サイバーセキュリティレポート

2024.09

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　OSINT モニタリングチーム

目次

【1 ページサマリー】

当レポートでは 2024 年 9 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『中国系ハッカーグループ DragonRank が SEO ランキングを操作』

- 中国系ハッカーグループ DragonRank が複数のマルウェアを用いて、アジアやヨーロッパの国々を標的とした SEO のランキング操作を行っていることが判明した。
- DragonRank の主な活動は、IIS サーバーを侵害してこれを制御し、SEO 操作に使う BadIIS マルウェアを埋め込み、ブラックハット SEO を行うことである。
- 今回の事件の攻撃手法は中国 APT との関連が想起されるが、攻撃の目的は国家の意思を実現しているとは考えにくく、中国 APT の高度な技術が国家の意思の外で利用されている可能性がある。

第 2 章『廃病院の Web サイト、復活』

- 閉院した病院のドメイン名を取得して、その病院の Web サイトを勝手に復元した会社役員の男性が、2024 年 9 月 11 日に著作権法違反の疑いで書類送検された。
- 男性はドメイン名も含めて Web サイトを復元することで、閉院前の病院の Web 検索における評価を引き継ごうとしたとみられる。
- 同様の手口がフィッシングサイト設置等のサイバー攻撃に用いられた場合、危険である。ドメイン名を安易に手放さないといった対策の周知だけでなく、医療機関等の公益性のある組織が廃業した後、ドメイン名が悪用されないようにする仕組みについての議論が必要である。

第 3 章『RansomHub の猛威と米国 4 組織によるセキュリティアドバイザリの発行』

- 2024 年 2 月に活動が確認された暴露型ランサムウェアグループ RansomHub が猛威を振るっている。同様の犯罪グループのうち、7 月以降は LockBit を抜いて、1 か月あたり最も多くの被害組織を記録している。
- FBI、CISA を含む米国の 4 組織は共同で、RansomHub の攻撃から組織を守るためのセキュリティアドバイザリを発行した。RansomHub と既存のグループの攻撃手法に大きな違いはみられない。
- 西側捜査機関の活動により、既存のランサムウェアグループは活動停止や縮小に追い込まれている。しかし、RansomHub のような新たなグループが現れ、ランサムウェア攻撃の脅威は途切れることなく続いている。国際秩序が回復するまではこの状況は大きく変わらないと考えられる。

1. 中国系ハッカーグループ DragonRank が SEO ランキングを操作

1.1. 概要

中国系ハッカーグループ DragonRank が、アジアやヨーロッパの国々で SEO ランキングの操作を目的とした活動を行っていることが、セキュリティ企業 Cisco Talos の調査で判明した。DragonRank は、ターゲットの IIS サーバーを侵害してこれを制御した状態を維持し、ここに SEO のために使用するマルウェアを埋め込む。そして、悪意のあるサイトや不正なコンテンツへ誘導するためにそのようなサイトが上位に表示されるようにしたり、ランキングを改変したりするためのブラックハット SEO を積極的に行っていた[1]。

1.2. SEO について

SEO とは Search Engine Optimization（検索エンジン最適化）の略である。これは、Google や Yahoo 等の検索結果において、自分の Web サイトをより上位に表示させてアクセス数を増やすための施策であり、これにはサイトのコンテンツの調整等が含まれる。

基本的に検索エンジンではクオリティの高いページを上位に表示しようとする。そしてこの特性に対応する手法として、ホワイトハット SEO とブラックハット SEO がある。ホワイトハット SEO は検索エンジンのガイドラインやアルゴリズムに従ってユーザーに有益なコンテンツを提供したり、検索エンジンが理解しやすい Web サイトを構築したりすることで検索エンジンでの評価を上げることを試みるものであるが、これに対してブラックハット SEO は不正な方法を用いて、特定のサイトが検索エンジンで上位に表示されるよう操作する。ブラックハット SEO はフィッシング詐欺等、悪意のあるサイトへの誘導にも利用されている[2]。

1.3. DragonRank の攻撃について

【攻撃対象】[3]

ハッカーグループ DragonRank は、その攻撃の戦術・技術・手順（TTP：Tactics, Techniques, and Procedures）から、簡体字中国語話者で構成されていると考えられる。被害者（個人／組織）は、タイ、インド、韓国、ベルギー、オランダ、中国など、さまざまな地域に広がっている。業種も、製造、輸送、風水、宝飾品、メディア、研究サービス、ヘルスケア、テレビおよびビデオ制作、宗教団体など多種にわたる。

[1] 出典：CISCO TALOS『DragonRank, a Chinese-speaking SEO manipulator service provider』
https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

[2] 出典：ディーボの SEO ラボ『ブラックハット SEO とホワイトハット SEO の違いとは？』
https://seolaboratory.jp/50555/

[3] 出典：CISCO TALOS『DragonRank, a Chinese-speaking SEO manipulator service provider』
https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

【侵害活動】[4]

DragonRank の攻撃は、Web アプリケーションサービス（phpMyAdmin や WordPress など）の脆弱性を利用し、標的のシステムへの侵入を試みることから始まる。これに成功し、リモートでのコマンド実行が可能になると、そのシステムへのアクセスを維持するための Web シェル（悪質なスクリプト）をインストールする。そして、外部から標的のシステムに対する操作を可能とするバックドア型マルウェアとして主に PlugX を利用して、ログイン情報等を収集する。

このようにして IIS サーバーはマルウェアに感染させられ、攻撃者の指令用サーバーとの通信に利用される。さらに、SEO 操作を行うため、BadIIS マルウェアを使用する。これにより、検索エンジンでの検索結果のページに表示される（Web サイトへの）リンクを変更することができる。また、同マルウェアは IIS サーバーからの HTTP レスポンス（Web クライアントから送信された HTTP リクエストに対する、Web サーバーからの応答）を、攻撃者が制御したコンテンツに書き換えて、検索エンジンで使用されているクローラー（同エンジンがそのデータベースの中から最適な検索結果を取得するためのプログラム）に渡すことで、SEO ランキングの操作を行う[5]。

DragonRank により侵害された IIS サーバーは 35 台以上に上ることが確認されている。これらのサーバーを利用して詐欺サイトの展開、宣伝を行い、そのようなサイトを検索エンジンでの検索結果の上位に表示させることで、ユーザーを詐欺サイトへ誘導していた。

【DragonRank の活動の特徴】[6]

この手のブラックハット SEO でよく使われる手法としては同種の脆弱性を持つ多数の公開 Web サーバーを侵害して SEO 操作を行うことが挙げられる。一方、DragonRank は標的のシステムに侵入し、1 台目のサーバーを侵害した後、同システムに存在する他のサーバーに侵害範囲を拡大していき、それらの制御を維持することが特徴である。

また、DragonRank は Telegram や QQ といったインスタントメッセージングアプリにおいて、「tttseo」というハンドル名を使用して、違法なビジネスの販売促進を行っていることも確認されている。同グループが提供するビジネスは、顧客のニーズに合わせてカスタマイズされた SEO 詐欺サービスで、顧客が宣伝したいキーワードと Web サイトの情報を送信すると、DragonRank がそれに基づいて詳細なプランを作成する。彼らは、特定の国や言語でのプロモーションを得意としており、この手のサイバー犯罪グループの中でも高いレベルのサービスを提供しているようである。

[4] 出典：CISCO TALOS『DragonRank, a Chinese-speaking SEO manipulator service provider』
https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

[5] 出典：Trend Micro『脅威データベース「Backdoor.Win32.BADIIS.A」』
https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/malware/backdoor.win32.badiis.a

[6] 出典：CISCO TALOS『DragonRank, a Chinese-speaking SEO manipulator service provider』
https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

図 1 ビジネスモデル（中国語版と英語版が存在）を紹介する DragonRank の商用 Web サイト[7]

1.4. まとめ

DragonRank の活動は、標的のシステムに侵入した後、アクセスを維持し、同システム内の他のサーバーにも侵害範囲を広げる活動を行う。これは APT の活動でよくみられる動きである。また、攻撃に利用されている PlugX も、中国の APT がバックドアツールとして使用していることが知られている。

このように DragonRank の攻撃手法は中国 APT との関連が想起されるが、攻撃の目的は国家の意思を実現しているとは考えにくく、中国 APT の高度な技術が国家の意思の外で利用されていると推察される。

今年 2 月には、中国のセキュリティサービス企業 i-Soon 社の大量のデータが GitHub（プログラムのソースコードをオンラインで管理するサービス）のサイトで公開される事件[8]があったが、その漏洩データから、中国政府機関が国内のセキュリティサービス企業にスパイ活動を外注していることが明かになった。このような外部の企業が関連している可能性も考えられるが、定かではなく、今後も同様に中国 APT の技術が金銭目的の犯罪で悪用されることがあるのか注視が必要である。

[7] 出典：CISCO TALOS『DragonRank, a Chinese-speaking SEO manipulator service provider』 https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

[8] 出典：Krebs on Security『New Leak Shows Business Side of China's APT Menace』 https://krebsonsecurity.com/2024/02/new-leak-shows-business-side-of-chinas-apt-menace/

2. 廃病院の Web サイト、復活

2.1. 概要

2023 年 4 月に、千葉県のある病院（以降、「A 病院」と表記）が閉院した。閉院後も病院の Web サイトは存続していたが、しばらくしてドメイン名の失効により消滅した。それから程なく、ある男性がドメインオークションで手に入れた A 病院のドメイン名を使用しコピーサイトを設置するという事件が発生した。なお、この男性は著作権侵害に当たる画像をコピーサイトで公開していた疑いで、2024 年 9 月に書類送検された[9]。

このコピーサイトの作成目的は健康食品の Web 広告の設置であったと男性は述べており、サイバー攻撃を意図したものでは無かった。しかし、Google 等の検索エンジンを欺くことを意識した本件の手法は、フィッシングサイトを効果的に展開する等、サイバー攻撃に悪用できる可能性がある。

2.2. 病院のドメイン名を利用したコピーサイトの設置

【病院の閉院とドメイン失効】

A 病院はローマ字で表記した病院名の JP ドメイン名（～.jp）を登録し、Web サイト等に使用していた(図 2)。A 病院は 2023 年 4 月に閉院し、その後もドメイン名はしばらく登録が有効であったが、7 月 31 日で有効期限が切れた。その後、ドメインオークションの事業者がこの登録の無いドメイン名を再登録し、2023 年 9 月にオークションに出品した。

【落札したドメイン名でコピーサイトを設置】

A 病院のドメイン名は、大阪府の広告会社役員の男性が落札した。男性は落札直後の 9 月 29 日に A 病院の旧 Web サイトをコピーして復元したサイトを設置した。旧 Web サイトを制作した会社がこのコピーサイトの存在を知り、犯罪に繋がりかねないことを危惧して 11 月に千葉県警に連絡した。コピーサイトは 11 月 13 日に閉鎖された[10]。

なお、A 病院の旧 Web サイトでは写真事務所が著作権を有する写真を使用していた。コピーサイトを設置することで、これらの写真を写真事務所に断りなくネット上に公開したことから、男性は著作権法違反（著作権侵害）の疑いで 2024 年 9 月 11 日に書類送検された[11]。

[9] 出典：千葉日報オンライン『閉鎖病院のホームページ勝手に復元、サプリ広告サイトに転用か　著作権法違反容疑で男性書類送検　千葉県警』 https://www.chibanippo.co.jp/news/national/1274778

[10] 出典：千葉日報オンライン『閉鎖病院のホームページ勝手に復元、サプリ広告サイトに転用か　著作権法違反容疑で男性書類送検　千葉県警』 https://www.chibanippo.co.jp/news/national/1274778

[11] 出典：産経ニュース『閉鎖病院の HP を再公開疑い、会社役員の男を書類送検　取り扱う健康食品の広告掲載』 https://www.sankei.com/article/20240911-7BKFCDM5YNI3DGG33A36IYZ7IM/

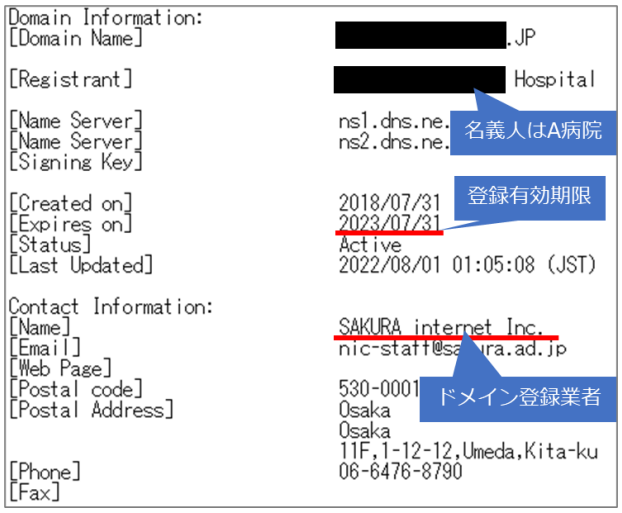

図 2 A 病院が登録していた時期の WHOIS 情報

登録の有効期限は 2023/07/31。
Registrant(名義人)は A 病院になっている。

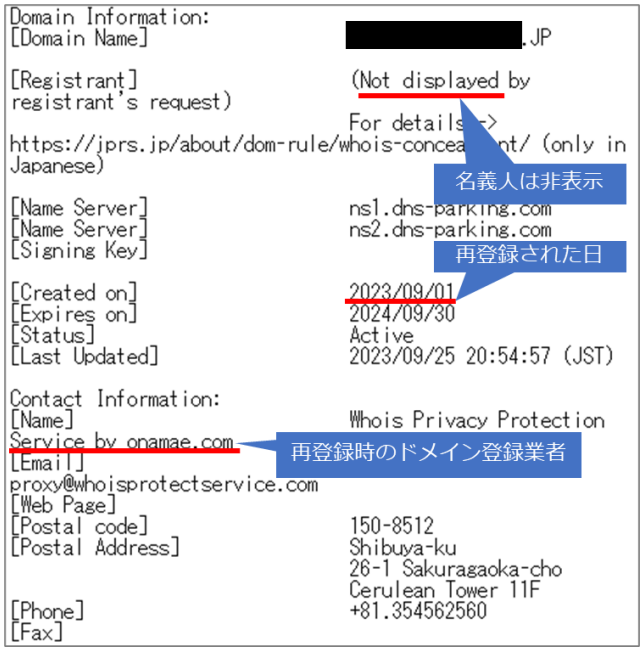

図 3 男性が登録していた時期の WHOIS 情報

A 病院の時とは別のドメイン登録業者(ドメインオークションの事業者と同一)が、2023/09/01 に再登録。
Registrant(名義人)は落札した男性とみられるが、非表示機能で隠されている。

2.3. 元サイトの評価にただ乗りするコピーサイト

検索エンジンにおける Web サイトの評価基準として、専門性、権威性、信頼性が重視されると言われている[12]。例えば医療情報分野では 2017 年に、キュレーションサイト（情報まとめサイト）によって人命に関わりかねない誤った情報が多数、Google 検索の上位に表示される問題が発覚したことがあった。これを契機に Google 社は、医療機関のサイトを優先して上位に表示するよう検索エンジンを修正した[13]。

かつて存在した病院のサイトを引き継いだように見せかける本件の手法は、このような Google 社の対策をかい潜るためであったと考えられる。報道によれば男性は、「病院の Web サイトは Web 検索で上位に表示されるので、病院の Web サイトを再掲してアクセス数が増えた後に、健康食品の広告を載せることで広告収入を増やすことを狙った」と述べている[14] [15]。

[12] 出典：GMO TECH『WEB 集客ラボ SEO に重要な E-A-T とは？Google の評価基準と対策方法を紹介』
https://gmotech.jp/semlabo/seo/blog/about_e-a-t/

[13] 出典：ITmedia NEWS『Google、医療・健康の検索結果を見直し 「より信頼性高いサイト」上位に』
https://www.itmedia.co.jp/news/articles/1712/06/news127.html

[14] 出典：千葉日報オンライン『閉鎖病院のホームページ勝手に復元、サプリ広告サイトに転用か 著作権法違反容疑で男性書類送検 千葉県警』
https://www.chibanippo.co.jp/news/national/1274778

[15] 出典：産経ニュース『閉鎖病院の HP を再公開疑い、会社役員の男を書類送検 取り扱う健康食品の広告掲載』
https://www.sankei.com/article/20240911-7BKFCDM5YNI3DGG33A36IYZ7IM/

2.4. まとめ

本件の手法はサイバー攻撃への応用が危惧される。例えばフィッシングであれば、疑うことが難しいフィッシングページを設置できることになる。検索の上位に表示されるうえ、ドメイン名等、サイト自体に不審な点はほとんど無いため、アクセスした人は認証情報や個人情報等を疑うこと無く騙し取られかねない。この手法は医療分野だけでなく、金融や福祉など専門性の高い他分野のサイトでも応用が利く[16]ため、注意が必要である。

本件のような手法の他にも、失効したドメイン名がドメインオークションなどを経て元の組織と関係のない組織に再利用されるといったケースが後を絶たない[17]。対策として、使わなくなったドメイン名は失効しないように登録を続けることが推奨されている[18]。しかし、A 病院のように組織が消滅する場合、ドメイン名を維持し続けることは困難である。医療機関など公益性の高い組織が使用していたドメイン名の再利用を防ぐ仕組みについて、議論が必要と考える。

[16] 出典：GMO TECH『WEB 集客ラボ YMYL とは？これからの SEO・サイト運営で気をつけるべきポイントを解説』
https://gmotech.jp/semlabo/seo/blog/ymyl_point/

[17] 出典：NHK『「パパ活」情報「Go To イート」URL で表示 ドメイン流用の実態』
https://www3.nhk.or.jp/news/html/20231125/k10014268791000.html

[18] 出典：日経クロステック（xTECH）『廃止ドメインに残る「価値」を積極的に減らす、トラブルを起こさない上手な手放し方』
https://xtech.nikkei.com/atcl/nxt/column/18/02729/013000003/?P=3

3. RansomHub の猛威と米国 4 組織によるセキュリティアドバイザリの発行

3.1. 概要

2024 年 2 月に活動が確認された新興の暴露型ランサムウェアグループ RansomHub が猛威を振るっている。

8 月末までの約 7 か月で 200 以上の組織が RansomHub の被害に遭い、その勢いは現在も続いている。

8 月 29 日、連邦捜査局（FBI）とサイバーセキュリティ・インフラセキュリティ庁（CISA）を含む米国の 4 組織は共同で、「#StopRansomware: RansomHub Ransomware」と題するセキュリティアドバイザリを発行し、RansomHub の攻撃から組織を守るための注意喚起を行った[19]。

図 4　RansomHub がダークネットで運営している暴露サイト

3.2. RansomHub について

RansomHub は、2024 年 2 月に活動が確認された暴露型ランサムウェアグループである。

RansomHub は RaaS（Ransomware as a Service）と呼ばれる、ランサムウェア開発と攻撃を分業する運用形態をとっている [19]。特定の国や業界をターゲットとすることはなく、政府機関、医療、情報技術、食品、金融といった様々な組織が RansomHub の被害に遭っている。

その活動は非常に活発で、2 月～8 月の 7 か月間で、世界中の 200 以上の組織が RansomHub の被害に遭った。またランサムウェアグループの中では、2022 年以降、1 年あたりの被害組織数が最も多い LockBit、2024 年の被害組織数が LockBit に次いで多い Play を抜いて、2024 月 7 月以降、RansomHub が 1 か月あたり最も多くの被害組織を記録している（図 5）。その背景には、2024 年 3 月頃に活動を停止した ALPHV や[20]、2024 年 2 月に英国家犯罪対策庁

[19] 出典：CISA『#StopRansomware: RansomHub Ransomware』
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

[20] 出典：BleepingComputer『BlackCat ransomware shuts down in exit scam, blames the "feds"』
https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/

（NCA）と FBI を中心とする捜査機関により IT インフラが差し押さえられた後[21]、5 月に首謀者が指名手配された[22]ことで勢いが弱まった LockBit から、アフィリエイト（攻撃の実働部隊）を取り込んでいることにある[23]。

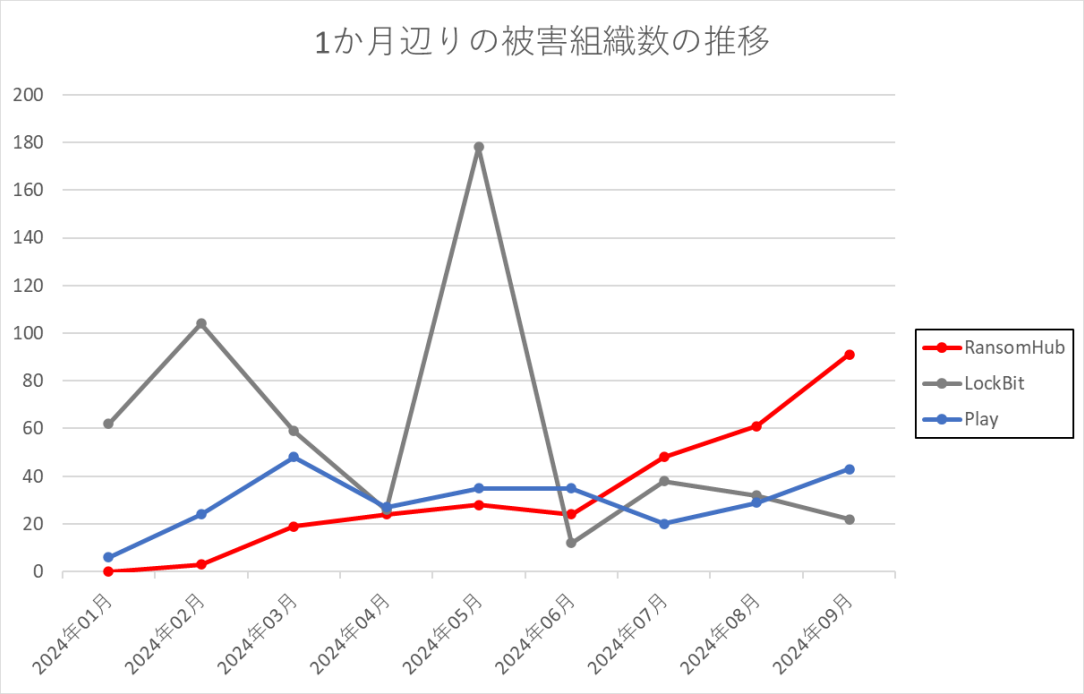

図 5 主要ランサムウェア 3 グループの 1 か月あたりの被害組織数の推移
※2024 年 5 月の LockBit の被害組織数が突出しているが
捜査機関の活動に反発し、同グループが実際には攻撃していない
組織も攻撃したと主張して被害組織を水増ししている疑惑がある。

使用するランサムウェアとこれにより攻撃を受けたコンピューターに残される脅迫メッセージ（ランサムノートと呼ぶ）の類似性から、RansomHub は 2 月に活動を終了した Knight（旧名 Cyclops）からランサムウェアのソースコードを購入し、それを修正して使用しているとみられている[24]。このように過去に活動していたグループの資産を活用する点も、RansomHub の攻撃能力に寄与していると考えられる。

3.3. 米国 4 組織によるセキュリティアドバイザリの発行

米国の FBI、CISA、多州間情報共有・分析センター（MS-ISAC）、保健福祉省（HHS）の米国 4 組織は 2024 年

[21] 出典：NCA『International investigation disrupts the world's most harmful cyber crime group』
https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

[22] 出典：NCA『LockBit leader unmasked and sanctioned』
https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned

[23] 出典：Google Cloud Blog (Mandiant)『Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools』
https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools

[24] 出典：Symantec『RansomHub: New Ransomware has Origins in Older Knight』
https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware

8 月 29 日に共同で、「#StopRansomware: RansomHub Ransomware」と題するセキュリティアドバイザリを発行した[19]。

これは、米国の政府組織が実施している、ランサムウェア攻撃から組織を守るための包括的な取り組み #StopRansomware[25]の一貫として発行されたものである。

このセキュリティアドバイザリでは、組織が RansomHub によるランサムウェア攻撃からシステムを保護できるように、攻撃の戦術・技術・手順（TTP：Tactics, Techniques, and Procedures）が紹介され、侵害の兆候を検知するための IP アドレス、URL、ファイルパスといった IoC 情報の提供、侵害が確認された場合の対応方法や緩和策について述べられている。

これを読むと、フィッシングメール、アカウント侵害、脆弱性の悪用により被害組織へ侵入し、その後は OS の標準機能やフリーソフトなどを利用して侵入後の攻撃を行うというように、RansomHub と既存のグループの攻撃手法に大きな違いは見られない。認証に MFA を利用する、システムを最新の状態に保つ、フィッシングメールを受信した場合に備えてユーザー教育を実施するといった基本的なセキュリティ対策が、新規のランサムウェアグループの攻撃に対しても有効な防御策であると考えられる。

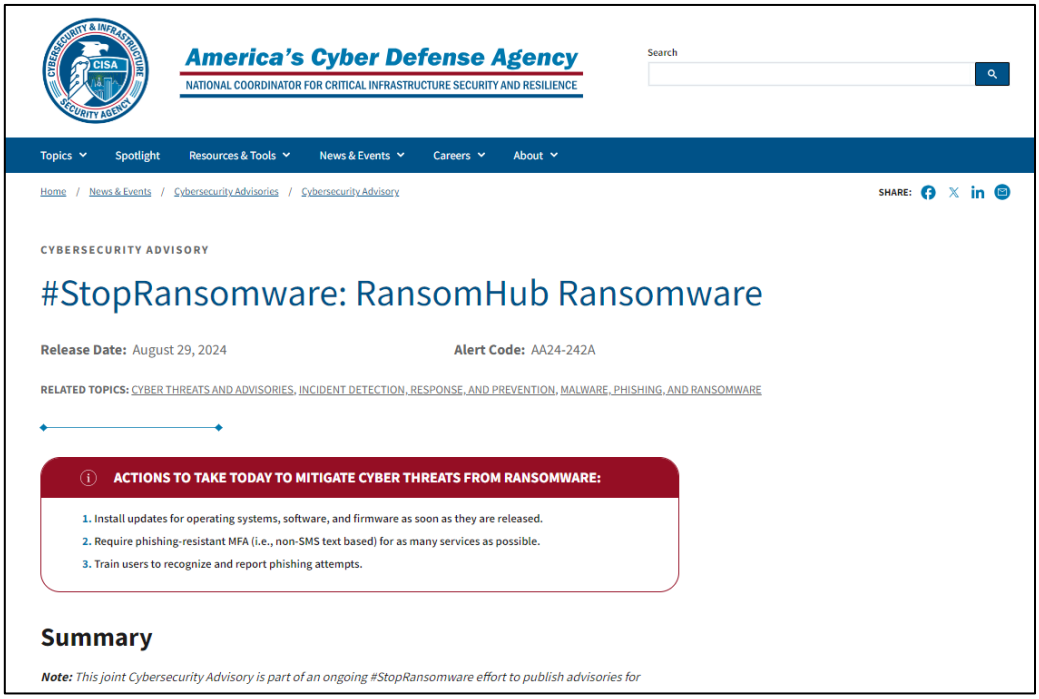

図 6 米国 4 組織が共同で発行した RansomHub に対するセキュリティアドバイザリ

3.4. まとめ

NCA や FBI といった捜査機関の活動により、猛威を振るっていた ALPHV や LockBit といったランサムウェアグループは活動停止や規模縮小に追い込まれた。しかし、RansomHub のような新たなグループが現れ、ランサムウェア攻撃の脅威は途切れることなく続いている。

[25] 出典：CISA『STOP RANSOMWARE』
https://www.cisa.gov/stopransomware

これはランサムウェアの活動拠点の多くがロシアにあり[26, 27]、西側捜査機関による取締りから暴露サイトの閉鎖や一部のアフィリエイトの逮捕に発展しても、主要メンバーや他の多くのアフィリエイトには法執行機関の手が伸びず、野放しの状況が続いているためと考えられる。ウクライナ侵攻前にはロシア政府がランサムウェアグループの関係者を逮捕するなどの動きもあったが[28]、国際秩序が回復するまでは、この状況は大きく変わらないと考えられる。

以上

[26] 出典：Krebs on Security『BlackCat Ransomware Raises Ante After FBI Disruption』
https://krebsonsecurity.com/2023/12/blackcat-ransomware-raises-ante-after-fbi-disruption/

[27] 出典：NCA『LockBit leader unmasked and sanctioned』
https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned

[28] 出典：BBC『REvil ransomware gang arrested in Russia』
https://www.bbc.com/news/technology-59998925

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　OSINT モニタリングチーム
メールアドレス：nsj-co-osint-monitoring@security.ntt