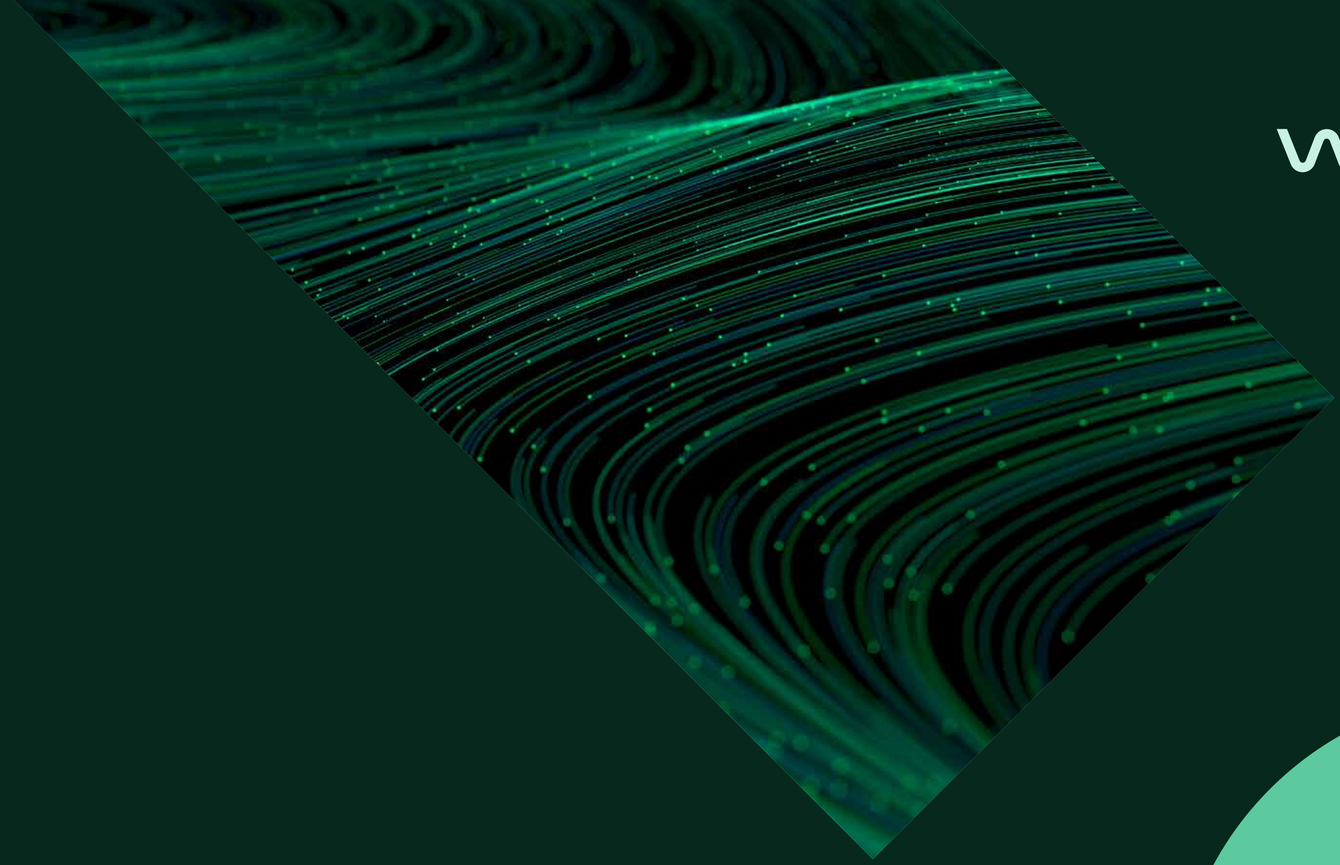
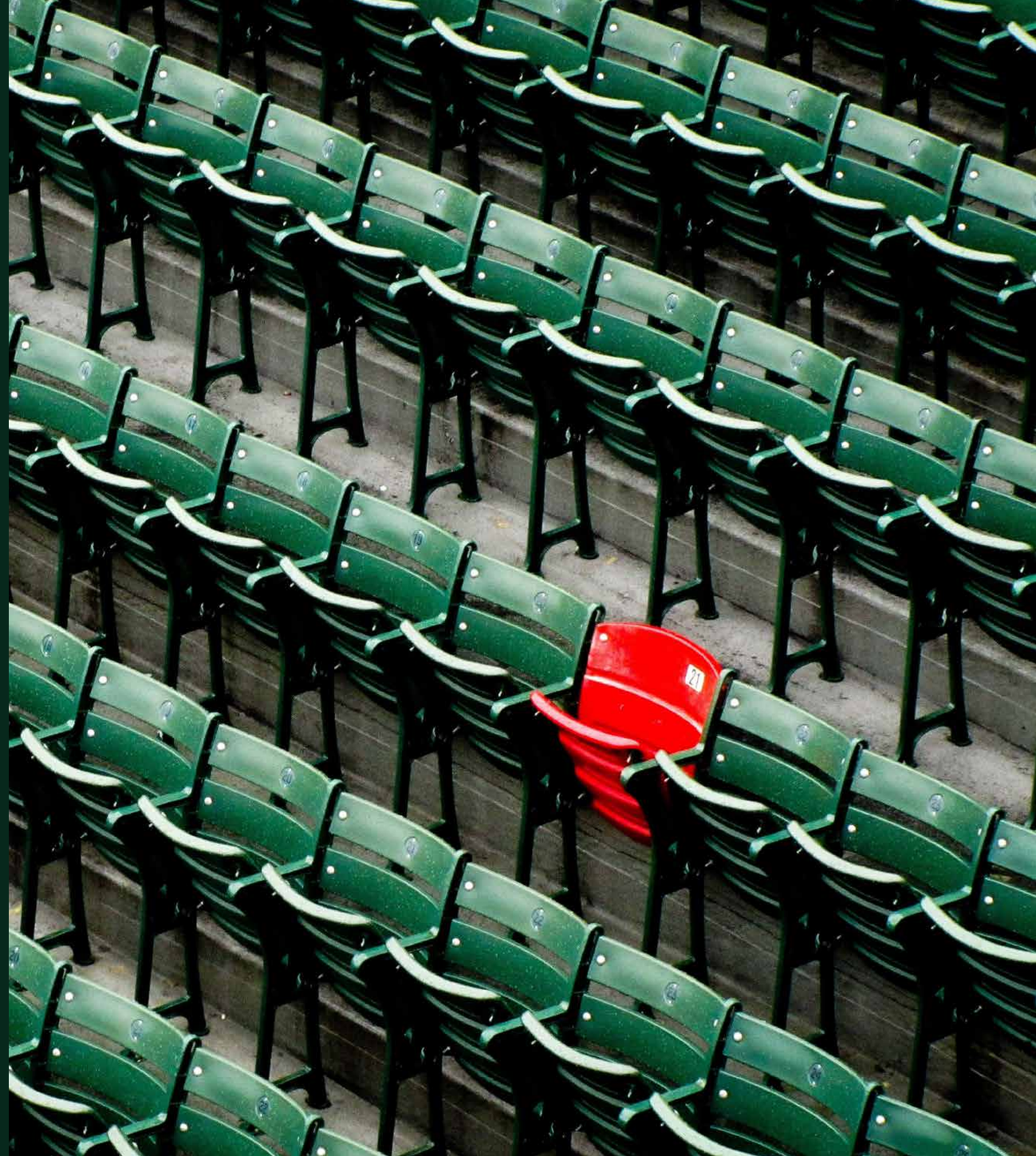
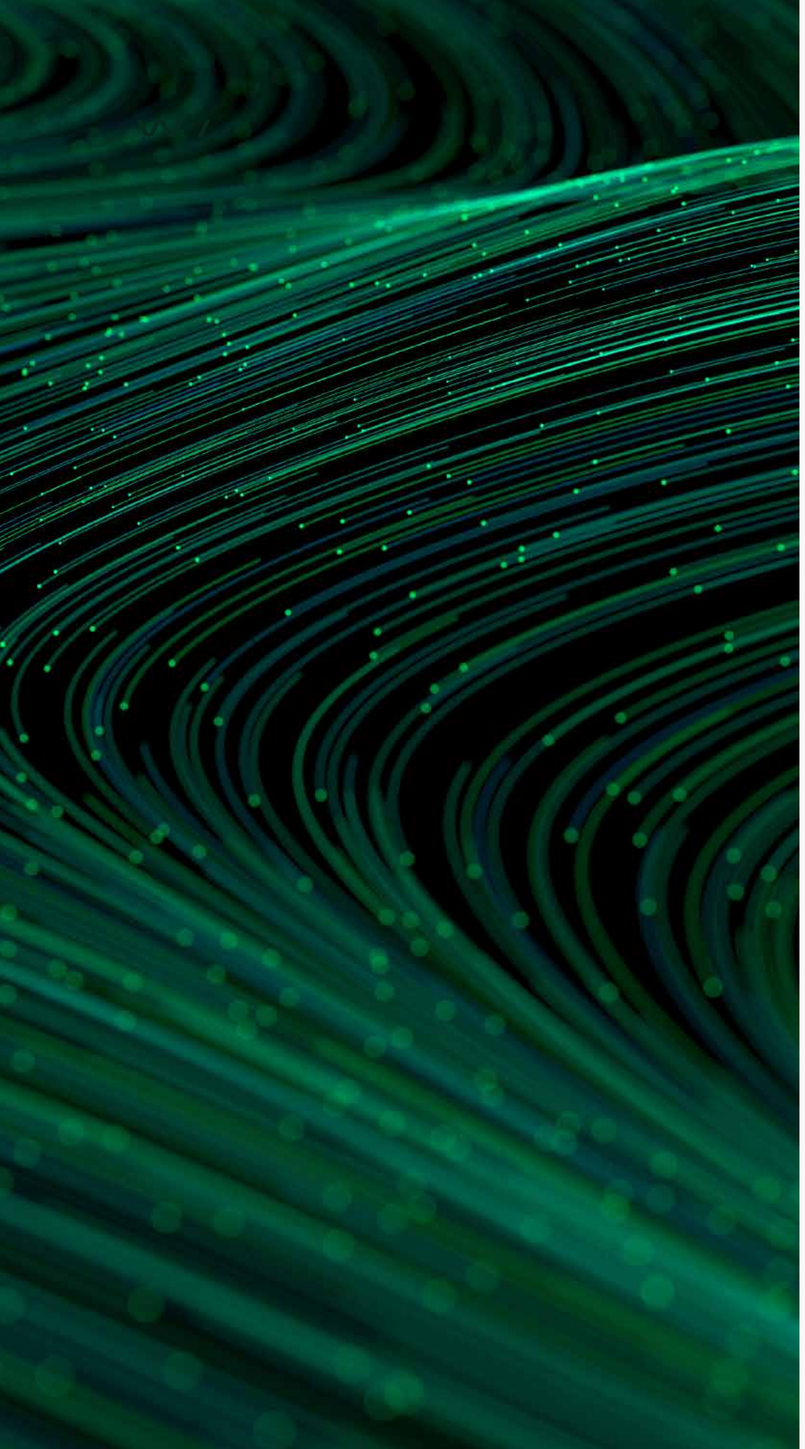


最新ランサムウェア脅威レポート

2022年6月

コンテンツ





はじめに

ランサムウェアは、過去10年にわたり人々や企業／団体を悩ませてきたマルウェアの一種です。当初はフロッピーディスクを送りつけ、郵便で身代金を要求するようなものでしたが、その後、ランサムウェアの脅威はますます巧妙になり、規模も拡大しています。身代金 (ランサム) の額が大きくなるにつれ、ランサムウェアは多国籍企業や数百万人が利用する重要な国家インフラを麻痺させる可能性のある問題へと変化しています。

本レポートは、ランサムウェアの脅威に関する動向と発展に関する最新情報を防御側に提供することを目的に、2021年の関連する見解を簡潔にまとめたものです。本レポートでは、新しいランサムウェアのファミリーや亜種の継続的な開発、ランサムウェアの能力と特性の進化、世界の脅威の状況におけるランサムウェアの普及、注目すべきランサムウェアファミリー／亜種、被害者や被害者になり得る人々に対して攻撃の検知／対応を提供しているウィズセキュアの実体験からの見解などの関連トレンドが紹介されています。

私たちの考察に基づき、ランサムウェアは企業／団体にとってクリティカルであるものの、十分に対処可能な脅威であると言えます。

数年間にわたるランサムウェアの進化

ランサムウェアは、ユーザーのマシンやデータの制御を奪う悪質なソフトウェア (マルウェア) の一種です。多くの場合、1台または複数台のデバイスに保存されているデータを暗号化することによって行われます。正規ユーザーのアクセスが遮断されると、攻撃者は「身代金を支払えばアクセスを回復する」という条件を持ちかけます。過去10年間で、この手法は、サイバー犯罪者やその他の脅威行為者にとって、オンライン恐喝の方法としてますます効果的になってきており、一般的にこれらの攻撃の主な動機となっています。

暗号化は、サイバー犯罪者が被害者に圧力をかけるための最も有名な方法です。しかし、最近では、攻撃者は、被害者の情報を流出させるなど、二重脅迫という身代金の強奪方法を採用しています。

ランサムウェアの被害は、身代金を支払わなくても、組織に深刻な経済的損失をもたらす可能性があります。攻撃によって業務が停止し、収益が減少する可能性があります。また、収益に結びつかないシステムであっても、オフラインになることで、組織にとって重要な生産性の時間が失われます。直接的な金銭的損失だけでなく、間接的なコストも発生します。企業／団体は、攻撃が発生するまでその事実を知ることはなく、通常、乏しい予算でこのような対策を計画することはありません。したがって、直接的にせよ、間接的にせよ、金銭的な損失が発生すると、ある部門から別の部門への資金の再配分を余儀なくされ、サービスの中断につながる可能性があります。

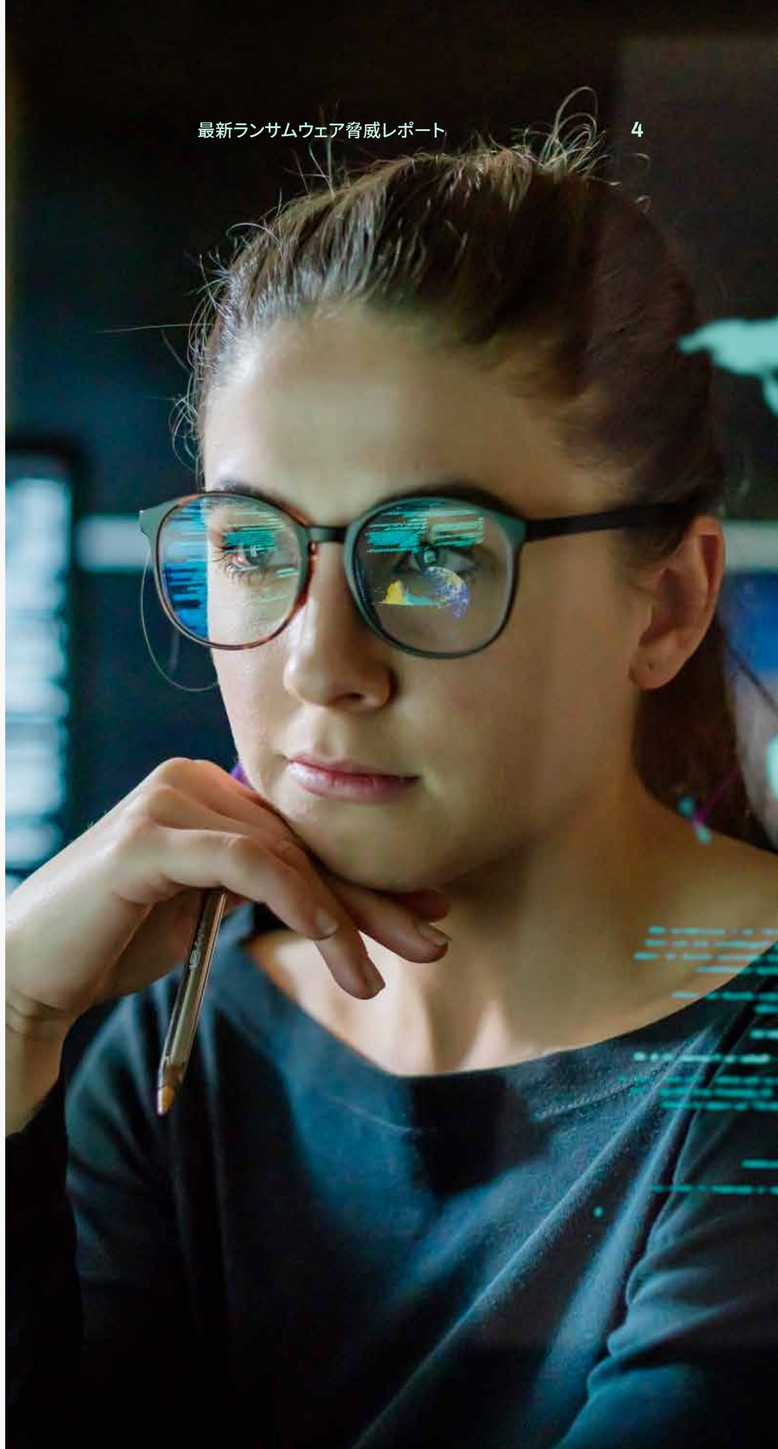


図1: ランサムウェアの脅威の進化.

初期のランサムウェア

ファイルを暗号化するものの、ファイルの破損やライセンス問題などによる問題であるかのように装い、有料でファイルを「修正」することを提案する。

主な例:
AIDS Information Trojan
File-Fix Professional

警察を装ったランサムウェア

ロック画面 (しばしば当局を名乗る詐欺的なもの) を使用し、「罰金」を支払わない限り、デバイスを使用できないようにする。

主な例:
Reventon
ICPP

ビットコイン・ブーム

身代金の支払いにビットコインやその他の暗号通貨を使用。
エクスプロイトキットやスパムでよく配布される。

主な例:
Cryptolocker
CTB-Locker　など

デジタル・ゴールドラッシュ

ユニークなファミリー／亜種の数が大量に増加。
大規模で無差別なキャンペーンで目立つペイロード。

主な例:
Locky
WannaCry

大企業を標的とした攻撃

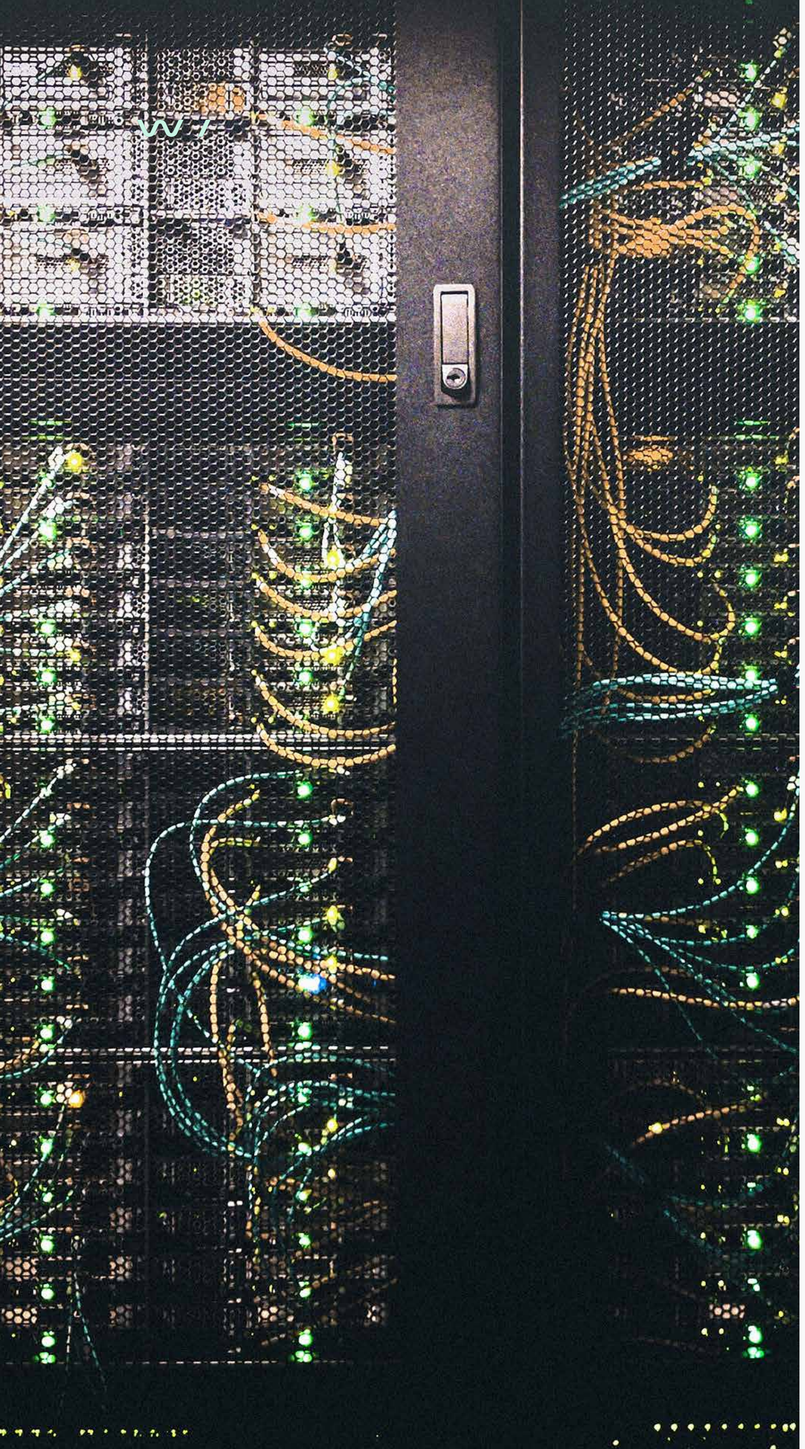
多額の身代金を支払うことができる大企業を危険にさらすのに適した手口 (脆弱な業務用ソフトウェアやインフラ、ハンズオンキーボード攻撃など) がより多く使われるようになる。

主な例:
Ryuk
GandCrab

ランサムウェア 2.0

攻撃者は、被害者を脅迫するために複数の戦術を用いる (例えば、暗号化前のデータを盗み、それを漏洩させると脅し、被害者に身代金を支払わせる圧力を強めるなど)。

主な例:
Maza
REvil



脅威としてのランサムウェアの歴史は1989年にまで遡りますが、当時はまだそのようなものとして認識されていませんでした。AIDSトロイの木馬は、一般的に史上初のランサムウェア攻撃と言われており、フロッピーディスクを介して配布され、ユーザーが189ドルの「料金」を支払わない限り、ファイルへのアクセスを阻止する基本的な暗号化が使用されました。[1]

しかし、それ以降も、攻撃者はこのようなビジネスモデルを様々な形で展開し続けています。身代金ではなく「料金」を支払うというアイデアは、攻撃者にとって魅力的なものであり、現実の問題に対する正当な解決策として復旧サービスを表現することができます。攻撃者の中には、ユーザーが行った何らかの違法行為に対応するために、当局に代わって拡散させたと主張する「警察を装ったランサムウェア」を開発するまでに至った者もいます。この種のランサムウェアは暗号化ではなく、単に画面を塞いで閉じられないようにするメッセージで、デバイスやデータへのアクセスを阻害することが多いのです。ユーザーが違法なことをしていると表示するこうしたメッセージに対して、ユーザーは何らかの犯罪を犯していると非難するメッセージを誰かに見られる前に料金を支払わなければならないというプレッシャーを感じていました。実際には、無実の人々や企業を脅すための手段でした。

ランサムウェアの人気は、暗号通貨の登場と人気の高まりに大きく助けられ、2010年代を通じて上昇し続けました。暗号通貨は、攻撃者がより伝統的で制約の多く厳しい方法に依存することなく、身代金の支払いをさせるための新たな方法を奇しくも提供することとなったのです。あるサイバー犯罪ギャングがCryptolockerランサムウェアを使用し、2013年から2014年にかけて50万人の被害者から約300万米ドルを奪い取ったことが、ビットコインの効果を物語るいい例だと言えます。[2]

この間、ランサムウェアの人気は急上昇し、専門性の異なる様々なサイバーギャングから大きな注目を集めました。この急増は、2017年にピークを迎えたようです。この時期、ランサムウェアは大規模で無差別なスパムキャンペーンによりますます普及し、できるだけ多くの被害者に感染させようとしました。この年は、悪名高いランサムウェア攻撃「WannaCry」が発生した年でもあります。WannaCryは、脆弱性のあるデバイスに自動的に拡散することが特徴的でした。WannaCryが標的とした脆弱性 (CVE-2017-0144)[3] に対するパッチは攻撃の2ヶ月前に提供されていましたが、多くの企業／団体はまだデバイスを更新していませんでした。その結果、WannaCryは世界中で急速に拡散していきました。[4]

1. https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#3

2. https://www.bbc.com/news/technology-28661463

3. https://www.cve.org/CVERecord?id=CVE-2017-0144

4. https://www.bbc.com/news/world-europe-39907965

2017年以降、ランサムウェアの攻撃はより高度化し、企業／団体への恐喝に適した、より切迫した脅威へと進化しました。ランサムウェアを使用するサイバーギャングたちは、標的の件数より質を重視し始めリソースを集中させることで、より少ないターゲットからより大きな金額をゆすり取れることを期待するようになりました。このような攻撃者は、無差別なスパムキャンペーンやドライブバイダウンロードだけに頼るのではなく、企業／団体が使用するソフトウェアの脆弱性を突くようになりました。

最近になって、ランサムウェアギャングは、身代金支払いの圧力を強める方法を考案し始めました。おそらく最も一般的な手法は、暗号化する前にデータを盗み、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脅すことで、この手法は防御側にとって大きな課題となりました。重要なデータやシステムの信頼できるバックアップ、万全のインシデント対応計画でランサムウェア攻撃に備えていた企業／団体でも、(機密情報を含む) データが公開された場合、ビジネス上の大きな困難に直面することになります。このような攻撃者は、さらなる攻撃 (SunCryptやRagnar LockerのDoS攻撃の利用など) で標的を脅し、この「二重脅迫」の手法は拡大し続けています。)[5]

「ランサムウェア産業」は現在、企業／団体に数十億米ドルの損害を与えているとの試算があります。[6] 最近では、攻撃後にデータを復旧させるために企業／団体が巨額の身代金を支払った事例が注目されています。2021年、食肉加工企業のJBSは、自社のシステムが侵害された後、ランサムウェア集団「REvil」に1,100万米ドルを支払ったことを認めました。[7] また同年末には、米国コロニアル・パイプライン社がダークサイドからの高度な攻撃を受けてパイプライン全体のコンピュータシステムが危険にさらされ、米国内で燃料不足とパニックに陥った後、440万米ドルの身代金を支払ったと報告されています。[8] これらの数字は、ランサムウェアのビジネスモデルがオンライン恐喝の有益な方法であることを示しています。

ランサムウェアの攻撃が成功すると、規模や業種に関係なく、企業／団体の活動が停止してしまう可能性があります。ランサムウェアに感染すると、企業／団体のビジネス上の利益が損なわれることが多く、犯罪者による身代金の要求が容易になります。多くの企業／団体は、ITシステムやデータベースに依存して事業を展開しており、顧客データを管理・保護する法的義務を負ってケースもあります。こうした理由から、企業／団体は身代金を支払うことで、ランサムウェア感染を迅速かつ穏便に解決しなければならないというプレッシャーを感じることが多いのです。

5. https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/

6. https://www.europarl.europa.eu/resources/library/images/20220126PHT21867/20220126PHT21867_original.jpg

7. https://www.bloomberg.com/news/articles/2021-06-09/jbs-paid-11-million-in-ransom-to-resolve-cyberattack-dj?s-ref=CIpmV6x8

8. https://edition.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html

Ransomware trends

図2: 2021年に発見された新しいランサムウェアファミリー／ユニークな亜種

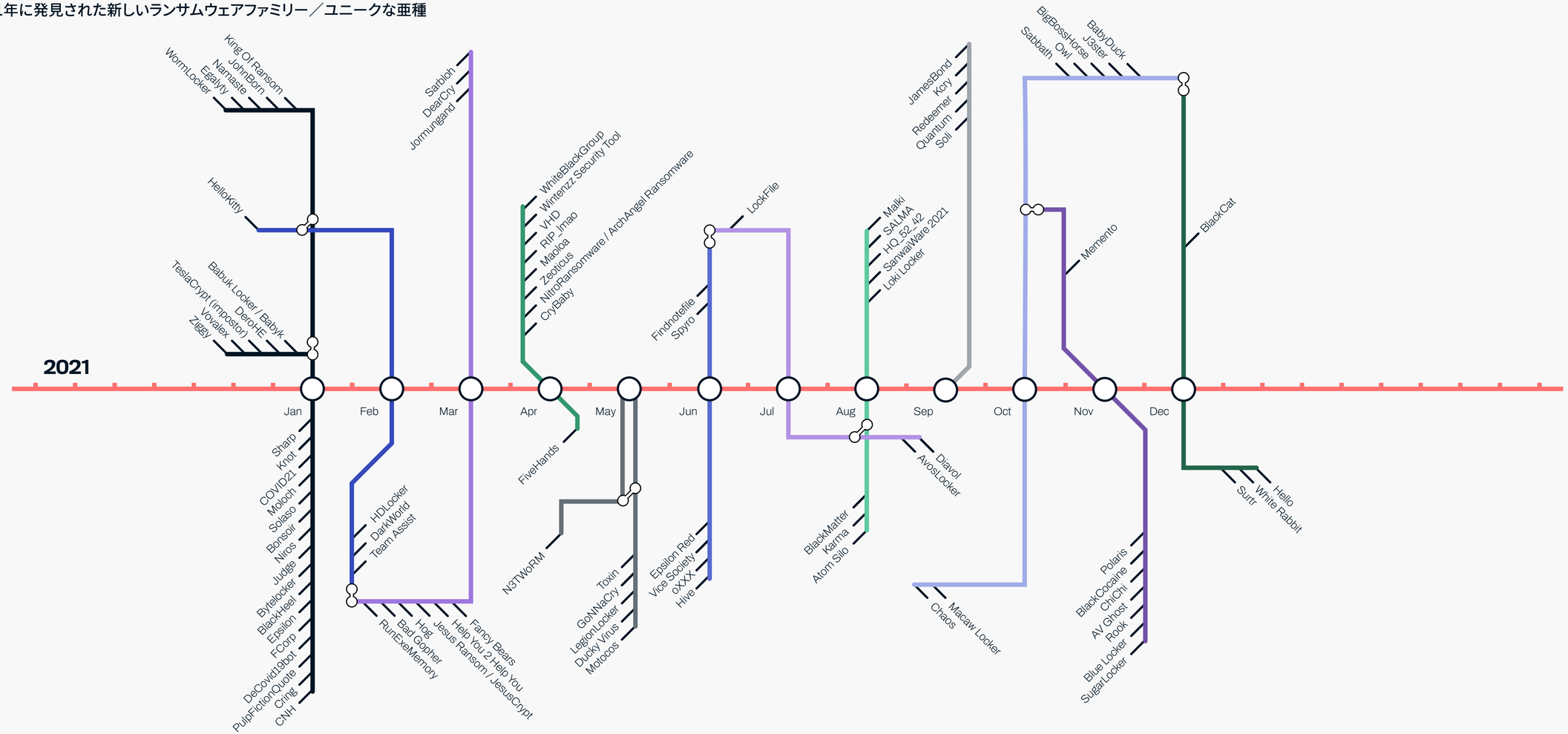


図3: 新しいランサムウェアファミリー／ユニークな亜種の年間発生数

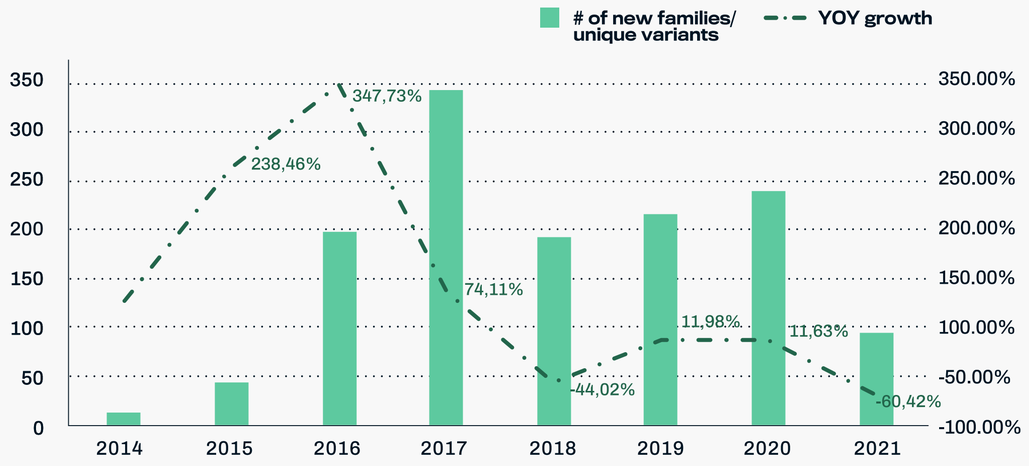
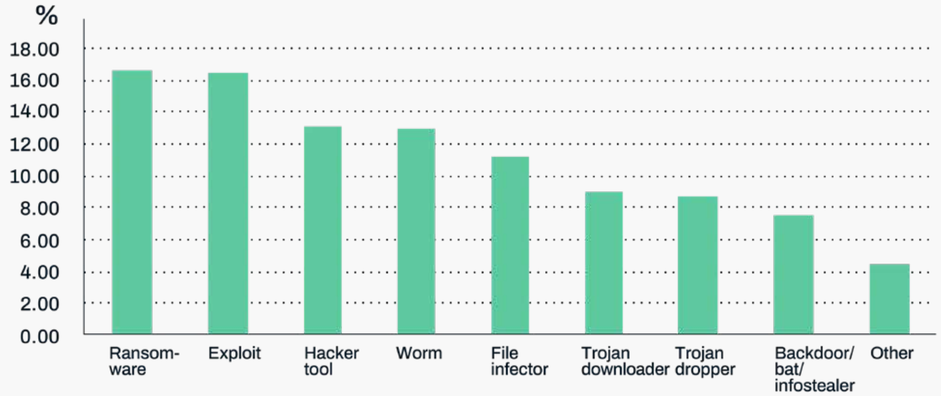


図4: 2021年におけるタイプ別の脅威の使用率



ランサムウェアは過去10年の大半の間、広く使用される脅威であり続けています。新しいランサムウェアの作成は比較的容易であり、被害者を脅迫することに成功したため、脅威アクターから大きな注目を集めています。その結果、毎年何百もの新しいファミリーやユニークな亜種が登場するようになりました。この活動は2017年頃にピークを迎えますが、その後は一時期比較的安定した状態が続いています。2021年には、セキュリティリサーチャーによって発見される新しいランサムウェアの量が大幅に減少しましたが、この背景に何があるのかを特定することは困難です。可能性の1つは、REvilのような既知のRaaS (ランサムウェア・アズ・ア・サービス) サービスの台頭だと考えます。これらのサービスは、サイバー犯罪者がランサムウェアやその他のインフラを独自に開発する必要をなくし、ランサムウェア・キャンペーンを実施するためのハードルを下げるものです。

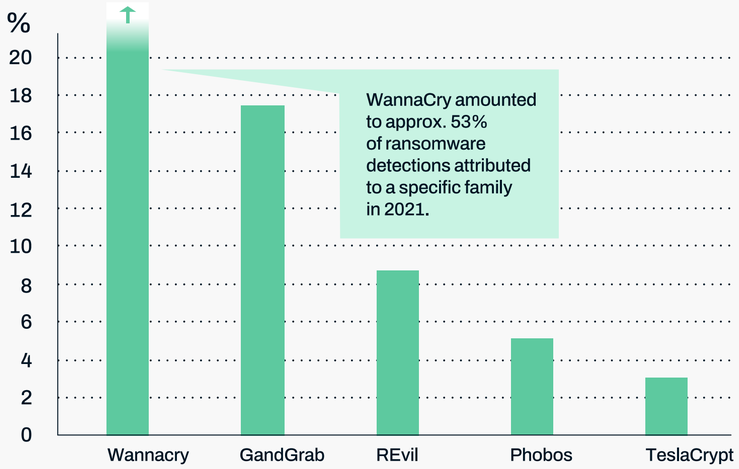
この減少にもかかわらずランサムウェアが引き続き流行していることは、企業／団体にとって重要な脅威であり続けることを明確に示しています。ランサムウェアは2021年にユーザーが遭遇した脅威の約5分の1を占め、その年に最も広く使用された脅威タイプとなっています。

WannaCryは、当社のテレメトリーで最も多く確認されたファミリーです。これはランサムウェアの検出数の半分以上を占め、それ以外に流行が観測された4つのランサムウェアファミリーを合わせた数よりも多くなっています。WannaCryの躍進は、自動化された拡散によるところが大きいと言えるでしょう。アクティブなキャンペーンに関与することなく、少数のホストに何度も感染を試みることができるため、他のファミリーより優位性が高まるものです。

次いで流行している3つのファミリー、GandCrab、REvil、Phobosは、全てRaaSで提供されているものです。2018年に初めて確認されたランサムウェアファミリーであるGandCrabは、2019年に活動停止を発表しました。しかし、明らかに停止しているにもかかわらず、GandCrabの活動停止発表の直前に初めて観測されたREvilは実際には同じサイバーギャングによって運営されていて、サイバーギャングが単にその装いを新たにしただけではないかと、多くの人が疑いの目を向けています。[9]

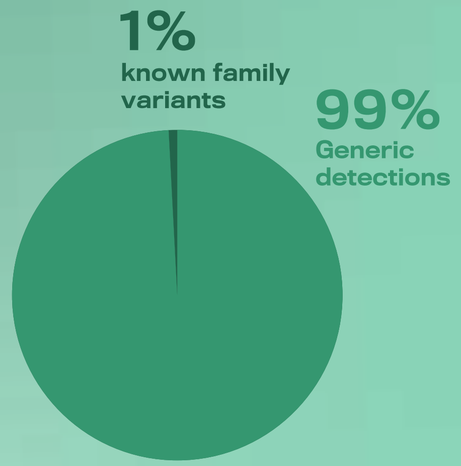
ランサムウェアの古い亜種であるTeslacryptが5位にランクインしていますが、このランサムウェアの流行は、2021年の第1四半期にやや急増したことに起因しています。この理由としては、この古いランサムウェアのファミリーを復活させるために、オリジナルを少し修正したバージョンを使ったことだと考えられます (ただし、成功したとは言い難いですが)。

図5: 2021年に最も使用されたランサムウェアファミリー



9. https://www.darkreading.com/attacks-breaches/gand-crab-developers-behind-destructive-revil-ransomware

図 6: 検出された一般的なランサムウェアと、既知のファミリー／亜種に関連するランサムウェアの比較



流行中のランサムウェアファミリーは注目すべきものですが、それが脅威の全体像を示しているわけではないことも理解する必要があります。テレメトリーでは、特定のファミリーに属するランサムウェアは約1%にすぎません。残りの99%は、特定のファミリー／亜種に関連付けるのではなく、その挙動 (ファイルの暗号化など) に基づいてランサムウェアとして識別されています。このアプローチを使用することで、リサーチャーが脅威を既存の亜種にマッピングしようと時間をかける前に、エンドポイント保護製品が新しい (または不明瞭な) ランサムウェアの亜種をブロックし、企業／団体が大量の潜在的ランサムウェア感染から防御するための迅速かつ効果的な方法を提供することができます。

深く潜むランサムウェア

図7: 2021年ランサムウェアのIR／DRTの業種別被害件数

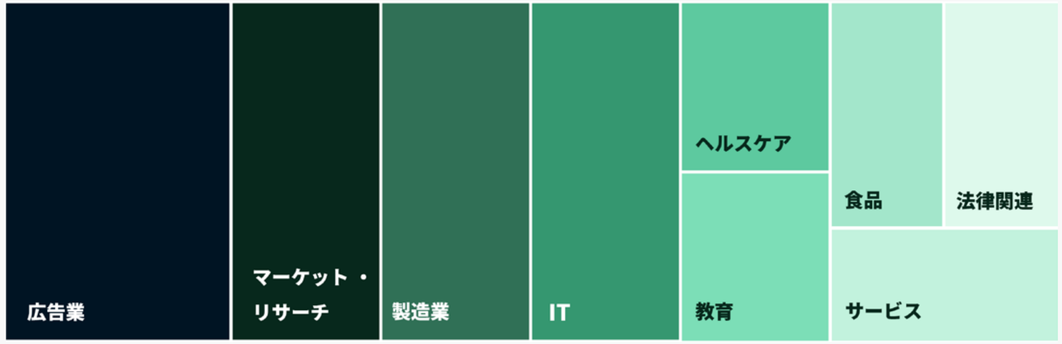


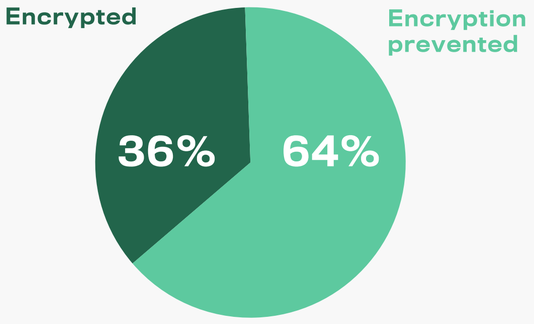
図 8: 2021年IR／DRTで観測された初期攻撃ベクトル
ランサムウェアのエンゲージメント

2021年、ウィズセキュアのインシデントレスポンスチーム (IR) と検知／対応 (DRT) チームは、数多くのランサムウェア攻撃に対処しました。これらの対応から、ランサムウェアは明らかに様々な業種に影響を及ぼす問題であることがわかります。基本的に、これらの攻撃者は身代金が取れそうであれば業種を問わず攻撃を実行します。

さらに、ランサムウェアギャングは様々な手法で企業／団体を危険にさらしています。2021年に最も多く観測されたのは、「悪意のあるOfficeファイル」と「悪意のあるダウンロード」の手法でした。これらの手法は、1つのキャンペーンで複数の企業／団体を日和見的に攻撃するために採用されることがよくあります。ウィズセキュアのIR／DRTチームが次いで多く観測した初期アクセスのベクトルは、脆弱性の悪用と露出したリモートデスクトッププロトコルポートを介したネットワークへのアクセスでした。これらの結果から、ランサムウェア攻撃やその他の侵害を防止するための基本的なセキュリティ対策の重要性が浮き彫りになりました。例えば、これらのベクトルの多くは、パッチが適用されていない脆弱性 (特にインターネットに面したインフラ)、脆弱なパスワード、オンラインアカウントのセキュリティのための多要素認証の欠如、その他企業／団体が本来対処可能である脆弱性を悪用しています。

幸いなことに、ウィズセキュアのIR／DRTチームが調査したランサムウェア攻撃のうち、大半は攻撃者が企業／団体に大きな損害を与える前に食い止められました。約3分の2は、攻撃者がデータを暗号化する前に阻止されたため、ダウンタイムや脅迫などによる大きな損失を免れることができました。

図 9 .データ暗号化に至ったIR／DRTランサムウェアの被害状況



ランサムウェアの影響を最小化するために

ランサムウェアは、世界中の様々な業界の企業／団体にとって大きな脅威であることが証明されています。しかし、ランサムウェアは決して手に負えない脅威ではありません。100万ドルの身代金要求やその他の問題は一見困難なように見えますが、ランサムウェアの攻撃によって発生する可能性のある損害を最小限に抑えることは可能です。

その具体的な内容は、様々な要素に左右されます。ランサムウェアは業界や地域を問わず企業／団体に影響を与える可能性がありますが、防御側のリソースはまた別の話です。例えば、大手銀行はランサムウェアやその他の脅威から自身を防御するために多額のリソースを投入しています。一方、小規模な食料品店チェーンは、脅威に対する認識も、身を守るためのリソースへの投資も同じようにはいかないかもしれません。

多くのサイバーセキュリティ上の課題と同様に、多層的な防衛戦略を持つことが重要です。このため、防御戦略は「複数のツールを導入すれば安全」なのではなく、継続して守っていく包括的なプランとして考えるのが適切です。

予防

「100の治療より1の予防」という諺があります。これはサイバー攻撃にも当てはまります。本レポートに含まれるデータが示すように、企業／団体が対処しなければならないランサムウェアの活動は相当な量にのぼります。エンドポイント保護には限界がありますが、それでもランサムウェアの感染を防ぐうえでの効果的なツールであることに変わりはありません。

検知

たとえ確実な予防策を講じていても、それが限界に達してしまうケースを想定しておくことは、企業／団体にとって重要です。このような事態は、人々が思っている以上に多くの理由で発生する可能性があります。全てが100%上手くいっていたとしても、今日最大のランサムウェア攻撃の多くは、十分な資金や技術を持つサイバーギャングたちによるものです。彼らは、前もってネットワークに侵入し、組織的に防御を無効にしつつ、標的に最も大きな損害を与えることができる攻撃箇所を学習していることが多いのです。

このため、企業／団体は自社ネットワーク内の悪意ある活動を検知できるように準備しておく必要があります。大規模な多国籍企業やセキュリティが死活問題である業界の企業などでは、こうした能力を自社で開発するために十分な投資を行っているところもあります。しかし、自社ネットワークの検知機能を提供するために提携できる外部パートナーは多数存在します。

対応

最後に、対応を伴わない検知は、消火計画やリソースがないのに煙探知機を設置するようなものです。差し迫ったランサムウェア攻撃や進行中の侵害を検知しても、実際に攻撃を阻止することはできません。企業／団体は、ランサムウェアを含む攻撃に対応するための準備をすることが重要です。

今日、サイバー攻撃への対応は、侵入したアカウントをロックするなどの単純なものから、多くの異なる部門を横断する対応を必要とする全社的なものまで、多岐にわたります。経営陣はサイバー攻撃を主にITの問題として捉えがちですが、その潜在的な影響は組織全体、さらにはその顧客にまで及ぶ可能性があります。このため、インシデント対応計画には技術的な配慮だけではなく事業の継続性を確保するための措置を含める必要があります。

一方で、ちょっとしたセキュリティインシデントで組織全体がパニックに陥ることのないようにすることも重要です。そのため、ランサムウェアなどのインシデントに備えるためのサイバーセキュリティパートナーを見つけることが、未然のサイバー攻撃によるリスクを軽減することにつながるのです。

WithSecure™について

WithSecureは、ITサービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちはAIを活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は30年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988年に設立されたWithSecureは本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は www.withsecure.com をご覧ください。また、Twitter @WithSecure_JP でも情報の配信をおこなっています。

ウィズセキュア株式会社
〒105-0004　東京都港区新橋2丁目2番9号　KDX新橋ビル 2階
Tel: 03-4578-7710 / E-mail: japan@f-secure.co.jp
https://www.withsecure.com/ja_JP/

2022.06 JP

WITH secure