サイバーセキュリティレポート
2025.12

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部 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 2025 年 12 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『暴露型ランサムウェア攻撃 2025 年活動まとめ』

- ランサムウェアグループが運営する暴露サイトにおいて、被害組織に関する投稿数は年々増加しており、2025 年は前年から約 50%増の 8,199 件が確認された。
- 捜査機関による摘発やグループ間の競争激化などにより、活動が活発なランサムウェアグループの顔ぶれが入れ替わったり、新規グループが乱立したりするなど勢力構造の変化が進んでいる。
- ランサムウェアグループの再編等の影響により、ランサムウェア攻撃の勢いは高止まりの状態が続くことが見込まれるため、企業側ではセキュリティ強化だけでなく、侵害時を想定した備えを進めることも重要である。

第 2 章『ポルトガル法改正、倫理的ハッキングを許可』

- ポルトガルは 2025 年 12 月、サイバー犯罪法を改正し、公共の利益に資するサイバーセキュリティ行為を規定する新しい条文「第 8-A 条」を追加した。
- この改正は、セキュリティ研究者や倫理的ハッカーによる責任ある脆弱性調査を一定条件下で合法化し、サイバー防御基盤の強化を目的とするものである。
- サイバー攻撃が高度化する状況下で、セキュリティ研究者が法的リスクを恐れずに活動できる環境づくりは、今後、日本でも検討の対象となることが考えられる。

第 3 章『北朝鮮の IT ワーカー潜入作戦』

- 北朝鮮のハッカーグループ「Lazarus」のサブグループ「Famous Chollima」は、企業スパイ活動、および制裁下にある北朝鮮への資金調達という任務を遂行するため、他人の身元を利用し、工作員を IT ワーカーとして米国やその他の国の企業に侵入させている。
- Chollima が採用面接を代理で受けてくれる者を募集していることに対し、セキュリティ研究者らは IT ワーカーに偽装した北朝鮮工作員の策略の全貌を暴くため、実際に Chollima のリクルーターに接触し、彼らが企業に潜入するプロセスを内部から観察するおとり調査を実施した。
- リモート面接を取り入れている限り、Famous Chollima が計画するような面接を防ぐことは容易ではない。本件はリモートワーク業務の盲点を突いたもので、応募者には実際に企業に来てもらい面接することや、採用後は定期的に(または不定期に)現場で業務を実施させることで防止・抑止できる可能性が考えられる。

1. 暴露型ランサムウェア攻撃 2025 年活動まとめ

1.1. 概要

弊社の OSINT モニタリングチームでは、暴露型ランサムウェアグループが運営する暴露サイトの投稿を日々モニタリングしている。このモニタリングの結果に基づいて、2025 年の暴露型ランサムウェアグループの活動・動向をまとめた。

1.2. ランサムウェア攻撃の増加

暴露型ランサムウェアグループとは、ランサムウェアを用いてターゲット組織のネットワークに存在するファイルを暗号化／窃取した上で、復号キーとの引き換えに身代金を要求し、さらに期限までに身代金が支払われなければ、窃取したファイルをグループが運営するサイトで公開(暴露)する、と被害組織を二重に脅迫する犯罪グループである。暴露サイトの多くはダークウェブに存在しているが、誰でもアクセスできるサイトや SNS を利用するランサムウェアグループもある。

暴露サイトでの被害組織に関する投稿総数は年々増加しており、2025 年は前年から約 50%増の 8,199 件が確認された(図 1)。

月別の投稿総数で見ても 2025 年は各月で前年の同月を上回っており、500 件以上であることが常態化している(図 2)。世界各国の捜査機関が連携し、ALPHV、LockBit などの活発なランサムウェアグループの摘発が行われてきたが[1,2]、ランサムウェア攻撃が沈静化には向かっていない実態が浮き彫りになっている。

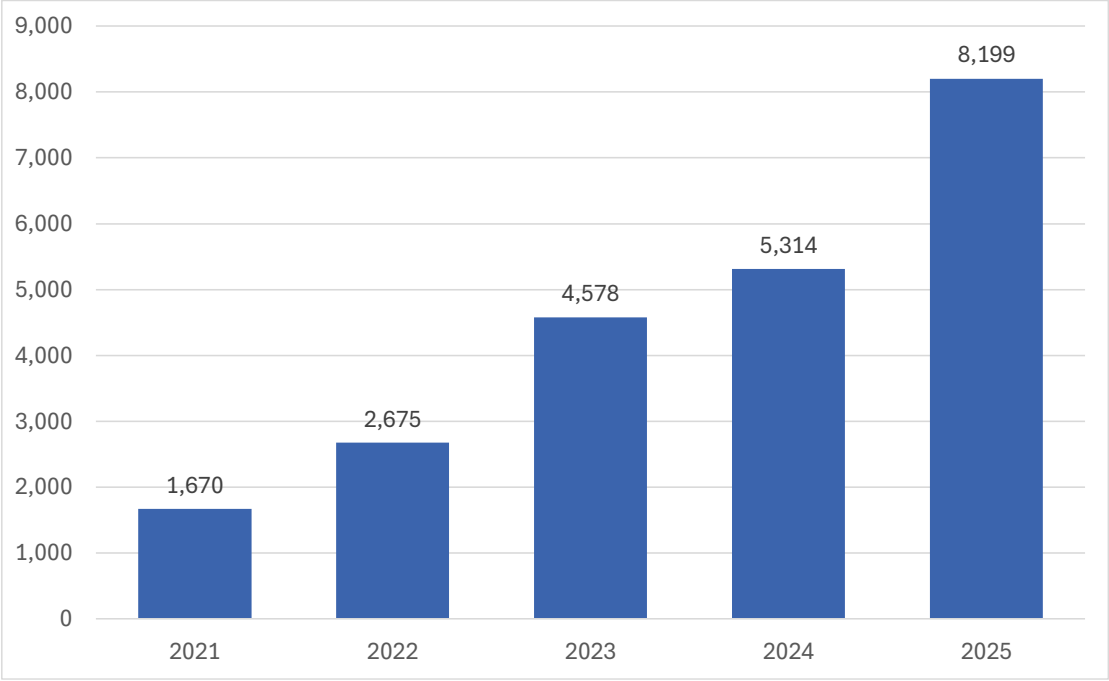

図 1 暴露サイトでの被害組織に関する投稿総数の推移

[1] 出典: U.S. Department of Justice『Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant』 https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

[2] 出典: National Crime Agency『The NCA announces the disruption of LockBit with Operation Cronos』 https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos

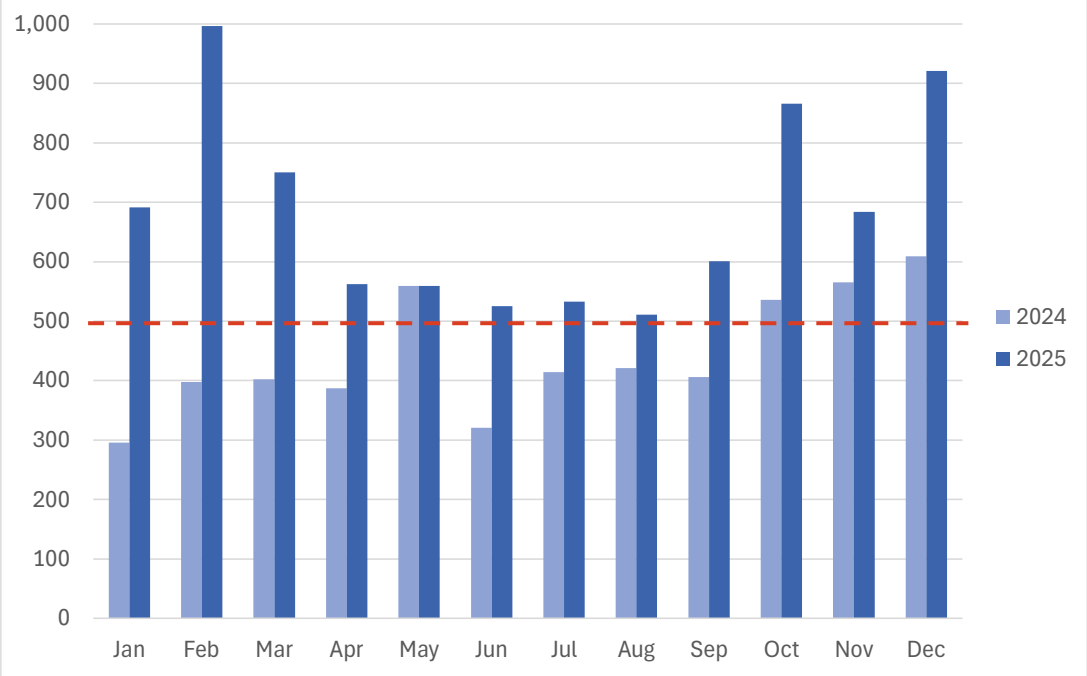

図 2 暴露サイトでの被害組織に関する月別の投稿総数

1.3. 群雄割拠のランサムウェアグループ

【活発なランサムウェアグループの顔ぶれの入れ替わり】

2025 年の年間の投稿数上位 10 グループの顔ぶれは、2024 年から半数が入れ替わり、摘発の影響を受けた「LockBit」や、解散を発表した「Hunters International」などのグループは圏外となった。

グループ名	1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	合計
Qilin	20	43	48	71	56	86	65	83	87	212	96	190	1,057
Akira	41	116	60	72	40	34	46	57	44	82	80	78	750
Cl0p	113	295	5	1	1	1	1	0	0	17	99	1	534
Play	15	47	29	50	41	33	23	28	52	27	27	22	394
Incransom	31	13	30	19	15	28	50	28	56	31	55	35	391
Safepay	28	13	43	12	65	34	42	19	31	14	16	68	385
Lynx	41	37	32	31	10	24	17	13	30	13	2	14	264
RansomHub	49	102	87	4	0	0	0	0	0	0	0	0	242
DragonForce	17	7	11	26	2	25	21	24	14	20	25	35	227
Babuk2	67	0	99	22	0	0	0	0	0	0	0	0	188

表 1 暴露型ランサムウェアグループの 2025 年投稿数トップ 10

一方で、アサヒグループホールディングスへの攻撃で日本国内でも注目を浴びた「Qilin」の活動が活発化しており、全グループ中、投稿数が最多となった。また、「Akira」が前年に比べ約 3 倍の数の投稿を行い、二番手となった。

これらのグループは RaaS (Ransomware as a Service [サービスとしてのランサムウェア])を提供しており、ランサムウェア攻撃の実行者である「アフィリエイト」をより多く獲得するために、高い利益配分や手厚い技術サポートを行っている[3]。活動停止等で弱体化した他のグループからアフィリエイトの流入を図ることで、活動を活発化させているとみられる。

三番手の「Cl0p」は、コンスタントに攻撃を行うのではなく、短期間に集中してゼロデイ脆弱性を悪用することで成果を上げている。2025 年年初に Cleo 製ファイル転送ソフトウェアの脆弱性 CVE-2024-50623 を、11 月には統合 ERP パッケージ Oracle E-Business Suite の脆弱性 CVE-2025-61882 を悪用し、攻撃キャンペーンを展開した[4]。他グループとは異なる特徴を見せており、アフィリエイトの採用は限定的とみられる[5]。

【ランサムウェアグループの再編】

グループの統合・リブランドが活発化したことも、2025 年の特徴である。「RansomHub」は 2024 年後半から活発な活動を見せていたが、2025 年 3 月下旬に突然活動を休止した。別グループである「DragonForce」に強制的に吸収されたとみられる[6]。また、「Hunters International」は 7 月に同グループの暴露サイトで、解散、および復号ツールの無償提供を発表したが、実際には「World Leaks」という新たなグループを立ち上げ、現在も活動を継続している[7]。これらの動きの背景として、ランサムウェアグループ間での勢力争いが活発になっていることの他に、捜査機関からの追跡逃れを意図していることも考えられる。

また、新規参入のランサムウェアグループが増加しており、2025 年には新たに 66 のグループが観測された。RaaS を提供するために必要となるプラットフォーム等のノウハウが拡散し、ランサムウェア業界への参入障壁が低くなっていることから、群雄割拠の状態が続く可能性がある。

身代金の支払い率が低下していることも[8]、ランサムウェアグループの再編に影響しているとみられる。収益を上げるためには、多くのアフィリエイトを集めて攻撃数を増やすことが必要となっている。しかし、グループの知名度・ブランド力を高めると当局による摘発につながるため、小規模でも差別化を図ってアフィリエイトを集めて、短期間に攻撃を集中させる動きにシフトしていると考えられる。

このような小規模で短命なグループは評判を重視する必要がないため、身代金が支払われても復号キーを提供しなかったり、そもそも復号手段を用意していなかったりする場合がある。このことが、暗号化されたデータの復旧率低下を招く恐れがある。また、グループの乱立により競争が激化し、これまで多くのグループが暗黙的に避けてきた原子力発電所等の重要インフラへの攻撃が行われることも危惧される[9]。

---

[3] 出典: Analyst1『Qilin - Threat Actor Profile』
https://analyst1.com/threat-actors/qilin-threat-actor-profile/

[4] 出典: Vectra AI『Cl0p Is Back, Exploiting Supply Chains Again.』
https://www.vectra.ai/blog/cl0p-is-back-exploiting-supply-chains-again

[5] 出典: Barracuda Networks Blog『Cl0p ransomware: The skeezy invader that bites while you sleep』
https://blog.barracuda.com/2025/05/16/cl0p-ransomware--the-skeezy-invader-that-bites-while-you-sleep

[6] 出典: SOPHOS『DragonForce targets rivals in a play for dominance』
https://www.sophos.com/en-us/blog/dragonforce-targets-rivals-in-a-play-for-dominance

[7] 出典: The Record from Recorded Future News『Hunters International ransomware group claims to be shutting down』
https://therecord.media/hunters-international-ransomware-extortion-group-claims-shutdown

[8] 出典: Coveware『Insider Threats Loom while Ransom Payment Rates Plummet』
https://www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet

[9] 出典: ReliaQuest『Ransomware and Cyber Extortion in Q3 2025』
https://reliaquest.com/blog/threat-spotlight-ransomware-and-cyber-extortion-in-q3-2025/

1.4. まとめ

2025 年は、アサヒグループホールディングスやアスクルのような日本の大手有名企業がランサムウェア攻撃の被害に遭い、事業停止が長期化するリスクが顕在化した[10,11]。ランサムウェアグループの再編の流れは続いており、グループ間の競争激化により、ランサムウェア攻撃の勢いは高止まりの状態が続くことが見込まれる。企業側ではサプライチェーンを含めたセキュリティを強化するとともに、事業継続計画が有効に機能するか検証するなど、侵害時を想定した備えを進めることも重要である。

[10] 出典：アサヒグループホールディングス『サイバー攻撃による情報漏えいに関する調査結果と今後の対応について』
https://www.asahigroup-holdings.com/newsroom/detail/20251127-0104.html

[11] 出典：アスクル株式会社『サービスの復旧状況について（ランサムウェア攻撃によるシステム障害関連・第 15 報）』(IR ポケット)
https://pdf.irpocket.com/C0032/hvir/JK91/fPxz.pdf

2. ポルトガル法改正、倫理的ハッキングを許可

2.1. 概要[12]

2025 年 12 月 4 日、ポルトガルはサイバー犯罪法を改正し、公共の利益に資するサイバーセキュリティ行為を規定する新しい条文「第 8-A 条」を追加した(この日から 120 日後に施行予定)。この改正は、セキュリティ研究者や倫理的ハッカー(防御強化を目的に脆弱性を調査するハッカー)による責任ある脆弱性調査を一定条件下で合法化し、サイバー防御基盤の強化を目的とするものである。

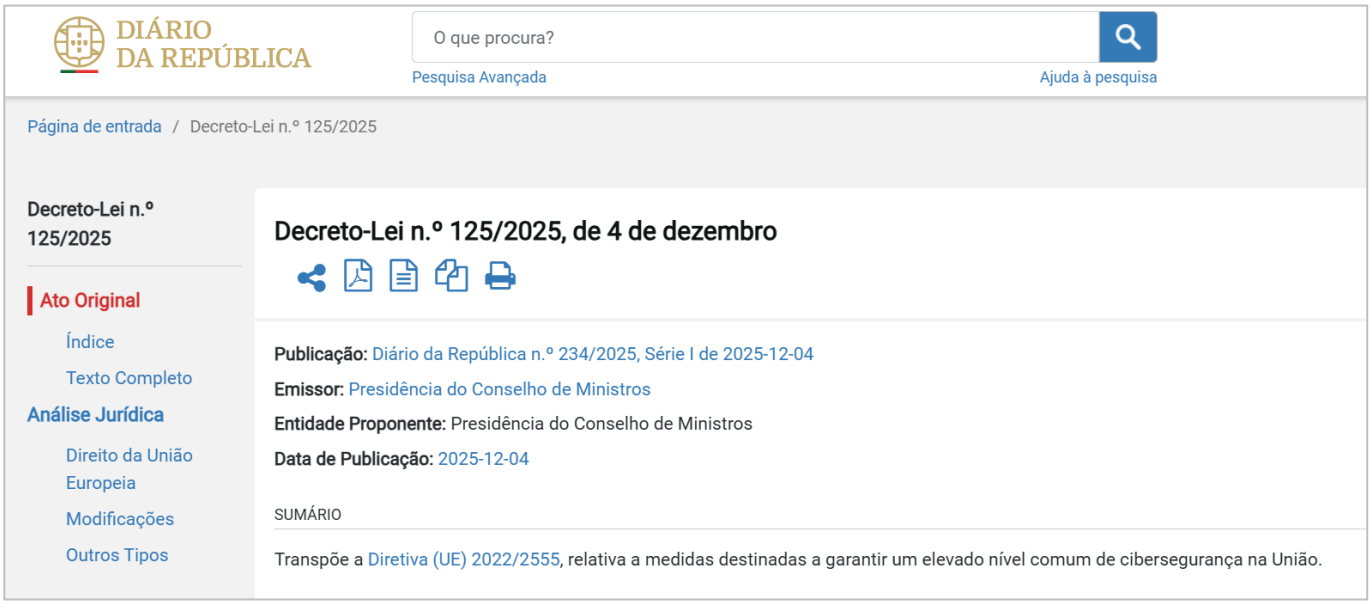

図 3 第 8-A 条を含む法令「Decreto-Lei n.º 125/2025」(ポルトガル政府広報より)[13]

2.2. 第 8-A 条について

【概要と適用条件】[13]

第 8-A 条は、「サイバーセキュリティにおける公益上、処罰されることのない行為」と題した規定。システム所有者や管理者の事前の同意を得ずにセキュリティ研究者が独自に脆弱性調査を行う場合、不正アクセスや通信傍受のように、以前は違法とされていた行為について、以下の条件を満たす場合に限り刑事責任を免除するものである [12]。

- 目的の限定
  脆弱性の特定とサイバーセキュリティの向上のみを目的とすること。
- 経済的利益の禁止
  通常の専門的報酬を超える経済的利益を求めず、受領しないこと。
- 即時報告義務

[12] 出典: Infosecurity Magazine『Portugal Revises Cybercrime Law to Protect Security Researchers』
https://www.infosecurity-magazine.com/news/portugal-cybercrime-law-security/

[13] 出典: Presidência do Conselho de Ministros『Decreto-Lei n.º 125/2025, de 4 de dezembro』(Diário da República)
https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401

発見した脆弱性を直ちに、システム所有者または管理者、取得した個人データの保有者、およびポルトガル国家サイバーセキュリティセンター(CNCS)に報告すること。

- 必要最小限の原則
  脆弱性調査を行う際は、脆弱性の検出に必要な範囲に限定すること。サービスの中断、データの改変・削除、または損害を発生させてはならない。
- 個人情報の保護
  GDPR および関連法令に従い、個人データの違法な取得・利用・開示を行わないこと。
- データの機密性保全と削除
  脆弱性調査中に取得したデータは、機密性を確保し、脆弱性が修正された後、10 日以内に削除すること。

【禁止される手法】[13]

以下の手法を用いた場合は第 8-A 条の適用外となり、刑事責任を問われる。

- DoS 攻撃および DDoS 攻撃
- ソーシャルエンジニアリング
- フィッシングおよびその類似行為
- パスワードや機密情報の窃取
- データの意図的な削除・改変
- 故意によるシステムへの損害
- マルウェアのインストールや配布

2.3. 国際的な動向の比較

ポルトガルの第 8-A 条と同様に、公共の利益に資する脆弱性調査を法的に保護する動きは、他国でも見られる。

【米国の動向】[14, 15]

米司法省は 2022 年 5 月に、CFAA(コンピューター詐欺・濫用防止法)に基づく起訴方針を改訂。公共の利益に役立つセキュリティ研究においては、(悪用の意図や不正利益を伴わず)脆弱性の発見・報告・修正によってシステムの安全性向上に資する行為は起訴しないという例外規定を、新たに設けた。これにより、責任ある脆弱性開示を促進し、セキュリティ研究者が法的リスクを恐れず活動できる環境整備が進んだ。ただしこの方針は、「セキュリティ調査を実施している」と主張する全ての者に対して免罪符として機能するわけではない。例えば、デバイスに脆弱性を発見して所有者を脅迫する行為は、正当とは言えない。また、検察官には CFAA 違反の起訴を検討する際に、本方針の適用判断について刑事部のコンピューター犯罪・知的財産部門に相談することが求められている。

---

[14] 出典: U.S. Department of Justice『Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act』
https://www.justice.gov/archives/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

[15] 出典: U.S. Department of Justice『9-48.000 - COMPUTER FRAUD AND ABUSE ACT』
https://www.justice.gov/archives/opa/press-release/file/1507126/dl?inline

【英国の動向】[16]

英国政府は現在、1990 年制定の CMA(コンピューター不正使用法)を改正しようとしている。起訴されるリスクにセキュリティ研究者をさらし、彼らに不必要な制約を与えてきたとして、同法に対しては批判の声が挙がっていた。

2025 年 12 月 3 日、ダン・ジャービス安全保障相は「法的根拠による防御(statutory defense：法律で定められた条件付き免責)」の導入により、脆弱性を発見・共有するセキュリティ研究者を法的に保護する方針を表明した。

【日本の動向】[17]

日本では、IPA(独立行政法人情報処理推進機構)と JPCERT/CC が運用する協調的脆弱性開示(CVD)ガイドラインにより、脆弱性の発見者、およびこの脆弱性を含む機器・ソフトウェア等の開発者が調整し、問題を修正・公表する仕組みが整備されている。目的は脆弱性が悪用される前に対策を講じ、利用者への影響を最小化することにある。しかし、このガイドラインは任意の指針であり、法的免責を保障するものではない。脆弱性調査は依然として不正アクセス禁止法に抵触する可能性があり、セキュリティ研究者の保護や、責任ある脆弱性開示に関する法的枠組みは未整備である。

2.4. まとめ

攻撃者とセキュリティ研究者の行為は技術的に類似しており、従来は両者を区別する法的枠組みが存在しなかった。そのため、脆弱性調査は公共の利益に資するものであっても違法と解釈される恐れがあった。ポルトガルの第 8-A 条は、責任ある脆弱性開示を法的に支援する制度であり、公共の利益を重視した取り組みといえる。米国では既に数年前に方針改訂が行われており、英国では現在、法改正に向けた動きが進んでいる。サイバー攻撃が高度化する状況下で、セキュリティ研究者が法的リスクを恐れずに活動できる環境づくりは、今後、日本でも検討の対象となることが考えられる。

[16] 出典: Computer Weekly『UK government pledges to rewrite Computer Misuse Act』
https://www.computerweekly.com/news/366635624/UK-government-pledges-to-rewrite-Computer-Misuse-Act

[17] 出典: 独立行政法人情報処理推進機構 (IPA)『情報セキュリティ早期警戒パートナーシップガイドライン』
https://www.ipa.go.jp/security/guide/vuln/ug65p90000019by0-att/partnership_guideline.pdf

3. 北朝鮮の IT ワーカー潜入作戦

3.1. 概要

北朝鮮のハッカーグループ「Lazarus(ラザルス)」のサブグループ「Famous Chollima(フェイマス・チョルリマ)」は、サイバー活動の一環として、他人の身元を利用し、工作員を IT ワーカーとして米国やその他の国の企業に侵入させている。偽装面接後にリモートワーカーとして派遣された工作員らは、企業スパイ活動、および制裁下にある北朝鮮への資金調達を担う。Famous Chollima の活動について、セキュリティ研究者らがおとり調査を実施。グループの興味深い手口が暴かれた[18]。

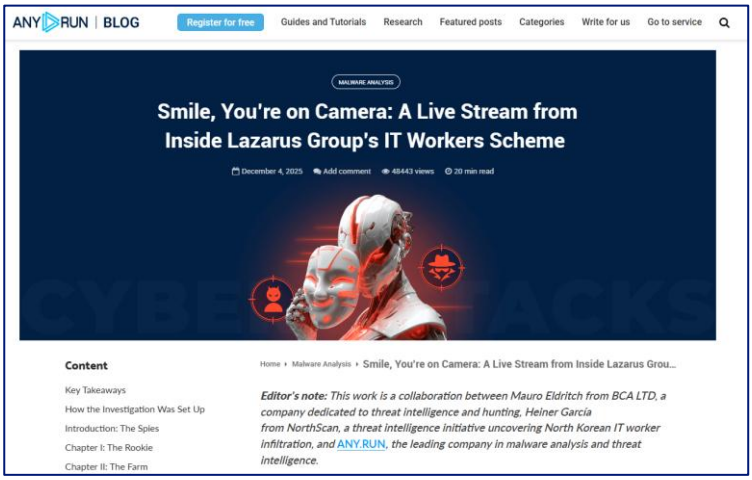

図 4 調査結果をまとめたレポート(ANY.RUN 提供)[19]

3.2. ハッカーグループ「Famous Chollima」とは

北朝鮮には、国家主導とされるハッカーグループがいくつも存在している。その中でも特に有名なのが Lazarus であり、近年は暗号資産(仮想通貨)業界を標的とした大規模なサイバー攻撃で知られている。その Lazarus に属する下位集団の一つが Famous Chollima である。このグループ名は西側のセキュリティ関係者らが名付けたものだが、元々、「Chollima」とは、北朝鮮の神話に登場する「千里馬」(千里を一日で駆ける馬)を指す他、過去には同国の急速な発展促進のために使われたスローガンとしても知られている。この名称は、当グループ(および、「Chollima」を名前に含む他のグループ)が素早く巧妙な攻撃手法を用いることを表すために付けられたと考えられる[20, 21]。

Famous Chollima(以下、「Chollima」と略す)は、IT ワーカー(フリーランス開発者や外注エンジニア等)として国外の企業に就職することにより、関連システムに侵入してスパイ活動に従事したり、その企業から得た給与(外貨)を北朝鮮政府に送

---

[18] 出典：ANY.RUN『Smile, You're on Camera: A Live Stream from Inside Lazarus Group's IT Workers Scheme』 https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/?utm_source=facebook&utm_medium=post&utm_campaign=lazarus_case&utm_term=091225&utm_content=linktoblog

[19] 出典：ANY.RUN『Smile, You're on Camera: A Live Stream from Inside Lazarus Group's IT Workers Scheme』 https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/?utm_source=facebook&utm_medium=post&utm_campaign=lazarus_case&utm_term=091225&utm_content=linktoblog

[20] 出典：innovaTopia『CrowdStrike 警告：中国系ハッカー、ラテンアメリカでの攻撃 150%増加 ― 5G インフラ狙う地政学的戦略』 https://innovatopia.jp/cyber-security/cyber-security-news/55128/

[21] 出典：毎日新聞『金正恩氏が命名、ロケット「千里馬」 伝説の馬になぞらえた威信』 https://mainichi.jp/articles/20230602/k00/00m/030/021000c

金したりしている。これまでに、金融、暗号資産、ヘルスケア企業への潜入が確認されており[22]、その中にはフォーチュン 500(売上高における米企業上位 500 社)にランキングされる組織も幾つか含まれていた[23]。

3.3. 採用面接への取り組み

Chollima が国外企業の求人に応募してオンライン面接に合格するための方法としては、以下のように 2 通りある。いずれにおいても、武器となるのは高度なマルウェアではなく、人の信頼や判断力の隙を利用する「ソーシャルエンジニアリング」と AI 技術の組み合わせである。

【Chollima が自身で応募する場合】[24]

盗難・流出したパスポートや運転免許証等を使って実在の人物に成りすましたり、AI で生成した顔写真を使って架空の人物を作り出したりして、偽の身分証明書や履歴書、ビジネス向け SNS の LinkedIn で紹介するためのプロフィール等を作成する。そして、AI で生成したディープフェイク(既存の画像や動画から新たなコンテンツを合成する技術)や合成音声を使うことで自身の身体的特徴も偽って、採用面接を受ける。リモートワークの拡大や AI 技術の進化により、企業がこれらの工作に気づくことは難しい。

【外部協力者を利用する場合】[25]

北朝鮮国外の IT ワーカーを、この「就職活動」に協力するよう報酬を提示し、リクルートする。募集は、GitHub(ソフトウェア開発者がソースコードを管理・共有するためのプラットフォーム)でのスパムメッセージの送信や、Telegram 上での勧誘等により、大掛かりに行われる。協力者には、自身の身元情報を提供することや、採用面接への出席等が求められ、対応が可能な度合いに応じて報酬が支払われる。

3.4. セキュリティ研究者らによるおとり調査[26]

【Chollima の人材募集】

サイバー脅威インテリジェンス企業「Birmingham Cyber Arms」の Mauro Eldritch 氏は、GitHub 上で複数の人物(アカウント)が.NET、Java、C#、Python、JavaScript、Ruby、Go 言語、ブロックチェーン等に関する採用面接を代理で受けてくれる者を募集していることを発見した。ただし、募集のメッセージには、応募者は技術的な分野に精通している必要は

---

[22] 出典：ANY.RUN『Smile, You're on Camera: A Live Stream from Inside Lazarus Group's IT Workers Scheme』 https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/?utm_source=facebook&utm_medium=post&utm_campaign=lazarus_case&utm_term=091225&utm_content=linktoblog

[23] 出典：BleepingComputer『North Korea lures engineers to rent identities in fake IT worker scheme』 https://www.bleepingcomputer.com/news/security/north-korea-lures-engineers-to-rent-identities-in-fake-it-worker-scheme/

[24] 出典：ZDNET Japan『北朝鮮の IT 技術者、就職での身元偽装に AI を駆使--セキュリティ企業が解明』 https://japan.zdnet.com/article/35232518/

[25] 出典：ANY.RUN『Smile, You're on Camera: A Live Stream from Inside Lazarus Group's IT Workers Scheme』 https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/?utm_source=facebook&utm_medium=post&utm_campaign=lazarus_case&utm_term=091225&utm_content=linktoblog

[26] 出典：ANY.RUN『Smile, You're on Camera: A Live Stream from Inside Lazarus Group's IT Workers Scheme』 https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/?utm_source=facebook&utm_medium=post&utm_campaign=lazarus_case&utm_term=091225&utm_content=linktoblog

なく、面接時には的確な回答ができるようようサポートが提供され、採用後は「(Chollima の)経験豊富な開発者チーム」が代わりに実作業をこなすことも可能であることや、応募者への報酬が月に 3,000 ドル程度となることが記されていた。

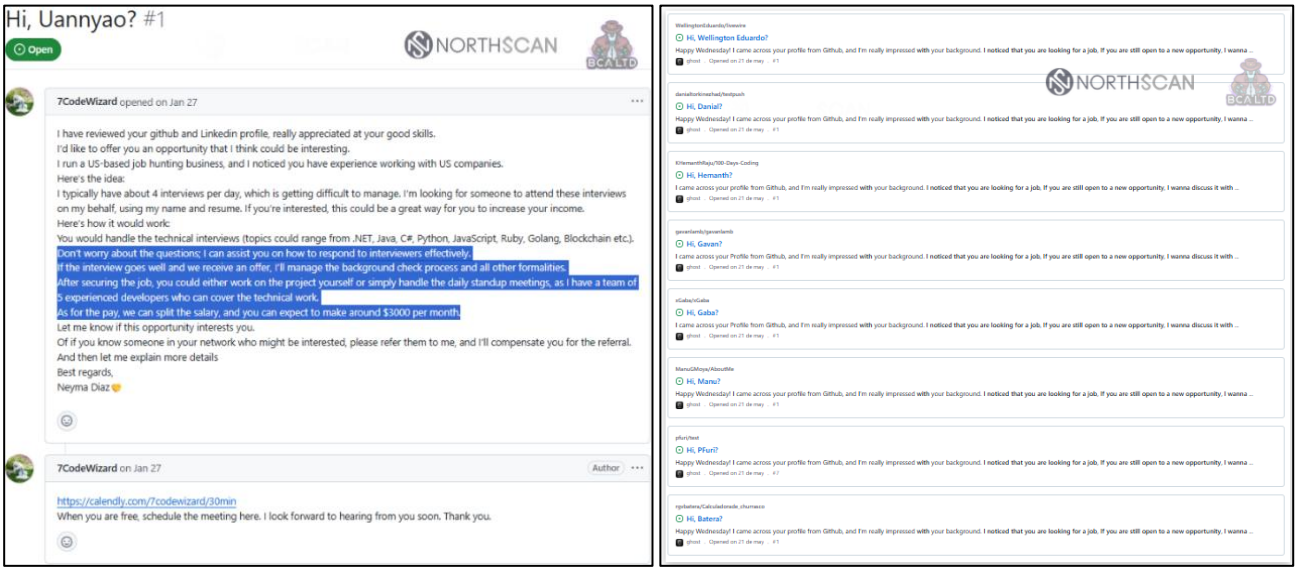

図 5 GitHub での代理面接募集のスパムメッセージ(ANY.RUN のレポートより)[27]

あなた(受信者)の Github と LinkedIn のプロフィールを確認し、興味深い機会を提供したいこと、自分の代わりに採用面接に出席してほしいこと、採用後は別の開発者に作業を担当させることも可能なこと、そして給与が得られること等が記されている。(左)

同様のメッセージが他の多くの開発者にも届いていることが、Github 上の送信者のアカウントにおいて一覧表示されている。(右)

Eldritch 氏は、これは北朝鮮工作員による、上記の「外部協力者を利用する場合」の募集であると考えた。そして、他の脅威インテリジェンス企業「NorthScan」の Heiner García 氏(以下、2 名とも「研究者」と記す)と共に IT ワーカーに偽装した北朝鮮工作員の策略の全貌を暴くため、実際に Chollima のリクルーターに接触し、彼らが企業に潜入するプロセスを内部から観察するおとり調査を実施することにした。

【研究者が Chollima に接触し、調査開始】

これまで Chollima は、Github の機能を悪用し、代理面接への出席を誘うコメント(メッセージ)を大量に送信していた。それらは公開されていたことから、研究者は、受信者の一人であった米国在住の Jones 氏に目を付け、そのプロフィールに酷似させた、同じ名前のアカウントを新たに作成した。

研究者が Chollima のメッセージに「Jones」として応答すると、そこから両者の間で Web 会議や Telegram を介したやり取りが行われるようになった。

研究者は、Web カメラをオフにして自身の姿を見せないようにしていたため、Chollima のリクルーターが不信感を持った様子が見て取れた。それでも研究者は、無邪気さを装いながら的確な質問をリクルーターに投げかけることで、成りすまし用 ID の使用に関する指示や意図等を含め、必要な情報を引き出していった。

---

[27] 出典：ANY.RUN『Smile, You're on Camera: A Live Stream from Inside Lazarus Group's IT Workers Scheme』 https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/?utm_source=facebook&utm_medium=post&utm_campaign=lazarus_case&utm_term=091225&utm_content=linktoblog

このようなやり取りの後、リクルーターは、自身が「Jones」の PC からリモートワークをするために、同機に常時アクセスさせてほしいと要求してきた。そして、ターゲット企業への採用面接に応募するにあたり、身分証明書、氏名、在留資格情報、住所が必要だと述べた。支払われる報酬については、リクルーターの全面的なサポートを受けながら「Jones」が面接を受ける場合は給与の 20%、「Jones」の個人情報と PC を使用してリクルーターが面接を受ける場合は 10%とのことだった。

図 6 Chollima のリクルーター(公開された動画より)[28]

【研究者に監視される Chollima】

研究者らは、リクルーターが要求した「常時アクセスできる PC の用意」に対し、マルウェア分析等で知られるセキュリティ企業 ANY.RUN の協力を得て、サンドボックス環境(プログラムやコードを実行・検証するための、本番環境とは切り離された安全な仮想環境)を用意した。また、住宅用プロキシを使用し、PC が米国に存在するように見せかけた。リクルーターは、「本物の米国人エンジニアの PC を乗っ取った」と信じて行動を開始。これを受けて研究者らも、彼の操作に対する常時監視を開始した。

以降、研究者らはリクルーターが悪意のある作業を実行するのを防ぐため、そしてひいては数週間程度の調査期間を確保するため、システムやネットワークにおいて度々、意図的な障害・遅延を密かに引き起こした。そしてこれらの責任を負わされたリクルーターは修復作業を余儀なくされた。

【使用ツール】

調査のある時点で、リクルーターがおとり調査用 PC において自身の Google アカウントにログインし、同期機能を有効にしたことで、研究者らはリクルーターが受信したメールの内容やグループの戦術等、多くの情報を得ることができた。例えば、グループは AI ツールを積極的に活用しており、その中には、求人応募書類に自動的に入力したり、面接を受けている最中の応募者に対してリアルタイムで回答案を提示したりするもの等が含まれていた。

【複数のチームの存在】

このリクルーターは Chollima 内のチームに所属しており、自身の指示によって作業する仲間もいる。

レポートによると、他にも複数のチームが存在する。研究者がリクルーターに(プレッシャーをかけるため)、別のチームの(架空の)人物からもスカウトされ、より高額の給与を提示されたと伝えると、リクルーターはこの架空の人物を汚い言葉で表現し、「彼を無視して、今後は自分とだけ仕事をしてほしい」と研究者に頼んだという。また、複数の工作員が、同じ日に同じターゲット企

[28] 出典：ANY.RUN『Lazarus #6: Asks to connect 24 7 and set a password for anydesk』(YouTube)
https://www.youtube.com/watch?v=PXsV7YpZvzk

業において同じ職種の採用面接に出席するよう手配されるケースがあり、これは異なるチーム間で調整が行われていない可能性を示唆するものだと、レポートは述べている。

【調査終了】

ある時、研究者らの意図的な操作により、リクルーターは突然、インターネットに接続できなくなった。PC の不具合が頻発していることについて彼から詰め寄られた研究者らは、プロキシを無効化し、改めてインターネット接続を可能にした。そしてリクルーターがオンラインで PC の所在地を調べると、それは今まで信じていた米国ではなく、(VPN 経由の)ドイツであった。ここで調査は終了。研究者らはリクルーターの疑念の声には取り合わず、PC をクラッシュさせた。

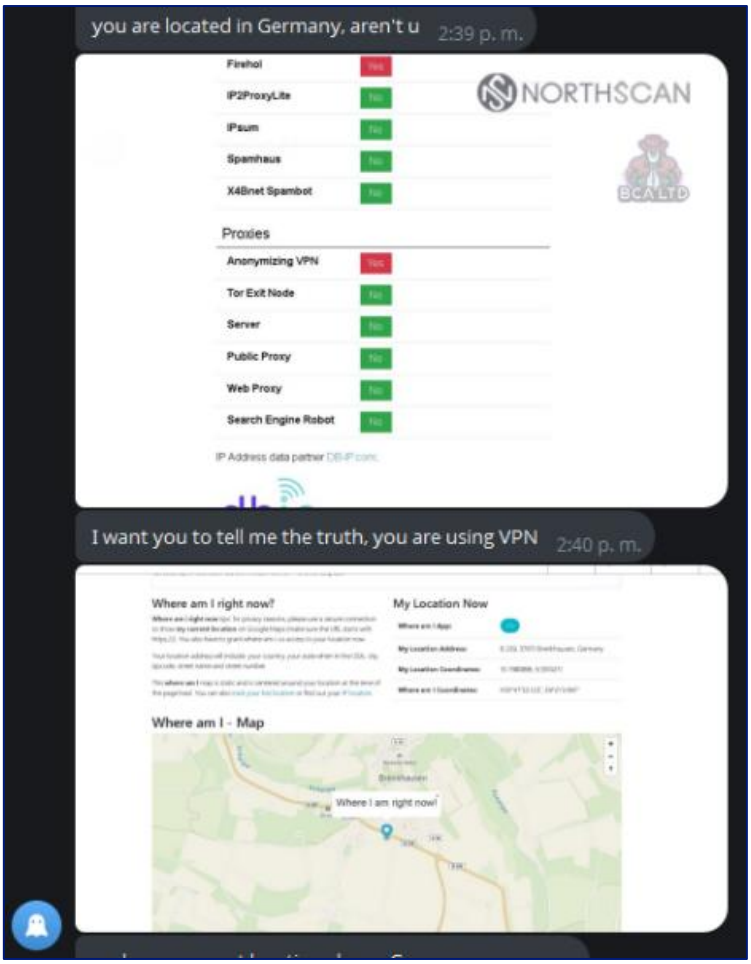

図 7 Chollima のリクルーターが PC の所在地(ドイツ)を確認した時の画面(ANY.RUN のレポートより)[29]
事態に気づいた Chollima のリクルーターは焦って研究者に問い詰める ー
「あなた、ドイツにいるのでしょう？」「正直に言ってほしい。あなた、VPN を使っているね」

[29] 出典：ANY.RUN『Smile, You're on Camera: A Live Stream from Inside Lazarus Group's IT Workers Scheme』 https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/?utm_source=facebook&utm_medium=post&utm_campaign=lazarus_case&utm_term=091225&utm_content=linktoblog

3.5. まとめ

今回のレポートは、北朝鮮の IT ワーカー潜入作戦を実際に内部から観察し、攻撃者の行動・心理・ツール・組織構造などが確認できる貴重な報告である。Chollima の武器は高度なマルウェアではなく、技術的な防御だけでは防ぎきれない人間行動の心理的操作に基づくソーシャルエンジニアリングが中心である。

企業側の対策として、求人への応募者の履歴書や職務経歴書の徹底確認、面接時の不自然な挙動に注意すること等が重要となるが、Chollima の募集に応じた IT ワーカーのような人物が本人として面接に対応する場合に見抜くことは難しく、リモート面接を取り入れている限り、このようなリスクを防ぐことは容易ではない。本件はリモートワーク業務の盲点を突いたもので、応募者には実際に企業に来てもらい面接することや、採用後は定期的に(または不定期に)現場で業務を実施させることで防止・抑止できる可能性が考えられる。また、ゼロトラストを推進することにより、最小権限の原則、継続的監視等の対策によって、内部で不正な活動をされた場合の被害低減を図ることが期待できる。

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
プロフェッショナルサービス部 OSINT モニタリングチーム
メールアドレス: nsj-co-osint-monitoring@security.ntt