サイバーセキュリティレポート

2023.03

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

© NTT Security Holdings

目次

© NTT Security Holdings

【当レポートについて】

当レポートでは 2023 年 3 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 Blackbaud 社、サイバー攻撃公表時の不備により 300 万ドルを支払う』

- 3 月 9 日、米証券取引委員会（証取委）は、クラウドソフトウェア企業の Blackbaud 社が 2020 年にランサムウェア攻撃を受け、100 万件以上のファイルが窃取された際に、投資家の判断を誤らせる情報開示をしていたことについて、同社が和解のために 300 万ドルを証取委に支払うことに同意したと発表した。
- 当初の発表では、Blackbaud 社は、攻撃者による銀行口座情報等への不正アクセスを否定していたが、実際にはそのようなアクセスが発生していた。また、適切なタイミングで情報開示ができなかった。証取委はこれらを重要な問題とみなした。
- 突然発生しかねないインシデントについて、スムーズに情報を提供するためのポリシーや手順を、企業の取締役会／技術・セキュリティ部門のメンバーの間で確認・準備しておくことは、投資家に対する大切な責務でもある。

第 2 章『北朝鮮系ハッカー「Kimsuky」の APT 活動』

- 3 月、北朝鮮系の APT グループである Kimsuky（キムスキー）によるものと考えられる標的型メールが検知された。Kimsuky は朝鮮半島情勢に関連した情報窃取を狙い、韓国の政府機関やシンクタンク、専門家をはじめ、日本、米国、ロシア、欧州諸国に対してもマルウェアを感染させる等の攻撃を行っている。
- 活発な活動に対し、同月にはドイツと韓国の情報機関が、ブラウザ拡張機能や Google アカウントの Android 端末の同期機能を利用する巧妙な手口を紹介し、Kimsuky による攻撃への注意喚起を行った。
- 北朝鮮のサイバー攻撃は、国家的に推し進めるミサイル開発等が背景にあり、Kimsuky の活動は今後も活発に行われると考えられる。様々に進化する侵入手段への警戒が必要である。

第 3 章『世界最大のハッカーフォーラム「BreachForums」のオーナー、逮捕される』

- 3 月 15 日、FBI は世界最大のハッカーフォーラム「BreachForums」のオーナーで、ニューヨーク州に住むコナー・ブライアン・フィッツパトリックを逮捕した。
- フィッツパトリック被告は、「pompompurin」と名乗り、ダークネット上ではよく知られているサイバー犯罪者であった。Tor や VPN 接続を使用し実際の居所がわからないようにしていたが、FBI は、昨年閉鎖された RaidForums のデータベースの解析等により同被告が pompompurin であると断定した。
- FBI は今回の捜査で BreachForums のデータベースも手に入れていることから、今後、その解析によって同フォーラムで活動していた他のサイバー犯罪者たちの特定が進むことも予測される。

© NTT Security Holdings

1. 米 Blackbaud 社、サイバー攻撃公表時の不備により 300 万ドルを支払う

1.1. 概要

2023 年 3 月 9 日、米国の証券取引委員会（以下、証取委）は 2020 年にランサムウェア攻撃を受けた Blackbaud（ブラックボード）社が、投資家の判断を誤らせる不十分な情報開示をしていたことについて、同社が和解のために 300 万ドルの民事制裁金を証取委に支払うことに同意したと発表した[1]。

図 1 証券取引委員会によるプレスリリース

1.2. Blackbaud 社について

Blackbaud 社はクラウドソフトウェア企業であり、米サウスカロライナ州チャールストンに本社を置く[2]。慈善団体、学校、高等教育機関、医療機関、宗教／文化団体等のさまざまな非営利組織に CRM（顧客関係管理ソフトウェア）を提供している。同社のサービスを通じて、毎年 1,000 億ドル以上の資金調達や投資が行われており、100 か国以上で利用されている[3]。NASDAQ で株式を公開しており、2022 年には 11 億ドルの収益を記録した[4]。

図 2 Blackbaud 本社

1.3. ランサムウェア被害

【不正アクセス発覚】

2020 年 2 月から、何者かが Blackbaud 社のシステムに対して不正アクセスを行っていた。同社の技術担当者がこの事

[1] 出典：U.S. Securities and Exchange Commission『SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors』 https://www.sec.gov/news/press-release/2023-48

[2] 出典：The Post and Courier『SC tech firm's cyberattack sent shockwaves across the globe and frustrated customers』 https://www.postandcourier.com/business/sc-tech-firms-cyberattack-sent-shockwaves-across-the-globe-and-frustrated-customers/article_dd46954a-eb88-11ea-8eb5-4ffd4b680168.html

[3] 出典：Blackbaud『About Blackbaud』 https://www.blackbaud.com/company

[4] 出典：Blackbaud『Blackbaud Announces 2022 Fourth Quarter and Full Year Results』 https://www.blackbaud.com/newsroom/article/2023/02/13/blackbaud-announces-2022-fourth-quarter-and-full-year-results

© NTT Security Holdings

を検知したのは同年 5 月 14 日。その後は、サイバーセキュリティチームが法執行機関等の協力を得て、20 日に攻撃者の侵入経路を塞いだことにより、社員らがシステムにアクセスできなくなったり、攻撃者がファイルを完全に暗号化したりする事態は防ぐことができた。しかし既に、同社の自己ホスト型環境から一部のデータのコピーが削除（および窃取）されていた。その後も攻撃者はシステムへのアクセスを取り戻そうとする試みを続けたが、6 月 3 日までに停止した[5] [6]。

攻撃者は、顧客に関するデータを窃取したことや、ビットコインでの身代金の支払い要求を伝える複数のメッセージを、同社のシステムに残しており[7]、更に 6 月 18 日には、どのファイルを窃取したのかについて同社に通知した[8]。

これらのことについて、同社のサイバーセキュリティ担当者はサードパーティベンダーに相談し、攻撃者と連絡を取った。そして最終的に、窃取した手元にあるデータを破壊するという攻撃者の約束と引き換えに、Blackbaud 社は身代金を支払った [7]。なお、この攻撃を行ったグループや人物については公表されていない。

【事件の公表】[7]

7 月 16 日、Blackbaud 社はこの侵害事件を初めて公表し、影響が及んだ顧客組織にも通知を行った。その中で、攻撃者はクレジットカード情報、銀行口座情報、社会保障番号にはアクセスしなかったと伝えた。だが、この判断は流出したファイルの内容ではなく、ファイル名の分析にのみ基づいた不十分なものであった。

事件公表後、数日間にわたり Blackbaud 社には、顧客組織から 1,000 件以上の連絡があった。多くの組織は、寄付者に関する上記のような機密データを暗号化されていないデータ領域に保存していたこと等について、懸念を示していた。

【身代金の支払いについて】

事件公表時、Blackbaud 社の広報担当者は、同社がサードパーティの専門家と協力しながら、サイバー犯罪者とコミュニケーションをとり、データコピーが破壊されたという信頼できる確認が取れた時に身代金を支払ったこと、予防措置として、外部に依頼し、ダークウェブを含むインターネットを監視させているが、流出情報が公開されたという証拠は見つかっていないことを述べた[9]。また同社のプレスリリースには、このインシデントの性質や調査結果を踏まえると、いかなるデータも悪用・公開されたと信じる理由はないと記載されていた[10]。

ただ、犯罪者が本当にデータを破壊したのか、客観的に検証する方法はなく、相手の言葉を信じて身代金を支払うという Blackbaud 社の対応は批判を集めた。現在と同様に 2020 年当時も、FBI は被害組織が身代金を支払うことを推奨／サポートしていなかった。これは、攻撃者が盗んだデータを保持・悪用しないという保証も、（システムが暗号化された場合に）

---

[5] 出典：The NonProfit Times『The Hack Of Blackbaud: Damage Is Still Being Assessed』
https://thenonprofittimes.com/npt_articles/the-hack-of-blackbaud-damage-is-still-being-assessed/

[6] 出典：HealthITSecurity『Blackbaud Ransomware Hack Affects 657K Maine Health System Donors』
https://healthitsecurity.com/news/blackbaud-ransomware-hack-affects-657k-maine-health-system-donors

[7] 出典：U.S. Securities and Exchange Commission『ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933 AND SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER』
https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf

[8] 出典：VeroNews.com『Thieves steal Vero Beach Museum of Art's donor info』
https://veronews.com/2020/08/13/thieves-steal-vero-beach-museum-of-arts-donor-info/

[9] 出典：The NonProfit Times『Breaking: Blackbaud Hacked, Ransom Paid』
https://thenonprofittimes.com/npt_articles/breaking-blackbaud-hacked-ransom-paid/

[10] 出典：BankInfoSecurity『Blackbaud's Bizarre Ransomware Attack Notification』
https://www.bankinfosecurity.com/blogs/blackbauds-insane-ransomware-attack-notification-p-2929

© NTT Security Holdings

組織がデータへのアクセスを回復できる保証も無いばかりか、攻撃者が今後も更に多くの組織を標的にする、または他の犯罪者もランサムウェア攻撃に興味を持ち、関与する可能性が存在するためである[11] [12]。

【被害の状況】[7] [13] [14] [15]

今回の攻撃により不正アクセスを受けたファイルの数は 100 万件以上であり、個人の氏名、住所や寄付履歴、配偶者や資産に関する情報等、顧客に関するさまざまなデータが含まれていた。

データ流出の影響を受けた組織は同社の顧客の約 4 分の 1 にあたる 13,000 以上。この中には英労働党や国際的な人権団体であるヒューマン・ライツ・ウォッチも含まれていた。更に影響が及んだ個人の数は、医療関連だけでも 1,000 万人以上とみられる。他にも例えば、ボーイスカウトアメリカ連盟の同窓生ネットワークは 5,000 万人を擁しており、侵害の広範な影響が懸念された。

1.4. 重要情報の更新

【開示情報の修正】

9 月 29 日、同社はこの事件に関する重要事項報告書[16]を証取委に提出し、**通知済みの顧客のうち一部において、暗号化されていなかったデータ領域（銀行口座情報、社会保障番号、ユーザー名やパスワード）にサイバー犯罪者がアクセスしていた可能性があると述べた。**この新たな事実は、関係する顧客へも通知されたが、事件の公表からすでに 2 か月半が経過していた。

【対応に追われる Blackbaud 社】

Blackbaud 社の 2020 年の年次報告書[17]によると、米国、英国、カナダの顧客が、今回のインシデントに関する費用の返済を要求し、その件数は約 570 に上った。また、同インシデントに関する Blackbaud 社の行為／不作為の疑いにより損害を受けたとして、米国とカナダで 30 件の消費者集団訴訟が行われた。

Blackbaud 社がこの年、インシデントに対処するため（主にサードパーティのサービスプロバイダーやコンサルタントへの、弁

[11] 出典：Top Class Actions『How Did the Blackbaud Ransomware Attack Occur?』
https://topclassactions.com/lawsuit-settlements/privacy/ransomware/how-did-the-blackbaud-ransomware-attack-occur/

[12] 出典：Federal Bureau of Investigation『Ransomware』
https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

[13] 出典：TechCrunch『SEC charges Blackbaud for failing to disclose 'full impact' of ransomware attack』
https://techcrunch.com/2023/03/10/sec-blackbaud-charged-ransomware/

[14] 出典：The HIPAA Journal『Blackbaud SEC Filing Provides Further Information on Data Breach and Mitigation Costs』
https://www.hipaajournal.com/blackbaud-sec-filing-provides-further-information-on-data-breach-and-mitigation-costs/

[15] 出典：The Dallas Morning News『Bush Presidential Center, Boy Scouts, Texas Tech, UT Austin hit in Blackbaud ransomware attack』
https://www.dallasnews.com/business/technology/2020/08/03/bush-presidential-center-boy-scouts-of-america-texas-tech-foundation-among-hundreds-hit-in-blackbaud-ransomware-attack/

[16] 出典：Blackbaud『Form 8-K』
https://investor.blackbaud.com/static-files/58a4ae64-afc5-45f7-81df-69dfc93888fc

[17] 出典：Blackbaud『Form 10-K (2020 Annual Report)』
https://investor.blackbaud.com/static-files/61e8a7e6-73d1-4e28-8c81-fd3013107288

© NTT Security Holdings

護士費用を含む支払い、及びサイバーセキュリティ対策の強化）の費用として計上したのは 1,040 万ドル。保険による回収見込み額は 940 万ドルであった。

【証券規制法違反および証取委との和解】[18] [1] [7] [19]

米国では、サイバー攻撃等により企業において情報漏洩が発生した場合、証取委が捜査や制裁を行う。

2023 年 3 月 9 日付のプレスリリースで、証取委は、Blackbaud 社が次の 2 つの証券規制法（に含まれる複数の条項）に違反したことを認定したと公告した。

一つ目は、「1933 年証券法」で、株式会社の情報開示の義務についてである。これは有価証券等の募集／販売において、重要な事実について不実の陳述や省略を行って金銭・財産を取得することと、購入者に対する詐欺、または詐欺として機能すると考えられる取引、慣行または業務過程に従事することを違法としている。

二つ目は「1934 年証券取引所法」で、証取委への報告義務についてである。これは債券の発行体が証取委の規則に準拠した四半期報告書を同委員会に提出することや、そのような報告書に必要な記述を誤解のないものにするために、あらゆる重要情報を含めること、更に本法に基づいて提出する報告書で開示が求められる情報を、同委員会の規則で指定されている期間内に処理するための開示統制・手続きを保持することを要求している。

Blackbaud 社は、証取委の調査結果を認めることも否定することもなく、違反行為を停止し、和解のために 300 万ドルの民事制裁金を支払うことに同意した。

1.5. Blackbaud 社の対応に見られた問題

証取委は、「公開会社には、投資家に対して正確かつタイムリーな重要情報を提供する義務があるが、Blackbaud 社はそれを怠った」と述べている [1]。同委員会は以下の 2 点を特に問題視した。

① 社内での報告体制の不備および更新情報開示の遅れ [7] [20]

Blackbaud 社は 7 月 16 日の事件公表時、複数の重要な個人情報種別を挙げ、それらに対する不正アクセスはなかったと述べていたが、その数日後、同社の技術および顧客対応担当者は、寄付者の（暗号化されていない形式で保存されていた）銀行口座情報と社会保障番号に、攻撃者がアクセスしていたことを知った。それにもかかわらず、**いずれの担当者もこの事実を、同社の情報開示に責任を持つ最上級管理職に報告しなかった。また、報告するためのポリシーや手順も存在しなかった。**このため、8 月 4 日付の四半期報告書では、当インシデントについて言及されていたものの、上記の重要なデータへの不正アクセスについての記載はなかった。最上級管理職が事実を知ったのは報告書提出から数週間後だった可能性がある。

また、このような管理上の不備に加え、インシデントの最初の公表からその内容が 9 月下旬に更新されるまで、約 2 ヶ月半も要したことに、証取委の厳しい目が向けられた。

---

[18] 出典：SOMPO CYBER SECURITY『米国証券取引委員会とは【用語集詳細】』
https://www.sompocybersecurity.com/column/glossary/sec-us

[19] 出典：U.S. Government Publishing Office『SECURITIES ACT OF 1933』
https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf

[20] 出典：Blackbaud『Form 10-Q』
https://investor.blackbaud.com/static-files/370a20eb-ef91-42cd-a212-e9b743b26ed1

© NTT Security Holdings

② 事実を仮定として記載 [7] [20]

上述の 8 月の四半期報告書には次のように記載されていた：「当社のデータセキュリティの侵害により、顧客または寄付者の個人情報または支払いカードのデータが不正に入手された場合、顧客等における当社の評判、ならびに当社の事業、営業成績、財務状況および流動性に悪影響を及ぼし、当社に対する訴訟または罰則の適用を招く結果となる**可能性がある**」

この記述について証取委は、Blackbaud 社の技術及び顧客対応の担当者らが、銀行口座情報等へ不正アクセスがあったことを知っていたにもかかわらず、同社はこの重要な情報を四半期報告書に含めず、**寄付者の機密情報の流出リスクを仮定に基づいた事柄として、誤解を招きかねない（投資家の判断を誤らせる）記述をしていた**と述べた。

ただしこの問題も、社内で情報を適切に伝達するためのポリシーや手順が整備されていなかったことが原因であるため、最上級管理職は、当報告書に「可能性がある」と記載した時点で、本当にそのように認識していた（意図的に重要情報を省略したり、投資家を欺いたりする意図はなかった）と考えられる。

1.6. 新たなサイバーセキュリティ規則

2011 年と 2018 年、証取委は「解釈的ガイダンス」を発行し、サイバーセキュリティのリスクおよびインシデントに関する開示について、既存の規則をどのように解釈すべきかについて、証取委の見解を示した[21]。ただ、証取委によるとこの後、重要なセキュリティインシデント、およびセキュリティのリスク管理・ガバナンスに関する開示のいずれも組織によって改善されたものの、開示の実践には一貫性がなかった[22]。

上記のガイダンスの改正に向け、2022 年 3 月、証取委はサイバーセキュリティ規則案を発表し、その中でさまざまな新しい要件を挙げた。例えば、組織に開示を求める事項として、①重要インシデント（開示時期は、インシデントが発生したと組織が判断してから 4 日以内）、②企業のサイバーセキュリティに関するポリシー、手順、ガバナンス、③取締役のサイバーセキュリティに関する専門知識を挙げている[23]。このサイバーセキュリティ規則は 2023 年 4 月に最終決定される予定であり、証取委はこれを踏まえて、今後も積極的に調査を進め、起訴を行うことが予想される。

1.7. まとめ

証取委による 2018 年の解釈的ガイダンスは企業に対し、「サイバーセキュリティ関連を含む重要な事象を正確かつ適時に開示することを可能にする（ための）、適切かつ効果的な開示統制と手続きを確立し、維持すること」を求めている他、企業は、（セキュリティインシデントの調査期間中であっても）過去の開示を再考／更新する必要があるかを検討するよう、述べている [23] [24]。Blackbaud 社はこのガイダンスに倣った対応を怠ったために、投資家に対して重要情報を適切に知らせることがで

---

[21] 出典：Deloitte『SEC Proposes New Requirements for Cybersecurity Disclosures』
https://dart.deloitte.com/USDART/home/publications/deloitte/heads-up/2022/sec-proposal-cybersecurity-disclosures

[22] 出典：U.S. Securities and Exchange Commission『FACT SHEET Public Company Cybersecurity; Proposed Rules』
https://www.sec.gov/files/33-11038-fact-sheet.pdf

[23] 出典：Cleary Cybersecurity and Privacy Watch『SEC Charges Public Company For Alleged Misleading Disclosures Surrounding Ransomware Attack』
https://www.clearycyberwatch.com/2023/03/sec-charges-public-company-for-alleged-misleading-disclosures-surrounding-ransomware-attack/

[24] 出典：U.S. Securities and Exchange Commission『Commission Statement and Guidance on Public Company Cybersecurity Disclosures』
https://www.sec.gov/rules/interp/2018/33-10459.pdf

© NTT Security Holdings

きず、多くの顧客組織や個人の間にも混乱を生じさせた。

重要インシデントの確認から 4 日以内の開示を求める証取委の新たなサイバーセキュリティ規則は間もなく発効するとみられる。また、EU 一般データ保護規則（GDPR）も、データ侵害に気付いてから 72 時間以内の監督機関への報告を義務付けている。

ランサムウェア攻撃を含め、突然発生しかねないインシデントについて、スムーズに情報を開示できるよう、そのためのポリシーや手順を企業の取締役会および技術・セキュリティ部門のメンバーの間で確認・準備しておくことは、投資家に対する大切な責務でもある。

© NTT Security Holdings

2. 北朝鮮系ハッカー「Kimsuky」の APT 活動

2.1. 概要

2023 年 3 月、韓国の北朝鮮関連の専門家らを標的とした、北朝鮮系の APT グループである Kimsuky（キムスキー）によるものと考えられる標的型メールが検知された。Kimsuky は以前から韓国を対象に情報窃取やアカウント乗っ取り等を行うサイバースパイ活動を目的として、マルウェア感染を狙った標的型メールを盛んに送信している。

活発な Kimsuky の活動に対し、同月にはドイツと韓国の情報機関が共同で注意喚起(図 3)を発表した[25]。

図 3 ドイツ連邦捜査局（BfV）と韓国国家情報院（NIS）による共同の注意喚起 [26]

2.2. Kimsuky とは

北朝鮮の情報収集と秘密工作を任務とする主要な対外情報機関として、総参謀部偵察局(RGB)がある。Kimsuky は、その傘下と考えられている APT グループ(図 4)で、2012 年頃から活動している[27]。

朝鮮半島の外交・安全保障問題、核政策、経済制裁等の情報収集を目的に、政府機関やシンクタンク、専門家を狙い、Kimsuky はサイバースパイ活動を行っている。活動は韓国をはじめ、日本、米国、ロシア、欧州諸国も標的としてきたことが確認されている。

攻撃手法としては、ソーシャルエンジニアリングやスピアフィッシング、水飲み場攻撃といった手法を駆使して標的をマルウェアに感染させ、情報を窃取する。2022 年初めからは、韓国のメディアとシンクタンクを狙った攻撃キャンペーンが確認されている[28]ほか、韓国の警察庁は、2022 年 4 月から 10 月にかけて、Kimsuky が外交・安全保障分野の専門家ら数百人を対象に標的型メールを送信し、個人情報やメールアドレスのリストを窃取したと発表した[29]。

国連安全保障理事会 北朝鮮制裁委員会の専門家パネルは、2023 年 4 月 5 日に公開された年次報告書[30]にて

---

[25] 出典：Recorded Future『North Korean APT group 'Kimsuky' targeting experts with new spearphishing campaign』 https://therecord.media/north-korea-apt-kimsuky-attacks

[26] 出典：ドイツ連邦憲法擁護庁『Bundesamt für Verfassungsschutz - Counter-intelligence - Joint Cyber Security Advisory』 https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2023/2023-03-20-joint-cyber-security-advisory.html

[27] 出典：MITRE ATT&CK『Kimsuky, STOLEN PENCIL, Thallium, Black Banshee, Velvet Chollima, Group G0094』 https://attack.mitre.org/groups/G0094/

[28] 出典：Kaspersky『Kimsuky's GoldDragon cluster and its C2 operations | Securelist』 https://securelist.com/kimsukys-golddragon-cluster-and-its-c2-operations/107258/

[29] 出典：ハンギョレ新聞『北朝鮮のハッカー組織、韓国の「記者・議員室」装い数百人にフィッシングメール』 http://japan.hani.co.kr/arti/politics/45493.html

[30] 出典：国連安全保障理事会北朝鮮制裁委員会『Final report of the Panel of Experts submitted pursuant to resolution 2627 (2022)』 https://undocs.org/S/2023/171

© NTT Security Holdings

Kimsuky のこれまでの活動について報告しており[31]、暗号資産を狙った攻撃等で知られる Lazarus(APT38)グループ等と並んで、北朝鮮の有力な APT グループのひとつに位置づけている。

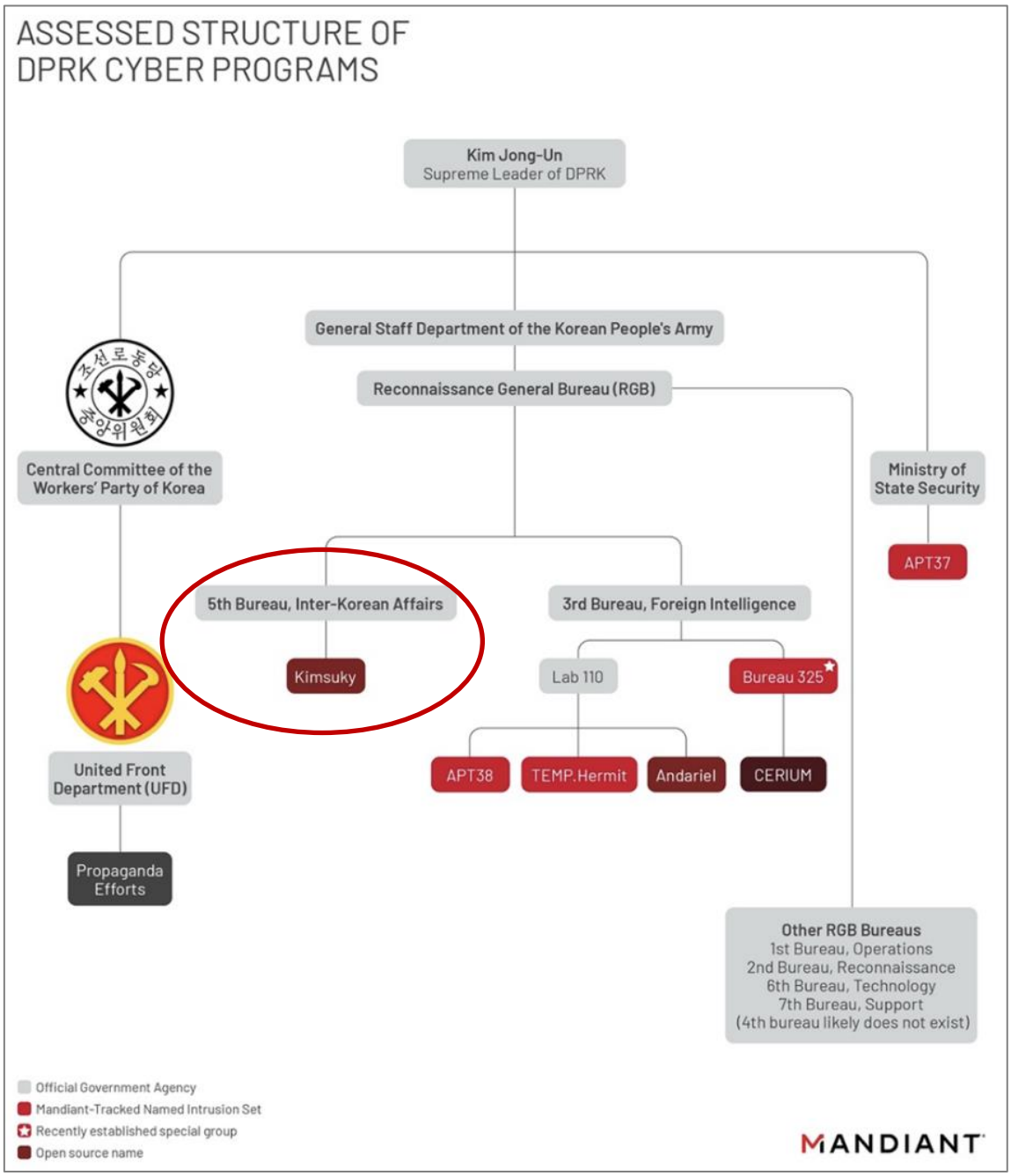


図 4 北朝鮮のサイバー攻撃組織図における Kimsuky [32]
（※Mandiant 作成の図に、Kimsuky の所在を赤丸で囲んだ）

[31] 出典：読売新聞『北朝鮮サイバー攻撃、暗号資産(仮想通貨)窃取 10 億ドル…2022 年』
https://www.yomiuri.co.jp/world/20230406-OYT1T50082/

[32] 出典：Mandiant『Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations』
https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government

© NTT Security Holdings

2.3. Kimsuky の最近の標的型メール攻撃

2023 年 3 月 7 日、韓国の北朝鮮関連の専門家らが標的型メールを受信した。送信者名は、韓国の公営テレビ局である KBS の現職の報道記者に詐称していた。「KBS 인터뷰 요청건'이라는 제목의 전자우편에는」（KBS インタビュー要請の件）という件名で、本文には、北朝鮮の急増するミサイル脅威と対外情勢の関係に知見の有る専門家にインタビューを要請し、返答を求める旨が記されていた（図 5）。

受信者が求めに応えて返信すると ZIP ファイルを添付したメールが送られてくるようになっていた（図 6）。韓国のセキュリティ会社である AhnLab の分析では、この ZIP ファイルの中にはアンケートに偽装した CHM ファイル（Windows ヘルプファイル）が格納されており、CHM ファイルを開くとスクリプトが実行されて情報窃取のマルウェアに感染することが判明している[33]。

図 5 KBS の取材に偽装した標的型メール [34]

図 6 返信で来たファイル添付メール [35]

以前に確認されている標的型攻撃の手口との類似性等から、この攻撃は Kimsuky によるものと分析されている。他にも同時期に、韓国の国民年金公団や警察庁サイバー安全局等に偽装したメールが観測されており、これらも北朝鮮 APT グループの標的型攻撃と考えられている。

2.4. 情報機関による Kimsuky への注意喚起発表

Kimsuky のサイバースパイ活動が盛んなことに対し、3 月 20 日に情報機関であるドイツ連邦捜査局（BfV）と韓国国家情報院（NIS)が、共同で注意喚起を発表した[36]。Kimsuky が過去数年間、標的型メールを使用して韓国とドイツの組織を標的にしていたことから、共同での発表になったとみられる。さらに、最近観察された攻撃キャンペーンの手法の分析から、「対北朝鮮外交と安全保障の世界的なシンクタンク」を標的にすることで、さらにその先を狙っていると警告している。

---

[33] 出典：AhnLab『対北朝鮮関連のアンケートに偽装した CHM マルウェア(Kimsuky) - ASEC ブログ』
https://asec.ahnlab.com/jp/49306/

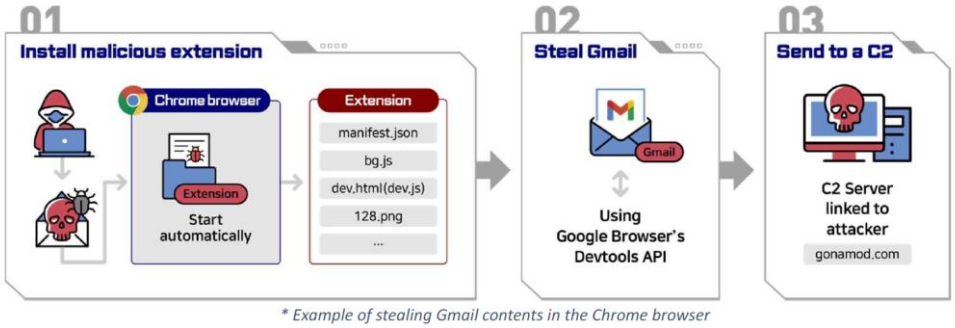
[34] 出典：RFA『KBS 통일외교부 기자 사칭한 북 해킹 시도 포착』
https://www.rfa.org/korean/in_focus/nk_nuclear_talks/hacking-03082023084805.html

[35] 出典：AhnLab『対北朝鮮関連のアンケートに偽装した CHM マルウェア(Kimsuky) - ASEC ブログ』
https://asec.ahnlab.com/jp/49306/

[36] 出典：ドイツ連邦憲法擁護庁『Bundesamt für Verfassungsschutz - Counter-intelligence - Joint Cyber Security Advisory』
https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2023/2023-03-20-joint-cyber-security-advisory.html

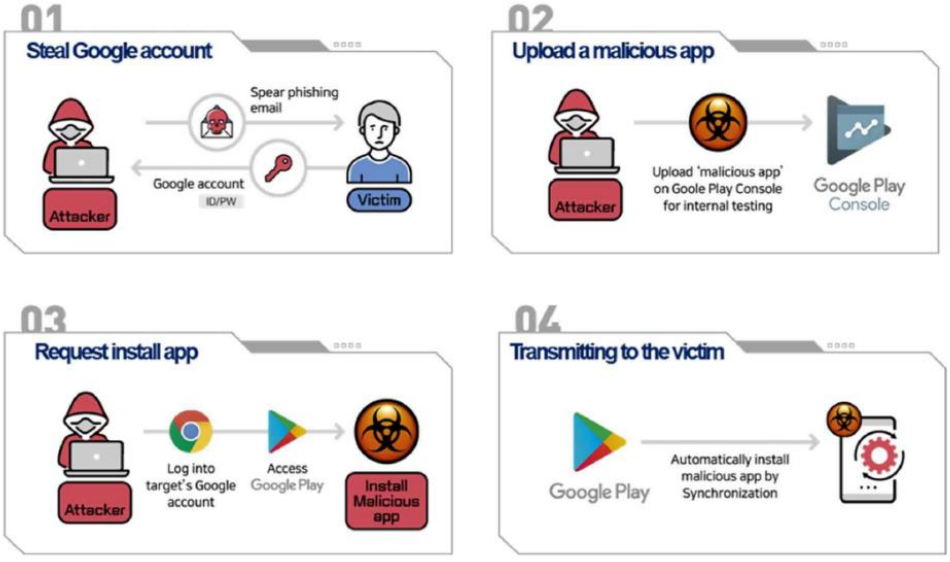
© NTT Security Holdings

この注意喚起では、先に紹介した 3 月の攻撃事例とはまた異なる、標的型メールを入り口として情報窃取をする手口を紹介している。悪性のブラウザ拡張機能をインストールさせる手口（図 7）と、Android 端末に悪性アプリを自動配信する手口（図 8）の 2 種類で、これらの手口で 2 要素認証等のセキュリティ設定を回避してバックドアを設け、標的に気づかれることなく情報を窃取し続けることを狙ったと考えられている。



1 メールのリンク先にある悪性のブラウザ拡張機能をインストールするよう、標的型メールでユーザーを誘導
2 インストールされたブラウザ拡張機能が Gmail アカウントの内容を窃取
3 ブラウザ拡張機能は、窃取した情報を攻撃者のサーバーに送信する

図 7 標的型メール攻撃を通じインストールされる、情報窃取を目的としたブラウザ拡張機能（注意喚起より）



1 標的型メールにより標的の Google アカウントを窃取
2 悪性アプリを開発者用の Google Play に登録しておく
3 窃取した標的の Google アカウントに不正アクセスし、開発者用の Google Play へ同アカウントを登録
4 Google Play から悪性アプリが、標的の Google アカウントに紐づく Android 端末へと自動的に配信される

図 8 標的型メール攻撃を通じた、Android 端末への悪性アプリインストール（注意喚起より）

© NTT Security Holdings

2.5. まとめ

最新の年次報告書で国連安保理北朝鮮制裁委員会は、Kimsuky 等のグループを統括する総参謀部偵察局の長官であるリ・チャンホ（리 창호）総局長（図 9）[37]を制裁対象リストに加えるよう勧告[38]しており、国際社会が北朝鮮の APT グループの活動に対して危機感を持っていることが窺える。また、2023 年 4 月 7 日には日米韓 3 カ国の北朝鮮担当高官が、度重なる弾道ミサイル発射や核開発の動きへの強い非難を表明する共同声明[39]の中で、北朝鮮の国家戦略を支援するために悪意あるサイバー活動を通じた資金窃取や資金洗浄、情報収集が行われていることについて言及し、深い懸念を表明している[40]。

北朝鮮が強硬な姿勢を強める現在、Kimsuky のサイバースパイ活動は今後も盛んに行われると予想され、注意喚起にあるような様々に進化する侵入手段への警戒が必要である。

図 9 リ・チャンホ
総参謀部偵察局総局長

[37] 出典：大韓民国統一部 北朝鮮情報ポータル『리 창호』
https://nkinfo.unikorea.go.kr/nkp/theme/viewPeople.do?menuId=PEOPLE&nkpmno=2307

[38] 出典：国連安全保障理事会北朝鮮制裁委員会『Final report of the Panel of Experts submitted pursuant to resolution 2627 (2022)』
https://undocs.org/S/2023/171

[39] 出典：外務省『北朝鮮に関する日米韓協議（結果）』
https://www.mofa.go.jp/mofaj/press/release/press1_001412.html

[40] 出典：Reuters『US, S.Korea, Japan concerned over N.Korea's 'malicious' cyber activities』
https://www.reuters.com/world/asia-pacific/us-south-korea-japan-express-concern-over-nkoreas-malicious-cyber-activities-2023-04-07/

© NTT Security Holdings

3. 世界最大のハッカーフォーラム「BreachForums」のオーナー、逮捕される

3.1. 概要

3 月 15 日、FBI は世界最大のハッカーフォーラム「BreachForums」のオーナーで、ニューヨーク州に住むコナー・ブライアン・フィッツパトリック（Connor Brian Fitzpatrick）を逮捕した[41]。彼は、ダークネット上では日本のキャラクター「ポムポムプリン（pompompurin）」を名乗り、活動していた。

その後 3 月 20 日頃から、BreachForums にアクセスするとエラーが表示され利用できない状態となり、閉鎖状態となった。

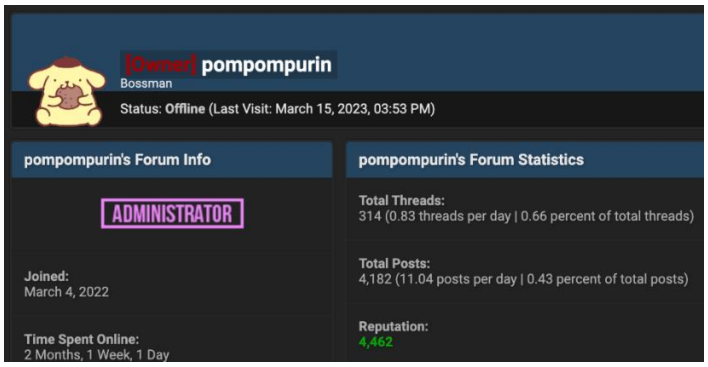


図 10 フィッツパトリック被告のプロフィール画面

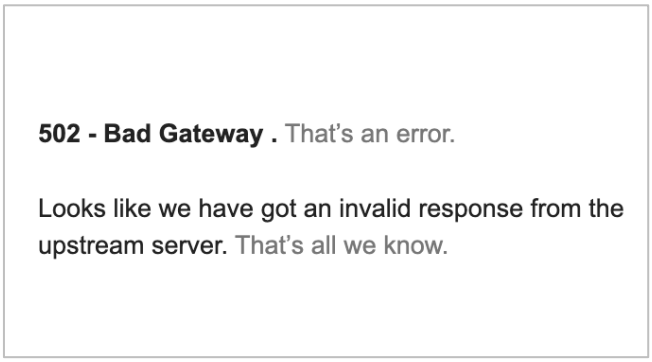


図 11 BreachForums のエラー画面

3.2. BreachForums とは

BreachForums は、2022 年 4 月に pompompurin と名乗る人物により開設された。サイバー攻撃により窃取された漏洩情報の売買や、攻撃手法についての情報交換等が行われるハッカーフォーラムであった。開設時は、当時世界最大だった別のハッカーフォーラム「RaidForums」が欧米の合同捜査により閉鎖された直後であったため、そのユーザー達を勧誘して本格的にスタートし、その後さらに多くのハッカーを集めた。同年 6 月には、取り扱う漏洩データのレコード数は 109 億件を突破した。pompompurin は「RaidForums のレコード数を追い抜いた」と投稿し、BreachForums は世界最大のハッカーフォーラムとなった。

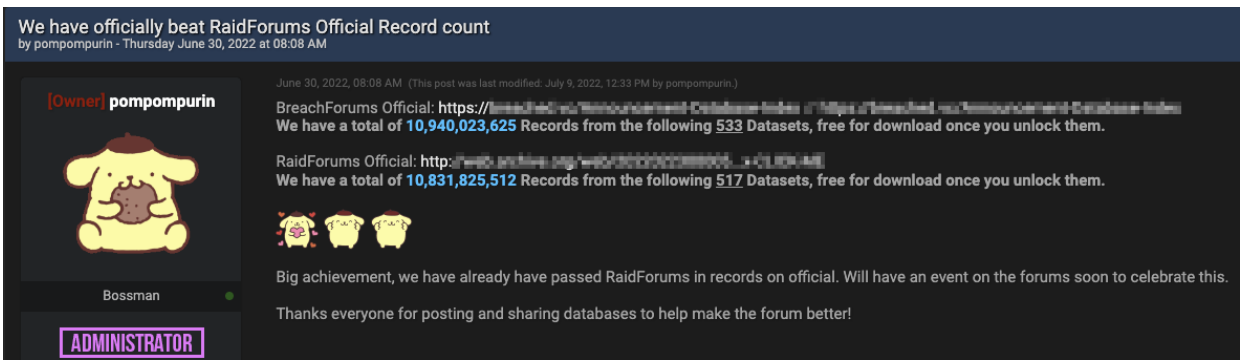


図 12 RaidForums を追い抜いたとする投稿

[41] 出典：Bleeping Computer『Alleged BreachForums owner Pompompurin arrested on cybercrime charges』 https://www.bleepingcomputer.com/news/security/alleged-breachforums-owner-pompompurin-arrested-on-cybercrime-charges/

© NTT Security Holdings

3.3.「pompompurin」と逮捕の経緯

【pompompurin とは】

フィッツパトリック被告は、ダークネット上では「pompompurin」と名乗り、BreachForums の立ち上げ以前から、RaidForums やロシアのハッカー掲示板などで活動していた。過去には、FBI のメールサーバーをハッキングして FBI の正規のメールアドレスから、あなたのシステムが攻撃を受けデータが窃取されている、といった偽の警告メールを送ったり[42]、米国で人気の投資アプリ「ロビンフッド」の顧客データを窃取し販売したり[43]する等、様々な企業や組織を攻撃しており、名の知れたサイバー犯罪者であった。

【逮捕の経緯】

フィッツパトリック被告は pompompurin としての活動時には、通常は Tor や VPN 接続を使用してアクセス元を秘匿し、実際の居所がわからないようにしていた[44]。しかし、VPN の接続に失敗した時に、自身のプロバイダーの IP アドレスから BreachForums のシステムにログインしていることを FBI に検知され、これが逮捕の決め手の 1 つとなった。

他にも、FBI は閉鎖された RaidForums のデータベースも所有しており、その解析によっても今回の逮捕につながる証拠を得た。例えば、pompompurin が利用していたアプリのデータベースが漏洩したという話を RaidForums のオーナーとチャットしている中で、自身のメールアドレス「**conorfitzpatrick**02@gmail[.]com」は漏洩したデータベースに含まれていなかった、と語っていることを FBI は発見した[45]。これに加えて、フィッツパトリック被告がそのアドレスを実際に使用していた記録を Google から得ることができた。こうした証拠を積み重ね、FBI はフィッツパトリック被告こそが pompompurin であると断定し、同被告もこれを認めた。

3.4. BreachForums 閉鎖までの動き

BreachForums にはフィッツパトリック被告以外にも複数の管理者がいた。そのうち「Baphomet」と名乗る者が、コミュニティを存続させるために善後策を講じようとして、Telegram や自身のサイト上でメッセージを投稿し、状況を伝えている。フィッツパトリック被告の逮捕後、当初 Baphomet は BreachForums を停止させ、新しい環境に移行させることを考えていた。しかし、移行作業中に自身や関係者のものではないログイン履歴があったことに気づいたこと等から、FBI がフィッツパトリック被告の PC や ID・パスワードといった情報を利用している可能性があると考えた。その結果、BreachForums に関しては、ソースコードを含め、安全なものは何もないと考え、フォーラムを閉鎖する決断を下した。今後の在り方についてユーザー達も交えて話合うためのグループを Telegram 上に設けているが、新しいフォーラムの開設についての具体的な動きは今のところない。

また、今回の閉鎖後にいくつか新しいハッカーフォーラムが立ち上がっているが、Baphomet は自身たちとは無関係だと主張している。現在までのところ、RaidForums 閉鎖後の BreachForums のように、急速にユーザーを集めているフォーラムはな

[42] 出典：Bleeping Computer『FBI system hacked to email 'urgent' warning about fake cyberattacks』 https://www.bleepingcomputer.com/news/security/fbi-system-hacked-to-email-urgent-warning-about-fake-cyberattacks/

[43] 出典：Bleeping Computer『Robinhood discloses data breach impacting 7 million customers』 https://www.bleepingcomputer.com/news/security/robinhood-discloses-data-breach-impacting-7-million-customers/

[44] 出典：Bleeping Computer『FBI confirms access to Breached cybercrime forum database』 https://www.bleepingcomputer.com/news/security/fbi-confirms-access-to-breached-cybercrime-forum-database/

[45] 出典：TechCrunch『How the FBI caught the BreachForums admin』 https://techcrunch.com/2023/03/24/how-the-fbi-caught-the-breachforums-admin/

© NTT Security Holdings

いようである[46]。

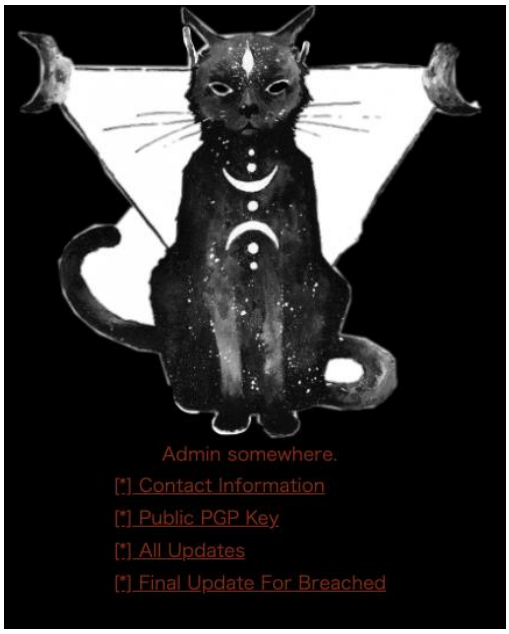


図 13 Baphomet の Web サイト

新しいフォーラムはいずれも我々と無関係であり、BreachForums のユーザー情報を提供するつもりはない。
新しいフォーラムへの参加は自由だが、いつも通り慎重にしてくれ。

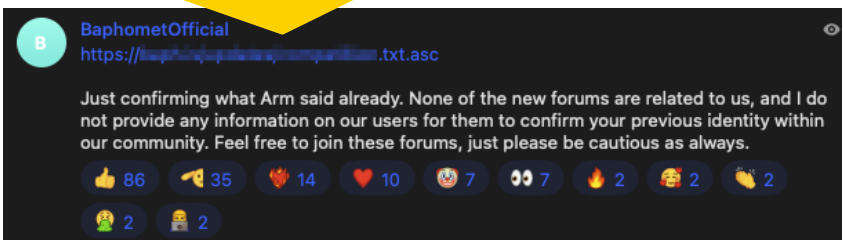


図 14 新興フォーラムは自分たちとは無関係という Telegram への投稿

3.5. まとめ

RaidForums の閉鎖後、これを実質的に引き継ぎ世界最大のハッカーフォーラムとなった BreachForums のオーナーが逮捕され、同フォーラムは閉鎖された。残された管理者 Baphomet らも、現時点では新しいフォーラムの立ち上げができておらず、慎重になっている様子であり、彼らが受けた影響は大きいようである。

FBI は今回の捜査で BreachForums のデータベースも手に入れていることから、今後、その解析によって同フォーラムで活動していた他のサイバー犯罪者たちの特定が進むことも予測される。

以上

[46] 出典：Bleeping Computer『Breached shutdown sparks migration to ARES data leak forums』
https://www.bleepingcomputer.com/news/security/breached-shutdown-sparks-migration-to-ares-data-leak-forums/

© NTT Security Holdings

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

© NTT Security Holdings