2023年第1四半期のランサムウエア被害組織とネットワークアクセスの販売状況

KELA

2023 年第 1 四半期のランサムウエア被害組織とネットワークアクセスの販売状況

KELA サイバー犯罪インテリジェンスセンター

目次

エグゼクティブサマリー

2023 年初旬、数千台もの ESXi サーバーを標的とする大規模なランサムウエアキャンペーンが発生し、ランサムウエアグループやデータリークグループが世界中の組織に危険をもたらし続けているという現状が浮き彫りとなりました[1]。さらに KELA でも、2023 年第 1 四半期（2023 年 1-3 月期）に発生したランサムウエア攻撃やデータリーク攻撃、売り出されたネットワークアクセスの件数が前年同期比で増加していることを確認しました（ネットワークアクセスは、ランサムウエアグループのサプライチェーンの中で重要な役割を果たしています）。今期我々がランサムウエアグループ、データリークグループ、初期アクセスブローカーの活動を監視して得た洞察の要点は、以下のとおりです。

- 2023 年第 1 四半期に発生したランサムウエア攻撃及びデータリーク攻撃の件数は、前年同期比（2022 年第 1 四半期比）で増加し、被害組織の数は約 900 に上りました。
- 今期、攻撃件数でトップ 5 にランクインしたランサムウエアグループ及びデータリークグループは、「LockBit」、「Clop」、「Alphv」、「Royal」、「Black Basta」となりました。今回初めてランクインした Clop は、Fortra 社製ファイル転送管理ソリューション「GoAnywhere MFT」のゼロディ脆弱性（CVE-2023-0669）を悪用しており、同グループの標的となった組織の数は 130 に上りました（Clop の主張に基づく）。
- 今期、ランサムウエアグループ及びデータリークグループの標的となった業界の 1 位は製造・工業製品であり、同業界に対する攻撃の 50%以上は LockBit、Royal、Alphv による犯行でした。
- 今期、ランサムウエアグループ及びデータリークグループの標的となった国の 1 位はこれまでと同じく米国であり、被害組織の 45%が米国の企業や組織でした。2 位は英国、3 位はカナダ、4 位はドイツ及びフランスとなりました。
- 2022 年に攻撃件数上位にランクインしていた Hive のオペレーションは、今期で活動を止しました。

[1]弊社プラットフォームで「ESXiargs Ransomware Campaign」に関するレポートをご覧いただけます。プラットフォームは、無料トライアル でアカウントを作成後ご利用いただけます。

- 今期新たに登場したランサムウエアブログ・データリークサイトは Vendetta、Medusa、Dark Power、Abyss、Money Message です。
- 今期 KELA が追跡調査を行ったネットワークアクセスの数は 600 件を超え、その希望販売価格の合計は約 58 万米ドルとなりました。
- 2023 年第 1 四半期に売り出されたネットワークアクセスの平均価格は約 1,100 米ドル、中央価格は 400 米ドルとなりました。

2023 年第 1 四半期におけるランサムウエア攻撃・データリーク攻撃の被害組織

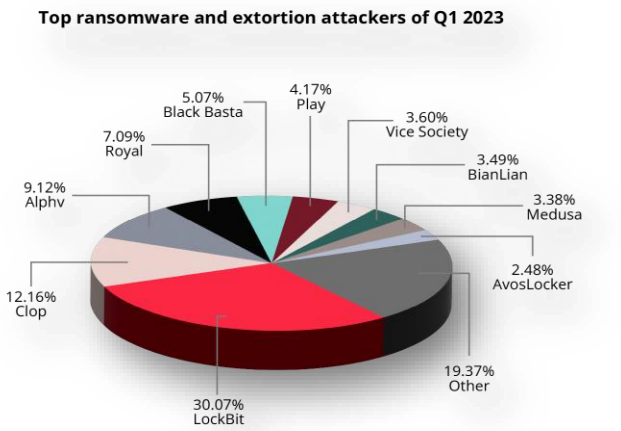
2023 年第 1 四半期、我々は監視対象とするソース（ランサムウエアグループのブログや交渉ポータルサイト、データリークサイト、報道やその他公表されている報告など）で約 900 の被害組織を確認しました。この数字は前年同期比で 30%増となります。また我々が確認した被害組織数をひと月あたりの平均数で見ると、前年同期は約 230 組織であったのに対し、今期は約 300 組織となっています。

攻撃件数上位のランサムウエアグループ

2023 年第 1 四半期に攻撃件数で上位に挙がったランサムウエアグループ及びデータリークグループは、LockBit、Clop、Alphv（別名 BlackCat）、Royal、Black Basta であり、各グループが公表した被害組織の数は 45～270 に上りました。LockBit は 265 を超える被害組織を公開し、引き続き 1 位のポジションを維持しました。なお、この 265 という数字は 2 位の Clop が公表した被害組織の約 2.5 倍に相当します。しかしその Clop も 2023 年 3 月に攻撃のペースを上げて 100 の被害組織を公開し、同月に公表した被害組織数では LockBit を追い抜きました。

攻撃件数で 3 位となった Alphv は、先日フォーラム「RAMP」でランサムウエアの新バージョン「"BlackCat 2.0: Sphynx」のリリースを発表しました。

なお、Clop と Royal は今期初めて攻撃件数トップ 5 にランクインしたグループです。両グループは 2022 年にはランクインしていなかったものの、トップグループの 1 つであった Hive のオペレーションが米連邦捜査局（FBI）にテイクダウンされた恩恵を受けて、それぞれ 2 位と 4 位の座を獲得できたようです。



LockBit、オペレーションの詳細を語る

2022 年、日本の警察庁は、最も活発に活動しているランサムウエアグループ LockBit の標的となった企業 3 社のデータを復元することに成功しました[2]。これを受けて 2023 年 1 月、LockBit の代表者である「LockBitSupp」が、サイバー犯罪フォーラムでオペレーションの詳細を一部公表しました。そしてその説明の中で LockBitSupp は、同グループのランサムウエアには復元可能となるようなバグはないと主張していました。また、同グループのランサムウエア・アズ・ア・サービス（RaaS）でアフィリエイトに提供しているランサムウエアには 4 つのバージョンがあり、そのうちの 1 つは、以前 Conti のランサムウエアから流出したソースコードを使って作成したものであると説明していました[3]。

LockBit は引き続き IT 企業を標的にし、またそれら IT 企業と関連のある第三者も侵害することで被害組織数を増やしていました[4]。2023 年 2 月 18 日に同グループが、「英国の IT 企業とその顧客を侵害した」と主張していたインシデントもそれに該当する 1 例です。またその後の 3 月には、米サイバーセキュリティ・インフラストラクチャ・セキュリティ庁（CISA）、米連邦捜査

[2] Japanese police successful in decrypting data attacked by LockBit ransomware

[3] 弊社プラットフォームのフィニッシュド・インテリジェンスで詳細をご覧いただけます。プラットフォームについては、無料トライアル でアカウントを作成後ご利用いただけます。

[4] 弊社の 2022 年アニュアルレポート

局（FBI）、その他セキュリティ関連当局も LockBit の戦術・技術・手順（TTP）についての合同勧告を発表し、同グループのランサムウエアオペレーションについて警告しました[5]。

LockBit が英国の IT 企業とその顧客を攻撃したと主張している投稿

新たにトップ 5 にランクインした Clop と Royal

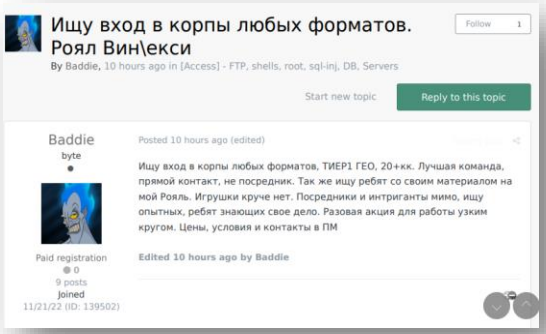
2023 年第 1 四半期、Clop は 100 を超える組織を攻撃し、攻撃件数で 2 位となりました。同グループが主に標的にした業界は、専門サービス、テクノロジー、医療・ライフサイエンスです。2023 年 2 月、同グループは Fortra 社の GoAnywhere MFT に存在するゼロディ脆弱性（CVE-2023-0669）を悪用して 130 の組織からデータを窃取したと主張し、世間の注目を集めました[6]。そして実際に、「Hitachi Energy」社や「Rubrik」社、「Hatch Bank」、トロント市（カナダ）をはじめとする組織が、Clop の攻撃を受けてデータ侵害が発生したことを公表しました（2023 年 3 月時点）。一方我々も、同グループが前述のゼロディ脆弱性を悪用していると発言して以降、106 の被害組織（同グループが 2023 年第 1 四半期に公表した全被害組織の 98%）をブログに掲載していることを確認しています。

[5] #StopRansomware: LockBit 3.0

[6] Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day

一方、2022 年に登場した Royal は今期、60 を超える被害組織を公表しました。2023 年 2 月に入って以降、同グループはオペレーションを拡大するべく Linux サーバーや ESXi サーバーも攻撃しており[7]、主に製造・工業製品、食品・飲料、専門サービス業界がその標的となっていました。

また我々の調査では、Royal と関連のあるアクター「Baddie」がサイバー犯罪フォーラムで、収益 2,000 万米ドル超を有する企業のネットワークアクセスを購入するために協力してくれる初期アクセスブローカーを探していたことが確認されています。そして他のアクターの発言によると、この Baddie が Royal の正式な代表者であるとされています。Baddie が Royal の単なるアフィリエイトである可能性も完全に排除されたわけではありませんが、同アクターが Windows や ESXi の特定のバージョンに言及していた投稿の中で、ランサムウエアオペレーション「Royal」を「my Royal（私の Royal）」と呼んでいたことが確認されています。



Baddie がネットワークアクセスを探している投稿：「ベストチームだ。仲介者ではないから直接の連絡を乞う。my Royal に自分の持っているアクセスを提供してくれるヤツを探している」

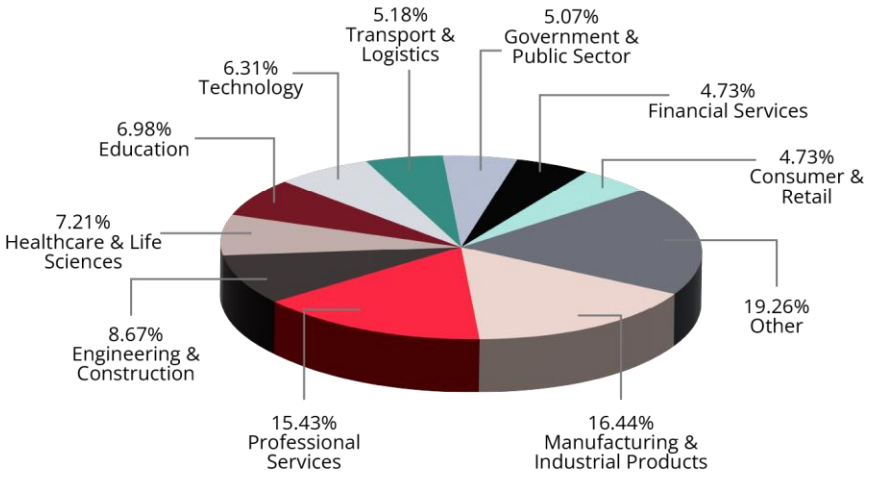
[7] Royal Ransomware Targets Linux ESXi Servers

ランサムウエアの標的となった業界

2023 年第 1 四半期、ランサムウエアグループやデータリークグループの標的となった業界の 1 位は製造・工業製品でした。同業界の組織に対する攻撃のうち 53%は、LockBit、Alphv、Royal による犯行であり、この 3 グループが攻撃件数で上位にランクインしているという事実と一致する結果と言えるでしょう。

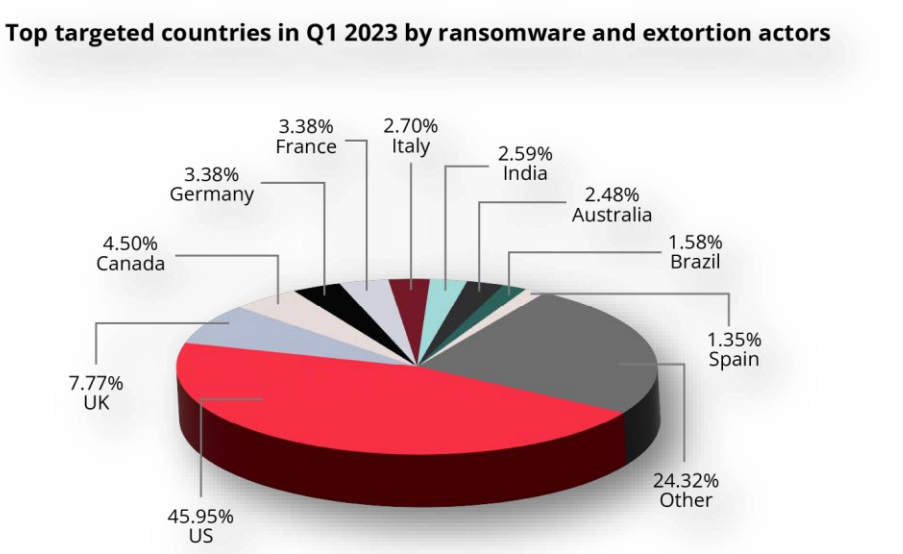
標的となった業界の 2 位は専門サービス、3 位は工事・建設、4 位は医療・ライフサイエンス、5 位は教育となりました。教育業界を標的とした攻撃の 20%以上は、Vice Society による犯行でした。同グループは、2022 年と同様に 2023 年第 1 四半期も大学を攻撃し、教育業界を脅かしています。

Top targeted sectors in Q1 2023 by ransomware and extortion actors



ランサムウエアの標的となった国々

ランサムウエア攻撃の標的となった国については、今期も米国が 1 位となりました。2023 年第 1 四半期に発生したランサムウエア攻撃やデータリーク攻撃の 45%は米国の企業や組織が標的となっており、2 位は英国、3 位はカナダ、4 位はドイツ及びフランスの企業や組織となりました。



注目を集めたランサムウエア攻撃

2023 年 1 月 31 日、英国のテクノロジー・データソリューションサービス企業である「ION Markets」社がランサムウエア攻撃を受けました[8]。その後の 2 月 2 日には、LockBit が自らのブログで ION Markets 社の名前と詳細情報を公開して犯行声明を出し、さらに翌 3 日にはロイター社の記者に対して「身代金は支払われた」と主張していました。ただし LockBit は身代金が支払われた証拠を見せておらず、身代金の額も公表していません。また、誰が身代金を支払ったのかについても明らかにせず、「very rich unknown philanthropist（非常に裕福な未詳の慈善家」が支払ったと説明していました[9]。

その他に注目を集めたランサムウエア攻撃として、アイルランドに本社を置く食品企業「Dole」社に対する攻撃が挙げられます。報告によると同社がランサムウエア攻撃を受けたのは 2023 年 2 月ですが、その翌月となる 3 月 22 日に、同社より攻撃の事実が公表されました。Dole 社の説明によると、「従業員の情報」に対する不正アクセスが発端となって攻撃を受けたものの、同社業務への影響は限定的であるということでした。しかし報道によると、消費者から「Dole 社の商品が 1 週間以上にわたって店頭から消えている」と不満の声がソーシャルメディアに投稿されていました[10]。このインシデントの背後にいるアクターについては、現在も明らかとなっていません。

また 2023 年第 1 四半期には、WMware ESXi サーバーを使用する組織を狙った大規模なランサムウエアキャンペーンが発生しました[11]。3,000 を超える組織が標的となったこのキャンペーンについては、ランサムウエア「ESXiArgs」のオペレーターがその実行犯であると考えられています。ESXiArgs は、ESXi サーバー上にある特定の拡張子（.vmxf、.vmx、.vmdk、.vmsd、.nvram）が付いたファイルを暗号化し、さらに暗号化した各ファイル毎に.args ファイルを作成します（この時作成された.args ファイルには、暗号化された文書のメタデータが含まれています）。過去には研究者から「ESXiArgs と Nevada の間にはつながりがある」との見解

[8] ION Cleared Derivatives Cyber Event

[9] Hackers who breached ION say ransom paid; company declines comment

[10] Cyberattack on food giant Dole, temporarily shuts down North American production

[11] New ESXiArgs ransomware version prevents VMware ESXi recovery

が報告されましたが、その後 ESXiArgs は ESXi サーバーを標的とする別のランサムウエア攻撃で使用された亜種がベースとなっていることが判明し、現在では両者のつながりは疑問視されています。なお、この亜種と ESXiarges については、いずれも 2021 年にリークされた Babuk のソースコードを使って作成されていることが確認されています。

また研究者の調査では、ベアメタルハイパーバイザー「ESXi」の「OpenSLP」に影響を及ぼすバッファーオーバーフローの脆弱性（CVE-2021-21974）が、ESXiArgs のオペレーションで侵害ベクトルとして悪用されていることが明らかとなっています。

新たに登場したランサムウエアブログとデータリークサイト（2023 年第 1 四半期）

Vendetta（今期公表した被害組織数：3）

2023 年 2 月、ランサムウエア「Cuba」のサブドメイン上で、ランサムウエア「Vendetta」のブログが運営されていることが確認されました。Vendetta は窃取したファイルのディレクトリも公開していますが、このディレクトリは TOR 上にある別ドメインでホストされています。

Medusa（今期公表した被害組織数：30）

2023 年 2 月、ランサムウエアグループ「Medusa」のブログがサイバー犯罪ソースで発見されました。発見時、このブログには 13 の被害組織が掲載されており、そのうちの少なくとも 1 組織が攻撃を受けた事実を公表しています。なお、Medusa は 2019 年に発見されたランサムウエアの亜種「MedusaLocker」と名称が似ていますが、両者のつながりを示す証拠は確認されていません。大半のランサムウエアグループとは異なり、Medusa が被害組織のデータをブログで公開することはありませんが、TOX を使って連絡をとるよう被害組織に要求します。ただし弊社が調査した限り、同グループからの返信は遅いものと思われます。

また Medusa は、「t0mas」と名乗るアクターと協力体制をとっているようです。この t0mas は、ウェブサイト「osintcorp[.]uk」と Telegram チャンネル「information support」を運営しており、information support については 1,700 人を超えるユーザーがチャンネル登録していることが確認されています（2023 年 3 月時点）。Medusa のブログと information support（t0mas の Telegram チャンネル）では被害組織の名称やデータが公開されており、osintcorp[.]uk では被害組織の機密情報を録画した動画が公開されています。なお、我々の調査では t0mas が 2021 年 9 月から 2022 年 2 月にかけて、RaidForums で「1941Roki」とのハンドル名で活動していたこと、また同フォーラムで主にロシア人やウクライナ人のデータベースを販売していたことが確認されています。

Dark Power（今期公表した被害組織数：10）

2023 年 3 月、我々は新たなブログ「Dark Power Ransomware」を発見しました。その時すでにブログには 10 の被害組織が掲載されており、Dark Power は被害組織に対し、窃取したファイルを取り戻したければ TOX を使って彼らに連絡するよう指示していました。また、同ブログを発見する以前の 2023 年 1 月には、Dark Power のオペレーターがチェコを標的にランサムウエア攻撃を行ったことが、同国の国家サイバー情報セキュリティ局（'NÚKIB'）により検知されました[12]。そしてその後の 2023 年 3 月 23 日には研究者が Dark Power のランサムウエアのサンプルを発見し、このサンプルによって、同グループが実際にランサムウエアを使用していることが裏付けられました[13]。またこの時検証されたインシデントで Dark Power が残した身代金メモには、1 万米ドル相当の身代金を暗号資産「Monero」で支払うようにとの指示が残されていました。

Abyss（今期公表した被害組織数：6）

2023 年 3 月、我々はデータリークサイト「Abyss」を発見しました。また発見時、このサイトには 6 つの被害組織が掲載されていましたが、サイバー犯罪フォーラム「Breached」が閉鎖される直前の時期、Abyss に掲載されている被害組織のいくつかをアクター「infoleak222」が同フォーラムで公開していたことから、この infoleak222 は Abyss のオペレーションに関連しているものと思われます。また infoleak222 については、2023 年 1 月から Breached で活動していることが確認されています。

U-bomb（今期公表した被害組織数：1）

2023 年 3 月、恐喝相手となった被害組織と交渉を行うポータル「U-bomb」が発見されました。我々が U-bomb と被害組織のやり取りを観察したところ、U-bomb は自らの活動をランサムウエアオペレーションと主張し、「復号ツール」の対価を支払うよう被害組織に要求していました。

[12] CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

[13] Shining Light on Dark Power: Yet Another Ransomware Gang

このポータルの認証ページは Hive の交渉用ポータルのものと似ていますが、その一方でポータルの URL は「Conti」の文字で始まっています。2023 年 3 月時点では、このポータルのオペレーションが Hive や Conti と関連していることを示唆する証拠は確認されておらず、また U-bomb はデータリークサイトを持っていないものと思われます。

Money Message（今期公表した被害組織数：2）

2023 年 3 月、新たなランサムウエアブログ「Money Message」が発見されました。発見当時、このブログには 2 つの被害組織が公開されていました。同名（Money Message）のグループによるランサムウエア攻撃については、これまでに少なくとも 1 件報告されています[14]。

[14] Money Message/Money Encryptor Ransomware (xxyyzzr) Support Topic

注目すべき出来事

ランサムウエアオペレーション「Hive」終了後も活動を続けるアフィリエイト

2023 年 1 月 26 日、法執行機関が合同作戦を実行し、Hive のインフラストラクチャを解体したことが発表されました[15]。これにより、Hive のブログと交渉用ポータルの両方がアクセス不可能となり、また両サイトには米連邦捜査局（FBI）が押収したことを示す通知が表示されました。米司法省の発表内容によると、当局は 2022 年 7 月に Hive のネットワークに侵入することに成功し、その後このアクセスを使って復号キーを入手したということでした。

一方サイバー犯罪者の間でも Hive がテイクダウンされたことに対する反応が見られ、例えば LockBit は Hive よりも慎重に復号キーを管理していると主張していました。また別のアクターは、当局は Hive のサーバーを解体しただけであって同オペレーションに関与していたアクターは逮捕できていないことに言及し、Hive のアフィリエイトはすでに他の RaaS オペレーションで活動し始めているであろうとも発言していました。

そしてこのアクターの発言は正しかったものと思われます。Hive のインフラストラクチャ解体が公表されたその 2 日後、我々は Hive で活動していたアフィリエイトが新たな働き先となる RaaS オペレーションを探していることを発見しました。この「Hive の元アフィリエイト」は自らの経歴として、北米やアジア、欧州で収益 500 万～20 億米ドルを有する企業のアクセスを入手し、ランサムウエア攻撃を実行した経験があると主張していました。また、「攻撃の際には自分で発見した初期感染ベクトルを使いたい、そしてその対価として身代金の 20%超が欲しい」という希望を掲載していました。この元アフィリエイトの活動は、ランサムウエアオペレーションが終了したところで、そのアフィリエイトまでもが単純に消滅するわけではない現状を表しています。彼らの多くは、活動をやめるよりも金銭を得られる別の場を探すことを選び、他のアフィリエイトプログラムに参加して企業を攻撃し続けています。

[15] U.S. Department of Justice Disrupts Hive Ransomware Variant

D0nut、他のデータリークグループとの協力体制をとっていたことを認める

2023 年 3 月、ランサムウエア「Monti」のオペレーターは「D0nut Leaks」の背後にいるアクターが「取引条件」を履行せず、Monti から 10 万米ドルを窃取したことをブログで公表しました（この「取引条件」とは、恐らく両グループの間で結ばれていたパートナーシップを指していると思われます）。またこの発言に加え、Monti は D0nut Leaks のウェブサイト管理画面の資格情報を公開していました。

D0nut Leaks のサイトが 2022 年 8 月に発見されて以降、同サイトに掲載された被害組織の中には過去に他のランサムウエアグループが犯行を主張していた組織もあったことが判明しています。したがって、D0nut Leaks が独自のランサムウエアを使用していたインシデントも確認されているものの、D0nut Leaks を運営しているアクターについては複数のランサムウエアオペレーションにアフィリエイトとして従事している、または何らかの形で協力体制をとっていると考えられています[16]。

サイバー犯罪者、ランサムウエアの普及に ChatGPT を悪用

サイバー犯罪社会では ChatGPT に関連した誇大広告が多数登場しています。またサイバー犯罪者の中でも、特にランサムウエアを操るアクターが ChatGPT を悪用していることが確認されています。例えば 2023 年 3 月には、アクター「DELUXXEN」が ChatGPT を使って作成したとするランサムウエアのコード（C++）を公開しました。またサイバー犯罪フォーラムに掲載されていた別の投稿では、ChatGPT のフィルターを回避してランサムウエアのスクリプトを作成する方法が説明されていました。

[16] D0nut extortion group also targets victims with ransomware

*アクター**DELUXXEN** が「**ChatGPT** を悪用してランサムウエアのコードを生成した」と主張している投稿*

2023 年第 1 四半期に売り出されたネットワークアクセス

2023 年第 1 四半期、我々が追跡調査を行った商品（ネットワークアクセス）は 600 件超、その希望販売価格は合計約 58 万米ドルとなりました。前年同期比で見たところ、今期の商品件数は 15%増加していましたが、希望販売価格の合計は 50%減少していました。売り出されたネットワークアクセスのひと月あたり平均件数は、前年同期が 175 件であったのに対し、今期は 200 件となりました。また平均価格は前年同期が 2,900 米ドルであったのに対し、今期は 1,100 米ドルとなりました。中央価格については前年同期と同じく今期も 400 米ドルとなりました。

また、最も多く売り出されていた商品は、RDP（リモートデスクトッププロトコル）を悪用したアクセスでした。

売り出し件数上位の初期アクセスブローカー

Paranoya

Paranoya は、2022 年 10 月からサイバー犯罪フォーラム「Exploit」と「XSS」で活動しています。大抵の場合、同アクターは 1 つの投稿に多数のアイテム（VPN や RDP を悪用したアクセス）を掲載して売り出しており、今期は約 60 件のネットワークアクセスを売り出しました。

Mafikeng

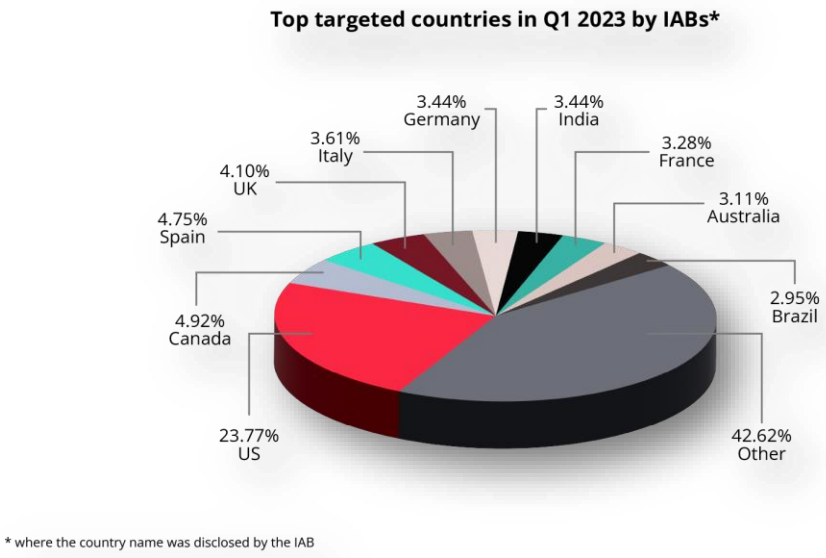
Mafikeng は 2022 年 12 月から XSS で活動しており、今期に入ってネットワークアクセスの販売広告を投稿するようになりました。同アクターの商品のほとんどは RDP を悪用したアクセスであり、その被害組織の国は多岐にわたっています。

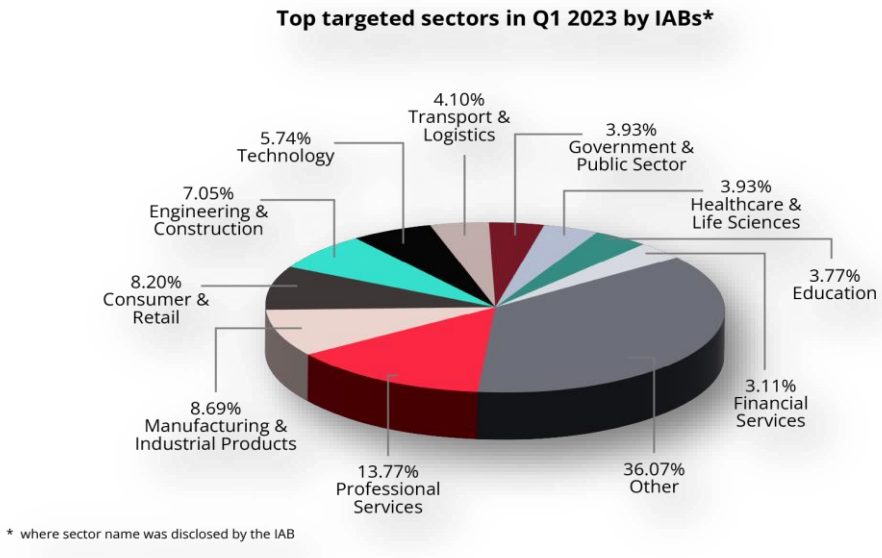
Sganarelle/Sganarelle2

Sganarelle（別名 Sganarelle2）は VPN や RDP を悪用したアクセスを 2016 年から売り出しており、経験豊富な初期アクセスブローカーであると思われます。同アクターは幅広いハッキング活動に関与しており、主にデータベースやクレジットカード情報を売買しています。

標的とされた国・業界

昨年に続き、2023 年第 1 四半期に初期アクセスブローカーの標的となった国の 1 位は米国であり（被害組織の約 23%）、その次にカナダ、スペイン、英国、イタリアが続きました。初期アクセスブローカーの標的となった業界の 1 位は専門サービスであり、その次に製造・工業製品、消費・小売が続きました。





注目すべき事例

最も高い収益を有していた被害企業

2023 年 2 月、我々は脅威アクター「Putin2023」が、インドに拠点を置き収益 820 億米ドルを有する多国籍コングロマリットのアクセスを売り出していることを確認しました。Putin2023 の説明によるとこのアクセスは VPN を悪用したものであり、ユーザー権限が付与された端末にログインできるということでした。このアクセスは 1 万 5,000 米ドルで売り出されましたが、その同日中に価格が 1 万米ドルへと引き下げられました。またこの投稿では、購入者がいない場合は Putin2023 自身がこのアクセスを悪用して多国籍コングロマリットのネットワークに不正アクセスすると記載されていました。そしてその後の 2 月 23 日、商品の売り出しが終了しました。

最も高額商品となった鉄鋼会社のアクセス

2023 年 1 月、我々は脅威アクター「Softlabgr」が、収益 8 億米ドルを有する鉄鋼会社のアクセスを売り出していることを確認しました。この売り出し投稿には、被害組織となる鉄鋼会社が拠点とする米国の他に、メキシコでも操業していることが記載されていました。Softlabgr の説明によると、このアクセスは RDP と VPN、AnyDesk を悪用したものであり、管理者権限が付与された端末にログインできるということでした。このアクセスは 3 Bitcoin（約 5 万米ドル相当）で売り出されていましたが、Softlabgr が売り出した商品はこのアクセス 1 件のみであるため、その信ぴょう性については疑問の余地があります。

VMware ESXi のアクセスを販売する初期アクセスブローカー

VMware 社製 ESXi に存在する脆弱性を標的としたランサムウエアキャンペーンが発生した 2023 年 2 月、我々は脅威アクターの間で、VMware 社製サーバーを介したアクセスを入手することについて関心が高まっていることを確認しました。例えばこの 2 月に脅威アクター「beffjezos」が

VMware 社製 vSphere サーバーの SSH アクセスを売り出した際には、早くもその同日中にアクセスを買い取られたことを発表していました[17]。

その他にも、VMware 社製 vSphere のコンポーネントである「vCenter」のアクセスを持っていると主張する脅威アクターが、vCenter を悪用してネットワークを侵害する方法について質問したり、別のアクターが RDP や VMware マシンをはじめとする仮想マシンに不正アクセスする方法を質問するなど、サイバー犯罪者が VMware 社製品を侵害することに関心を持っている様子が観察されました。

その他の不正なサービスを提供する初期アクセスブローカー

初期アクセスブローカーは次々と新たなサービスを提供しており、ネットワークアクセス以外の不正なサービスを提供している者もいます[18]。例えば、2023 年第 1 四半期に売り出し商品件数でトップ 5 にランクインした「nixploiter」は、アクセスの有効性をチェックする新サービスを宣伝していました。nixploiter によるとこのサービスを使うことで、購入したアクセスが初めて売りに出された商品であるのか、それとも過去に他のアクターが複数回販売した「中古品」であるのかを調べ、詐欺師を特定することができるということでした。nixploiter はこのサービスを無料で提供しており、その代わりに寄付先として自身のウォレット情報を掲載していました。

MSP や IT 企業を標的とするアクター

2023 年第 1 四半期、脅威アクターは引き続き MSP（マネージドサービスプロバイダー）や IT 企業に不正アクセスし、そのパートナー企業や顧客も侵害していました[19]。例えば 2023 年 1 月 12 日、我々は脅威アクター「570RM」が、顧客のバックアップファイルを保存するクラウド

[17] VMware 社の vSphere はクラウドコンピューティングシステムを構築する仮想化プラットフォームであり、仮想マシンの管理に使用されています。vCenter は vSphere のコンポーネントであり、複数の ESXi ホストを制御する統合管理ツールです。詳細については VMware vSphere vs. vCenter vs. ESXi – Differences, Benefits, and More をご覧ください。

[18] 弊社 2022 年アニュアルレポート

[19] 弊社ブログ— 狙われる MSP： 脅威アクターの一石二鳥 （多鳥）な攻撃術

サービス企業のアクセスを売り出していることを確認しましたが、その売り出し投稿にはこの IT 企業のみならず、その顧客に関する情報（一部を編集した資格情報など）を映したスクリーンショットも掲載されていました。このアクセスはオークション形式で売り出されましたが、2023 年 1 月 12 日付の投稿に記載された情報から、1,500 米ドルで何者かに落札されたことが判明しています。

組織の防御者として活動される皆様への提言

過去数年の間に、サイバー犯罪のエコシステムは全体的により高度に、そしてより複雑になりました。一方ランサムウエアグループやデータリークグループは、このエコシステムを利用して攻撃の規模を拡大しています。また彼らにとっては、このエコシステムのおかげで攻撃を実行することがこれまでよりも容易になっており、特にアンダーグラウンドで売り出されているネットワークアクセスが彼らにとって「見込み客（標的）」の重要なソースになっていることが判明しています。

組織のネットワーク防御に従事される皆様がサイバー犯罪者の一歩先を行くためには、堅牢なセキュリティ戦略が必要となります。その一環として、セキュリティ強度の高いパスワードや多要素認証、最新のソフトウエア、ファイヤーウォールを導入すること、そしてサイバー犯罪者を正確に理解することが求められます。

また、脅威アクターの活動を理解して最新の脅威の先を行くためには、サイバー犯罪脅威インテリジェンスを利用することが鍵となります。これについては、脅威アクターやサイバー犯罪ソースを監視して、以下の点を理解することが含まれます。

- アンダーグラウンドで展開されている様々な犯罪活動
- 脅威アクターが使用しているマルウエアやハッキングツールの種類、悪用している脆弱性
- 脅威アクターが標的としている業種
- 同業他社のアタックサーフェスの露出状況

さらに、オンライン上で身を守る方法について従業員にトレーニングを行うことも重要です。各従業員が、オンラインの作業に潜むリスクとその回避方法を理解しておく必要があります。

また、攻撃が発生した場合の戦略（従業員や顧客への通知など情報伝達に関する計画や、事後処理の対応計画など）を策定しておくことも重要です。

上記のアプローチを採用することで、組織として積極的な防御を実現し、現実に即したセキュリティ戦略を策定し、サイバー犯罪者の一歩先を行くことが可能となります。

サイバー犯罪者をリードするために KELA のサービスをご活用いただけます。

弊社のサイバーインテリジェンスプラットフォームの無料トライアルを、今すぐお試しください。