす可能性があるサードパーティ要素、パートナー要素、サプライ チェーン要素を特定する必要もあります。こうして得た知識があれば、優先順位を付けた軽減ロードマップを作成し、そのなかに戦略的ビジネス目標に合わせた組織のセキュリティ目標達成要件の詳細を盛り込むことができます。

4 インシデント レスポンス計画をレビューして検証する

最新のランサムウェア脅威情報に基づいて、インシデント レスポンス計画が実際に使えるものになっているか定期的な演習・更新を行い、机上演習とパープル チームによるテスト シミュレーションを実施します。模擬インシデント レスポンス ウォークスルーを実施してランサムウェア攻撃への対応能力を事前測定すると、ランサムウェア グループによく見られる戦術、手法、手順に対抗する能力を評価できます。上記のタイプの演習は、ギャップ領域と改善領域を特定し、対応準備能力を高め、ランサムウェアに対抗するサイバー防御能力全般の強化に役立ちます。

こうした対策の一環として、リーダーは正式なデシジョン ツリーを策定し、それを主要利害関係者間に浸透させ、メンバーの議論と積極的関与を促しましょう。関係者の人事異動があればデシジョン ツリーを見直し、必要に応じて更新します。インシデント発生前に踏み込んだ会話をしておくことで、貴重な時間の節約、そして最重要課題である重要業務の維持と常態復帰への専念が可能になります。

- どのような状況であれば身代金を支払うか
- マスコミがうわさであふれ、株価が低迷している場合、どのようにして顧客の信頼を維持するか
- 自社のCISOが行動できないときにインシデントが発見されたらどうするか
- アクティブなインシデントが山火事のように広がるのを阻止するために誰を呼ぶか

5 ゼロ トラストの実装

ゼロ　トラストは、組織を保護し、暗黙の信頼を排除し、デジタル インタラクションのすべての段階を継続的に検証するサイバーセキュリティへの戦略的アプローチです。ゼロ トラスト モデルは、デジタル トランスフォーメーションに対応し、変化し続けるセキュリティ情勢への適応を求められる経営陣の関心を集めています。統合に難のある個別ポイント製品をだましだまし使っている組織はいまだに多く、こうした製品では経営幹部の求める戦略的アプローチには応えられません。適切に導入されれば、ゼロ トラストはユーザーからデバイス、接続元、アクセス方法までのセキュリティを1つのユースケースにまとめてリスク管理を簡素化・統一してくれます。

6 公開されている資産を特定する

インターネットに一般公開されている自組織の全資産、システム、サービスを追跡する記録システムを実装しましょう。この追跡対象にはすべての主要クラウド サービス プロバイダ、(商用・家庭用の)インターネット サービス プロバイダ(ISP)が動的にリースする空間も含めます。そのさいは、包括的な指標を使い、一般的なポートやプロトコルを(ありがちな設定ミスに気をつけて)広くカバーしておきます(たとえばHTTPとHTTPSのWebサイトだけを追跡する従来の視点に捉われないようにします)。たとえばランサムウェア アクターの最初の攻撃経路として最も人気があるのはリモート デスクトップ プロトコル(RDP)で、ほとんどのランサムウェア感染でRDPが利用されています。これは現在在宅勤務が一般化していて、RDPの検出は容易だからです。また、M&Aやサプライチェーン、IoTによる変更管理のバイパスは、もう1つの人気のある攻撃経路となっています。たとえば、新型コロナウイルス感染症の拡大を背景にM&Aの動きは史上最多を記録しており、ほぼ一夜でネットワークの状況を変えてしまいます。セキュリティ チームも健闘はしているのですが、インフラストラクチャが急速に変化することから、静的IPアドレスの保護だけでは不十分となっています。

攻撃対象領域管理(ASM)プラットフォームを使えばインターネットからグローバルに接続可能な組織の資産と設定ミスを網羅した正確なインベントリを得られます。こうしたプラットフォームを利用して外部からの攻撃対象領域に存在するセキュリティ問題を継続的に検出・評価・軽減し、危険性の高い通信の阻止、サプライヤーのリスク評価、RDPインスタンスの検出、買収先企業のセキュリティ評価に役立てます。

7 既知・未知の脅威を阻止する

既知の脅威を阻止するには、既知のエクスプロイト、マルウェア、コマンド&コントロールのトラフィックのネットワーク侵入をブロックする必要があります。既知の脅威がブロックされれば、攻撃者は、マルウェアの亜種を新たに開発し、あまり知られていない脆弱性を悪用した新たなエクスプロイトを仕掛けるしかなくなります。つまり攻撃を実行するにも手間がかかるようになり、攻撃が発生する確率が低下します。

また、既知の悪意のあるフィッシングURLに対するアクセスを妨げることによって、ユーザーが悪意のあるペイロードを不注意でダウンロードしたり、認証情報を盗まれたりしないようにする必要もあります。このような脅威をブロックすることにより、環境からすべての既知の脅威が排除されます。既知の脅威をブロックしたら、攻撃に利用されるケースが増えているSaaSベースのアプリケーションで、既知のマルウェアをスキャンする必要があります。スキャンにより発見されたマルウェアやエクスプロイトは必ずブロックしなければなりません。エンドポイントについても同様に、既知のマルウェアやエクスプロイトを処理します。

既知の脅威をブロックした後は未知の脅威を識別・ブロックしなければなりません。攻撃者はたえず新たにゼロデイ攻撃を展開し、ランサムウェア亜種を開発しているからです。ネットワーク上のすべてのトラフィックを特定し、潜在的にハイリスクな未知のトラフィック(インターネットからダウンロードされたマクロなど)をネットワーク境界でブロックし、Web上のトラフィックとWeb以外のトラフィックに確実に対応します。次に、ファイルやURL内の未知の脅威を検出します。新しいファイルを検査用に提出したら、悪意のある動作の有無を分析・検知し、判定結果に基づいた処理をそこで行える必要があります。

また、攻撃を食い止めるにはセキュリティ インフラストラクチャのさまざまな部分に最短時間で自動的に保護を適用する必要があります。こうした保護には、攻撃者、マルウェア、攻撃コンテキスト、攻撃関連IoCへの理解が必要です。未知の脅威や不審な振る舞いの傾向を特定・ブロックしたら、エンドポイントで未知のマルウェアとエクスプロイトをブロックし、すべてのアクセス ポイントを確実に保護します。

このプロセスの最終的な目標は、攻撃のライフサイクル全体にわたって、未知を既知に変え、攻撃者によるマルウェアとエクスプロイトの開発よりも速いペースで新しい保護によりセキュリティ態勢を改善することです。

8 可能な限り自動化する

イベントの自動修復をサポートしてくれるツールの実装を検討しましょう。またそのツールでは、事前に用意されたプレイブックを使ってインシデント対応や復旧処理を行うようにします。そうすればインシデント レスポンス(IR)チームやSecOpsチーム、脅威インテリジェンス チームは、複数のツールからバラバラに上がってくる情報をつなぎ合わせるのにかける時間と手間を減らせます。SOAR(セキュリティ オーケストレーション、自動化およびレスポンス)製品を導入すると、セキュリティ情報とイベント管理(SIEM)、ファイアウォール、エンドポイント セキュリティ、脅威インテリジェンス ソースを対象としたオーケストレーションによって、ユーザー調査からエンドポイント隔離、通知、エンリッチ化、脅威ハンティングに至るプロセス全体を自動化できます。結果、レスポンス チームはランサムウェア攻撃をすみやかに終息させ、データ損失リスクを最小化し、身代金による財政的被害を抑えられます。

9 クラウド ワークロードの保護

クラウド ワークロードのランサムウェア保護対策は、セキュリティ態勢の構築からはじめます。必ずすべてのクラウド インフラストラクチャ、Kubernetes、コンテナ イメージをセキュアに設定し、脆弱性を最小限にする措置を講じます。暗号化やMFA削除、バージョン管理、バックアップなどの標準ポリシーがクラウド プロバイダのサービスに組み込まれており、かつそれらがデフォルトでオフになっている場合は、オンに切り替えて、設定が適切か確認します。オープン ソース パッケージやライブラリをチェックし、パッチを適用可能な脆弱性がないか探します。制限が緩すぎるか、未使用のIAM権限を特定して削除します。開発ライフサイクル全体でこのチェックを行い、コードを確実にセキュアにしてからクラウド アプリケーションやインフラストラクチャを構築するのが最適です。実働環境への移行後は、侵害を示す既知の不正な活動や異常な活動をチェックします。プロセス、ファイル、ネットワークのレベルで不正な動作を追跡し、ブロックします。意図的な依存関係を除いてサービスを隔離し、運用上必要とされない水平方向(East-West)のアクセスと外部からのアクセスをブロックします。これらすべてのレベルで脅威の動きをブロックすれば、セキュリティを最大化する多層型アプローチが実現されます。

10 リテーナーで応答時間を短縮する

潜在的な侵害を特定したらすみやかに措置を講じることが重要です。IRリテーナー契約をしておけば、IR専門家が自組織のチームを補強してくれ、サポートが必要になったらいつでもすぐに連絡できます。問題が生じてからリソースを必死に探す必要はなくなり、適切な専門家が数時間以内に連絡してくれます。IRコンサルタントは顧客環境を把握しているので、インシデント発生時にはより迅速・正確に対応できます。「急いで問題を解決したいのに情報を把握していないサードパーティ調査員の基本的な質問から答えなければならない」というフラストレーションからも解放されます。インシデント レスポンス予算を事前に想定して計上しておくと、攻撃の影響を最小化する措置をすみやかに講じられます。

ランサムウェア攻撃に対して準備を整えるには: 専門家にご相談ください。

いずれかのランサムウェア ファミリによる被害を受けた可能性があると思われる場合は、弊社までご連絡ください。

Unit 42のインシデント レスポンス チームは24時間、週7日、365日対応可能です。また、サイバー保険に加入されている場合は、Unit 42を指名して対応を依頼できます。また、ランサムウェア準備状況評価をお申込みいただき、予防的な対策を取り入れることも可能です。

調査方法

本レポートは、内外の複数の情報源からのデータに基づいています。被害者ではなく脅威アクターを明らかにすることを目的としているため、すべての事例データは匿名化され、業界、地域、攻撃経路などのトピックのみに基づいて分類されています。本レポート全体で参照される特定のデータの情報源を以下に示します。

(主にセクション2で参照される)本レポートの内部データは、主に米国に本拠を有するお客様とのセキュリティ コンサルティングとインシデント レスポンス活動中に収集した匿名情報です。Unit 42セキュリティ コンサルティング チームが実施している1つのサービスは、お客様に代わってランサムウェアの交渉を行うことです。このサービスを利用し、身代金の支払いを選択する一部のお客様について、Unit 42は重要な情報を追跡します。この情報には、ランサムウェアの亜種、初回の要求額、支払額、および脅威アクターが当初合意された金額の支払い時に復号ユーティリティを提供したか否かが含まれます。本レポートの追加データは、マネージド脅威ハンティング、製品のセキュリティ テレメトリ、および業務中に系統的に作成された脅威リサーチから入手しました。

(主にセクション3で参照される)外部データは、二重脅迫を実行しているランサムウェア ファミリを特定するために、ランサムウェア リーク サイトから照合し、分析しました。ほとんどの場合、ランサムウェアの身代金要求メモには、リーク サイトを被害者に示すTorへのリンクが含まれています。このようなサイトは、年間を通じて活動を把握するために、リポジトリにホストされ、チームによって監視されています。ほとんどのサイトは一般に公開され、「ダーク ウェブ」にあります。このため、チームは、被害者の名前、日付、データがホストされているサイトの情報を収集できます。データの収集後に、チームは、被害者の業界、セクター、場所、識別可能なその他の詳細によってデータをエンリッチ化します。

弊社は、身代金要求額と支払額の平均を計算するために使用する方法を見直しました。この結果、2020年の平均支払額を(2021年ランサムウェア脅威レポートで公開した312,493ドルから)303,757ドルに修正しました。

パロアルトネットワークスについて

世界的なサイバーセキュリティのリーダーであるパロアルトネットワークスは、個人や組織の運用方法を変革するテクノロジを利用して、クラウド中心の未来を構築しています。弊社ではサイバーセキュリティ パートナーとして選ばれることで、デジタル時代における皆さまの生活をサイバー攻撃から守ることです。人工知能、分析、自動化、オーケストレーションといった分野における最新の飛躍的進歩を取り入れた絶え間ないイノベーションによって、世界最大のセキュリティ課題に対応します。また、統合されたプラットフォームを提供し、パートナーのエコシステムを成長させることで、何万もの組織のクラウド、ネットワーク、そしてモバイル デバイスを最前線で保護しています。私たちのビジョンは、昨日よりも今日、今日よりも明日が安全になる世界を築くことです。詳細については、www.paloaltonetworks.jpをご覧ください。

パロアルトネットワークスは、ファイル サンプルやセキュリティ侵害の兆候を含む調査結果をCyber Threat Alliance(CTA)の会員と共有しました。CTAの会員は、この情報を利用して、その顧客に対して迅速に保護を提供し、悪意のあるサイバー アクターを組織的に妨害しています。詳細については、Cyber Threat Allianceを参照してください。

Unit 42について

パロアルトネットワークスのUnit 42は世界に名だたる脅威リサーチャーとセキュリティコンサルタントの精鋭チームがひとつになり、インテリジェンス主導でインシデント対応可能な組織となりました。同チームは事前のサイバー リスク管理に重きをおき精力的にお客様のご支援にあたっています。業界屈指の脅威インテリジェンス提供で知られるUnit 42は、その業務内容を拡大し、最新のインシデント レスポンスとサイバー リスク管理サービスをご提供しています。弊社コンサルタントはしかるべき脅威へのセキュリティ対策を評価・検証し、脅威情報に基づくアプローチでセキュリティ戦略を転換し、迅速にインシデントに対応する信頼できるアドバイザーの役割を果たします。paloaltonetworks.com/unit42をご覧ください。

パロアルトネットワークスのランサムウェア機能

パロアルトネットワークスでは、ランサムウェアを阻止する包括的機能を搭載した製品を多数提供しています。ランサムウェア アクターに関するUnit 42のリサーチとパロアルトネットワークスが特定の状況に対して提供する製品の詳細については、Unit 42のブログをご覧ください。

ネットワーク セキュリティ

クラウド配信型セキュリティ サービスは、数千社単位のお客様企業がもたらすネットワーク効果をさまざまなセキュリティ テクノロジに行き渡らせることで、インテリジェンスの連携や、あらゆる攻撃ベクトルに対する一貫した保護の提供を行っています。ハードウェアPA-Series、ソフトウェアVM-Series/CN-Series、クラウド配信型Prisma® Accessなど、弊社のML-Powered NGFW製品群に展開されている数々のサービスは、セキュリティ対策の抜け漏れ解消に役立ちます。各製品とサービスの詳細については、以下のリンク先を参照してください。

WildFire®マルウェア分析サービスは、すべてのパロアルトネットワークス製品にネイティブに統合され、既知および未知のランサムウェア亜種およびその他のファイルベースの脅威に関連する活動をブロックします。

Advanced URL Filteringを設定すると、既知・未知の悪意のあるURLへのアクセスをブロックし、疑わしいコンテンツ/マルウェアをホストしているとパロアルトネットワークスがみなしたWebサーバーにホストがHTTPを介してアクセスすることを防止できます。

Advanced Threat Preventionは、ファイアウォールの可視性を利用して、すべてのトラフィックを検査し、ポート、プロトコル、SSL暗号化にかかわらず既知のエクスプロイト、マルウェア、スパイウェアを自動的に防御します。

DNSセキュリティはDNSプロトコルを特異的に悪用するコマンド&コントロールやデータ漏出試行をブロックします。DNSプロトコルの悪用はランサムウェアを含め、85%超の侵害で確認されています。

IoTセキュリティは、すべてのIoT、OT、IT、Bluetoothデバイスに対する可視性を提供し、最小権限(ゼロ トラスト)ポリシーを推奨します。これにより、攻撃者が管理外デバイスを足がかりにしてランサムウェアなどの悪意のあるファイルを配布するリスクを最小限にします。

Enterprise DLP(企業向け情報漏えい防止サービス)は、企業ポリシーに反する機微データの安全でない転送を自動的に検出・防止し、企業全体、リモート ユーザー、クラウド アプリケーションで機微データの公開を最小限にします。

CORTEX

Cortex® XDR™は、ランサムウェアと無数の他の危険な攻撃を阻止するために、あらゆるソースからのデータを統合する業界初の拡張ディテクション&レスポンス プラットフォームです。Cortex XDR Agentは、エンドポイントを標的とするエクスプロイト、マルウェア、ファイルレス攻撃を自動的にブロックします。エンフォースポイントとの緊密な統合により、アナリストは、ランサムウェアの拡散を迅速に阻止し、デバイス間のネットワーク アクティビティを制限し、不正ドメインなどの脅威防止リストを更新できます。Cortex XDRでは次のことが可能です。

- 包括的なエンドポイント保護スタック(エクスプロイトの防御、振る舞いベースの脅威からの保護、AIを活用したローカル分析、アンチマルウェア モジュールを含む)により、攻撃ライフサイクルのすべてのステップでランサムウェア攻撃をブロックする。
- エンドポイント、ネットワーク、クラウド、IDデータにわたるクロスデータ分析により、ラテラルムーブやデータ漏出などのステルス性の高い攻撃を検出する。
- 根本原因分析でインシデント調査を迅速化する。
- 協調的かつ柔軟なレスポンスで脅威を封じ込める。

Cortex XSOARは、ユーザーおよびホスト データのエンリッチ化、悪意のあるインジケータのブロック、感染エンドポイント/ユーザーの分離/隔離の全プロセス自動化、ランサムウェア検出における発見・修復の迅速化に役立ちます。

PRISMA

Prisma® Cloudは包括的クラウド ネイティブ セキュリティ プラットフォームです。ハイブリッド クラウドやマルチクラウドなどさまざまな環境で、アプリケーション、データ、クラウド ネイティブ テクノロジ スタック全体に、業界で最も幅広いセキュリティとコンプライアンスを、開発ライフサイクル全期間にわたって提供します。Prisma Cloudの統合アプローチにより、SecOpsチームとDevOpsチームは迅速な対応を維持し、効果的なコラボレーションを行い、クラウド ネイティブなアプリケーションの安全な開発と導入を推進できます。

クラウド セキュリティ態勢管理 – ラテラルムーブを妨げるためにサービスをセグメント化し、侵害成功からくる影響を制限します。

Unit 42は世界に名だたる脅威リサーチャーとセキュリティコンサルタントの精鋭チームがひとつになり、インテリジェンス主導でインシデント対応可能な組織となりました。同チームは事前のサイバー リスク管理に重きをおき精力的にお客様のご支援にあたっています。

ランサムウェア準備状況評価 – 最新の脅威インテリジェンスを利用し、準備状況の評価とランサムウェア プレイブックの作成でお客様をご支援します。実情に即した侵害シナリオや侵害状況の評価、経営陣向け助言コンサルティングをご提供することにより、お客様が専門家のようにランサムウェア攻撃を管理できるようにします。

インシデント レスポンス – ランサムウェア攻撃を受けてファイルやアプリケーションにアクセスできなくなった場合は、弊社の精鋭Unit 42インシデント レスポンス チームにご連絡ください。業務をすみやかに復旧できるよう、お客様に代わって脅威を調査し、封じ込め、根絶します。

〒100-0011
東京都千代田区内幸町2丁目1番6号
日比谷パークフロント15階
電話番号: 03-6205-8061
http://www.paloaltonetworks.jp