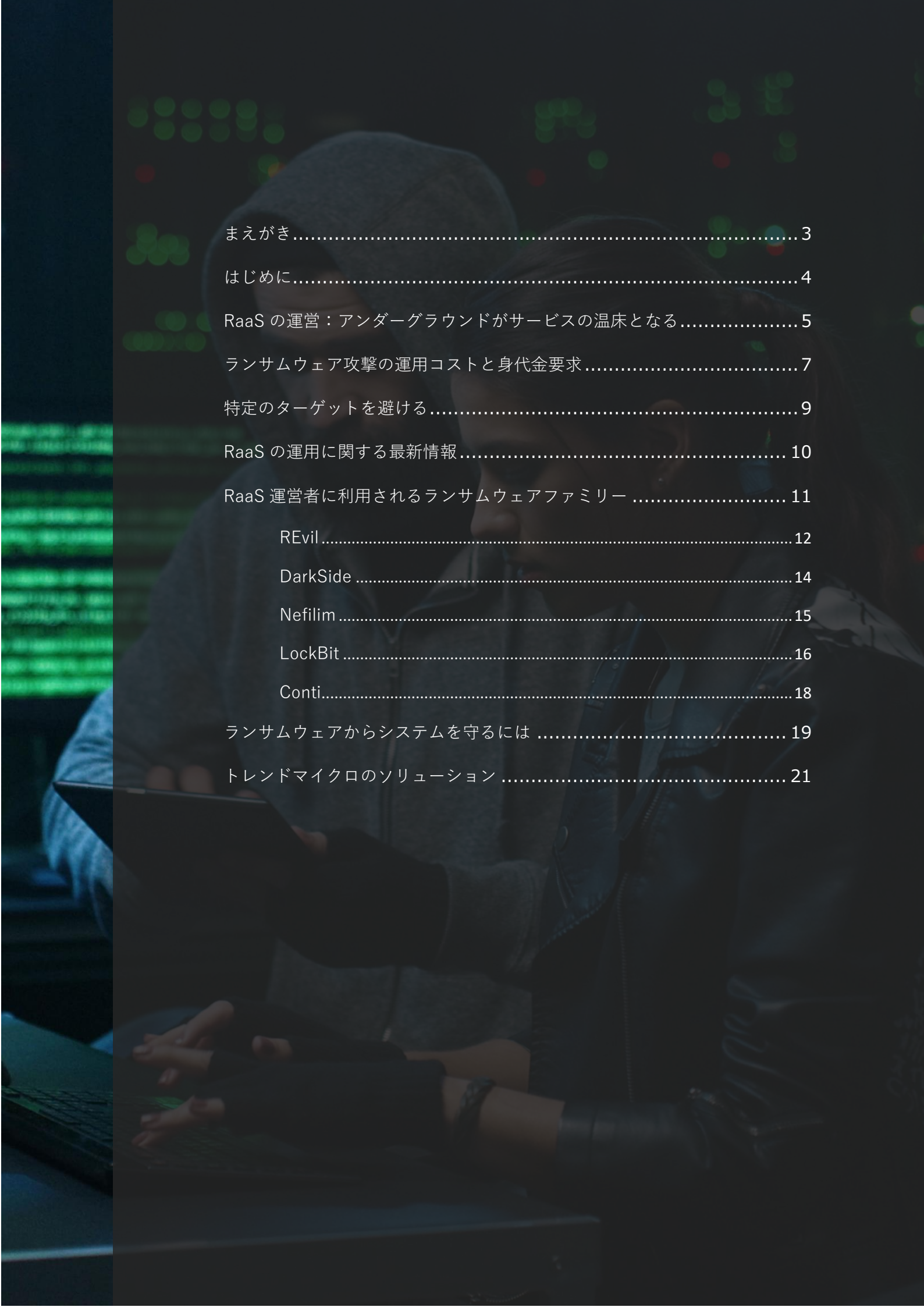
# 広範な攻撃を可能にするサービスとしてのランサムウェア（RaaS）

By Fyodor Yarochkin
Additional insights by Janus Agcaoili, Byron Gelera, and Nikko Tamaña

TREND MICRO | research




まえがき ..... 3

はじめに ..... 4

RaaS の運営：アンダーグラウンドがサービスの温床となる ..... 5

ランサムウェア攻撃の運用コストと身代金要求 ..... 7

特定のターゲットを避ける ..... 9

RaaS の運用に関する最新情報 ..... 10

RaaS 運営者に利用されるランサムウェアファミリー ..... 11

- REvil ..... 12
- DarkSide ..... 14
- Nefilim ..... 15
- LockBit ..... 16
- Conti ..... 18

ランサムウェアからシステムを守るには ..... 19

トレンドマイクロのソリューション ..... 21

# まえがき

サービスとしてのランサムウェア「Ransomware as a Service（RaaS）」を利用すれば、最低限の技術や知識しか持たない攻撃者であっても、攻撃を開始することが可能となります。このサービスが駆使されることで、ランサムウェアの脅威は、多くの標的を狙って速やかに拡散する事態を招いてしまいます。RaaS とはどのようなものであり、このサービスは、どういった種類のランサムウェアや手口を提供しているのでしょうか。

# はじめに

ランサムウェアの攻撃が急増している主な理由の 1 つとして、サービスとしてのランサムウェア「Ransomware as a Service（RaaS）」[1]の利用が挙げられます。RaaS とは、簡単に言えば、アフィリエイターと呼ばれる利用者向けにランサムウェアを販売・レンタルするサービスのことを意味します。

これまでのランサムウェアの攻撃は、ランサムウェアの作成および運営をこなす攻撃者自身が仕掛けるものが中心でした。しかし、RaaS が登場したことで、技術的な知識を持たない攻撃者でも自分たちが狙う対象に対して容易にランサムウェア攻撃を仕掛けることが可能になりました。

こうした中、トレンドマイクロでは、RaaS を提供する攻撃グループが組織的な分業体制を駆使していることを確認しています。このような体制により、サイバー犯罪活動全体のエコシステムにおいて、ある者はネットワークへの侵入に専念し、ある者はランサムウェアの実行や被害者との身代金交渉に専念するなど、それぞれが特定のタスクに応じて、高い習熟度と専門性による活動が展開されるようになりました。

こうした専門的な分業体制の他、洗練された恐喝手口[2]や技術戦略[3]などが加わり、現代のランサムウェアは、より深刻な脅威となってきています。こうした脅威は拡大の一途をたどり、ランサムウェアによる攻撃は、今後 10 年間で数十億米ドル[4]の被害をもたらすと予測されています。

---

[1] https://www.trendmicro.com/vinfo/us/security/definition/ransomware

[2] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

[3] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021

[4] https://www.zdnet.com/article/the-cost-of-ransomware-around-the-globe-to-go-beyond-265-billion-in-the-next-decade/

## RaaS の運営：アンダーグラウンドがサービスの温床となる

RaaS[5]は、SaaS（Software-as-a-Service）モデル[6]に基づいており、オンラインでソフトウェアをサブスクリプションベースで利用できる形を採用しています。そしてサービスとして独自の進化を続けるエコシステム[7]を構築しつつ、主要な攻撃者に利用されながら、サイバー犯罪アンダーグラウンド市場で繁栄しています。

そしてこのサービスの主要なキープレーヤーは、ランサムウェアを開発して販売する RaaS 運営者でしょう。彼らは、通常、グループで組織されており、リーダー、開発者、インフラやシステムの管理者などといった役割が割り当てられています。さらに高度なグループの場合は、リクルーター、ペネトレーションテスター（別名ペンテスター）、被害者分析の担当者、交渉担当者[8]などの役割も存在しています。

また、こうしたいくつかの役割やツールなどは、外部委託やアフィリエイトプログラムを通じて入手されることもあります。例えば、AaaS（Access-as-a-Service）[9]を利用して、標的となる企業や組織にさまざまなアクセスの手法を提供する事業者も存在しています。その他、例えば、強力なペネトレーションテストチームであっても必要なランサムウェアが不足しているグループの場合、このようなペネトレーションテストチームは、RaaS の利用者となって、自分たちのランサムウェア攻撃活動において、アフィリエイトプログラムで入手できるランサムウェアツールやインフラを調達することができます。こうしたアフィリエイト関係は、組織的な犯罪活動の一貫として実行されたり、単発の関係性で取引されたり、さまざまな形が存在します。

---

[5] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-what-this-means-for-enterprises

[6] https://www.investopedia.com/terms/s/software-as-a-service-saas.asp

[7] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/commodified-cybercrime-infrastructure-exploring-the-underground-services-market-for-cybercriminals

[8] https://www.zdnet.com/article/ransomware-as-a-service-negotiators-between-hackers-and-victims-are-now-in-high-demand/

[9] https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/

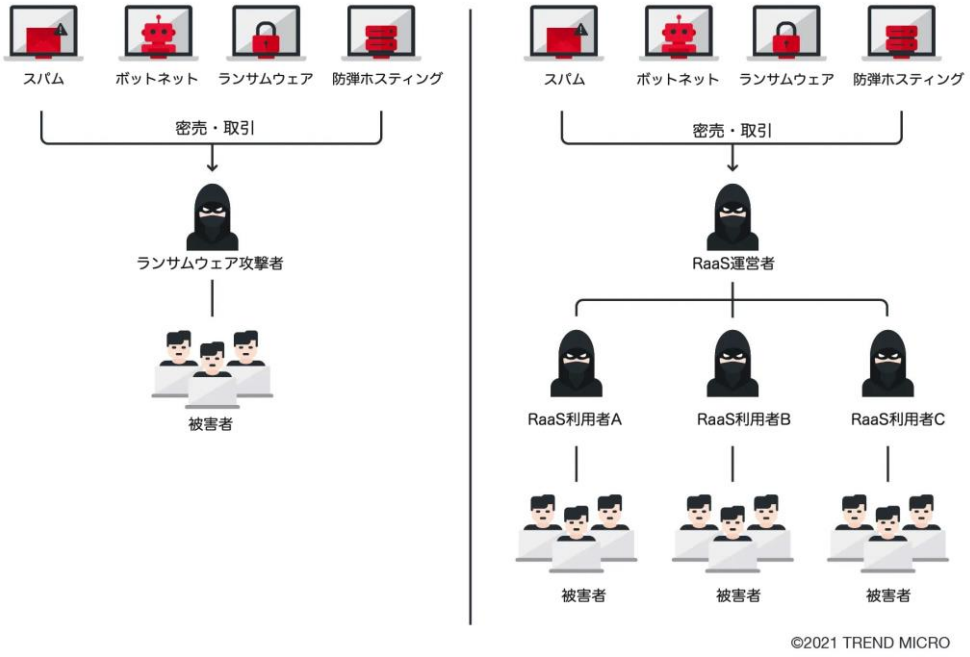



図 1：ランサムウェアの直接運用（左）および RaaS を介した運用（右）の比較

RaaS を介した運用の場合、RaaS を運営する犯罪グループ側が、まず運営者としてランサムウェアのソフトウェアやインフラを開発・入手する必要があります。この際、オンラインフォーラムやテレグラムチャンネル、個人的なつながりなどを通じて参加者を募るなど、勧誘活動[10]のために 10 億円もの資金を投じられるケースもあります。こうした事業体制が整った上で、RaaS の利用者は、このサービスにより自分たちの攻撃を仕掛けることが可能となります。

RaaS では、このように運営者と利用者の双方がそれぞれの専門性を発揮し、Win-Win の状況で高い収益[11]を得ることができます。利用者は、ランサムウェアを開発することなく、ランサムウェア攻撃を実行して収益を得ることができ、運営者は、利用者からサービス使用料として利益を得ることができます。サービス料金の支払いは、通常、サブスクリプションの収益モデルが採用されます。サブスクリプション以外の収益モデル[12]としては、ワンタイムペイメント、プロフィットシェアリング、アフィリエイトマーケティングなどが考えられます。こうしたビジネスモデルにより、RaaS の運営者は、ランサムウェアのソフトウェア開発や運営改善などに専念することが可能となり、ターゲットへの侵害やランサムウェアの配布といった攻撃活動にリソースを費やす必要がありません。そういった攻撃活動は、利用者が専念する領域となります。

---

[10] https://www.forbes.com/sites/simonchandler/2020/10/06/revil-ransomware-gang-offers-1-million-as-part-of-recruitment-drive/?sh=64e7a3b7bab2

[11] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them

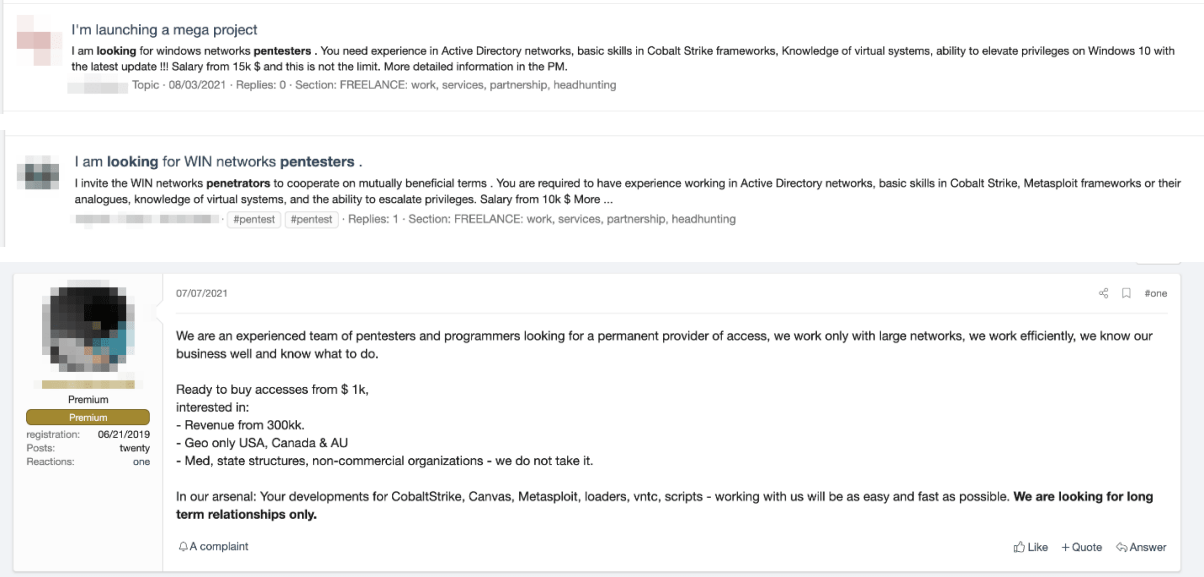
[12] https://www.beforecrypt.com/en/what-is-ransomware-as-a-service-raas-and-how-does-it-work/

## ランサムウェア攻撃の運用コストと身代金要求

攻撃グループがランサムウェア攻撃を実行する際にはコストが必要となります。この場合のコストは、ツール、熟練した人材、月々の運用経費などのことであり、その意味では、ランサムウェア攻撃は高コストの活動といえます。このため、攻撃グループのリーダーは、経常的な費用をどう賄うかを考えなければなりません。特にネットワークインフラのレンタルにはそれなりの費用がかかり、被害者からの身代金が得られる得られないに関わらず、攻撃グループのメンバーの多くは、給料制で金銭を支払う必要が生じてきます。この点からも、ランサムウェア攻撃の実行に際しては、経常的な運用コストがかさみ、ランサムウェア攻撃の成功に伴う収益は不可欠なものとなります。

ランサムウェア攻撃に利用するツールの購入にも、それなりのコストがかさみます。ランサムウェア攻撃グループやネットワーク侵入チームは、そうしたツールを自ら開発するのではなく、例えば、標的の企業や組織への初期侵入用のツールなどは、多くの場合、サードパーティのソフトウェアベンダーやアンダーグラウンド市場のソフトウェア開発者から購入しています。また、ツール使用の自由度やカスタマイズの有無などによっても価格はさまざまです。

RaaS を介して二重恐喝の手口などを用いる攻撃グループの場合、そうしたキット販売者や RaaS 提携プログラム自体の報酬額が高騰しています。こうした状況を受けて、下図のアンダーグラウンドフォーラムの広告[13]でも示されているとおり、ペンテスター、被害者分析担当者、交渉担当者など、ランサムウェア攻撃の運用担当者をまとめて求人するケースも散見されます。




[13] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trading-in-the-dark

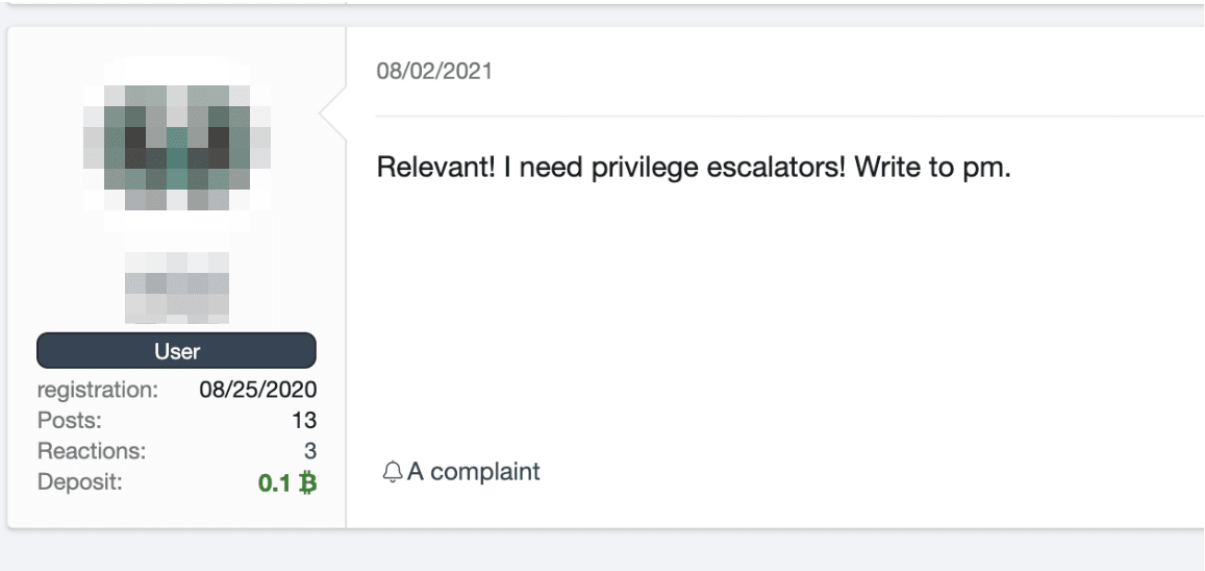



図 2：企業のネットワークにアクセスして権限拡大を実行できるペンテスターや
プログラマーを募集するアンダーグラウンドフォーラムの求人情報

こうして雇われた担当者のほとんどは、月給制かプロジェクトベースかにかかわらず、彼らが貢献するサービスへの支払いが必要となります。さらに平均的な月額費用（給料、サーバ、仮想プライベートサーバーのレンタル、サービスプロバイダ、ツール、アクセス、インフラなど）の見積りも加えると、ランサムウェアの攻撃グループは、運営維持のために少なくとも 10 万米ドル以上の費用が必要となります。例えば、10 社を標的にしたランサムウェア攻撃の場合、身代金の支払う相手が 1 社でも存在すれば、その 1 社からの収益により、この攻撃グループが期待する利益に加え、すべての費用もそこから負担されることになります。

現在、多くの企業や組織は、社内規定や政府の規制、当局の支援などがあるため、身代金要求に対する支払いを拒否し始めています。ランサムウェアの攻撃グループは、こうした支払い拒否に対しては、報復措置を行使しようとしてきます。例えば、攻撃グループ「Mespinoza」[14]の場合、身代金の支払いを拒否した企業や組織に対しては、窃取した機密情報の暴露だけでなく、彼らの違法行為（税金詐欺や脱税など）などを告発するなどと脅してきています。

[14] https://www.zdnet.com/article/this-ransomware-gang-hunts-for-evidence-of-crime-to-pressure-victims-into-paying-a-ransom/

## 特定のターゲットを避ける

サイバー犯罪アンダーグラウンド市場では、ランサムウェアの攻撃者が、どのターゲットを避けるべきかを判断するための戦略が徐々に確立されてきているようです。例えば、米国は、あらゆるタイプの攻撃活動のトップターゲットの１つであることに変わりはありませんが、ランサムウェアの攻撃者の中には、米国を避けることを検討しているケースも確認されています。米国では、数々の話題となったランサムウェア攻撃を受けて、同国の法執行機関や政府機関当局[15]が高い関心[16]を寄せています。こうした結果、身代金を支払わないノーペイポリシー[17]、身代金交渉のための被害者への政府支援[18]、支払われた身代金を回収するための技術[19]などが充実し、米国の企業や組織を狙ったランサムウェア攻撃で儲けることは、今後難しくなる可能性があります。

一部の攻撃グループは特にアジア地域に目を向けていますが、そうした中、例えば、台湾の企業を狙うことは避けているケース[20]も確認されています。この場合は、同国の厳格なマネーロンダリング防止政策により、被害を受けた同国の企業や組織が仮想通貨を合法的に購入することが難しく、身代金の支払いができない可能性が想定されているためのようです。

その他、攻撃グループが特定の地域を攻撃しない理由としては、運営者の愛国心、国の貧困レベル、ターゲットが置かれている地政学的状況などが挙げられます[21]。経済的にも政治的にも苦境に立たされている国や地域、あるいは運営者が愛国心を抱いている国などに対しては、身代金を直接要求せず、窃取した資産を別の利用者向けに販売・レンタルしたり、キーロガーで窃取した認証情報を個別に販売したり、サイバー犯罪アンダーグラウンドビジネスモデルの「クラウドオブログ」[22]を通じて販売したりするなど、別の収益化活動を実施しています。

---

[15] https://www.trendmicro.com/en_us/research/21/h/biden-releases-memo-on-critical-cybersecurity-infrastructure-bill.html

[16] https://thehill.com/policy/cybersecurity/559947-fbi-asks-congress-for-40-million-to-help-combat-wave-of-ransomware?rl=1

[17] https://securityboulevard.com/2021/07/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority/

[18] https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov

[19] https://www.businessinsider.com/fbi-used-hackers-bitcoin-password-to-recover-colonial-pipeline-ransom-2021-6

[20] https://geminiadvisory.io/ransomware-unmasked-dispute-reveals-ransomware-ttps/

[21] https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

[22] https://www.trendmicro.com/ja_jp/download/documents/security/wp/m294-web-cloud-of-logs.html

## RaaS の運用に関する最新情報

2021 年、サイバー犯罪アンダーグラウンド市場では、一時的ですが、顕著な変化が確認されました。DarkSide による Colonial Pipeline 社への攻撃の後、多くのアンダーグラウンドフォーラムでランサムウェアに関するすべてのトピックが禁止されるなど、派手な活動によって不用意な摘発を避ける傾向が確認されました。RaaS 運営者の多くは、システム管理者やペンテスターなど、正規の業務に見えて目的不明の求人広告をアンダーグラウンドフォーラムで掲載するのを控えるようになりました。これらの求人広告の投稿が、実際にランサムウェア運用を目的としたものであることが判明すると、そのアカウントが停止される措置まで取られていました。

また、ランサムウェアの運営者は、ターゲットをより慎重に選択するようになっています。実際、アンダーグラウンドのフォーラムでも、公的機関や民間企業を狙う場合、攻撃対象の選定に慎重になるべきで、特に政治的に重要なインフラや、ヘルスケア分野を狙う攻撃は避けた方がよいなどというトピックでの議論などが散見されました。

RaaS における利益配分の割合にも変化が見られました。かつて身代金の要求額が 5〜6 桁程度だった頃は、利益の割合は、70％と 30％で RaaS 利用者が有利になる料金設定になっていました。現在、7 桁までの高額の身代金を要求する攻撃グループでは、まずは初期アクセスの取得に対して 20％の発見者報酬を割り当てられ、その後のラテラルムーブメント（横展開）・内部活動、侵入テストなどは、給与報酬で雇われている担当者グループで実施されるようになっています。この利益配分は、Nefilim のような攻撃グループの活動において確認されました。アンダーグラウンドのフォーラムでは、こうしたトピックでの議論も活発化しており、今後、給与報酬の担当者グループの一員としてペンテスターを雇用することや、アクセス取得に特化した AaaS のプロ化が進み、Raas 運営者側への割り当て分が増える可能性が予想されます。

その意味では、最近確認されたランサムウェア攻撃は、今後の傾向を理解するヒントにもなり得ます。例えば、REvil（別名：Sodinokibi）[23]や DarkSide[24]による「Linux ベースの VMware ESXi サーバ」および「ネットワーク接続型ストレージ（NAS）」を狙った攻撃事例からは、今後、RaaS を利用する他の攻撃でも、対象が Windows 以外のサーバへ拡大され、POSIX（Portable Operating System Interface）準拠の Linux CentOS や Linux RedHat、その他の UNIX フレーバーなど、他の OS を狙われてくる可能性が推測されます。

[23] https://www.bleepingcomputer.com/news/security/revil-ransomwares-new-linux-encryptor-targets-esxi-virtual-machines/

[24] https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vms-targeted.html

## RaaS 運営者に利用されるランサムウェアファミリー

最近のランサムウェアファミリー[25]は、そのほとんどが RaaS のビジネスモデルを採用しています。トレンドマイクロの「2021 年上半期セキュリティラウンドアップ」[26]で言及されたランサムウェアファミリーの検出台数トップ 10 では、実際、8 つのランサムウェアが RaaS の運営者や関連会社によって使用されたことがあるものでした。Locky[27]、Cerber[28]、GandCrab[29]などのいくつかのファミリーも、過去に RaaS の運営で使用されたことがあります。これらのファミリーは、最近では積極的に活用されていないように見えるものの、依然として被害を受けた感染端末から検出されています

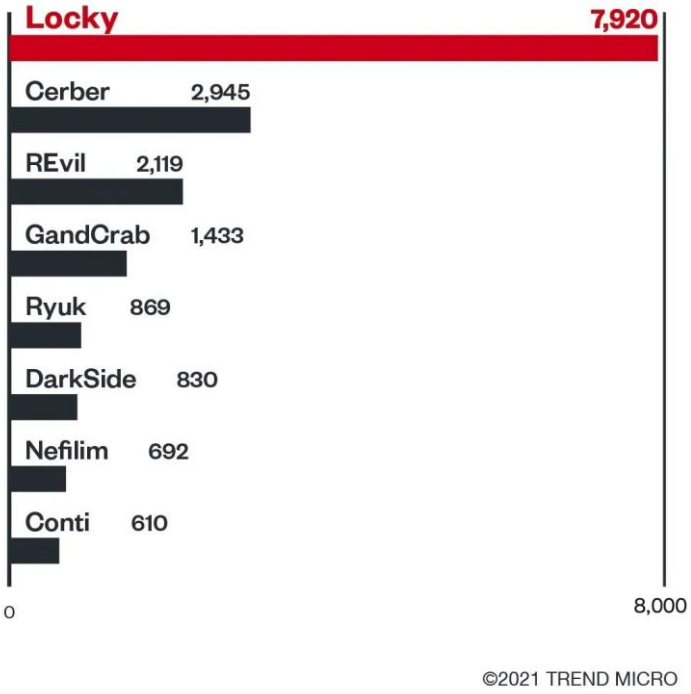



図 3：検出台数上位のランサムウェアファミリーのほとんどが RaaS に利用されていた（2021 年上半期）

これらのランキングの中から、2021 年に注目されたランサムウェア攻撃事例において、RaaS 運営者や関連会社が利用されたランサムウェアファミリーを以下に示します

[25] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them
[26] https://blog.trendmicro.co.jp/archives/28934
[27] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
[28] https://www.varonis.com/blog/cerber-ransomware/
[29] https://www.varonis.com/blog/cerber-ransomware/

## REvil

ランサムウェア「REvil」（「SODINOKIBI」として検出対応）[30]は、食肉業者の JBS 社[31]や IT 企業の Kaseya 社[32]への攻撃など、注目度の高い攻撃事例で 話題をさらっていましたが、2021 年後期以降はこうした大規模攻撃としての利用はそれほど確認されなくなりました。それでも、2021 年上半期のトレンドマイクロのデータでは、最も多く検出されたランサムウェアファミリーとして第 4 位に位置しており、検出台数が 2,119 件に達していました。大規模な攻撃でこのランサムウェアファミリーを利用する攻撃グループは、約 2 か月間姿を消した後に再びインフラを復活させ、新たな活動の兆し[33]があることが懸念されていました。しかしながら、その後の 2022 年 1 月、ロシア当局は REvil のメンバーを逮捕起訴したことを発表[34]しました。

REvil による攻撃では、身代金が巨額であることで知られており、実際、Kaseya 社[35]への攻撃では、7,000 万米ドルという記録な額[36]が要求され、また、JBS 社への攻撃[37]では、2,250 万米ドル（うち 1,100 万米ドルは支払われた）の身代金が要求されました。

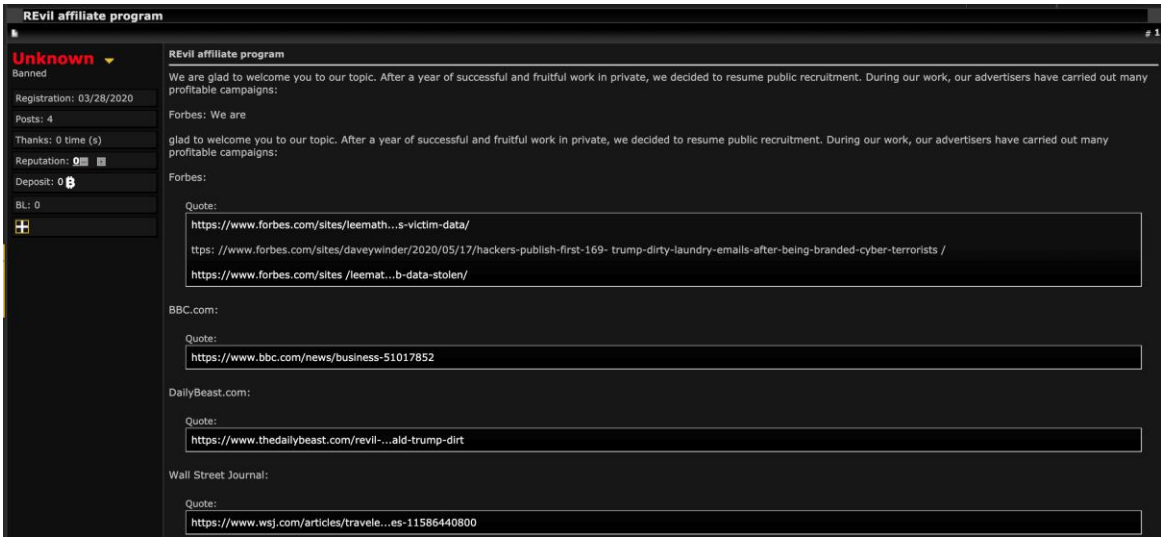



図 4：アンダーグラウンドフォーラムに掲載された
REvil のアフィリエイト募集に関する投稿

[30] https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html
[31] https://www.zdnet.com/article/fbi-attributes-jbs-ransomware-attack-to-revil/
[32] https://www.trendmicro.com/en_us/research/21/g/it-management-platform-kaseya-hit-with-sodinokibi-revil-ransomwa.html
[33] https://www.bleepingcomputer.com/news/security/revil-ransomware-is-back-in-full-attack-mode-and-leaking-data/
[34] https://www.bbc.com/news/technology-59998925
[35] https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/
[36] https://www.crn.com/news/security/revil-demands-record-70m-in-kaseya-ransomware-attack
[37] https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/

**詳細**

このランサムウェアの攻撃者が使用する手法の多くは、最近確認されたもの[38]であり、特に以下のような新たな手法が特筆されます。

**ダウンロードおよび実行**

- スパムメールの添付ファイル（PDF ファイルなど）を介してマルウェア「Qakbot」が標的の端末に投下され[39]、その後、このマルウェアにより、追加のコンポーネントやペイロードをダウンロードされます。
- 標的となった企業 Kaseya 社の VSA サーバに影響を与えるゼロデイ脆弱性「CVE-2021-30116」[40]が、同社へのサプライチェーン攻撃で使用されました。

**新たな確認事項**

- 攻撃対象となるネットワークの発見には、AdFind、SharpSploit、BloodHound、NBTScan などの正規ツール[41]が採用されていました。

[38] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021

[39] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/80/qakbot-a-prevalent-infostealing-malware

[40] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116

[41] https://www.trendmicro.com/vinfo/tmr/?/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021

## DarkSide

ランサムウェア「DarkSide」[42]は、Colonial Pipeline 社への攻撃により、最近のニュースでも話題になっています。標的となった同社は、500 万米ドル[43]の身代金の支払いを強要されました。このランサムウェアファミリーは、2021 年上半期の最も多く検出されたランサムウェアファミリーとしては、検出台数が 830 件に達して第 7 位にランクされています。

ただし同社への攻撃の後、このランサムウェア攻撃のグループは、米国政府当局や法執行機関からの圧力を懸念し、攻撃を停止する[44]と主張しています。しかし、他のランサムウェアファミリーによる攻撃と同様、しばらくの間、身を潜めてから再登場するか、あるいは新たな後継者が現れてくるかもしれません。

### 詳細

以前のレポート[45]でも解説しましたが、DarkSide が利用した注目すべき技術には次のようなものがあります。

### 諜報活動

- こうした事前調査の段階で DarkSide は、PowerShell、Metasploit Framework、Mimikatz、BloodHound などのさまざまな正規ツール[46]を使用します。

### ラテラルムーブメント・内部活動

- ラテラルムーブメントや内部活動の際、DarkSide は、ドメインコントローラ（DC）[47]や Active Directory へのアクセスを試みる。これにより、認証情報の取得、権限の拡大、情報窃取などの活動を行います。
- そしてアクセスした DC ネットワークを利用して、接続された端末へランサムウェアを展開します。

---

[42] https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

[43] https://www.crn.com/news/security/colonial-pipeline-paid-5m-to-darkside-hours-after-attack-report

[44] https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html

[45] https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

[46] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021

[47] https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware

## Nefilim

ランサムウェア「Nefilim」は、2021 年半ばのランサムウェアの中では、9 番目に多く検出され、692 件の検出台数を記録しています。このランサムウェアファミリーの背後の攻撃者は、10 億米ドル規模の収益[48]を上げている企業に限定してターゲットを定めています。

最近のランサムウェアファミリーの多くがそうであるように、Nefilim も二重恐喝[49]の手口を採用しています。Nefilim を利用する攻撃者[50]は、被害を受けた企業が身代金の要求に屈しない場合の対抗措置が、特に悪質だと言われており、窃取した情報を長期間にわたって暴露し続けます。

**詳細**

Nefilim は、以下のようなさまざま手法[51]を駆使しています。

**初期侵入**

- インターネットに露出した RDP を介して初期侵入のためのアクセスを得ます。
- 「Citrix Application Delivery Controller の脆弱性（CVE-2019-19781）」[52]を利用して、対象の端末へ侵入することも可能です。

**ラテラルムーブメント・内部活動**

- PsExec や Windows Management Instrumentation（WMI）などのツールを使って、ラテラルムーブメントや内部活動を行います。
- PC Hunter、Process Hacker、Revo Uninstaller などのサードパーティ製ツールを使用して、検出を回避します。

---

[48] https://www.trendmicro.com/en_vn/research/21/f/nefilim-modern-ransomware-attack-story.html

[49] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

[50] https://www.trendmicro.com/en_us/research/21/f/nefilim-modern-ransomware-attack-story.html

[51] https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html

[52] https://nvd.nist.gov/vuln/detail/CVE-2019-19781

## LockBit

ランサムウェア「LockBit」[53]は、2021 年半ばに「LockBit 2.0」として再登場し、二重恐喝の手口[54]を採用することで、より多くの企業[55]をターゲットにしています。トレンドマイクロの調査によると、チリ、イタリア、台湾、英国が最も被害を受けた国となっています。最近注目された攻撃では、身代金の要求額が 5,000 万米ドルにも達していました。

LockBit 2.0 の攻撃者は、ランサムウェアの中でも、このランサムウェアファミリーが最も高速の暗号化技術を備えていると主張しています。また、「Ryuk」や「Egregor」などのよく知られたランサムウェアファミリーとの類似性も確認されています。

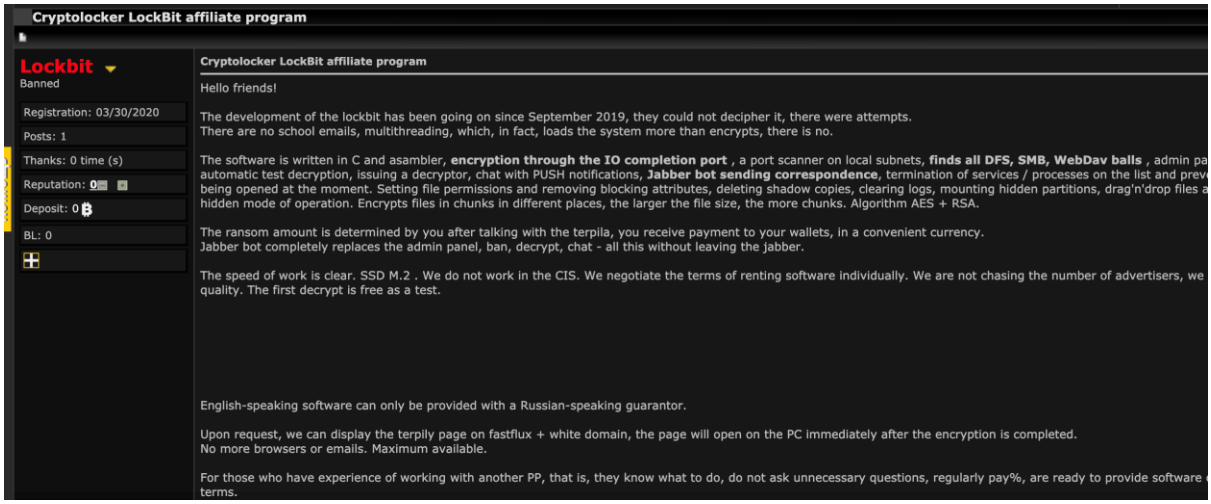



図 5：アンダーグラウンド市場のフォーラムにおける LockBit のアフィリエイト募集の投稿

### 詳細

このランサムウェアの最新の手法は、以下のとおりとなります。

### 情報送出

- 自動的に情報窃取できるツール「StealBit」（「TrojanSpy.Win32.STEALBIT.YXBHM」として検出）を利用者に提供することで、情報窃取活動をやりやすくしています。

### 検出回避

検出回避のため、以下のバッチファイルにより、感染端末内のプロセスやサービスを終了します。

---

[53] https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html

[54] https://www.trendmicro.com/vinfo/tmr/?/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

[55] https://www.cyber.gov.au/acsc/view-all-content/alerts/lockbit-20-ransomware-incidents-australia

- delsvc.bat（「Trojan.BAT.KILLPROC.D」として検出対応）は、重要なプロセス（MySQL や QuickBooks など）やサービス（Microsoft Exchange など）を利用できなくします。
- AV.bat（「Trojan.BAT.KILLAV.WLDX」として検出対応）は、ウイルス対策プログラム「ESET」をアンインストールします。
- LogDelete.bat（「PUA.BAT.DHARMA.A」として検出対応）は、Windows のイベントログを消去します。また、Defoff.bat（「Trojan.BAT.KILLAV.WLDX」として検出）は、リアルタイム監視などの Windows Defender 機能を無効にします。

**ランサムウェアの被害**

- Active Directory のグループポリシーを利用して、Windows 上のデバイスが自動的に暗号化されます。

## Conti

ランサムウェア「Conti[56]」の攻撃者は、おそらく今日活動している最大のランサムウェア攻撃グループの 1 つでしょう。ランサムウェア「Ryuk」との類似点が確認されることから、Ryuk の後継とも言われています。例えば、拡散手法としては双方とも、Emotet、Trickbot、BazarLoader といったマルウェアを介して実行[57]されます。「2021 年上半期セキュリティラウンドアップ」[58]によると、Conti は、610 件の検出台数を示し、10 番目に多く検出されたランサムウェアとなっています。

また最近、米連邦捜査局（FBI）および米国の CISA（Cybersecurity and Infrastructure Security Agency）からは、Conti の攻撃が急増していることに関して注意喚起[59]が告知されました。注意喚起の中では、Conti の攻撃に悪用される可能性のあるペネトレーションテストの文書が流出[60]したと報じられています。

**詳細**

**初期侵入**

- スパムメールを介して対象の端末に侵入します。
- 既知の脆弱性を悪用して初期アクセスを行う場合もあります。

**感染対象の発見、ラテラルムーブメント・内部活動、感染端末に滞在維持**

- PowerSploit[61]、Metasploit、ADFind、Cobalt Strike[62]などのオープンソースや既製の商用ツールにより感染対象の発見やラテラルムーブメント・内部活動を行うことができます。
- AnyDesk などの他の商用ツールも、感染端末に滞在するために使用されます。

**情報送出**

- 情報送出の段階では、大規模なクラウドストレージが利用されます。

**検出回避**

- 検出回避の手法としては、PC Hunter、Process Hacker、Revo Uninstaller などのサードパーティツールが使用されます。
- 感染端末で確認された各種セキュリティツールも無効にされます。

---

[56] https://blog.trendmicro.co.jp/archives/30172

[57] https://www.trendmicro.com/en_us/research/21/c/vision-one-tracking-conti-ransomware.html

[58] https://blog.trendmicro.co.jp/archives/28934

[59] https://us-cert.cisa.gov/ncas/alerts/aa21-265a

[60] https://github.com/ForbiddenProgrammer/conti-pentester-guide-leak

[61] https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/

[62] https://michaelkoczwara.medium.com/conti-ransomware-group-cobalt-strike-c2-analysis-rdp-persistence-cc535d35eaba

## ランサムウェアからシステムを守るには

企業や組織がランサムウェアの攻撃[63]から身を守るためには、ランサムウェアの脅威に関するセキュリティ対策を講じることが有効です。この対策は、CIS（Center of Internet Security）[64]や NIST（National Institute of Standards and Technology）[65]などによるセキュリティフレームワークのガイドラインに基づいて作成することができます。これらのガイドラインは、ランサムウェアの脅威に対する予防、防御、復旧のための優先順位付けやリソース管理などにも有効です。

こうした対策では、攻撃手法の技術的な側面だけでなく、標的の企業や組織で確認された弱点（顧客データ、個人識別情報（PII）の誤処理、会計上のミスなど）を脅しとして利用して身代金の交渉額を引き上げてくるなど、戦略面に関しても理解しておくことが重要です。そして企業や組織は、ランサムウェアの脅威への対策状況を評価する際には、これら技術および戦略的な側面のさまざまな要素を考慮にしておく必要があります。

上述のセキュリティガイドラインによるベストプラクティス[66]は以下のとおりとなります。

**セキュリティ事項のインベントリ作成および監査の実施**

特に以下の事項に注意すること

- 利用可能な資産およびデータ
- 許可された、または許可されていないデバイスおよびソフトウェア
- セキュリティイベントおよびインシデント

**適切な設定および監視活動の徹底**

特に以下の事項の管理および把握に注力すること

- ハードウェアおよびソフトウェアの設定
- 管理者の権限とアクセス
- ネットワークポート、プロトコル、サービスのアクティビティ
- ファイアウォールやルータなどのネットワークインフラ機器やセキュリティ設定

**修正パッチおよびセキュリティアップデートの管理徹底**

ソフトウェアやアプリケーションに対して、以下の事項を定期的に実施すること

- 脆弱性の評価

---

[63] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22

[64] https://www.cisecurity.org/controls/

[65] https://www.nist.gov/cyberframework

[66] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/return-to-sender-preventing-ransomware-while-working-from-home

- 修正パッチもしくは仮想パッチの適用
- バージョンの最新化

**システムの保護およびデータの復旧に関する対応の実施**

以下の事項を実施すること

- データ保護、バックアップ、リカバリー対策
- 多要素認証（MFA）の採用

**各レイヤーにおけるセキュリティの確保の徹底**

以下の各事項位を実施すること

- **多層防御：**潜在的な脅威に対して複数の防御層（レイヤー）を設けること。例えば、未使用のサービスをファイアウォールだけでなくサーバ上でもブロックすること。
- **ネットワークのセグメンテーションと最小権限付与の原則：**特にシステムユーザ、サービス、役割への権限付与の際には、これらに従うことが最も重要となる。
- **メールの静的解析および動的解析：**双方を駆使することで不審かつ不正なメールをチェックしてブロックする機能の実装が可能となる。
- **システムのすべてのレイヤーに対応する最新版のセキュリティソリューション：**これらのレイヤーには、メール、エンドポイント、ウェブ、ネットワークが含まれる。
- **攻撃の初期兆候の監視：**システム内のさまざまなツール[67]の不審な存在を特定することで、企業や組織は起こり得る攻撃を食い止める時間と労力を大幅に削減することが可能となる。
- **高度な検知技術：**特に AI や機械学習を駆使したテクノロジーは、強固な保護を提供する。

**セキュリティトレーニングおよびテストの実施**

以下のような従業員・担当者向けのトレーニングやシステム等へのテストを定期的に実施すること

- セキュリティスキルの評価とトレーニング
- レッドチーム演習、ペネトレーションテスト

[67] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021

## トレンドマイクロのソリューション

Trend Micro Vision One™[68]は、多層的な防御および挙動検知により、単一のレイヤーからの監視では取るに足らないと思われるような不審な活動に見えても、総合的な判断から検知してブロックします。このため、システム上のどこにランサムウェアが潜んでいても速やかに検知してブロックすることができます。

Trend Micro Cloud One™ - Workload Security[69]は、脆弱性を悪用する既知の脅威および新たな脅威の双方に対してリアルタイムの防御を可能にします。これらは、仮想パッチ、機械学習技術、グローバルな脅威インテリジェンス等によって実現されます。

Trend Micro™ Deep Discovery™ Email Inspector[70]は、カスタムサンドボックスおよび高度な解析技術を実行します。これらにより、不正メールを媒介としたランサムウェアの潜在的な攻撃を効果的に抑止します。

Trend Micro Apex One™ [71]は、最新の技術を駆使して、ランサムウェアやファイルレスの脅威など、さまざまなセキュリティ上の問題に対して、エンドポイントでの自動防御、脅威の検知、迅速な対応を実現します。

注：本稿は、2021 年 10 月 11 日の時点で確認された RaaS 使用のランサムウェアファミリーに基づき更新されています。

[68] https://www.trendmicro.com/ja_jp/business/products/detection-response.html

[69] https://www.trendmicro.com/ja_jp/business/products/hybrid-cloud/cloud-one-workload-security.html

[70] https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/email-and-collaboration/email-inspector.html

[71] https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/endpoint.html

**TREND MICRO**

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。

トレンドマイクロ株式会社が書面により事前に承諾している場合を除き、形態および手段を問わず本書またはその一部を複製することは禁じられています。本書の作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

本書に記載されている各社の社名、製品名、およびサービス名は、各社の商標または登録商標です。

〒151-0053

東京都渋谷区代々木 2-1-1　新宿マインズタワー

大代表 TEL：03-5334-3600 FAX：03-5334-4008

**http://www.trendmicro.com**

トレンドマイクロはサイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。

© 2021 Trend Micro Incorporated. All Rights Reserved.