サイバーセキュリティレポート

2024.02

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】 2
1. 米国、重要インフラを侵害する Volt Typhoon へのアドバイザリを発表 3
1.1. 概要 3
1.2. 発表されたアドバイザリについて 4
1.3. Volt Typhoon について 4
1.4. Volt Typhoon によるシステムへの侵入と潜伏 4
1.5. FBI が KV Botnet の駆除を実施 5
1.6. まとめ 6
2. LockBit への大規模な押収作戦の実施 7
2.1. 概要 7
2.2. ランサムウェアグループ LockBit 7
2.3. 捜査機関によるインフラ押収作戦 8
2.4. 押収作戦に対する LockBit の反応 9
2.5. まとめ 10
3. 香港でディープフェイクを使用した BEC 詐欺が発生 11
3.1. 概要 11
3.2. 事件の詳細 11
3.3. ディープフェイクと悪用の増加 12
3.4. 日本におけるディープフェイクの悪用事例 13
3.5. まとめ 14

【1 ページサマリー】

当レポートでは 2024 年 2 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『米国、重要インフラを侵害する Volt Typhoon へのアドバイザリを発表』

- CISA 等の米国を含む各国の政府機関が、中国関連の APT グループ「Volt Typhoon」に関するアドバイザリを発表した。
- 同グループの特徴として、ステルス性の高い戦術を用いて、標的とする重要インフラのシステム内で長期間にわたり潜伏を続けることが挙げられる。
- Volt Typhoon は、将来の有事の際に米国の重要インフラを攻撃することで、介入を妨害することを狙っていると考えられている。

第 2 章『LockBit への大規模な押収作戦の実施』

- 2 月 20 日、NCA（英国家犯罪対策庁）と FBI（米連邦捜査局）を中心とする捜査機関が、ランサムウェアグループ LockBit への大規模な押収作戦を実施したことが明らかとなった。
- 捜査機関は、暴露サイトを含む IT インフラや暗号化されたファイルの復号鍵など多くの情報を押収した。
- 捜査機関は今後も捜査を続けるとしており、LockBit の新たな関係者の逮捕や、国際的な包囲網の広がりが、攻撃活動に対する大きな制約に繋がると考えられる。

第 3 章『香港でディープフェイクを使用した BEC 詐欺が発生』

- 2 月 4 日、香港警察は、ある英国の多国籍企業がディープフェイクを利用したビデオ会議を用いた詐欺に遭い、2 億香港ドル（約 38 億円）を騙し取られたことを発表した。
- AI 技術の発展により、特別な知識や高性能なコンピューターがなくても、ディープフェイクコンテンツを作成できるようになった。2023 年には、インターネット上で同様のコンテンツが前年の 10 倍検出され、犯罪に悪用される例が増えている。
- 受け取ったメールや電話の内容に不審な点があれば、信頼できる方法で入手した連絡先に折り返しの電話をするなどして本人確認を行うことを徹底し、組織全体のディープフェイクに対する意識を高めていくことが重要である。

1. 米国、重要インフラを侵害する Volt Typhoon へのアドバイザリを発表

1.1. 概要

2024 年 2 月 7 日、米国のサイバーセキュリティー・インフラセキュリティー庁（以下、CISA）をはじめとする複数の国々のセキュリティ機関等が、中国政府の支援を受けるハッカーグループ「Volt Typhoon（ボルト・タイフーン）」について、アドバイザリを共同で発表した。Volt Typhoon は、発見されるまで少なくとも 5 年間に渡り、米国の重要インフラを侵害してアクセスを維持していた。このことを受け、アドバイザリは重要インフラ組織に対し、Volt Typhoon の攻撃手法等の有用な情報を提供する他、緩和策の適用や、ガイダンスに従い悪意あるサイバー活動を追跡することを強く促している[1, 2]。

図 1 サイバーセキュリティアドバイザリ（PDF 版）の表紙[3]

[1] 出典：CISA『CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance』 https://www.cisa.gov/news-events/alerts/2024/02/07/cisa-and-partners-release-advisory-prc-sponsored-volt-typhoon-activity-and-supplemental-living-land

[2] 出典：CNN Politics『Chinese hackers have lurked in some US infrastructure systems for 'at least five years'』 https://edition.cnn.com/2024/02/07/politics/china-hacking-us-agencies-report/index.html

[3] 出典：CISA『JOINT CYBERSECURITY ADVISORY』 https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf

1.2. 発表されたアドバイザリについて

このアドバイザリは米国の CISA、国家安全保障局（NSA）、連邦捜査局（FBI）とファイブアイズ（アメリカ、イギリス、カナダ、オーストラリア、ニュージーランドの情報機関で機密情報を共有する枠組み）が共同でリリースしたもので、重要インフラ組織に対してハッカーグループ Volt Typhoon によるサイバー攻撃の脅威を警告している。アドバイザリによると同グループは、大規模な軍事危機や紛争が発生した際に深刻なサイバー攻撃を実行する目的で、事前準備を行っている。このような活動において、米国の重要インフラのネットワーク上で 5 年以上に渡り、検知されずに侵入を続けていたケースが確認されている。グループの活動の背後には将来的な有事を見据えた中国の野心が窺え、米国政府は自国の安全保障に対する脅威が増大していると警戒感を強めている。

米諜報機関の責任者は、中国が台湾に侵攻した場合、米軍の作戦を支援する重要インフラをサイバー攻撃によって侵害し、遠隔操作で大混乱させる可能性があることを議会で述べ、その脅威について警鐘を鳴らした[4, 5, 6]。また、同時に発表された各国でのアドバイザリも、Volt Typhoon による自国の重要インフラに対する攻撃の脅威について述べており、侵害のリスクと影響を低減させることを目指している。

1.3. Volt Typhoon について

Volt Typhoon は、中国の APT グループ（国家の支援を受けて、特定の組織に対し高度な技術で継続的なサイバー攻撃を行う集団）である。2021 年半ばよりグアムや米国本土などの国民生活や経済活動の基盤となる重要インフラ、つまり、通信、エネルギー、水処理施設、輸送システム等を標的としている。2023 年 5 月、重要インフラを標的とした活動を発見したマイクロソフトが警告を発したことにより、Volt Typhoon は知られるようになった。同グループは、侵入後の検出を回避するための高度な手法を使いながら、将来の紛争時に米国の重要インフラをサイバー攻撃で停止させ、米軍の行動を妨害することを狙ってその土台作りをしていると考えられている[7, 8]。

1.4. Volt Typhoon によるシステムへの侵入と潜伏

Volt Typhoon は、インターネット上に公開されているネットワーク装置のゼロデイ脆弱性などを利用して、重要インフラ組織の IT 環境へ初期アクセスを試みる。成功すると、上位の管理者権限のアカウントを窃取する等、システムの奥深くまで侵入。さらに、窃取したアカウントにより、いつでもシステムへのアクセスが可能な状態にしておき、潜伏状態を保持する。

Volt Typhoon の大きな特徴として、ターゲットのシステムにおいて侵入を深める際、Living off the Land（環境寄生

---

[4] 出典：CISA『CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance』
https://www.cisa.gov/news-events/alerts/2024/02/07/cisa-and-partners-release-advisory-prc-sponsored-volt-typhoon-activity-and-supplemental-living-land

[5] 出典：CISA『PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure』
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[6] 出典：CNN Politics『FBI director warns that Chinese hackers are preparing to 'wreak havoc' on US critical infrastructure』
https://edition.cnn.com/2024/01/31/politics/china-hacking-infrascture-fbi-director-christopher-wray/index.html

[7] 出典：Microsoft『Volt Typhoon targets US critical infrastructure with living-off-the-land techniques』
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[8] 出典：BleepingComputer『Chinese hackers hid in US infrastructure network for 5 years』
https://www.bleepingcomputer.com/news/security/chinese-hackers-hid-in-us-infrastructure-network-for-5-years/

型［以下、LotL］）という手法を用いて検出を避けるようにすることが挙げられる。LotL においては、侵害したシステム上で新たにマルウェア等を仕込むことはせず、PowerShell といった既存のツールを使用して活動するため、攻撃の検出が困難となる。また、事前に標的組織への大規模な偵察を行ってシステムの状況などを把握しているため、侵害後は常に当該システムの状態に合わせて戦術・技術・手順（TTP）を調整し、継続的にアクセスすることができる。CISA は、これらの方法により Volt Typhoon が 5 年もの長期にわたってひそかに不正アクセスを続け、潜伏していたことを確認した。

重要インフラの監視システム内のカメラに、Volt Typhoon の攻撃者がアクセスできるようになっていた事例等から、CISA は、Volt Typhoon が重要インフラの機器の制御に関わる OT（Operational Technology）機器へのアクセスを重点的に狙っていると分析している[9, 10]。

1.5. FBI が KV Botnet の駆除を実施

Volt Typhoon は攻撃の兆候を隠すため、ネットワークトラフィックの転送用に C＆C（Command and Control Server:マルウェア感染したシステムに命令を送るサーバー）インフラ環境を構築していた。C＆C インフラ環境は複数段の踏み台を使用した構成になっている。Volt Typhoon はその踏み台の取得と使用に、ボットネットを形成していた。まず、インターネットに公開されていた脆弱な SOHO デバイス（小規模事業またはホームオフィスで使用）を次々と「KV Botnet」マルウェアに感染させ、自身のボットネットに取り込んでいった。そして、これらのデバイスを複数経由して、標的のシステムに対し LotL 等を利用しながらアクセスを行っていた。悪用されたデバイスは、主にシスコおよび NetGear の、メーカーサポートが終了してアップデートができなくなった脆弱な製品とされる[11]。

2024 年 1 月 31 日、FBI はこのボットネットを利用した攻撃を妨害するため、裁判所の許可を得て KV Botnet の駆除を実施したと発表した。この作戦では、ボットネットを管理する C&C サーバーをハッキングした後、米国内の KV Botnet に感染したルーターをボットネットから切り離して再接続ができないようにした上、当該ルーターにてマルウェアの駆除も行った[12, 13]。さらに同日、CISA と FBI は Volt Typhoon の継続的な攻撃を防ぐため、SOHO ルーターのメーカー向けガイダンスも発行し、開発段階で悪用可能な脆弱性を排除する方法や既存のデバイス構成の調整方法等を案内している[14]。

なお、これまでにも APT41、APT31、APT15、TEMP.Hex 等の様々な中国のグループが、IoT デバイス、スマートデバイス、ルーターを利用してボットネットを構築する事例が数多く確認されている。過去 10 年間を振り返ると、中国のグループがサイバースパイ等の明確な目的の為に、ボットネットを構築する手法を導入し、攻撃をステルス性の高いものへと進化させているこ

---

[9] 出典：CISA『PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure』 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[10] 出典：BleepingComputer『Chinese hackers hid in US infrastructure network for 5 years』 https://www.bleepingcomputer.com/news/security/chinese-hackers-hid-in-us-infrastructure-network-for-5-years/

[11] 出典：CISA『PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure』 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[12] 出典：U.S. Department of Justice『U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure』 https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

[13] 出典：BleepingComputer『FBI disrupts Chinese botnet by wiping malware from infected routers』 https://www.bleepingcomputer.com/news/security/fbi-disrupts-chinese-botnet-by-wiping-malware-from-infected-routers/

[14] 出典：CISA『Secure by Design Alert: Security Design Improvements for SOHO Device Manufacturers』 https://www.cisa.gov/resources-tools/resources/secure-design-alert-security-design-improvements-soho-device-manufacturers

とがわかる[15]。

1.6. まとめ

Volt Typhoon の背後には中国国家があり、同グループは将来大規模な危機や紛争が発生した場合に、米国の重要インフラへのサイバー攻撃を行うことでその機能を停止させ、米国の介入の遅延・妨害を狙っていると考えられる。そのために検出を避けながら重要インフラへのアクセスを長期間維持している。そして、将来的なさらなる攻撃を見据えた足場固めをしながら、これらの重要なリソースを即座に停止・制御できる態勢を目指していると思われる。

CISA のアドバイザリによると、Volt Typhoon が狙った先にはグアムが含まれていた[16]。グアムは、中国の軍事行動の際に即応する米軍の、東アジア・西太平洋における重要な軍事拠点である。台湾を巡る政治情勢によっては、事態が急速に変化する恐れがあり、今後もこのグループの動向が懸念される。重要インフラ組織は将来のリスクに備え、このアドバイザリに従って対策を実行することを推奨する。

[15] 出典：Mandiant『ステルス性増す中国のサイバースパイ：検知回避の戦術がさらに進化』
https://www.mandiant.jp/resources/blog/chinese-espionage-tactics

[16] 出典：CISA『PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure』
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

2. LockBit への大規模な押収作戦の実施

2.1. 概要

2 月 20 日、NCA（英国家犯罪対策庁）と FBI（米連邦捜査局）を中心とする各国の捜査機関が、ランサムウェアグループ LockBit への大規模な押収作戦を実施したことが明らかとなった[17, 18, 19]。

捜査機関は、暴露サイトを含む IT インフラや暗号化されたファイルの復号鍵などを LockBit から押収し、2 名の関係者を逮捕した。捜査機関は今後も、LockBit に対する捜査を続けるとしている。

図 2 LockBit の暴露サイトに表示された各国の捜査機関による押収メッセージ

2.2. ランサムウェアグループ LockBit

LockBit はロシアを拠点とするランサムウェアグループである[20]。2019 年 9 月に初めて活動が観測され、当初は「ABCD」と自称していた[19]。その後、2020 年 1 月に現在の名称に変更した[21]。

LockBit は RaaS（Ransomware as a Service）と呼ばれる運用形態を取り、グループの管理者がランサムウェアなど

---

[17] 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

[18] 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

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

[21] 出典：CISA『Understanding Ransomware Threat Actors: LockBit』
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

の攻撃ツールを用意し、それらを利用してアフィリエイトと呼ばれる実行役が攻撃を行う。RaaS では通常、グループの管理者が被害組織から身代金を受け取りアフィリエイトに分配するが、LockBit ではアフィリエイトが先に身代金を受け取り、グループの管理者へ分配する。この方法を用いると、管理者による身代金の持ち逃げが発生せず、アフィリエイトも自身の取り分を確保できるため、同グループは多くのアフィリエイトを集めることに成功した [21]。

その攻撃活動は非常に盛んであり、2022 年 [21] と 2023 年には、最も多くの被害組織を生み出したランサムウェアグループとなった。2023 年の LockBit の被害組織として 1,035 件が確認されており、これは 2 位 CL0P の 419 件、3 位 ALPHV の 418 件の 2 倍以上であった（2023 年の被害組織数は当社調べ）。

これまで、世界中で 2,000 以上の組織が LockBit の被害に遭い、1 億 2,000 万ドル以上の身代金を支払っている [18]。このうち日本国内では、100 以上の組織が被害に遭っており[22]、特に 2022 年 10 月の徳島県のつるぎ町立半田病院[23]、2023 年 7 月の名古屋港コンテナターミナルの被害[24]は大きな話題となった。

2.3. 捜査機関によるインフラ押収作戦

NCA[17]、米司法省 [18]、Europol（欧州刑事警察機構）[19] は 2 月 20 日、LockBit に対する大規模な押収作戦を実施したことを発表した。この作戦は、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 Europol が協力して実施している、LockBit に対する捜査活動 **Operation Cronos** の一環である。

図 3 Europol によるニュースリリース [19]

[22] 出典：朝日新聞『サイバー犯罪集団「ロックビット」主要メンバー摘発　サーバーも閉鎖』
https://www.asahi.com/articles/ASS2N6DBKS2NUTIL035.html

[23] 出典：つるぎ町立半田病院『コンピュータウイルス感染事案有識者会議調査報告書について』
https://www.handa-hospital.jp/topics/2022/0616/index.html

[24] 出典：名古屋港運協会『NUTS システム障害の経緯報告』
https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf

今回の作戦により、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、14,000 以上の不正なアカウントが押収され、200 以上の暗号通貨アカウントが凍結された。また、ポーランドとウクライナで 2 人が逮捕され、フランスとアメリカで 3 件の国際逮捕状の発行と 5 件の起訴が行われた。

押収されたサーバーには、LockBit に身代金を支払った被害組織から窃取されたデータが残っていた。これは、ランサムウェアグループに身代金を支払っても、窃取されたデータが必ずしも約束通り削除されるわけではないことを意味する。

これまで、捜査機関がランサムウェアグループの暴露サイトを押収した場合、**図 2** のような押収メッセージが表示されるだけであった。しかし LockBit の場合、同様の押収メッセージを表示するだけでなく、捜査機関は元の暴露サイトを模したサイトを用意し、置き換えた。このサイトは、プレスリリースやファイル復号ツールへのリンク、LockBit から押収したサーバーの管理画面やチャット履歴など、捜査機関の情報発信の場として利用された（**図 4**）。中には、LockBit の代表者 LockBitSupp に向けた挑発的なメッセージもあり、捜査機関の LockBit に対する力の入れようを感じさせるものであった。置き換えられた暴露サイトは、当初より 2 月 24 日をもって公開を終了すると捜査機関が案内していた通り、公開は終了している。

捜査機関は、今後も LockBit の捜査を続けるとしている。日本の警察庁も、情報の提供や暗号化されたファイルの復号ツールの作成など、本作戦への協力を行ったことを発表している[25, 26]。

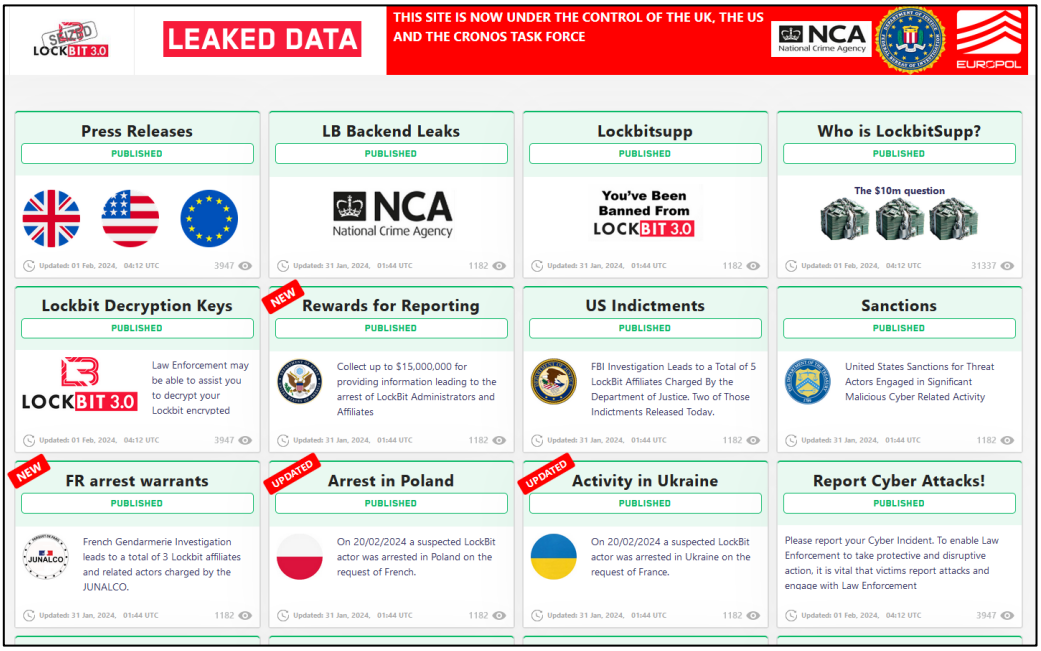

図 4 捜査機関による情報発信の場に変更された LockBit の暴露サイト

2.4. 押収作戦に対する LockBit の反応

暴露サイトやサーバーの押収が実施された 2 月 19 日以降、LockBit に表立った活動は見られなかった。しかし 24 日、

[25] 出典：警察庁『ランサムウェア被疑者の検挙及び関連犯罪インフラのテイクダウンに関するユーロポールのプレスリリースについて』 https://www.npa.go.jp/news/release/2024/20240214001.html

[26] 出典：警察庁『ランサムウェアによる暗号化被害データに関する復号ツールの開発について』 https://www.npa.go.jp/news/release/2024/20240214002.html

LockBit 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た。

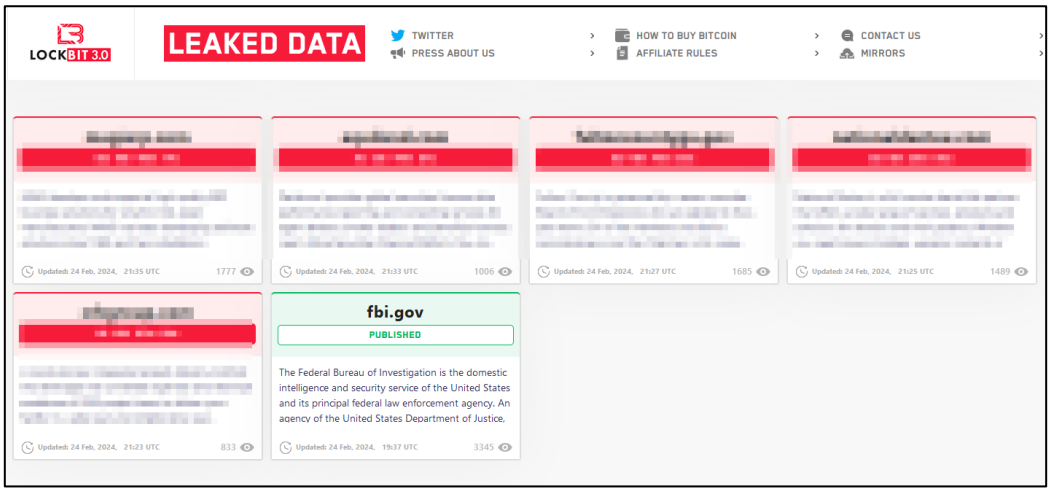

図 5 LockBit が新たに立ち上げた暴露サイト
※最初の投稿（下段右）が捜査機関に向けたメッセージへのリンクとなっている

新しい暴露サイトでは、英語とロシア語の両方で、捜査機関に向けたメッセージが公開されている。この中で、LockBit 側は次のような主張や説明を行っている。まず、捜査機関が今回の押収作戦の実施を決めたのは、同グループが米国ジョージア州フルトン郡を攻撃して窃取した情報に、トランプ前大統領の裁判に影響を与える内容が含まれていたからであると真偽不明の主張をしている。また、同グループが一部サーバーの PHP の更新を怠り脆弱性が存在するバージョンを使用していたため、捜査機関にその脆弱性を利用されサーバーの押収に繋がったと説明している。他にも、押収された復号鍵は LockBit が保持する鍵のうち一部でしかないといったことを主張している。また、今後もランサムウェア攻撃を続けると宣言しており、捜査機関を挑発する内容となっている。

2.5. まとめ

新たな暴露サイトへの投稿には、以前ほどの勢いは見られない。今回の作戦で、捜査機関は実際に攻撃活動に使用されていたサーバーやアカウントを押収しており、現時点では LockBit の攻撃能力を削ぐことに成功したと考えられる。また、このような作戦の積み重ねと入手した情報の分析によって、LockBit の体制など内部情報が明らかとなり、新たな関係者の逮捕や、国際的な包囲網の広がりが LockBit の攻撃活動に対する大きな制約に繋がると考えられる。

3. 香港でディープフェイクを使用した BEC 詐欺が発生

3.1. 概要

2 月 4 日、香港警察は、ある英国の多国籍企業がディープフェイクを利用した詐欺により、2 億香港ドル（約 38 億円）を騙し取られたことを発表した[27]。当該企業の従業員がビデオ会議に出席していたが、財務部門の最高責任者らが映し出されたその会議映像は、ディープフェイクで作成されたものであった[28]。ディープフェイクを悪用したビジネス電子メール詐欺（BEC）事件としては、香港史上最高額であるとして大きな話題となった。

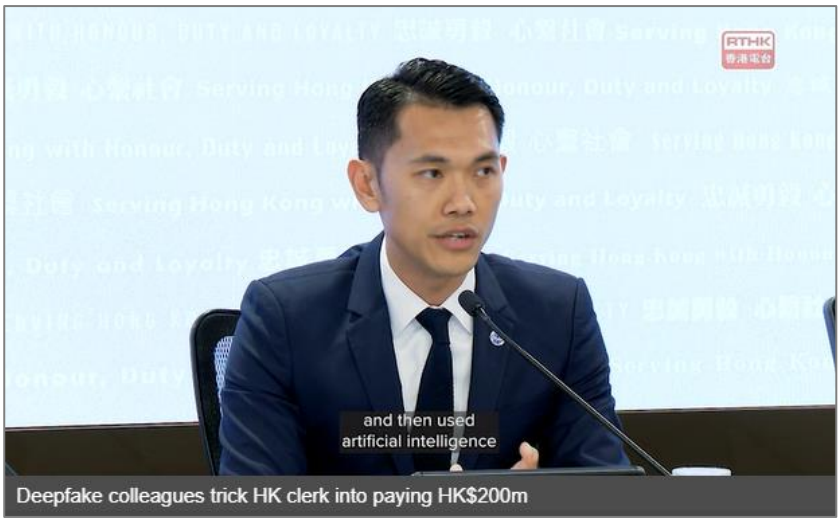

図 6 今回の事件についての記者会見を行う香港警察のバロン・チャン氏[29]

3.2. 事件の詳細

この事件で狙われたのは、ある多国籍企業の香港支社の財務担当者（以下、A）だった。1 月中旬、A は、英国本社の最高財務責任者（CFO）から、秘密の商取引に関するメールを受け取った。この時点では、A はフィッシングメールであることを疑っていた。その後、その CFO や複数の同僚が出席するビデオ会議に招待された。会議では、同僚らも普段と変わらない様子であったことから、A は、CFO から受け取っていたメールおよびこの会議が詐欺目的ではなく、本当に商取引についてのものであると信じてしまった[30]。しかし実際には、その CFO や同僚全員の映像はディープフェイクを用いて偽造されたものであった。つまり、その会議に実際に出席していた社員は、A 一人だけだったのである。会議の後、A は自身が受けた指示通りに 2 億香港ドルを 15 回に分け、5 カ所に宛てて振り込んだ。数日後、香港支社が英国本社に状況を確認したところで、上記の一連の過

[27] 出典：Hong Kong Free Press『Multinational loses HK$200 million to deepfake video conference scam, Hong Kong police say』
https://hongkongfp.com/2024/02/05/multinational-loses-hk200-million-to-deepfake-video-conference-scam-hong-kong-police-say/
[28] 出典：21 经济网『震惊！"变脸"冒充 CFO，骗走两个亿！香港最大 AI 诈骗案细节曝光』
https://www.21jingji.com/article/20240206/herald/b324fcdf262eb9e6b9480db048159488.html
[29] 出典：香港電台網站『Deepfake colleagues trick HK clerk into paying HK$200m』
https://news.rthk.hk/rthk/en/component/k2/1739119-20240204.htm
[30] 出典：CNN『Finance worker pays out $25 million after video call with deepfake 'chief financial officer'』
https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

程が詐欺であったことが判明した。犯人は、同社が公開していた YouTube での動画等を素材として利用し、ディープフェイク（後述）により偽映像を作り出したとみられている。

3.3. ディープフェイクと悪用の増加

【ディープフェイクとは】

ディープフェイクとは、AI の学習手法の一つである「ディープラーニング（深層学習）」と、偽物を意味する「フェイク」を合わせた言葉で、AI を利用して偽物の画像や音声、動画等を作成する技術である[31]。2017 年に海外の掲示板に投稿された、有名女優を偽装した動画がきっかけで、世間に広く知られるようになった[32]。登場した当初は、専門的な知識や高性能な PC 等が必要であったが、その後、関連技術の発展により Web から利用できるツールやスマホのアプリ等が提供されるようになった。現在では、こうしたツールを使用することで、多くの人が容易にディープフェイクを作成できるようになっている。

【サイバー攻撃への悪用】

ディープフェイク技術を今回のような BEC 等の犯罪に利用したいと考える攻撃者は数多く存在する。ハッカーフォーラムや Telegram 等の SNS では、ディープフェイクの始め方、ディープフェイクで顔認証を突破する方法、Web カメラの映像をディープフェイクに置き換える方法といった、ディープフェイクをサイバー攻撃に悪用するための様々な情報が交換されている。

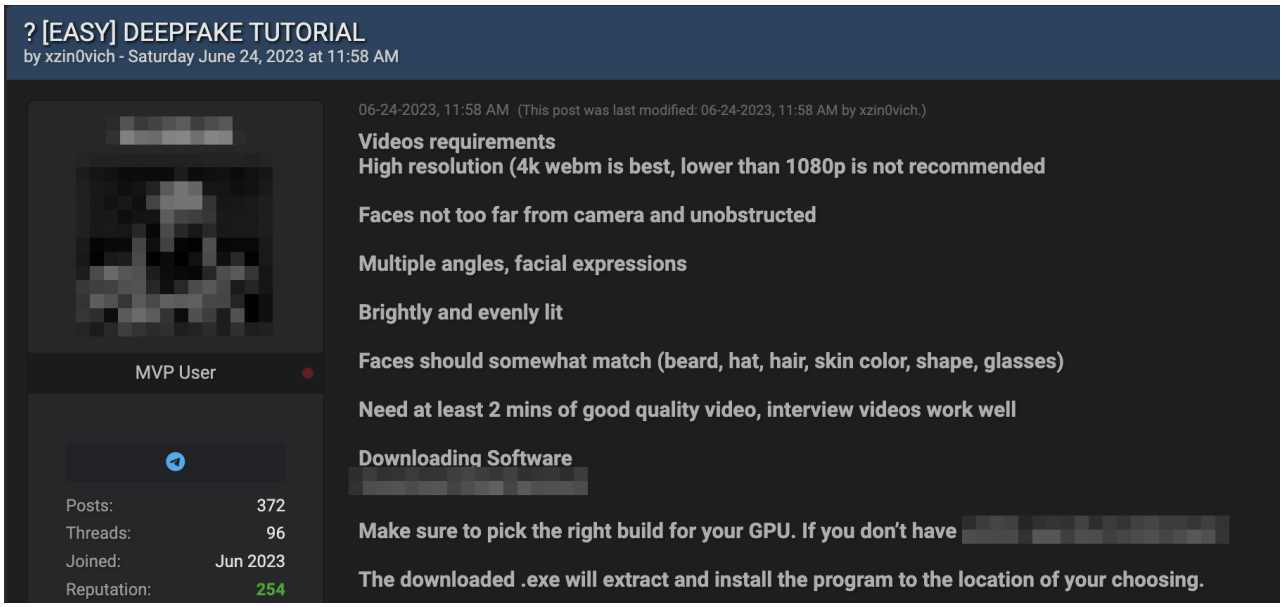

図 7 ディープフェイクの始め方を説明するハッカーフォーラムの投稿

[31] 出典：docomo business Watch『ディープフェイクとは？サイバー攻撃に使われるセキュリティリスク』
https://www.ntt.com/bizon/deepfake.html

[32] 出典：PALOALTO INSIGHT『ディープフェイクとはどんな技術？』
https://www.paloaltoinsight.com/2022/08/29/deepfake/

【急増するディープフェイクを利用した詐欺】

昨年末、セキュリティ企業「Sum and Substance」は、「Identity Fraud Report 2023[33]」（なりすまし詐欺レポート2023）を発表した。同レポートによると、ディープフェイクで作られたコンテンツは年々増加しており、2023 年は前年の 10 倍検出された。同時にディープフェイクを詐欺に利用するケースが増加している。特に、米国とカナダでの増加が顕著だが、世界的に見ても増加傾向にあると分析している[34]。

3.4. 日本におけるディープフェイクの悪用事例

ディープフェイクを悪用した BEC は海外に限ったことではない。日本の BEC の被害状況を集約している IPA のレポート[35]でも、昨年発生した事例が紹介されている。それによると犯人は、日本企業の海外関連会社に対し、送信元を偽装して、日本企業の本社の会長からと見せかけたメールを送信した。本社の専務の声を真似た電話もかけており、この音声にディープフェイクを利用した可能性が指摘されている。なお本件は、関連会社が詐欺に気づくことができたため、金銭的な被害には至らなかった。

また、直接的に金銭を狙った事例以外にも、政治家や芸能人を対象にいたずらや嫌がらせ目的でディープフェイク動画が作成され、問題となることが増えている。昨年 11 月頃、岸田首相が下品な文章を読みあげる動画が SNS 上で拡散された。動画の内容が首相の名誉を傷つけていたことや、日本テレビの報道番組のロゴを使用していたこと等で問題視された[36]。この動画の作成者は、後に動画を削除し、X（旧 Twitter）に謝罪文を投稿した。メディアの取材に対し作成者は、ディープフェイク動画の作成は容易であり、プログラミングの知識はなかったが、ツールを使用し 1 時間弱で作成できたと語っている。

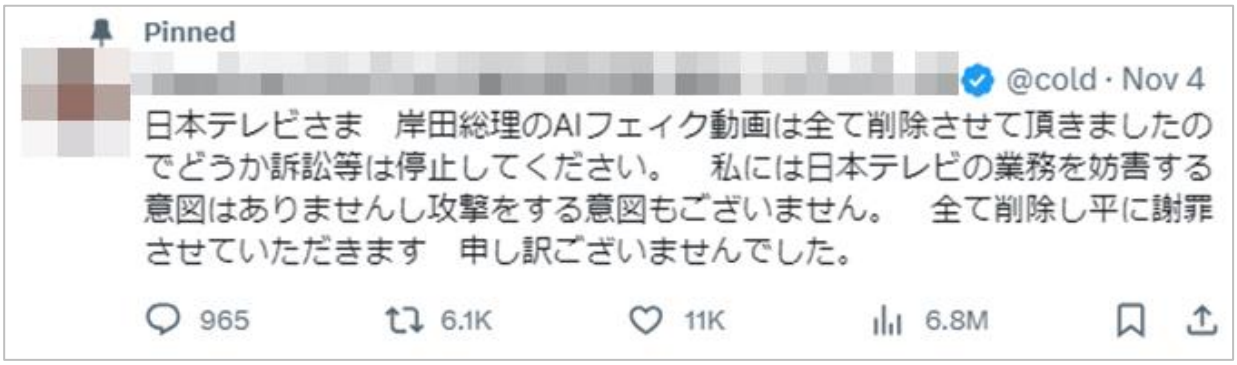

図 8 動画作成者から日本テレビへの謝罪文（アカウントは凍結されており現在はアクセスできない）

[33] 出典：Sum and Substance『2023 Identity Theft & Fraud Statistics』
https://sumsub.com/fraud-report-2023/
[34] 出典：KnowBe4『ディープフェイク：詐欺の新たな主役』
https://www.knowbe4.jp/blog/deepfakes-the-new-face-of-fraud
[35] 出典：IPA『サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023 年 4 月～6 月]』
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q1-report.pdf
[36] 出典：産経新聞『「首相偽動画」が拡散、精巧化するディープフェイクのリスク 技術向上で簡易に』
https://www.sankei.com/article/20231114-LLOVR22LSNOVNFWVGOIRN5JIBU/

3.5. まとめ

AI 技術の発展により、特別な知識や高性能な PC がなくてもディープフェイクでコンテンツを作成できるようになった。企業の重役が映った公式サイトの画像や動画により、攻撃者はフェイクコンテンツの素材を容易に見つけることができる。ディープフェイクを BEC 等の犯罪に悪用する例も急増しており、差し迫った危機であると考えられる。前述の IPA の報告書では、メールや電話の内容に不審な点があれば、信頼できる方法で入手した連絡先に折り返し電話して確認を行うことや、そのメールの送信者や電話の発信者しか知らない質問をして本人確認を行うことを推奨している。こうした対処方法を、社員教育を通じて周知徹底することで、組織全体のディープフェイクに対する意識を高めていくことが重要である。

以上

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