サイバーセキュリティレポート

2024.05

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 5 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『北朝鮮 IT 労働者が米企業でリモート就労、賃金は核・ミサイル開発資金源に』

- 5 月 15 日、米司法省は、北朝鮮の IT 労働者が身分を偽って米企業でリモートワークを行えるようにし、その賃金を北朝鮮に送金する手助けをしたとして、アリゾナ州在住のクリスティーナ・チャップマンら計 5 人を起訴した。
- 日本国内においても、制裁対象国である北朝鮮の IT 労働者を雇用し賃金を支払うことは、外国為替及び外国貿易法等の国内法に違反するおそれがあると警察庁は指摘している。
- 北朝鮮の労働者は、直接雇用の他に、業務委託や人材派遣を介して採用される可能性がある。誤って北朝鮮の労働者を雇い入れないよう、委託先や人材派遣会社との契約の見直し（採用手続きや監査の徹底等において）や、直接雇用の際の採用プロセスの厳格化、従業員のトレーニング等を通じた対策を講じる必要がある。

第 2 章『ランサムウェアグループ Lockbit の首謀者が特定され起訴、制裁対象に指定される』

- 英国家犯罪対策庁（NCA）、米司法省、欧州刑事警察機構（ユーロポール）は、ランサムウェアグループ LockBit の首謀者を特定し、その人物を発表した。首謀者はまた、米国などで起訴や制裁の対象に指定された。
- 2 月に捜査機関が実施した押収作戦に引き続き、首謀者の特定は、LockBit の攻撃能力削減や活動抑止を狙ったものと考えられる。
- 捜査機関は、今後も新たな作戦の実施や、捜査で明らかになった事実を継続的に発表することが予測され、LockBit はさらに追い詰められた状況に陥るであろう。

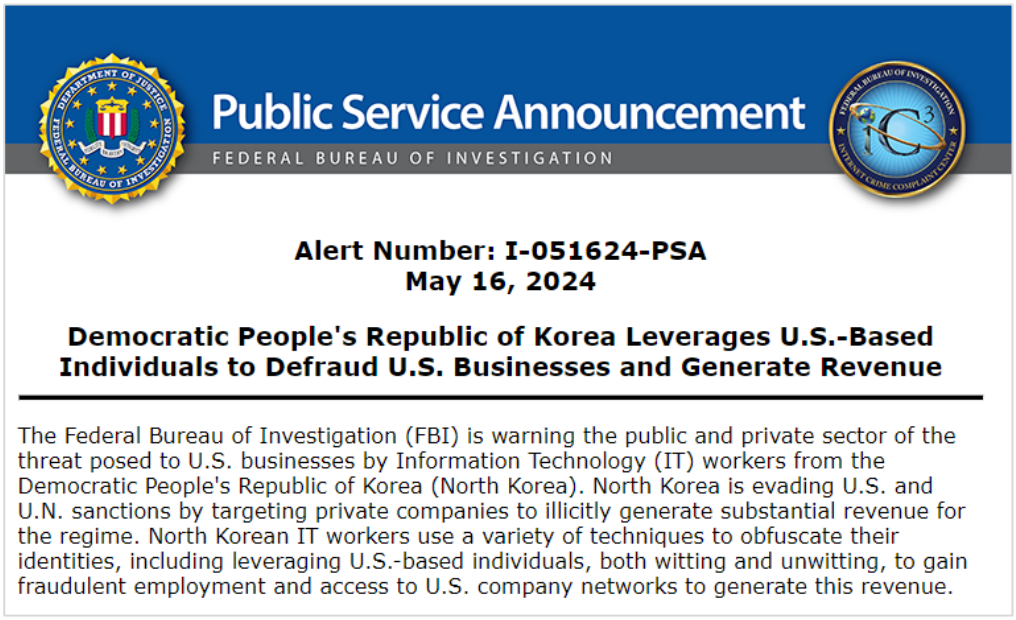
第 3 章『Wi-Fi 標準規格の脆弱性を悪用した「SSID 混乱攻撃」』

- VPN 関連のレビューサイト「Top10VPN」は、5 月、Wi-Fi 標準規格の設計上の欠陥を悪用した「SSID 混乱攻撃」（SSID Confusion Attack）について報告した。
- この攻撃では Wi-Fi のネットワーク識別名である SSID の確認の欠如を突くことにより、Wi-Fi クライアントを騙して安全性の低い回線に接続させる。これにより攻撃者に通信が傍受される等の恐れがある。
- この脆弱性の根本的な原因は Wi-Fi 標準規格の仕様の問題であるが、クライアント側で VPN を適切に使用することは傍受対策として効果的と考えられる。

1. 北朝鮮 IT 労働者が米企業でリモート就労、賃金は核・ミサイル開発資金源に

1.1. 概要

5 月 15 日、米司法省は、アリゾナ州在住のクリスティーナ・チャップマンをはじめとする、計 5 人を起訴した[1]。同容疑者らは、朝鮮民主主義人民共和国（以下、北朝鮮）の IT 労働者が身分を偽って米企業にてリモートワークを行えるようにし、その賃金を北朝鮮に送金する手助けをした疑いを持たれている。同日、FBI は、「北朝鮮は米国在住の個人を利用して米国企業を騙し、収益を上げている」と題した注意喚起を発表した[2]。北朝鮮の IT 労働者による外貨獲得の問題はここ数年国際的に問題視されており、国連安全保障理事会（以下、国連安保理）の北朝鮮制裁委員会専門家パネルの報告書等で、北朝鮮の IT 労働者に支払われた賃金の核・ミサイル開発への利用が指摘されている[3]。



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-051624-PSA
May 16, 2024

Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue

The Federal Bureau of Investigation (FBI) is warning the public and private sector of the threat posed to U.S. businesses by Information Technology (IT) workers from the Democratic People's Republic of Korea (North Korea). North Korea is evading U.S. and U.N. sanctions by targeting private companies to illicitly generate substantial revenue for the regime. North Korean IT workers use a variety of techniques to obfuscate their identities, including leveraging U.S.-based individuals, both witting and unwitting, to gain fraudulent employment and access to U.S. company networks to generate this revenue.

図 1 FBI による注意喚起

1.2. 国連安保理決議に基づく制裁

これまで北朝鮮の核・ミサイル開発への対応として、国連安保理は、様々な制裁を科してきた。例えば、2017 年 12 月に安保理にて全会一致で採択された 2397 号決議では、北朝鮮の労働者による収益が核・ミサイル開発に利用されているとし

[1] 出典：BleepingComputer『US woman allegedly aided North Korean IT workers infiltrate 300 firms』 https://www.bleepingcomputer.com/news/security/five-arizona-ukraine-charged-for-cyber-schemes-infiltrating-over-300-companies-to-benefit-north-koreas-weapons-program/

[2] 出典：FEDERAL BUREAU OF INVESTIGATION『Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue』 https://www.ic3.gov/Media/Y2024/PSA240516

[3] 出典：警察庁『北朝鮮 IT 労働者に関する企業等に対する注意喚起』 https://www.npa.go.jp/bureau/security/NK_it.pdf

て、北朝鮮の労働者を 2 年以内に自国から追放することを加盟国に求めている[4]。こういった過去の決議を受け、米国の財務省外国資産管理室（OFAC）は、米国人に対して、北朝鮮との間の物品・サービス・技術の輸出及び輸入や、北朝鮮に変わってソフトウェアの販売・供給・譲渡を行うこと等を禁じている[5]。

1.3. 事件について

【事件の詳細】[6]

チャップマン容疑者は他の容疑者と共謀し、北朝鮮の IT 労働者が国連安保理の制裁を逃れて米企業にてリモートワークに従事できるようにし、さらにその賃金を北朝鮮へと送金する手助けをしていた。同容疑者らの協力によって、北朝鮮の IT 労働者たちは、盗まれた個人情報を利用して米国人になりすまし、300 社以上の企業で仕事を得ていた。テレビ局や防衛企業、自動車メーカー等の大手企業も含まれており、約 700 万ドルの賃金が北朝鮮に送金されたとみられている。チャップマン容疑者は、国家に対する詐欺の共謀、個人情報の窃盗、マネーロンダリング、通信詐欺、個人情報詐欺、銀行詐欺の共謀で起訴され、最長で 97.5 年の懲役に処される可能性がある。

【ラップトップファーム】

国連安保理からの制裁を逃れるために、北朝鮮にいる IT 労働者が身分を偽って米国等の企業と契約してリモートワークを行うことにより、収入を得たり、企業の情報を窃取したりすることは以前から警戒されていた。2022 年 5 月 16 日には、米国の国務省、財務省、FBI が連名で「北朝鮮の IT 労働者に関するガイドライン」を発表し、警戒を呼び掛けていた[7]。

今回北朝鮮は、「laptop farm」（ラップトップファーム）と呼ばれる仕組みを利用することで、取り締まり等をかいくぐるよう偽装していた。ラップトップファームは、一種の場所貸しである。ラップトップファームのサービス提供者は、リモートワークを依頼する企業が IT 労働者に貸与するノートパソコン等の機器を国内（本件では米国）にある自拠点に設置し、それらを国外から遠隔操作できるように設定し提供している。

今回のチャップマン容疑者らも、自宅等にこのラップトップファームを設置していた。IT 労働者たちは実際には北朝鮮に住んでいたが、VPN 接続やリモートデスクトップ接続等を利用して、ラップトップファームにあるリモートワーク用のパソコンを操作することで、あたかも米国内で就労しているかのように見せかけることができた。

---

[4] 出典：Arms Control Association『UN Security Council Resolutions on North Korea』
https://www.armscontrol.org/factsheets/UN-Security-Council-Resolutions-on-North-Korea

[5] 出典：Hunton Andrews Kurth『U.S. Issues Guidance to Companies Warning of Cybersecurity and Sanctions Risks Posed by IT Workers Directed by North Korea』
https://www.huntonak.com/privacy-and-information-security-law/u-s-issues-guidance-to-companies-warning-of-cybersecurity-and-sanctions-risks-posed-by-it-workers-directed-by-north-korea

[6] 出典：BleepingComputer『US woman allegedly aided North Korean IT workers infiltrate 300 firms』
https://www.bleepingcomputer.com/news/security/five-arizona-ukraine-charged-for-cyber-schemes-infiltrating-over-300-companies-to-benefit-north-koreas-weapons-program/

[7] 出典：Office of Foreign Assets Control『GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS』
https://ofac.treasury.gov/media/923126/download?inline

【公的機関の反応】

5 月 16 日、FBI は本件に関して、「北朝鮮は米国在住の個人を利用して米国企業を騙し、収益を上げている」というタイトルで注意喚起を発表した（図 1）[8]。この中で、リモートワーカーの採用面接時には、居住地に関する情報やこれまでの経歴に関する質問に答えられるかを確認することや、採用時には、E-Verify（国土安全保障省の提供する米国人・外国人が米国で働く資格があるかを確認できるサービス）で身分証明書情報を確認すること等を推奨している。特に、IT 業務をアウトソーシングしている企業は雇用するプロセスに直接関わる機会がないため、より注意が必要であると述べている。具体的な対策として、企業が人材派遣会社に対し、その会社が厳格な採用手続きを実施し、定期的に採用手順を監査し、労働者の住所や給与の受け取り方法に変更があった際には通知することを要求すること等を推奨している。

また、5 月 17 日、FBI はチャップマン容疑者の共謀者である北朝鮮の IT 労働者 3 名とそのマネージャーである Zhonghua という人物を指名手配し、関連する情報について、最大 500 万ドルの報奨金を出すと X（旧 Twitter）等で発表した。

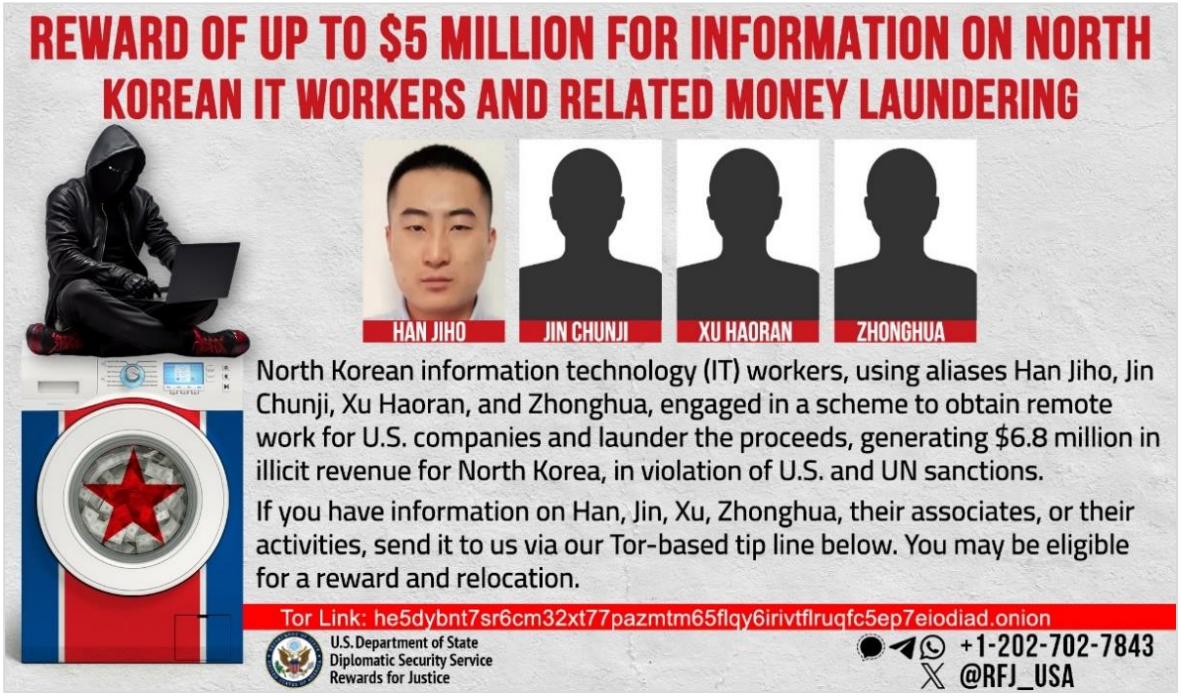


図 2 FBI による手配書[9]

1.4. 日本の事例

北朝鮮の IT 労働者が海外の仕事で収入を得る事例は米国に限ったことではない。北朝鮮の IT 労働者に日本国内の業務を発注し、賃金を送金していた広島市の IT 関連会社社長の男が 3 月 6 日に逮捕された。現時点での容疑は失業手

[8] 出典：FEDERAL BUREAU OF INVESTIGATION『Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue』
https://www.ic3.gov/Media/Y2024/PSA240516

[9] 出典：X『@RFJ_USA』
https://x.com/RFJ_USA/status/1791129092273611226

当の不正受給等であるが、全容を解明すべく捜査が続けられている[10]。

3 月 26 日には、警察庁が「北朝鮮 IT 労働者に関する企業等に対する注意喚起」を発表[11]。同文書は、「北朝鮮 IT 労働者に対して業務を発注し、サービス提供の対価を支払う行為は、外国為替及び外国貿易法等の国内法に違反するおそれがあります（一部省略）」と呼び掛けている。

1.5. まとめ

制裁対象となっている北朝鮮の労働者を雇用することは、違法行為として刑事罰を受ける恐れがあるだけではなく[11,12,13]、従業員とみなして付与したアクセス権を北朝鮮のサイバー攻撃者と共有される等のリスクも生じる[14]。また、賃金が北朝鮮の核・ミサイル開発に利用されていることに加えて、同国が大量破壊兵器や弾道ミサイル関連部品を調達する際にも、これらの労働者が関与している可能性が指摘されている。誤って北朝鮮の労働者を雇い入れないよう、警察庁や米司法省の注意喚起等を参考にしながら、採用プロセスの厳格化、従業員のトレーニングの実施等を通じて対策を講じる必要がある。また、委託先や人材派遣会社との契約について、スタッフの採用手続きを厳格化することや採用手順について監査を行うこと等を契約書に盛り込むといった、外部組織からの人材への対策も検討することが求められる。

[10] 出典：産経新聞『北ＩＴ技術者に業務発注か　韓国籍の男、邦人企業隠れみのに　神奈川県警など再逮捕へ』
https://www.sankei.com/article/20240327-LN7ZQ3DFXVIQXMV5F6QB7CLZDI/

[11] 出典：警察庁『北朝鮮 IT 労働者に関する企業等に対する注意喚起』
https://www.npa.go.jp/bureau/security/NK_it.pdf

[12] 出典：Office of Foreign Assets Control『GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS』
https://ofac.treasury.gov/media/923126/download?inline

[13] 出典：BleepingComputer『US sanctions orgs behind North Korea's 'illicit' IT worker army』
https://www.bleepingcomputer.com/news/security/us-sanctions-orgs-behind-north-koreas-illicit-it-worker-army/

[14] 出典：Hunton Andrews Kurth『U.S. Issues Guidance to Companies Warning of Cybersecurity and Sanctions Risks Posed by IT Workers Directed by North Korea』
https://www.huntonak.com/privacy-and-information-security-law/u-s-issues-guidance-to-companies-warning-of-cybersecurity-and-sanctions-risks-posed-by-it-workers-directed-by-north-korea

2. ランサムウェアグループ Lockbit の首謀者が特定され起訴、制裁対象に指定される

2.1. はじめに

5 月 7 日、英国家犯罪対策庁（NCA）、米司法省、欧州刑事警察機構（ユーロポール）は、ランサムウェアグループ LockBit の首謀者 LockBitSupp を特定し、この人物がロシア国籍で同国に在住するドミトリー・ホロシェフ（31 歳）であると発表した[15, 16, 17]。

併せて、ホロシェフが米国において恐喝、通信詐欺、共謀など 26 件の罪で起訴されたこと、英国、米国、オーストラリアで、制裁対象に指定されたことも発表された。

News

LockBit leader unmasked and sanctioned

A leader of what was once the world's most harmful cyber crime group has been unmasked and sanctioned by the UK, US and Australia, following a National Crime Agency-led international disruption campaign.

The sanctions against Russian national Dmitry Khoroshev (pictured), the administrator and developer of the LockBit ransomware group, are being announced today by the FCDO alongside the US Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Australian Department of Foreign Affairs.

Khoroshev, AKA LockBitSupp, who thrived on anonymity and offered a $10 million reward to anyone who could reveal his identity, will now be subject to a series of asset freezes and travel bans.

US partners have also unsealed an indictment against him and are offering a reward of up to $10m for information leading to his arrest and/or conviction.

The actions targeting Khoroshev form part of an extensive and ongoing investigation into the LockBit group by the NCA, FBI, and international partners who form the Operation Cronos taskforce.

図 3 NCA のニュースリリース [15]
※画像の人物がドミトリー・ホロシェフ

[15] 出典：National Crime Agency『LockBit leader unmasked and sanctioned』
https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned

[16] 出典：U.S. Department of Justice『U.S. Charges Russian National with Developing and Operating LockBit Ransomware』
https://www.justice.gov/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware

[17] 出典：EUROPOL『New series of measures issued against the administrator of LockBit』
https://www.europol.europa.eu/media-press/newsroom/news/new-measures-issued-against-lockbit

2.2. Lockbit について

LockBit は、ロシアを拠点とするランサムウェアグループであり、その活動は 2019 年に始まった[18]。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。ランサムウェアグループの中でも LockBit の活動は非常に盛んで、2022 年から現在に至るまで、最も多くの組織に被害をもたらしているグループである。

2.3. 2 月に行われた捜査機関による押収作戦

NCA と FBI を中心とする 10 ヵ国（日本の警察庁を含む）の捜査機関とユーロポールは協力して、LockBit に対する捜査活動 Operation Cronos を実施している[19]。その一環として、捜査機関は今年 2 月 19 日、LockBit に対する大規模な押収作戦を実施した[20, 21]。

この作戦により、捜査機関は LockBit の暴露サイト等として稼働していた 34 台のサーバーを含む IT インフラ、暗号化されたファイルの復号鍵約 1,000 個、不正なアカウント 14,000 件以上を押収し、200 以上の暗号通貨アカウントを凍結した。また、ポーランドとウクライナで 2 人を逮捕した他、フランスとアメリカで 3 件の国際逮捕状を発行し、5 件の起訴を行った。

押収作戦実施後、LockBit に表立った活動は見られなかった。しかし 2 月 24 日、同グループは暴露サイトを新たに立ち上げ、被害組織を脅迫するための投稿を再開し、現在も活動を継続している。

2.4. 捜査機関による LockBit の首謀者特定に関する発表

5 月 7 日、NCA、米司法省、ユーロポールは、ランサムウェアグループ LockBit の首謀者 LockBitSupp を特定し、この人物がロシア南西部の都市ヴォロネジに在住するロシア国籍のドミトリー・ホロシェフ（31 歳）であると発表した[15, 16, 17]。

さらに捜査機関は、LockBit から押収した暴露サイトを再利用して、ここでも同様の発表を行った（[図 4] なお、5 月 10 日をもって、このサイトの公開は終了している）。

また、ホロシェフが米国において恐喝、通信詐欺、共謀など 26 件の罪で起訴され、英国、米国、オーストラリアで制裁対象に指定されたことも併せて発表された。これにより、ホロシェフはそれらの国々において資産凍結と渡航禁止の対象となった。

---

[18] 出典：U.S. DEPARTMENT OF THE TREASURY『United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group』
https://home.treasury.gov/news/press-releases/jy2114

[19] 出典：EUROPOL『Law enforcement disrupt world's biggest ransomware operation』
https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[20] 出典：National Crime Agency『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

[21] 出典：U.S. Department of Justice『U.S. and U.K. Disrupt LockBit Ransomware Variant』
https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant

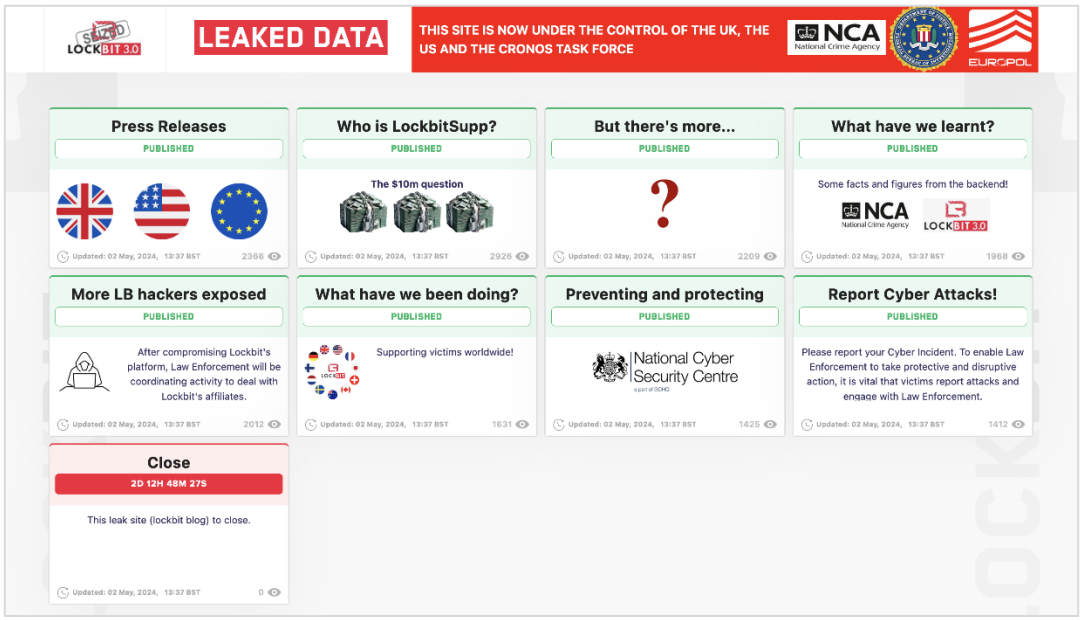


図 4 捜査機関が作成・公開した LockBit 情報サイト（同グループの旧暴露サイトを再利用）
※内容は LockBit 首謀者の情報に関するものに差し替えられた

米国で提出された起訴状によると、これまで LockBit とその実行部隊であるアフィリエイトが、被害組織から受け取った身代金の総額は約 5 億ドルである。ホロシェフは開発者として、その内の 20%に当たる約 1 億ドルを得ており、そこから LockBit の運営費を出しているとされる[22]。

日本の警察庁も 5 月 8 日、NCA 等が行った発表を受けて、国内で発生したランサムウェア事件の捜査で得られた情報を提供するなど、外国の機関と連携してランサムウェアに対する捜査を推進している旨を発表した[23]。

捜査機関の発表に対し、LockBitSupp は 5 月 9 日、自分はホロシェフではないとする主張を、LockBit の暴露サイトにロシア語と英語の両方で投稿している。

【NCA によるその他の発表】

NCA は、LockBit の首謀者特定の発表と共に、2 月に実施していた押収作戦の成果も発表した。それによると、2022 年 6 月から 2024 年 2 月の間に、LockBit とそのアフィリエイトは世界中で約 7,000 の組織に対して攻撃を行っていた。また、英国ではこの作戦の実施後、LockBit の攻撃が 73%減少し、他国でも同様に減少が見られること、これまで確認されている 194 人のアフィリエイトの内、現在活動しているのは 69 人と大幅に減っていることなど、LockBit の弱体化についても述べた。

2.5. まとめ

捜査機関や政府が、サイバー攻撃・サイバー犯罪の犯人や手口を特定し公表することをパブリック・アトリビューションと呼ぶ。これは、調査能力を示すことで更なる攻撃・犯罪を抑止することや、犯人を非難することなどを目的として実施される。

[22] 出典：U.S. Department of Justice『lockbit_indictment.pdf』
https://www.justice.gov/opa/media/1350921/dl

[23] 出典：警察庁『ランサムウェア「LockBit」被疑者の起訴等について』
https://www.npa.go.jp/news/release/2024/20240507001.html

捜査機関が、2 月に実施した押収作戦と、その影響によるアフィリエイトの減少により、LockBit の攻撃能力は大きく弱体化した。今回、捜査機関が LockBit の首謀者とされるホロシェフを特定し、詳細を発表したことは、LockBit に更なる制限を与え、その活動を終了に追い込むことを目的としていると考えられる。

捜査機関は、引き続き国際的に連携して捜査を続けるとしている。今後も新たな作戦の実施や、捜査で明らかとなった事実の継続的な発表を行うことで、LockBit はさらに追い詰められた状況に陥るであろう。

3. Wi-Fi 標準規格の脆弱性を悪用した「SSID 混乱攻撃」

3.1. 概要

VPN（Virtual Private Network）のレビューサイト「Top10VPN」は、5 月、Wi-Fi 標準規格の設計上の欠陥を悪用した「SSID 混乱攻撃」（SSID Confusion Attack）について報告した。この攻撃は、Wi-Fi のネットワーク識別名である SSID の確認の欠如を突くことにより、クライアントを騙して攻撃者のコントロール下にあるセキュリティの低い回線に接続させるものである。影響を受けるのは SSID 認証を使用しないモードにある Wi-Fi クライアントで、攻撃者に通信が傍受されるなどの恐れがある[24]。

3.2. SSID 混乱攻撃について

Wi-Fi のアクセスポイントは、SSID を含む信号を周囲に定期的に発信している。その信号を受信したデバイス（クライアント）が Wi-Fi ネットワークに接続する際、クライアントとアクセスポイントの間で通信暗号化と認証のためのやり取りが行われるが、Wi-Fi の標準規格である IEEE 802.11 では SSID の認証を常に行わないモードが存在する。この設計上の欠陥（CVE-2023-52424）を悪用したのが SSID 混乱攻撃である。

SSID 混乱攻撃で攻撃者はまず、自身でコントロール可能な、不正なアクセスポイントを用意する。これにより、通信に介在して通信内容を改ざんする、マルチチャネル中間者攻撃を可能にする [24]。

SSID 混乱攻撃は下記の方法で実行される [24]。

- 攻撃のターゲット（クライアント）は、自身が接続したことのある信頼済みのネットワークに接続しようとする。
- 攻撃者は、用意した不正なアクセスポイントの認証情報をこの信頼済みネットワークと同一に設定し、クライアントに通信が届く範囲に設置する。
- 攻撃者は、不正なアクセスポイントを介在させることで、信頼済みのネットワークとは異なるネットワークを、正しいものであるとクライアントに誤認させ、これに接続させる（クライアントの利用者は気付かない）。接続先がセキュリティの低いネットワークであった場合、この後、通信内容ののぞき見や遠隔操作等が行われる可能性がある。

[24] 出典：TOP10VPN『CVE-2023-52424 WiFi Vulnerability: The SSID Confusion Attack』
https://www.top10vpn.com/research/wifi-vulnerability-ssid/

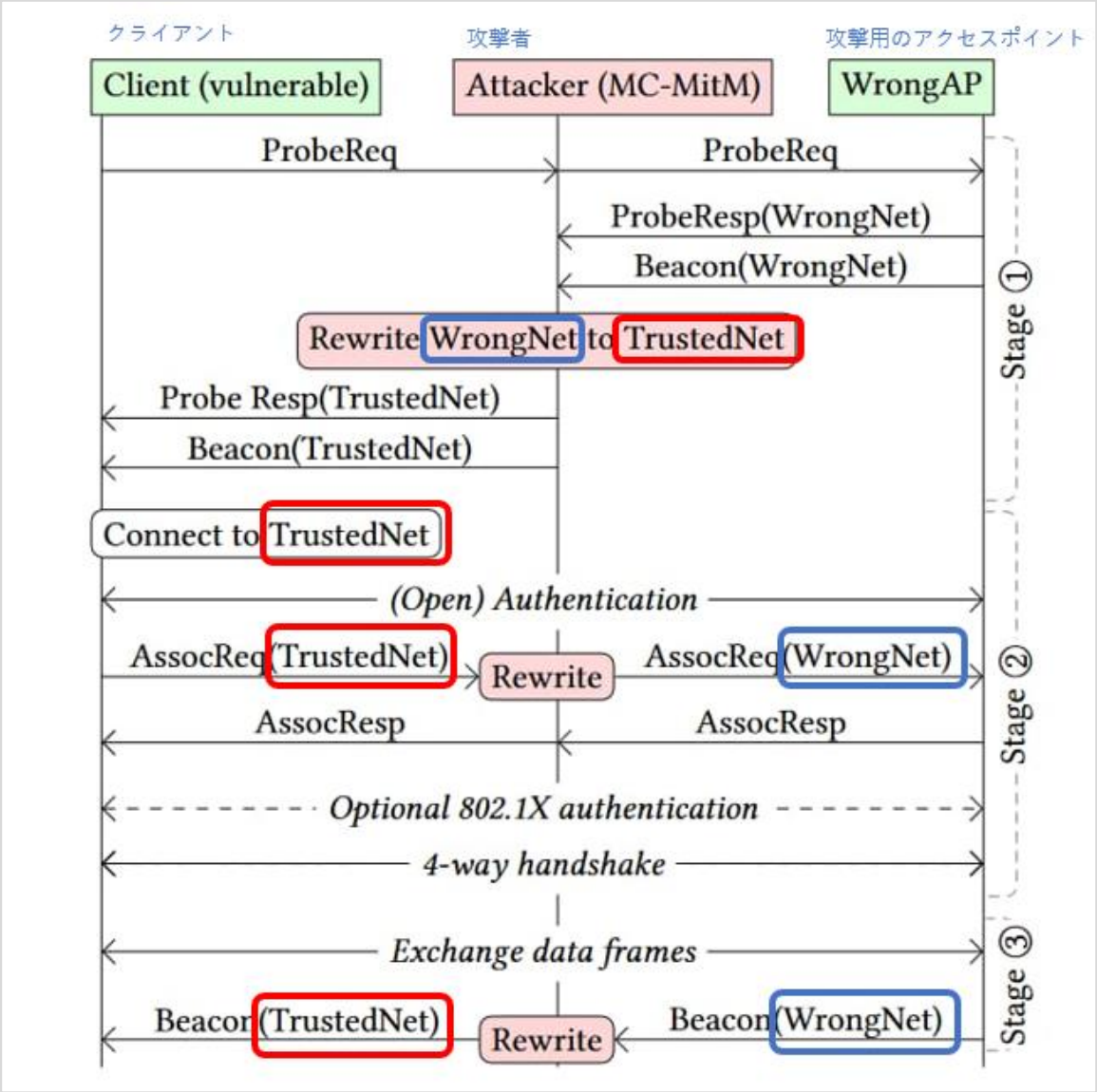


図 5 SSID 混乱攻撃 の接続までの流れ [24]（赤／青枠および日本語は当社記入）

クライアントは信頼できるネットワーク(TrustedNet)への接続を行おうとするが、中間の攻撃者によりセキュリティの低いネットワーク(WrongNet)に接続するよう誘導される。これへの接続が確立されることで攻撃が成功する

3.3. 防御策

防御策として最も有効な方法は、Wi-Fi 標準規格（IEEE 802.11）を設定している機関が、保護されたネットワークへの接続時に SSID の認証を要求するよう仕様変更することである。TOP10VPN は Wi-Fi Alliance（Wi-Fi に関連する多数の企業から成り、Wi-Fi の普及と進化を促進している世界的な非営利団体[25]）に本件を報告している [24]。

なお、攻撃が発生した場合でも、通信が暗号化されていれば攻撃者による傍受は防げるので、VPN を適切に使用することでこの攻撃に対するリスクは大幅に軽減できる。ただし、Cloudflare の WARP、hide.me、Windscribe などの一部の VPN は、信頼できるネットワークに接続すると自動的に VPN を無効にする機能があり、攻撃者の介入を招く可能性があるた

[25] 出典：Wi-Fi Alliance『Wi-Fi Alliance について』
https://www.wi-fi.org/ja/who-we-are

め注意が必要である[24]。

3.4. まとめ

Wi-Fi への攻撃時は電波が届く範囲に近接する必要があり、世界中の攻撃者から狙われるような脆弱性とは異なる。しかし、標的型攻撃では、これまで繰り返し Wi-Fi が狙われており[26]、ターゲットへの有力な攻撃経路として利用されている。

この脆弱性は Wi-Fi 標準規格の仕様の問題であるが、クライアント側で VPN を適切に使用すれば通信が暗号化され、傍受対策として当面は効果的と考えられる。ただ、多層防御の一角が崩れている状況は安全とは言い難く、Wi-Fi Alliance での標準規格の改善や Wi-Fi クライアントのアップデート情報に注視をしたい。

以上

[26] 出典：Kaspersky『「Darkhotel」の脅威とは』
https://www.kaspersky.co.jp/resource-center/threats/darkhotel-malware-virus-threat-definition

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： WA_Advisorysupport@ntt.com