RANSOMWARE eBOOK

BE THE HUNTER, NOT THE HUNTED

2022 年 12 月版

SISA Information Security
and
Fime Japan

Contents

まえがき

ランサムウェア：ボスになって防衛戦略を構築せよ

ビジネスにおいて、恐怖を呼び起こすことができる言葉はあまりありません。結局のところ、ビジネスとは不確実性の中に機会を求めることなのです。リスクを取れば取るほど、あなたのビジネスはより強力で収益性の高いものになるかもしれません。しかし、”ランサムウェア ”はどうでしょう。この言葉は、あらゆるビジネスチームの心に恐怖を呼び起こすことができます。

つい最近まで、ランサムウェアの標的は個人と消費者でした。しかし、ランサムウェアの闇の世界は鋭く抜け目なくなってきました。ランサムウェアの新たな標的は、あらゆる形態や規模のオンラインビジネスです。

報酬が大きくなるにつれて、ランサムウェアの運営者の戦略も洗練されたものになってきています。また、ランサムウェアを検知することも難しくなっています。そして、ランサムウェア攻撃を仕掛けるためのツール、プロセス、人材が自由に利用できるようになりました。信用が資本の世界においてランサムウェアの運営者は、自分たちが損害を与えることができる企業は、その信用を守るために莫大な金額を支払うことを理解しているのです。

ランサムウェアを専門とするオペレーターもまた、機敏に動きます。彼らは、成功とは自分たちのやり方を捨て、別のやり方を生み出すタイミングを知ることだと理解しています。彼らは小規模で、レガシーというコレステロールを持たないため、迅速に行動することができます。その一方で、被害者は（時には無意識のうちに）時代遅れのテクノロジーを使い続け、セキュリティ対策に注力できず、チームはランサムウェアを防止、特定、管理するために必要なトレーニングを受けていません。これらの企業がサイバー脅威に対応する場合、その行動は限られており、タイタニック号のデッキチェアを並べ替えるのと同じようなものです。

また、ランサムウェアを深く理解したテクノロジーパートナーが、迅速かつ効果的に問題に対処し、お客様のビジネスを安全に保つことができることを示すことで、本資料がお客様の安心につながることを願っています。

Mahendran Chandramohan
BU Head – MDR
SISA Information Security Pvt. Ltd.

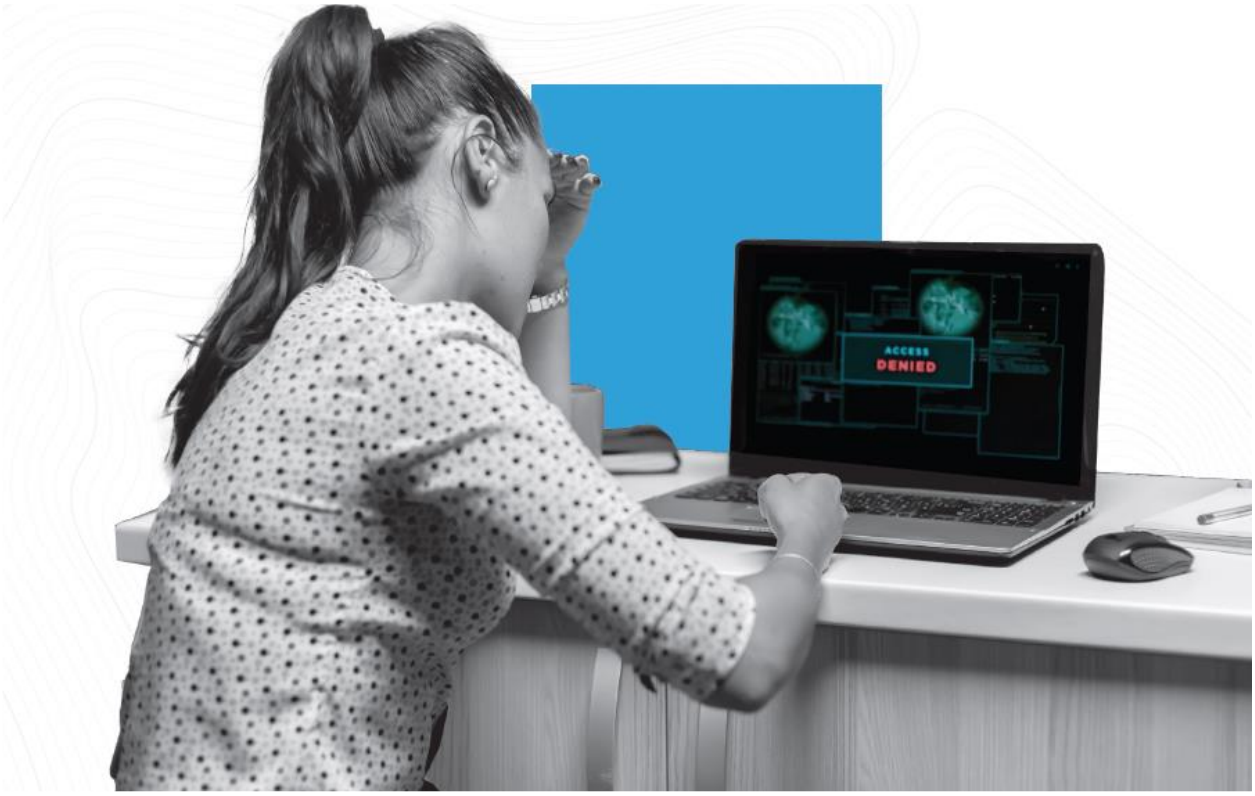
はじめに

ランサムウェアが存在する理由は、あなたのビジネスにある

11 秒に 1 回起きているランサムウェア攻撃[1]。それがもたらすニュースは、組織に眠れぬ夜をもたらします。2021年7月のIDC（International Data Corporation）のレポート「IDC's 2021 Ransomware Study：Where You Are Matters！[2]」によると、世界の組織の 3 つに 1 つは、過去 12 カ月間にランサムウェアの攻撃または侵入を経験しています。さらに悪いことに、ランサムウェアの被害に遭った組織のうち、身代金を支払わなかったのはわずか 13%でした。それ以外はすべて支払ったのです。例えば、米国最大の石油精製品のパイプラインシステムである Colonial Pipeline は、ビットコインで 440 万ドルの身代金[3] を支払い、東海岸と米国南部のいくつかの地域で一時的に燃料配送を停止することを余儀なくされました。世界最大の食肉業者である JBS は、身代金として 1,100 万ドルを支払いました。

ランサムウェアの脅威は拡大しています。2018 年、ランサムウェアの標的の 71%は中小企業[5]で身代金の平均要求額は 11 万 6,000 ドルでした。明らかにこの 3～4 年で、ランサムウェア集団はより大胆になっています。米国財務省の報告によると、2021 年上半期のランサムウェア関連の活動は 5 億 9000 万ドルで、前年の 4 億 1600 万ドルを上回っています[6]。

このデータは、緊急に何らかの介入する必要性を物語っています。サイバー犯罪者は、より大胆になっただけでなく、より巧妙になっています。彼らは常にゲームを改善し、検出を回避し、犯罪を逃れています。組織は無力です。最新のランサムウェアの脅威がもたらす課題に直面するための十分な準備ができていないのです。



ランサムウェアのビジネス

ランサムウェア・アズ・ア・サービス(RaaS)のエコシステム

ランサムウェアはここ数年、新鮮なビジネス色を帯びてきています。ランサムウェアの攻撃に関する専門知識は、Ransomware-as-a-Service(RaaS)というビジネスモデルの創造につながりました。
ランサムウェア攻撃を仕掛けるための既知の能力とツールを持つグループは、彼らの顧客から報酬が支払われます。
このような能力には、チーム内の開発者、システム管理者、ペンテスト、ホスティング、自動キーロガー、スニッファー、盗まれた認証情報のライブラリなどのアセットが含まれます。RaaS グループは、身代金支払の一定割合を取得します。

エコシステム全体が、高収益をもたらすランサムウェア産業の歯車を回し続けているのです。例えば、FIN7 は、ネットワーク侵入の専門家を雇う目的で、「Bastion Secure」という名前の偽のペンテスト会社[7]を運営していたと考えられています。

RaaS の顧客(すなわちランサム攻撃を仕掛けたい者)リストには、政府、企業体、悪意のあるダークウェブ関係者が含まれる可能性があります。RaaS は SaaS に似ており、顧客は手に入れたものに対して対価を支払います。顧客は技術的な能力を必要とせず、RaaS オペレーターはターゲット・インフラに侵入するためにツールやコードを調整しします。すなわち顧客は RaaS が持つ様々な能力を手に入れることができるのです。

典型的な RaaS 事業者は、ダークウェブ上で自社のサービスを宣伝しています。今日のｅコマースプラットフォームのように、RaaS サービスの顧客は、RaaS オペレーターに対するレビュー、成功率、経験を見ることができます。

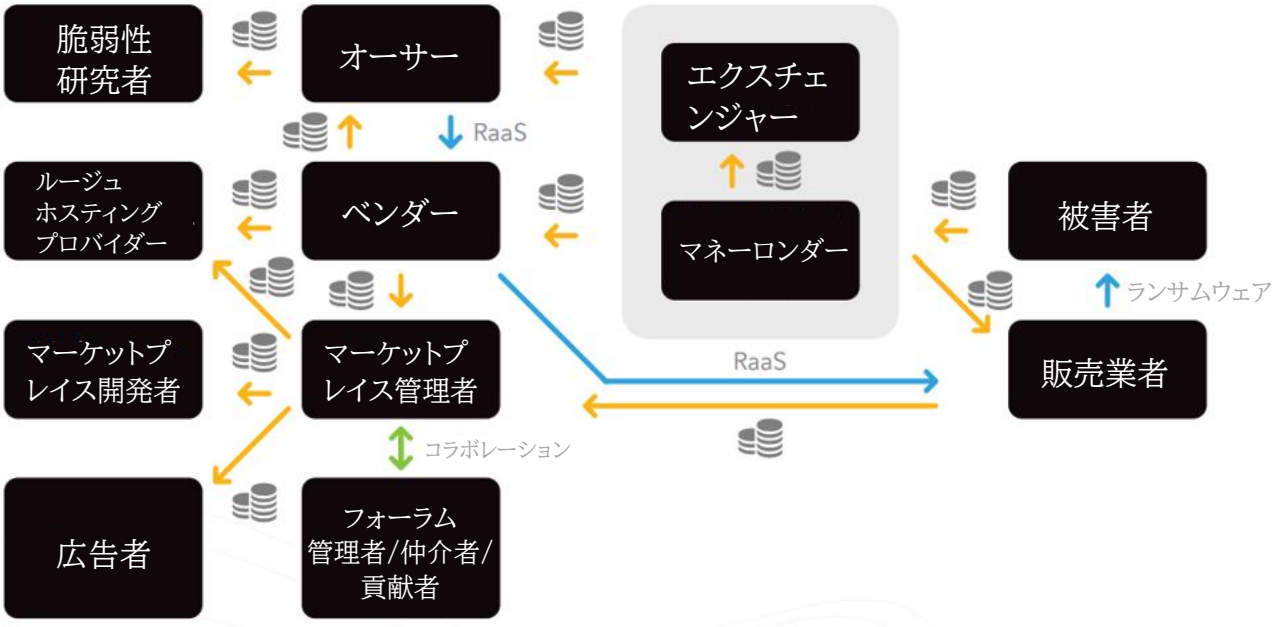
このレビューは、RaaS オペレーターが、コードを購入またはリースする低レベルのハッカー、クラッカー、ブラック ハット、およびフリークとのアフィリエイトおよびチャネルのネットワークを構築するのに役立ちます。これらのアフィリエイトは、独自の攻撃を開始したり、RaaS オペレーターに代わって独自の最高品質のランサムウェアを使用して攻撃をしたりする可能性があります。

アフィリエイトは、ツール、カスタムエクスプロイトコード、インフラ、サポート、攻撃キャンペーンを開始し進捗を監視するダッシュボード、身代金交渉人、および RaaS オペレーターの匿名身代金支払いポータルにアクセスすることができます。ターゲットが感染し、キャンペーンが成功したと宣言されると、身代金の要求が行われます。事実上、RaaS の有料モデルは、攻撃者が自らコードを書き、独自の手口を作らなければならなかった時代に終止符を打ったのです。

RaaS のバリューチェーン

RaaS は、ダークネットマーケットプレイスを通じて提供されるフランチャイズとなっており、意欲的なサイバー犯罪者がランサムウェア経済に参加することを可能にしています。RaaS 経済に関与するステークホルダーやアクターは、さまざまな責任を負い、さまざまな種類のリスクにさらされています。ResearchGate の調査によると、RaaS のバリューチェーン（下図）は、複数の事業者が複雑に絡み合った網の目のようなもので、それぞれが高度に専門化し、異なる一連の業務を行っていることが分かっています。

Figure 1 - RaaS バリューチェーン



これに関わる様々なアクターとその役割については、以下の通りです。

脆弱性研究者

脆弱性研究者は、ゼロデイ脆弱性の情報を発見し、悪用コードを書くことができる人に販売します。彼らは、ハードウェアとソフトウェアに関する高い専門性を持っています。

オーサー

オーサーは、脆弱性を利用したマルウェアを作成する開発者であり、その一部は脆弱性研究者から購入したものです。オーサーは、ダークネット上で自らを晒すことはほとんどなく、むしろリスクを取ることを他人に委託する一方で、身代金額のかなりの部分を収穫しています。

ベンダー

ベンダーは、マーケットプレイスや自分のプライベートなウェブサイトでマーケティングや販売を行います。ベンダーはオーサーである場合もありますが、ダークネットのベンダーの大半は、プログラミングの知識がほとんどなく、デジタル商品とは限らない幅広い商品を販売しています。

販売業者

販売業者が RaaS を購入・入手し、被害者の端末に感染させます。

被害者

ランサムウェアに感染し、データを失うか、身代金を支払うか（またはその両方）を迫られます。

マーケットプレイス管理者

ベンダーやディストリビューターが取引に利用できるマーケットプラットフォームを提供します。

マーケットプレイス開発者

管理者のためのマーケットプレイスプラットフォームを開発する技術的専門知識を有する者。高いセキュリティ能力が要求されます。

広告者

ダークネットのリンクを表のウェブに掲載し、そこから発生する取引に成功した場合にキックバック金を受け取るマーケットプレイスのアフィリエイト。例 DeepDotWeb。

フォーラム管理者/仲介者/貢献者

フォーラムのコンテンツと会員アクセスの管理を担当する人。通常、1 つまたは複数のマーケットプレイスの管理者と密接な関係を持ちます。

ルージュホスティングプロバイダー

捕まるリスクを低減したダークネットでのウェブサイトホスティングサービスを提供します。

マネーロンダー

被害者から受け取った身代金は、仲介者、プロのマネーロンダリング業者または送金していることを意識していない誰かを介して送金されます。現代のランサムウェアの実行者は、その利益を有名なビットコイン・ロンダリング・オペレーションを通じて直ちに洗浄する傾向があり、彼らはそのサービスに対して手数料（約 2.5%）を取ります。

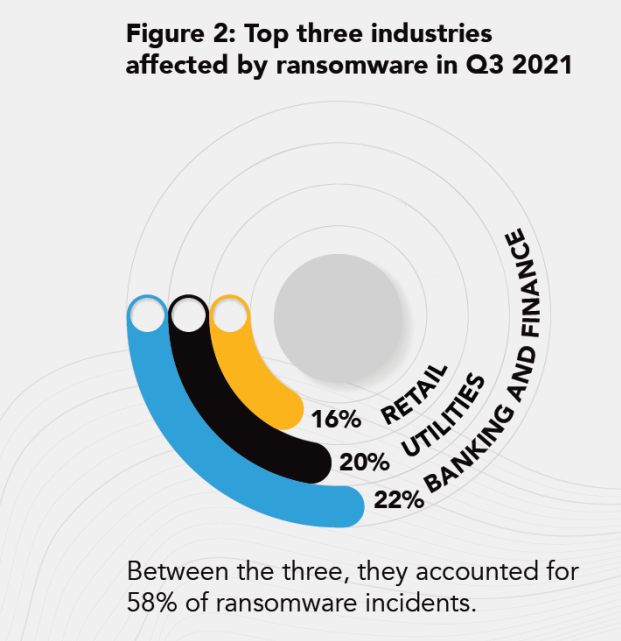
エクスチェンジャー

交換業者は検証済みのアカウントを所有し、その耐性を利用してサイバー犯罪者に通貨交換サービスを提供します。

ターゲット

RaaS のモットー：誰も逃すな

ランサムウェアの脅威に最も脆弱な業界は、サイバー犯罪者にとって最も報酬が高い業界、または最も侵入しやすい業界であることは、言うまでもありません。Trellix[8]（旧 McAfee Enterprises および FireFly）による調査では、どの業界も安全ではありません。



2021 年第3四半期にランサムウェアの影響を受けたトップ3インダストリー
RETAIL ＝ 小売業
UTILITIES ＝ 電気・ガス・水道などの公共事業
BANK AND FINANCE ＝ 金融機関

- 2021 年 3 月、台湾の電子機器大手エイサーがランサムウェアによって過去最高額の 5000 万ドル[9]の被害に遭いました。同社が身代金を支払ったかどうかは不明です。
- ドイツのデュッセルドルフ大学クリニック[10]で、ランサムウェア攻撃による治療の遅れが原因で患者が死亡する事故が発生しました。
- 米国のハワード大学では、ランサムウェアの攻撃を受けて、授業の中止を余儀なくされました[11]。
- フォーチュン 500 社の複数の企業を代理する著名な裁判事務所 Campbell Conroy & O'Neil は、最近、"ランサムウェア[12]による影響を受けた "と発表しました。

これらは、2021 年にランサムウェア攻撃を経験した組織の最近の例を無作為に抽出したものです。これらは、大小を問わず、すべての組織がランサムウェアに脆弱であるという、1 つの事実を指し示しています。ランサムウェアの被害に遭うのは、確率の問題ではないかもしれません。 組織がそのような攻撃を防ぐための適切な措置を講じない限り、それは時間の問題かもしれません。

リーダー

RaaS の伝説：最恐リスト

ランサムウェア攻撃の背後にいるグループ（「ギャング」と言う人もいます）は、まるでシスの暗黒卿 [13]（あるものは DarkSide とさえ呼ばれている）[14] のようです。これらのグループは、優秀で、カルト的な支持者を持ち、非常に恐れられています。彼らはよく組織化され、正式な管理構造を持ち、日常的に報道声明を出し、広報に長けていいます。2020 年、DarkSide は 2 つの慈善団体に 1 万ドル分のビットコインを寄付しました [15]。ランサムウェアグループが CSR に似た目標を持つとは、誰が想像したことでしょう。

ランサムウェアのグループは流動的です。変幻自在、突然変異、合併、消滅、そしていくつかは復活を遂げます。最も恐れられているグループのリストは、専門によって異なりますが、実質的にすべてのリストに含まれている名前もあります。

LockBit: LockBit は、現在、世界で最も多発するランサムウェアであり、2022 年 3 月から 8 月の間のこのグループによる感染数は、次に近い4つの競合の合計よりも多い 430 件に達しています [16]。このグループは、二重の恐喝をプレイブックに取り入れて以来、手ごわい脅威となっており、2022 年 1 月にフランスの法務省に対する攻撃の成功を得て以来、この戦術に傾倒していると報告されています。2022 年第 2 四半期には、ランサムウェアのデータ流出サイトに掲載されるインシデントの 32.7%を LockBit が占めています [17]。LockBit のメンバーは、大規模なターゲットに対する知名度の高い感染を自慢することで、自分たちの名前を広めようとするのではなく、比較的目立たないようにすることを選択し、その結果、他のランサムウェアのメンバーが集めた、警察や政府の不要な注意を避けてこられました。

Conti（aka IOCP Ransomware）: サイバー犯罪シンジケート Conti は、最も攻撃的なランサムウェアの運用を行っており、関連組織が 1 カ月余りで 40 社以上をハッキングするほど、高度に組織化されています [18]。2022 年 3 月、FBI は Conti が全世界で 1,000 件以上の攻撃に関与していると発表しています [19]。Conti は、ブロワード郡公立学校への攻撃の犯行を主張し [20]、4000 万ドルというセンセーショナルな金額を要求しています。5 月には、Conti はコスタリカ政府を崩壊させると脅し [21] Rodrigo Chaves 大統領は、このサイバー犯罪者集団と「戦争中」であると発言しました。2022 年 5 月に一味は活動を停止し、その後、小さなセルに分散していったと考えられています。

BlackCat: BlackCat ランサムウェアグループ、別名「ALPHV」は、プログラミング言語 Rust で作成されたランサムウェアファミリーで、暗号化、データ盗難、サービス妨害（DoS）、嫌がらせを活用し、被害者に支払いを迫っていわゆる「四重の強要」を実践する急成長中の RaaS（Ransomware as a Service）地下組織の 1 つです。BlackCat は少なくとも 2021 年 11 月から活動を開始し、2022 年 1 月にはドイツの燃料会社 OilTanking GmbH を、2022 年 2 月には航空会社 Swissport に対して大規模な攻撃を仕掛け、最近では米国の防衛関連企業 NJVC[22] をハッキングしたと主張しています。RaaS アフィリエイトへ身代金の 90%もの報酬を支払う手厚い対応により、アンダーグラウンド市場における主要な競争相手となりつつあります [23]。

REvil（別名：Sodin または Sodinokibi）：GandCrab の開発者が設立したとされる REvil は、2021 年上半期のランサムウェア攻撃の 13.1%を占めています。REvil は、Tata Steel[24] を標的にし、Apple のサプライチェーンに含まれるメーカーである Quant[25] から技術設計を盗み、米国に拠点を置く宇宙開発企業 HX5[26] を攻撃し、IT サービス企業 Kaseya の信頼できる分散メカニズムを使用して広範囲なサプライチェーン攻撃を指揮するなど、いくつかの実績があります。2021 年 10 月に主要メンバーの逮捕や複数政府による作戦を経て活動を停止しましたが、2022 年 5 月にグループのリークサイトが再稼働し、活動を再開したと伝えられています。

Grief: 2019 年、DoppelPaymer という RaaS グループが出現し、その被害者は教育機関、医療機関、政府などでした。2020 年、DoppelPaymer は COVID-19 のパンデミックの最中、人工呼吸器 [27] のメーカーである米国の Boyce Technologies Inc.を無慈悲に攻撃し、数千人の命を危険にさらしました。この RaaS グループは、Grief として再ブランド化されたと考えられています。その根拠は、DoppelPaymer と Grief が同じ暗号化ファイル形式を共有し、同じ流通経路を使用していることにあります。Grief の地下リークサイトに掲載されている企業の半数以上は、イギリスとヨーロッパに拠点を置いています[28]。Grief ランサムウェアギャング は、その手口を変えたようで、以前はホットターゲットであった米国よりも、英国や欧州の企業や公共団体をより多くターゲットにしています。

CLOP：CLOP は、2021 年に企業とそのパートナーのデータを取得し、その企業のパートナーに対して被害企業に身代金の支払いの通知を郵送するよう促したことで話題を集めました（CLOP がパートナーのデータをダークウェブで公開すると脅したためです）。
Royal Dutch Shell[29]、航空機メーカーBombardier[30]、アメリカの銀行 Flagstar[31]、ハワイ最大のスーパーマーケットチェーン Foodland[32] などが CLOP 攻撃を経験しています。CLOP が最も標的としたのは工業部門であり、CLOP ランサムウェア攻撃の 45%は工業企業を、27%はハイテク企業を標的にしています。2021 年、CLOP のメンバー6 人がウクライナのサイバー警察によって逮捕されました [33]。

Figure 3: トップギャング

オペレーション

戦術・技術・手続きのインサイドトラック（TTPS）

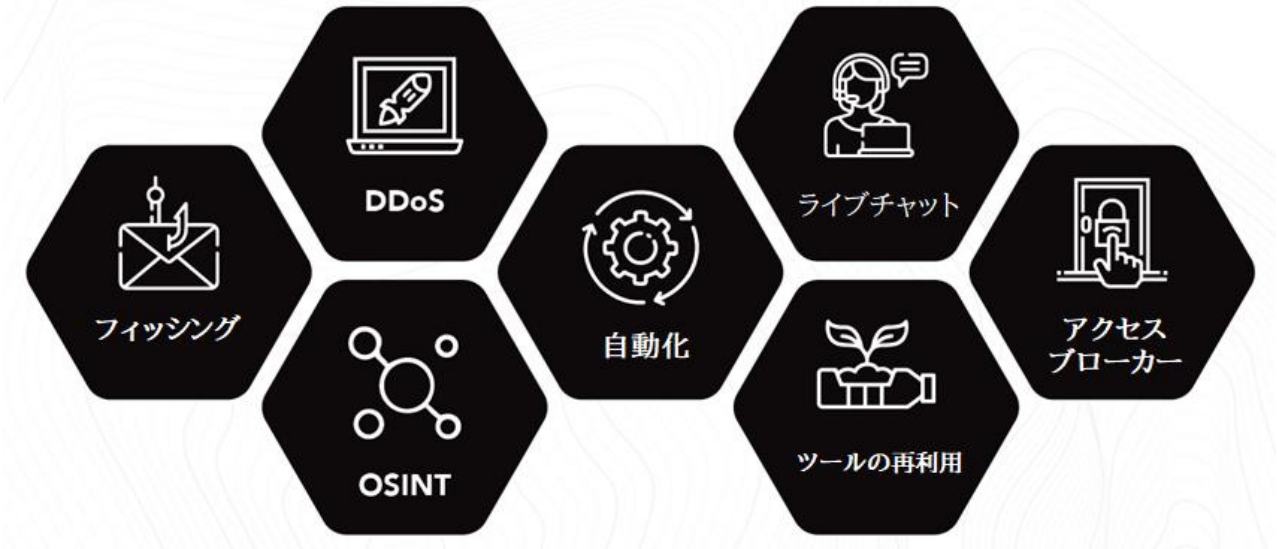
ランサムウェアギャングの積極的な活動は、ランサムウェア攻撃の急増に拍車をかけている重要な要因であり、彼らはより大きな報酬を得るために新しい技術を考案し、協調したキャンペーンを実施し、カルテル化したオペレーションを実行しています。複雑なベクトルと独自の戦術を駆使して、これらのギャングたちはランサムウェアの状況を再構築し、コモディティスタイルの乱射攻撃から、より対象を絞り込み、破壊的なインパクトを与える攻撃に移行しつつあります。しかし、ランサムウェアの集団は、具体的にどのように攻撃を指揮し、どのような重要な手段を用いているのでしょうか。フィッシングやDDoS、カスタムツールの使用、自動化、ライブチャットなど、さまざまな方法があります。

ツールの再利用：あるランサムウェア集団は、イランの MuddyWater などの他の APT グループが開発したカスタムツールを再利用し、盗んだ認証情報を使って被害者のネットワークに不正にアクセスしたと報告されています。

フィッシング：フィッシングは、ランサムウェア攻撃を仕掛けるための最も一般的な方法です。
攻撃側の専門家がユーザーの行動を調査し、ソーシャル・エンジニアリングを駆使して、標的の組織や組織のシステムから情報（パスワードや製品/顧客/パートナーのデータなど）を盗み出すことを目的とした攻撃を仕掛けるのです。

攻撃側の専門家は、正規に見えるソースを偽装した電子メールを送信します。しかし、そのメールには、悪意のあるファイルや悪意のあるファイルへのリンクが含まれています。

Figure 4: ランサムウェアギャングの戦術、テクニックおよび手段



このファイルは、ターゲット組織のシステム内でランサムウェアを密かに起動し、資金の起源の痕跡をすべて消してしまいます。

システムが十分に無力化されるとランサムウェアは追加のコードをダウンロードし、データを取得する作業を開始します。

ランサムウェアは、追加のコードをダウンロードしてデータを取得する作業を開始することができます。データは、所有者がアクセスできないように暗号化されるか、または RaaS オペレーターのストレージインフラに送られるかのいずれかです。

RaaS オペレーターがデータを取得した場合、被害者に対して、復号キーの提供やデータの削除を行うための身代金が要求されます。また、RaaS オペレーターがデータを取得した場合、RaaS 事業者がデータの公開やダークウェブでの販売、競合他社への販売などを意図していることが脅威となる場合があります。

ランサムウェア攻撃の被害者は、ダークウェブサイトからブラウザをダウンロードし、それを使って指定されたゲートウェイで支払いを行うための詳細な情報を RaaS オペレーターから提供されます。支払いは、追跡が困難な暗号通貨で要求されることがほとんどです。RaaS 事業者は、身代金の出所の痕跡を消すために、委託した洗浄業者に身代金を送ることもあります。

DDoS と OSINT:ランサムウェアグループの強奪手法は進化を始めています。彼らは、かつて標準的なスタイルであった復号化のための支払いモデルを超えています。その多くは、信頼できる分散型サービス妨害(DDoS)攻撃に頼る一方、盗んだデータをダークウェブで公開し、被害者を名指しで貶めるような脅しをかけるものもあります。一方、REvil は、オープンソースのインテリジェンス(OSINT)を使用して、被害者の上級役員や顧客[35] を追跡し、まさにその上級役員や顧客を使って支払いを強要する説得力のあるキャンペーンを展開しています。

アクセスブローカー: ランサムウェア業界は、アクセスブローカーにも依存し始めています [36]。アクセスブローカーは、ターゲットとなりうる環境をスキャンして脆弱なデバイスを探し出し、ランサムウェア集団のためにオープンなバックドアを残します。アクセスブローカーは、このアクセスをダークネットで宣伝し、興味を持ったランサムウェアグループに情報を売り、悪用させます。

自動化:攻撃の速度と量を増加させるために、ランサムウェアグループは、システムに侵入するために自動化されたボットを使用するようになりました。一部のグループは、Wake-on LAN 機能を使用して、ランサムウェアのペイロードを自動的に注入できるホストを検出しています。

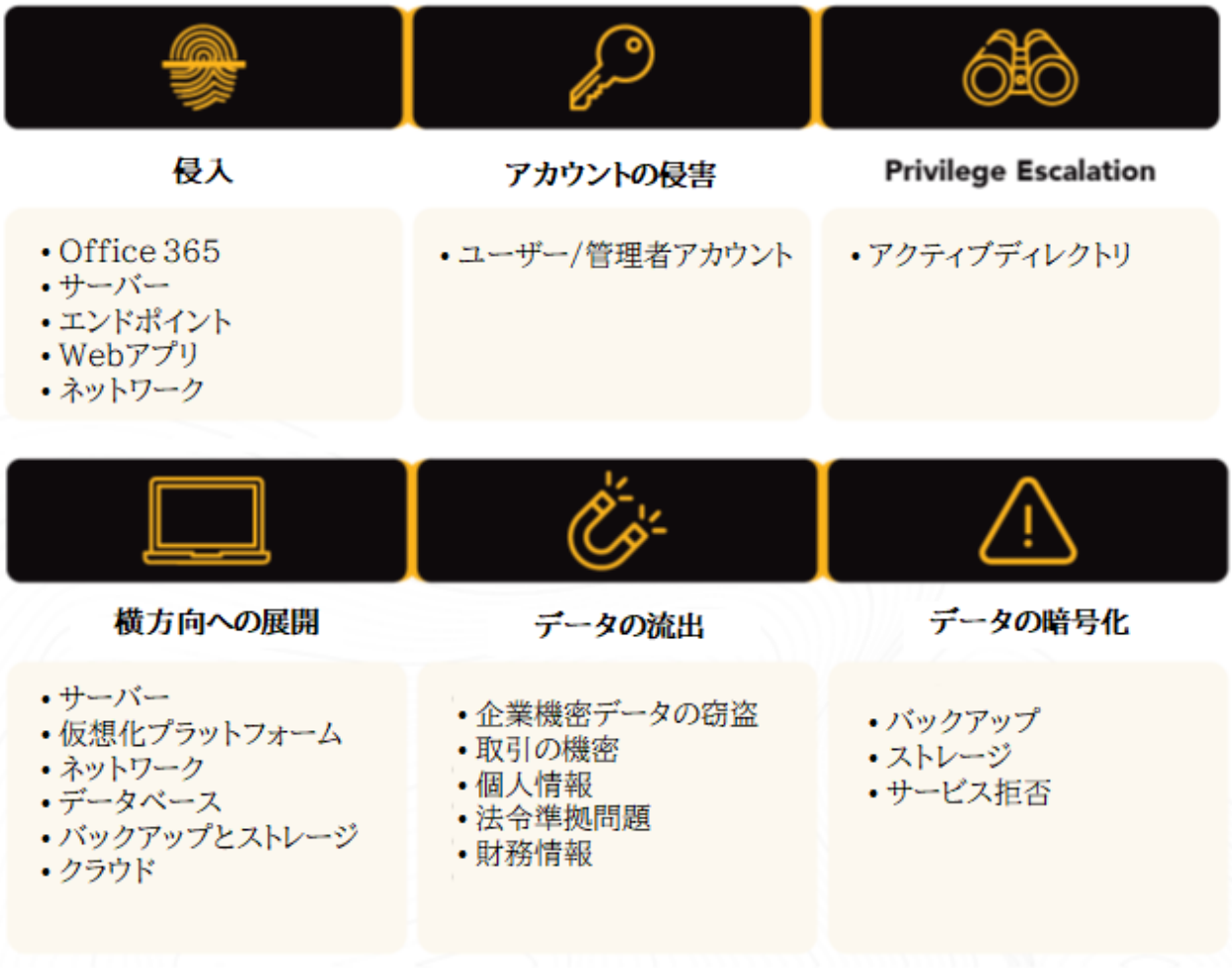
ライブ チャット: Hive ギャングは、確立された手順に興味深いひねりを加えて「営業部門」にリンクされた身代金メモを使用します。 被害者は、有名なカスタマー サービスを模倣したライブ チャットを介して身代金を支払うために「営業部門」とやり取りすることになります [37]。

ライフサイクル

ランサムウェアの攻撃を解読

企業や組織は、ランサムウェア攻撃のライフサイクルを理解し、インシデントへの備えを向上させる必要があります。ランサムウェアはいくつかの段階に分かれた問題であり、どの段階においても攻撃を効果的に封じ込めるためには、各段階に応じたソリューションが必要です。典型的なランサムウェアの攻撃は、6 つの明確な段階を経ており [38]、それぞれの段階を解析することは、組織の準備と対応戦略の強化に役立ちます。

Figure 5: ランサムウェアのライフサイクル



潜入： 最初の段階は、攻撃者がシステムに侵入することです。これには、フィッシング・メールの送信、悪意のあるウェブサイトの開設、RDP（リモートデスクトップ）接続の弱点の悪用、ソフトウェアの脆弱性への直接攻撃、ゼロデイ・エクスプロイトの採用など、いくつかの方法があります。一般に公開されている Web アプリケーションや、VPN や RDP などの脆弱性を持つネットワーク機器が悪用され、ネットワークに侵入される。この段階では、サーバーやエンドポイントも影響を受けます。

アカウントの不正アクセス：侵入が完了すると、次の段階として、アカウントが侵害されます。不正アクセスは、ローカルユーザーや管理者アカウントが侵害された場合に発生し、一般的には、組織全体で同じローカルパスワードと管理者パスワードが適用されている場合に起こります。

悪意のあるコードは、攻撃者とつながるコミュニケーションラインをセットアップします。ランサムウェアの攻撃者は、このコミュニケーションラインを使用して追加のマルウェアをダウンロードすることができます。この時点で、ランサムウェアは、攻撃者が攻撃を開始するまでの間、数日、数週間、または数ヶ月間、隠れた状態で休眠状態になる可能性があります。多くの場合、企業や組織はシステムが侵害されていることに全く気付かず、攻撃者は攻撃を開始する最適なタイミングを見計らいます。

Privilege Escalations：ランサムウェアの攻撃サイクルにおける第 3 の段階は、privilege escalation 攻撃です。これは、セキュリティ境界内のシステムに不正にアクセスするために使用されるネットワーク攻撃の一種です。この攻撃を実行するために最も悪用されるサービスは、Active Directory です。

Active Directory は、一般的に「王国への鍵」と呼ばれています。Active Directory（AD）が侵害されると、攻撃者はドメイン管理者/エンタープライズ管理者の資格情報にアクセスできるようになり、ランサムウェアの実行者がネットワークにさらに侵入することが容易になります。AD の侵害を防ぐには、効果的な検知メカニズムが非常に重要です。Privilege Access Management（PAM）ソリューションと効果的なエンドポイント検出および応答（EDR: Endpoint detection and response）ツールを導入することは、AD の侵害を防ぐのに役立ちます。

横方向への展開：Privilege Escalation 攻撃に成功すると、ランサムウェアの実行者は、横方向への展開の実行に移行します。彼らは、サーバー、仮想プラットフォーム、データベースなどの環境内を自由に移動し、クラウドやバックアップ・ストレージなどにアクセスできるようになります。デジタル資産内での権限と駐留を獲得すると攻撃の最終段階へと進みます。最近のランサムウェアには、保存されているパスワードを自動的に検索し、ネットワーク上に拡散させる機能が組み込まれています。より洗練されたランサムウェアは、環境ごとに異なる特徴を持つように設計されており、シグネチャが常に変化するため、従来のソリューションでは検出が難しくなっています。

データの流出：攻撃の第五段階は、データの窃盗と恐喝を組み合わせたデータの流出です。

ランサムウェアの攻撃者は、企業や組織の防御力を低下させ、財務記録、知的財産、企業秘密、ビジネスデータなど価値を持つ機密データを流出させます。

ダークウェブ上でデータを売りに出し、その価値を確認した後、攻撃者は被害者に連絡し、売られないように支払いを要求します。

この場合、攻撃者は、データの公開によって生じる大きな風評被害、規制当局のファイル、およびその他の影響力を利用します。

被害組織から身代金を引き出した後、ランサムウェアの実行者が被害者の顧客に接触して身代金を要求するという、三重の恐喝が蔓延している危険なトレンドがあります。

データの暗号化：キルチェーンの最後の段階は、データの暗号化であり、脅威者は被害者の機密資産を盗んで暗号化し、金銭を脅し取ります。従来、ランサムウェアは被害者のデータを暗号化し、身代金と引き換えに復号化キーを渡していました。しかし、最近では、ランサムウェアのキャンペーンにおいて、被害者のデータを流出させると恐喝することが一般的になっています。この方法は、被害者がファイルへのアクセスを回復し、かつデータの漏洩を防ぐという 2 つの理由で身代金を支払うことができるため、一般的ま手法になってきています。

現状維持

ランサムウェア対策の現状

アナリスト、政府機関、メディアなどのデータによると、ランサムウェアのインシデントが増加しており、対策の不十分さを示しています。ランサムウェアグループは、自動化、人工知能（AI）、機械学習（ML）などの高度な技術を駆使して脆弱性を突いています。敵対的生成ネットワーク（GAN: Generative Adversarial Network）技術を用いたパスワード推測 [39] のディープラーニングアプローチが優れてきており、フィッシングを冗長化させています。これに対し、企業や組織は、防御メカニズムをスピードアップさせることができていません。

チェック・ポイントのモバイル・セキュリティに関する最新レポート [40] によると、46%の組織で、少なくとも 1 人の従業員が悪意のあるモバイル・アプリケーションをダウンロードしており、世界のモバイル・デバイスの少なくとも 40%は、本質的に攻撃に対して脆弱であると言われています。IoT 機器もまた、攻撃対象領域を拡大させています。インテリジェントな攻撃者は、サプライチェーンを利用して、悪意のあるコードを流通、製造、保守の各システムに導入し、そこから活動を開始します。

Go や Rust[41] のような新しい、そして難解な言語が台頭しています。これらの言語は、ランサムウェアがプロセス、機能、パフォーマンスを向上させるために使用することができます。RaaS グループにとって、これらの言語にはいくつかの利点があります。第一に、サイバーセキュリティの専門家はそれらに馴染みがないこと。第二に、分析ツールが入手しにくいため、攻撃者が発見されずに済む時間が長くなることです。

サイバーセキュリティは、企業や組織の課題として低いものではありませんが、より焦点を絞る必要があります。多くの場合、課題は予算ではなく、アプローチにあります。このことは、企業の役員に就任している CISO（最高情報セキュリティ責任者）がわずか 4 パーセントであるという事実からも明らかです [42]。

2020 年、サイバーセキュリティの専門知識を持つ取締役は、欧州では 6%、米国では 8%に過ぎません。世界の他の地域の数字も良くないと考えた方が無難でしょう。良いニュースもあります。ガートナー社は、2025 年までに 40%の取締役会がサイバーセキュリティの専門委員会を設置すると予測しています [43]。もし、あなたの会社や組織が取締役会に CISO を配置している、または、配置を検討しているのであれば、ランサムウェアのインシデントに備えるためのより良い道をすでに歩んでいると言えるでしょう。

ランサムウェアは、通常追跡不可能な暗号通貨を要求します。最悪のシナリオに対応するために、暗号通貨のウォレットを取得することは、組織の標準的な手法になるでしょう。暗号通貨ウォレットを導入している企業や組織は、すでに正しい方向に進んでいると言えるでしょう。攻撃された場合、組織はバックアップデータ、リストア、設定、および検証ツールに頼りたいはずです。ここでも、組織が最新の復旧ツールに投資していれば、正しい道を歩んでいることになります。

ランサムウェア攻撃への備えを示す確実な指標は、ランサムウェアに対する保険への投資とコミュニケーションプランの 2 つです。もし、あなたの組織がサイバー保険に加入しておらず、ランサムウェア攻撃時に使用するコミュニケーション戦略を持っていないなら、その組織は準備が不十分であることが分かります。

最後に、”エンドポイント、電子メール、IoT デバイス、ネットワーク、バックアップインフラ（オンプレミスおよびクラウド、エアギャップ、イミュータブルコピー）、データ、IAM に対して、私の会社や組織がどの程度のセキュリティ制御を行っているか？”という質問を投げてみましょう。この質問に対する答えが、セキュリティ投資への注力を後押しすることになります。

アクション

備えあれば憂いなし

ランサムウェアの急速かつ絶え間ない進化は、企業や組織が油断することができないことを示唆しています。したがって、ランサムウェアの脅威に対処するためには、多層的な「保護と検知」のアプローチを採用する必要があります。

このアプローチには、Active Directory、バックアップ、ネットワーク、クラウド、Office 365 といった 5 つのインフラ層の保護が含まれます。

これら 5 つのサービス層は、他のサービス層よりも緩和策を適用した場合の影響が大きいことを考慮して優先順位が設定されています。

Active Directory：Active Directory をランサムウェアの脅威から保護するには、MFA（多要素認証）を有効にすることが重要です。強力なパスワードの複雑さと長さ、パッチ適用とソフトウェア・アップデート、ネットワークの暗号化など、基本的なサイバー攻撃予防策に従うことは、効果的な保護策となり得ます。OS の硬化、最小権限アクセスとジャストインタイムアクセスによる権限アクセス管理、バックアップの 3-2-1 ルール（3つのバックアップコピーを 2 つの異なるストレージ媒体に保存し、少なくとも 1 つのオフラインコピーを維持する）なども有効な対策となります。ランサムウェアの検出については、リスクと問題を事前に診断し、ギャップを埋めるための最適手法を提案するマイクロソフトの Active Directory セキュリティのオフライン評価（OAADS）を受けることが推奨されます。次に、ゴールデンチケットを迅速に検出する能力を備えた堅牢なセキュリティ監視ツールを導入することが不可欠です。最後に、定期的なコンプライアンス監査、脆弱性スキャン、侵入テストを実施することで、異常の早期発見につながります。

Active Directory のセキュリティは非常に重要です。これらのアクションとベストプラクティスは、組織が使用するすべてのディレクトリサービスに適用できることに留意することが重要です。

ネットワーク マイクロセグメンテーションは、侵入者の横方向展開を効果的に阻止することができる重要なセキュリティ対策です。

また、経路ドメインの分離、役割ベースのアクセス制御（RBAC: Role-Based Access Control）の実装、侵入防御システム（IPS）の導入、エアギャップ・インフラの開発などの対策も、ランサムウェアの侵入からネットワークを保護するために有効です。効果的な検知のためには、SSL トラフィックの復号化、Web フェイシングデバイスの最小限のアクセス設定、効果的な SIEM（Security Information and Event Management）ツールの導入などの対策が強く推奨されます。

Figure 6: 5層の「防御と検出」アプローチ

リカバリーとバックアップ：バックアップ環境の攻撃対象領域を減らすには、セキュリティ対策の組み合わせが必要です。3-2-1 ルールに従うことは、そのような対策の 1 つです。また、ライトワンス（WORM :Write Once and Read Many Times）コピーの使用は、管理者アカウントであってもアクセスを困難にすることができるため、有効な手段です。強力なバックアップ保持ポリシーの導入、バックアップの暗号化、不変のバックアップコピーの使用、ホストや IP アクセスの制限なども、バックアップを保護するための標準的な最適手法と言えます。脅威を事前に検知するために、企業や組織は脆弱性スキャン、定期的なデータ復元テスト、コンプライアンス監査の実施を検討する必要があります。

Office 365: 効果的なメールセキュリティは、マルウェアを含んだ添付ファイルや URL、認証フィッシングサイト、何百万通ものメッセージに隠されたなりすまし攻撃など、最も危険なサイバー脅威を検知・ブロックする動的な防御機能を備えている必要があります。最適手法としては、EOP（Exchange Online Protection）への加入、専用の管理者アカウントの設定、データアーカイブ、MFA（多要素認証）などが挙げられます。

効果的な監視ソリューションを導入し、脆弱性スキャンを実施することで、検出率を向上させることができます。また、組織のセキュリティ状況を評価し、スコアを算出し、セキュリティ向上のためのアクションを推奨する分析ツールである Microsoft Secure Score を実行することも推奨されます。

さらに、オンプレミス、クラウドを問わず、あらゆるメッセージングサービスにこれらの措置を適用し、強固なメールセキュリティを確保することを推奨します。

クラウド：クラウドモデルが普及するとサイバー攻撃の格好のターゲットとなるため、企業はクラウドシステムを保護する方法と手段に注目しています。

最も簡単な方法は、MFA（多要素認証）、データマスキング、ID 管理など、組み込みの保護メカニズムを利用することです。ネットワークの暗号化、鍵の管理、条件付きアクセスポリシー、監査された管理者アクセスなども、組織がクラウド環境を保護するために導入できるコントロールです。

検知の観点からは、コンプライアンス監査や脆弱性スキャンを定期的に実施し、継続的に監視するためのツールを導入することが最適手法として挙げられます。

RaaS は決して眠りません。24 時間 365 日、積極的かつ継続的なセキュリティプロセスを計画します。データのバックアップや災害復旧計画を持っているだけでは、攻撃者がデータの公開や売却を計画している場合には役に立ちません。つまり、予防は治療に勝るのです。ランサムウェアに対抗できると思われることはすべて行いましょう。ML（マシンラーニング）や自動化など、AI の全分野を利用して、悪意のあるコードを調査し、関連付け、実行を防ぐ、インテリジェントで適応性のある防御システムを構築してください。

ほとんどの企業や組織がスタートラインに立つのに苦労しています。では、どこからランサムウェア対策に着手すればよいのでしょうか。

SISA が提供する SISA の推奨サービスは以下のようなものがあります。

ランサムウェア対策ラーニングセッション：SISA は、ランサムウェアのビジネスリスク、その影響、侵入時の事業継続を確保する方法について組織を教育することに焦点を当てた、対話型の 1 対 1 のセッションを提供しています。これらのセッションを通じて、運用レベルと戦略レベルの両方で敵の戦術に対する認識を高め、ランサムウェアのギャングの動作のニュアンスを理解し、従うべきガイドラインとベストプラクティスを確立することができます。

ランサムウェア防止監査/アセスメント：SISA のランサムウェア対策監査は、現在のセキュリティギャップ、コントロール、ソリューションを評価し、予防措置を講じたいと考えている組織向けにデザインされています。

4 段階の監査は、世界中の業界のベストプラクティスを満たすために NIST フレームワークを使用して実施され、以下の内容をカバーしています。

セキュリティーインフラ監査

レッドチーム演習（侵入、持続、横方向展開および活動のシミュレーション）

インシデント対応計画のレビュー

データバックアップとリカバリ手順のレビュー

ランサムウェアのシミュレーション演習：ランサムウェアのシミュレーションにより、企業は実際の攻撃環境でセキュリティ防御をテストし、その対応と修復の能力を評価することができます。

また、この演習は、攻撃者が使用する手法に対する従業員の意識を高めることにもつながります。SISA は、エンドポイントとネットワーク・サーバーの両方をカバーする 2 重のアプローチを採用し、360°の保護機能を提供します。SISA のランサムウェア・シミュレーション演習は、以下の内容をカバーしています。

現在のインフラの強さと迅速な対応体制の評価

ランサムウェア攻撃のライフサイクル全体にわたるインフラのテスト

ランサムウェアの攻撃者による実際の試み、使用されるペイト、セキュリティチームの対応などをシミュレート

ランサムウェアの攻撃者に対する防御を強化するためには、継続的な準備と学習が重要です。リスクを軽減し、被害を最小限に抑えるためには十分な準備が重要ですが、攻撃を阻止する保証はありません。SISA ProACT[45] のようなマシンラーニングベースの脅威ハンティング [44] ソリューションの導入は、検知・対応プロセスの立ち上げに理想的であり推奨されるものです。このソリューションは、当社のフォレンジックインテリジェンスを搭載し、拡張されたユースケースと実用的な脅威アドバイザリーを組み込んでおり、当社の主要なインシデントレスポンスおよびフォレンジックサービスをカバーしています。

ランサムウェア対策についてのお問い合わせは Fime Japan までお問い合わせください。SISA は Fime Japan のセキュリティービジネスパートナーです。

Email: salesjapan@fime.com

SISA のランサムウェア関連のページ（英語）

https://www.sisainfosec.com/cyber-resilience/ransomware-prevention-services/

参考文献等

1. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)
2. IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach
3. Colonial CEO says ransomware hackers exploited legacy VPN | Cybersecurity Dive
4. JBS Paid $11 Million to Resolve Ransomware Attack - WSJ
5. 71% of Ransomware Attacks Targeted Small Businesses in 2018 (healthitsecurity.com)
6. Financial Crimes Enforcement Network: Ransomware Trends in Bank Secrecy Act Data between Jan 2021 and June 2021
7. How are Ransomware Gangs Evolving their Expansion and Attack Strategy? (sisainfosec.com)
8. Trellix ATR Threats Report | January 2022
9. Taiwan's electronics giant Acer hit by record ransomware attack | Taiwan News | 2021-03-20 16:45:00
10. Hospital ransomware attack leads to fatality after causing delay in care | Healthcare IT News
11. Hit with ransomware attack, Howard University forced to cancel classes - ABC News (go.com)
12. Campbell Conroy & O'Neil Provides Notice of Data Privacy Incident – Campbell Conroy & O'Neil, P.C. (campbelltriallawyers.com)
13. Dark Force | Wookieepedia | Fandom
14. How ransomware groups like Darkside became professional - Tech Monitor
15. Mysterious 'Robin Hood' hackers donating stolen money - BBC News
16. LockBit gang leads the way for ransomware, Sep 8, 2022 (TechTarget.com)
17. Ransomware in Q2 2022: Ransomware is back in Business, July 11, 2022 (digitalshadows.com)
18. Conti ransomware hacking spree breaches over 40 orgs in a month, June 23, 2022 (bleepingcomputer.com)
19. Conti Ransomware | CISA
20. Ransomware gang wanted $40 million in Florida schools cyberattack (bleepingcomputer.com)
21. Conti Ransomware Gang Shutdown, Conti ransomware rebranding 2022 (cybertalk.org)
22. BlackCat ransomware gang claims to have hacked US defense contractor NJVC, Oct 2, 2022 (securityaffairs.co)
23. Aggressive BlackCat ransomware on the rise, Feb 1, 2022 (darkreading.com)
24. iTWire - Indian steel giant Tata Steel hit by Windows REvil ransomware
25. Apple Menaced After REvil Ransomware Attack Against Supplier | CRN
26. REvil cybergang hits HX5, defense contractor with Army, Navy, Air Force, NASA customers - Washington Times
27. Ransomware Reportedly Hits Ventilator Maker - BankInfoSecurity
28. Grief ransomware gang claims 41 new victims, Oct 18, 2021 (esentire.com)
29. After oil giant Shell hit by Clop ransomware gang, workers' visas dumped online as part of extortion attempt • The Register
30. Clop ransomware gang leaks online what looks like stolen Bombardier blueprints of GlobalEye radar snoop jet • The Register
31. 1.5m people's info stolen from Flagstar Bank in cyberattack • The Register
32. Notice of data breach Foodland Supermarket Limited., Coffee Pacific LLC., and Food Pantry Ltd.
33. Ukranian police nab six tied to CLOP ransomware - krebsonsecurity.com June 16, 2021
34. How are Ransomware Gangs Evolving their Expansion and Attack Strategy? (sisainfosec.com)
35. How are Ransomware Gangs Evolving their Expansion and Attack Strategy? (sisainfosec.com)
36. Ransomware-as-a-Service - Key Players, Tactics, and Prevention Strategies (sisainfosec.com)
37. How are Ransomware Gangs Evolving their Expansion and Attack Strategy? (sisainfosec.com)
38. Decoding the anatomy of a ransomware attack (sisainfosec.com)
39. PassGAN: A Deep Learning Approach for Password Guessing (arxiv.org)
40. Mobile Security Report 2021 by Check Point | Mobile Threat Defense | Check Point Software
41. FBI: This ransomware written in the Rust programming language has hit at least 60 targets | ZDNET
42. 2021 Global Chief Information Security Officer (CISO) Survey | Insights | Heidrick & Struggles
43. Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025
44.]Advanced Forensic Based Cyber Threat Hunting Services | SISA (sisainfosec.com)
45. Managed Detection and Response (MDR) Service to strengthen Cybersecurity (sisainfosec.com)

翻訳：Fime Japan

翻訳補助ツールとして DeepL Translator を使用