サイバーセキュリティレポート

2023.08

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

【1 ページサマリー】

当レポートでは 2023 年 8 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『国際共同捜査で警察庁が海外フィッシング犯を初めて逮捕』

- 8 月 8 日、警察庁はフィッシング攻撃によってクレジットカード情報を収集し不正に利用したとして、インドネシア在住のデア・カリスナ容疑者を現地警察らと協力し逮捕したと発表した。
- デア容疑者はフィッシングでクレジットカード情報を収集。これを用いて購入した電化製品等を、日本在住の共犯者に転売・現金化させ、自身に送金させていた。
- 本件は、日本のサイバー特別捜査隊が国際共同捜査を行い、容疑者の逮捕に繋げた初の事例となった。

第 2 章『北朝鮮がロシアのトップミサイル企業をハッキング』

- 北朝鮮政府と繋がりのあるハッカーグループが、情報窃取を狙ってロシア軍と関わりの深いミサイル企業にハッキングをしていたことが明らかになった。
- 北朝鮮の複数のハッカーグループにより Windows にバックドアが設置され、電子メールサーバーを含む機密性の高い内部インフラへのハッキングが行われていた。
- 北朝鮮はロシアのミサイル開発技術に高い関心を持っており、その技術を入手するためなら友好国すらハッキングの標的にすることが今回の件で示された。

第 3 章『SMS トラフィックポンピング詐欺』

- SMS トラフィックポンピング詐欺と呼ばれる、SMS で通知を行っている企業に多額の電話代を負わせる詐欺が発生している。
- SMS 認証等で大量の SMS 送信リクエストを受け付ける企業が、被害に遭っている。
- 被害防止のため、SMS を業務で送信している企業は送信制限の導入等の対策を講じておく必要がある。

© NTT Security Holdings

1. 国際共同捜査で警察庁が海外フィッシング犯を初めて逮捕

1.1. 国際共同捜査で容疑者を逮捕

8 月 8 日、警察庁は、フィッシング攻撃によってクレジットカード情報を収集し不正に利用したとして、インドネシア在住のデア・カリスナ容疑者を現地警察らと協力し逮捕したと発表した[1]。

本件は、日本で発生した事件について、警察庁サイバー特別捜査隊が他国の法執行機関と協力し、容疑者逮捕に至った初の事例となった。

図 1 サイバー特別捜査隊のシンボルマーク

1.2. 事件と捜査

【事件の概要】

逮捕されたデア容疑者は「16Shop」と呼ばれるフィッシングサービスを利用し、偽サイトを作成。このようなサイト等に騙された人々から個人情報やクレジットカード情報を収集していた[2, 3]。デア容疑者は、このクレジットカード情報を利用して電化製品等を購入すると、これらを日本在住のインドネシア人の男らに転売および現金化させ、自身宛てに送金させていた。盗んだクレジットカード情報の現金化を目的として、身元の特定を避けるために、このような方法を用いたと考えられる。

【容疑者逮捕の経緯】

デア容疑者が捜査線上に浮かび上がったきっかけは、2022 年 8 月に大阪府警が共犯者（前述）を逮捕したことであった。容疑は、2019 年 10 月に発生した、インターネット通販でのパソコンの不正購入で、この時に使用した他人のクレジットカード情報は、デア容疑者が 16Shop のサービスを介して窃取したものであった。

今年 4 月、大阪府警とサイバー特別捜査隊は本件捜査のための合同捜査本部を設置した。7 月には、インドネシア警察が来日し、日本の警察と協力して捜査を行った。その結果、デア容疑者が主導したことが裏付けられ、7 月 9 日、インドネシアで同容疑者が逮捕されるに至った。デア容疑者の犯罪により、日本での被害総額は、16 億ルピア（約 1,520 万円）に上った[4]。

[1] 出典：産経ニュース『フィッシング容疑でインドネシア人逮捕　警察庁、国際共同捜査で初』
https://www.sankei.com/article/20230808-EP5Q3NPC6NIEDPOD5D6JQFQLQI/

[2] 出典：朝日新聞 DIGITAL『初の国際サイバー捜査、インドネシア人逮捕　世界的詐欺ツールを使用』
https://www.asahi.com/articles/ASR884RWLR87UTIL040.html

[3] 出典：WNEWS247『Japan-Indonesia phishing probe leads back to a teenage 'genius'』
https://wnews247.com/2023/08/09/japan-indonesia-phishing-probe-leads-back-to-a-teenage-genius/

[4] 出典：DIVISI HUMAS POLRI『Bareskrim Ungkap Peretasan Kartu Kredit di Jepang, Kerugian Capai 1,6 Milyar』
https://humas.polri.go.id/2023/08/08/bareskrim-ungkap-peretasan-kartu-kredit-di-jepang-kerugian-capai-16-milyar/

© NTT Security Holdings

図 2 日本との捜査協力によって容疑者を逮捕した事について記者会見を行うジャカルタサイバー犯罪局[5]

1.3. 16Shop と PaaS

デア容疑者が利用した 16Shop は、PaaS（Phishing-as-a-Service）と呼ばれる、フィッシング攻撃を行うために必要なツールや環境など一式を提供しているサービスのひとつである。近年のフィッシング攻撃では PaaS の利用が増加していることが知られている。PaaS を利用することで、サイバー犯罪者たちは自分で個々のツールやサーバーを用意する必要が無く、気軽に攻撃を開始できる。PaaS の一般的な機能としては、有名なショッピングサイト等に似せたフィッシングサイトを作成するためのツール、詐欺メール配信機能、被害者の情報を確認するためのダッシュボード、といったものが挙げられる[6]。

16Shop は 2018 年頃から運営されており、上記の PaaS の一般的な機能に加えて、セキュリティ企業の IP アドレスからアクセスされた場合にはフィッシングサイトを表示しないようにして、検知を困難にする機能等も備えていた[7]。同サービスはサイバー犯罪者達に販売され、少なくとも 7 万人の被害者が出ていた[8, 9]。なお、2021 年にインターポールが主導した捜査により 16Shop は閉鎖され、運営者も逮捕されている。この捜査情報を得られたことが、上記の警察庁による国際捜査に繋がった

[5] 出典：DIVISI HUMAS POLRI『Bareskrim Ungkap Peretasan Kartu Kredit di Jepang, Kerugian Capai 1,6 Milyar』 https://humas.polri.go.id/2023/08/08/bareskrim-ungkap-peretasan-kartu-kredit-di-jepang-kerugian-capai-16-milyar/

[6] 出典：Bleeping Computer『Interpol takes down 16shop phishing-as-a-service platform』 https://www.bleepingcomputer.com/news/security/interpol-takes-down-16shop-phishing-as-a-service-platform/

[7] 出典：McAfee Blog『フィッシングキット「16Shop」が Amazon ユーザーをターゲットに』 https://ascii.jp/elem/000/001/898/1898098/

[8] 出典：INTERPOL『Notorious phishing platform shut down, arrests in international police operation』 https://www.interpol.int/en/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation

[9] 出典：朝日新聞 DIGITAL『16SHOP「43 カ国 7 万人以上に販売」 ICPO が国際捜査発表』 https://www.asahi.com/articles/ASR8953J9R89UTIL01B.html

© NTT Security Holdings

と考えられている[10]。

1.4. まとめ

今回のデア容疑者の逮捕は、国外の捜査機関との共同捜査により、サイバー特別捜査隊が国際的なサイバー犯罪を摘発した初のケースとなった。多くのサイバー犯罪が国境を越えて行われていることから、捜査機関の国際協調は不可欠であり、今後も更なる活躍を期待したい。

[10] 出典：サイバーディフェンス研究所『16Shop 関係者逮捕の舞台裏』
https://io.cyberdefense.jp/entry/16Shop/

© NTT Security Holdings

2. 北朝鮮がロシアのトップミサイル企業をハッキング

2.1. 概要

2023 年 8 月 7 日、北朝鮮のハッカーグループがロシアの大手ミサイル企業のネットワークに、2022 年前半頃の 5 カ月以上に渡って不正アクセスを行っていたと、ロイター通信が報じた。ロシアからミサイル技術を窃取するため、北朝鮮が数少ない友好国もサイバー攻撃の標的にしていたことが判明した[11]。

2.2. ハッキングについて

【北朝鮮のハッカーグループによる不正侵入】

本件についての情報を提供したのは、米サイバーセキュリティ企業の SentinelOne（センチネルワン）である。

北朝鮮政府と繋がりのあるハッカーグループ「Lazarus（ラザルス）」と「ScarCruft（スカークラフト）」が少なくとも 2021 年 12 月 1 日から 2022 年 5 月の間、ロシアのミサイル企業「NPO マシノストロイェニヤ」（以下、NPO Mash）のロケット設計部署のシステムに、遠隔操作をするための侵入口となるバックドアツールを密かにインストールし、データへのアクセスを繰り返していた。なお、具体的にどのような情報にアクセスしていたかまでは明らかではない[11, 12]。

【SentinelOne の調査結果】[11, 13]

最初に、Lazarus は「OpenCarrot」と呼ばれる Windows バックドアを NPO Mash のシステムに仕掛けた。その背後でもうひとつのハッカーグループである ScarCruft が、NPO Mash の電子メールサーバーを含む機密性の高い内部インフラのハッキングを行っていたとみられる。これらのグループの関係性は不明だが、いずれも北朝鮮国家の戦略に沿って活動していると考えられており、一つのターゲットに対し複数の攻撃グループを割り当てることで、北朝鮮国家が侵害成功の確率を高めようとしていたのではないかと指摘されている。

SentinelOne がこのような事実を確認したのは、同社が北朝鮮のハッカーについて調査をしていた時に、NPO Mash 内部の電子メールのアーカイブデータを入手したことによる。このデータは NPO Mash が自社のハッキング被害を発見し、これを調査していた時に誤って流出させたものであった。この電子メールで議論されているハッキング被害の情報について、他のサイバー攻撃の証跡等と突き合わせることにより、上記のグループの活動との関連性を発見することができた。

---

[11] 出典：REUTERS『North Korean hackers breached top Russian missile maker』
https://www.reuters.com/technology/north-korean-hackers-breached-top-russian-missile-maker-2023-08-07/

[12] 出典：時事通信ニュース『北朝鮮ハッカー、ロシア企業に侵入か＝ミサイル情報狙う？―不正アクセスで技術窃取・ロイター報道』
https://sp.m.jiji.com/article/show/3015587?free=1

[13] 出典：SentinelLabs『Comrades in Arms? | North Korea Compromises Sanctioned Russian Missile Engineering Company』
https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/

© NTT Security Holdings

図 3 NPO Mash 内部から流出した、ハッキング被害の調査に関する電子メールの例
（NPO Mash が疑わしいネットワーク通信として検出した、攻撃者に関連する IP が記載されている）[14]

2.3. 被害組織について

本件で被害に遭った NPO Mash は、ミサイルや宇宙ロケット開発などに従事する企業であり、ロシア軍の機密性の高い知的財産も所有する。また、同社が開発した極超音速巡航ミサイル「ジルコン」は、プーチン大統領から高い評価を得ている。

一方、北朝鮮は、米国本土を攻撃できる大陸間弾道ミサイル（ICBM）を製造しており、NPO Mash が関係する技術や分野に強い関心を抱いていたことが想像できる。

ミサイルの専門家は、北朝鮮がジルコンに関する情報を入手しても、すぐにジルコンを生産できるようになるとは限らないとの見解を示している。一方で、ミサイル燃料関連の製造プロセス等、同社の他の技術についても情報を得ようとした可能性についても指摘している。なお、NPO Mash へのハッキング後、北朝鮮は弾道ミサイル開発に関していくつかの進展を公表したが、ハッキングとの関連性は不明である[11]。

2.4. ロシア国防大臣の北朝鮮訪問

2023 年 7 月 26 日、ロシアのセルゲイ・ショイグ国防大臣は、朝鮮戦争休戦 70 年の記念行事に出席するため北朝鮮を訪問した。北朝鮮のラジオ局はショイグ氏が朝鮮人民軍を「最強」と称賛したと報道。ショイグ氏は、翌日の軍事パレードでは金正恩総書記の隣で閲兵台にも登壇したが、これは極めて異例のことであった[15]。

[14] 出典：SentinelLabs『Comrades in Arms? | North Korea Compromises Sanctioned Russian Missile Engineering Company』
https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/

[15] 出典：REUTERS『North Korea's Kim shows off banned missiles to Russian minister』
https://www.reuters.com/world/north-koreas-kim-jong-un-meets-russian-defence-minister-2023-07-27/

© NTT Security Holdings

ウクライナとの戦争が長引く中で武器の不足に直面しているロシアが、プライドを捨てて友好国に助けを求めるという行動に出たのが、今回の北朝鮮訪問であった可能性がある[16]。

図 4 - 訪問先の北朝鮮で兵器を視察するロシアのセルゲイ・ショイグ国防大臣と案内をする北朝鮮の金正恩総書記 [11]

なお、7 月 31 日にもロシア軍の VIP 専用機が平壌に留まっていることが確認され、その際にも武器取引の話をしたことが推測されている[17] 。このようにロシアが北朝鮮に接近する動きが目立つ中、前述の通り北朝鮮が NPO Mash へハッキングを行った可能性があることについてロイター通信が報道したのは、その 1 週間後のことであった。

また、9 月 13 日時点で、北朝鮮の金正恩総書記が会談のためロシアを訪問しており、ロシアのプーチン大統領と弾薬提供を含む軍事協力について協議するとみられている[18]。

2.5. まとめ

国民のほとんどがインターネットに接続できないような環境であるにも関わらず、北朝鮮は高い水準のサイバー攻撃能力を持っており、今回の件では、そのサイバー攻撃能力を用いて友好国すらハッキングの標的にすることが示された。

サイバー空間における北朝鮮のミサイル開発技術への貪欲な活動は周辺国の安全保障環境に大きな影響を与えている。

---

[16] 出典：NHK サタデーウオッチ 9『異例！国防相の北朝鮮訪問、つなぎとめたいアフリカ、外交活発化するロシアの狙いは』
https://www.nhk.jp/p/ts/7K78K8ZNJV/blog/bl/pZWdy5qgmE/bp/p2n9q1mPE6/

[17] 出典：Bloomberg『北朝鮮にロシア軍のＶＩＰ専用機－兵器取引との懸念強まる』
https://www.bloomberg.co.jp/news/articles/2023-08-07/RZ0DX2T1UM0W01

[18] 出典：朝日新聞 DIGITAL『金正恩氏とプーチン氏が会談見込みの宇宙基地　一体どんな場所？』
https://www.asahi.com/articles/ASR9D72LVR9DUHBI038.html

© NTT Security Holdings

3. SMS トラフィックポンピング詐欺

3.1. 概要

企業による SMS 送信は、顧客と個別に結びつく電話番号にメッセージを直接送れる為、マーケティングやアプリからの通知等に幅広く利用されている。だが、この SMS の送信に乗じて、電話代から多額の利益を得る詐欺を犯罪グループが行っていることが、最近注目されるようになった。**SMS トラフィックポンピング詐欺** [19]と呼ばれている。

3.2. SMS トラフィックポンピング詐欺の手法

【SMS トラフィックポンピング詐欺の仕組み】[19, 20]

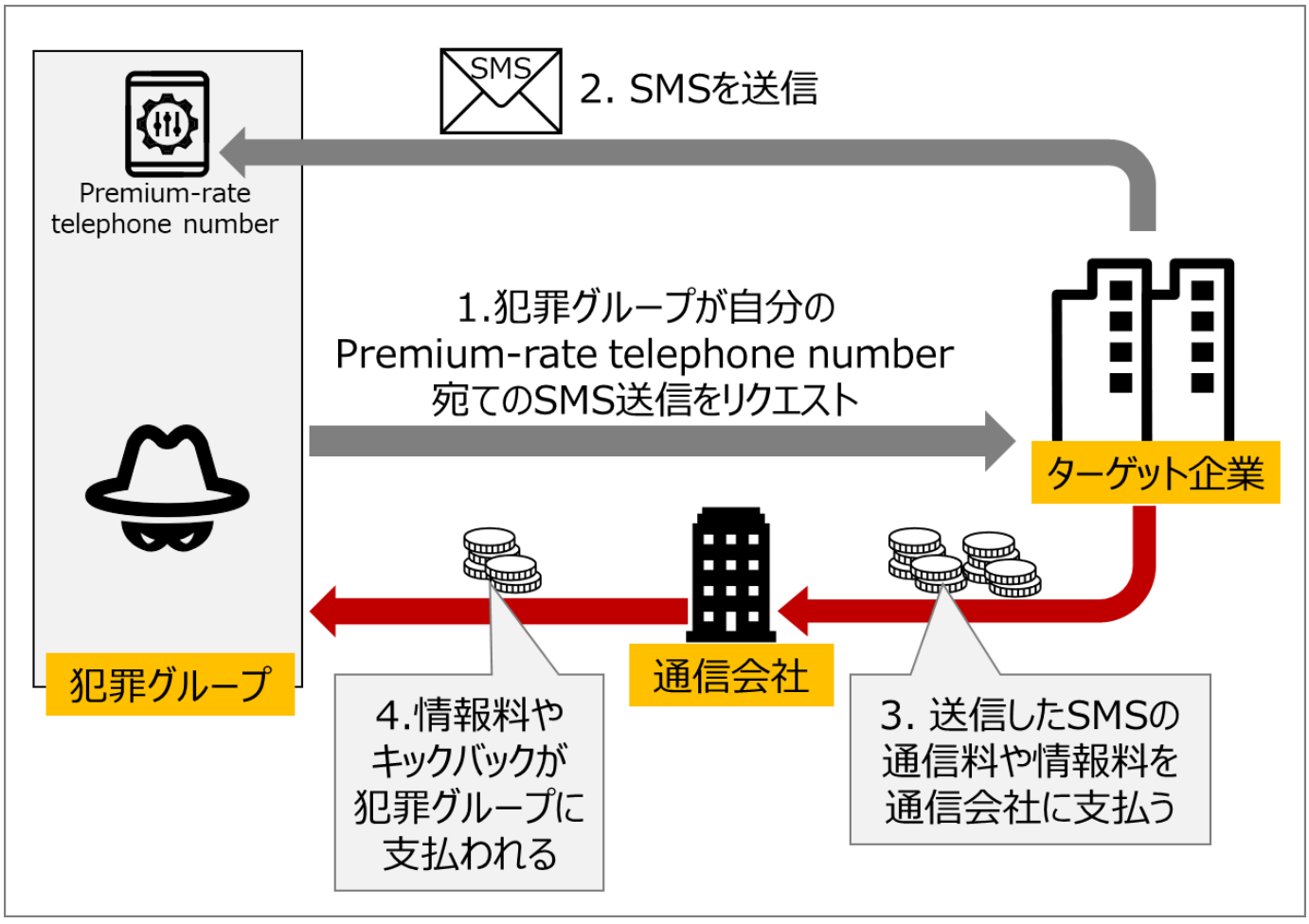

図 5 SMS トラフィックポンピング詐欺の仕組み

[19] 出典：Twilio『SMS Traffic Pumping Fraud』
https://support.twilio.com/hc/en-us/articles/8360406023067-SMS-Traffic-Pumping-Fraud

[20] 出典：kasada『SMS Fraud Takes A Toll: The Evolving Threat of SMS Pumping and Toll Fraud』
https://www.kasada.io/sms-fraud-evolving-sms-pumping-toll-fraud/

© NTT Security Holdings

米国等では、**「Premium-rate telephone number」**と呼ばれる、特別な電話番号を通信会社が提供するサービスがある。**この番号に電話を掛けたり、SMS を送信したりすると、情報料等により割り増しされた高額な電話代が請求される。**（※日本でかつて提供されていた、電話で有料の情報番組等を配信する「ダイヤル Q2」[21]に類似したサービス）

詐欺グループはまず、Premium-rate telephone number を通信会社から取得する。そして、ユーザーへのアプリからの通知等に SMS を使用している企業をターゲットに定める。詐欺グループはターゲット企業に対して、自分の Premium-rate telephone number 宛てに SMS を送るようリクエストを乱発する。リクエストに応じて SMS を送信したターゲット企業は、その対価として高額な電話代を通信会社に支払うことになる。（図 5）

SMS トラフィックポンピング詐欺では、通信会社に支払われた電話代の一部が犯罪グループに流れて収益となる。これは、犯罪グループが情報料支払いの仕組みを悪用して儲けるケース、もしくは通信料の増収を目論む通信会社が、犯罪グループとの結託等によりキックバック（謝礼金）を犯罪グループに支払っているケースの 2 種類があると考えられている。

【被害例】

この詐欺の典型例として、Web サービス等で提供されている SMS 認証を悪用する手口が挙げられる。被害の実例が Twitter（現・X）のサービス変更である。

Twitter はそれまで利用者であれば誰もが使えていた SMS 認証を、2023 年 3 月から有料サービス利用者のみに制限した。制限の導入にあたって Twitter のイーロン・マスク代表は、SMS トラフィックポンピング詐欺による認証リクエストの乱発で Twitter は大量の SMS を送信させられ、北米を除く国々で年間 6,000 万ドルの損失を被っていると主張した [22]。

3.3. 対策

SMS を送信している企業は、SMS トラフィックポンピング詐欺による多大な金銭的喪失の可能性を想定して、対策を講じておく必要がある。

まず、以下のような制限を導入することで、詐欺を狙った SMS 送信を予防する [19, 20]。

- サービス提供外の国への SMS 送信を禁止
- 送信にレート制限や遅延を設定し、頻繁な SMS 送信を抑制
- CAPTCHA 等でボットによる送信リクエストを抑制

また、SMS の送信状況を監視し、詐欺の疑いのある送信先を見つけて送信制限を実施する。

さらに、リクエストを受けて SMS 送信をするサービスの中でも SMS 認証には、中間者攻撃への耐性が低い等のセキュリティ上の問題が他にも多数ある。根本的な対策として、SMS に頼らない FIDO や OTP トークンといった多要素認証の採用を検討する。

「Premium-rate telephone number」の存在と SMS トラフィックポンピング詐欺による脅威について認識した上で対策をとることは、今後の SMS 送信の利用において必要なことと考えられる。

以上

[21] 出典：INTERNET Watch『「ダイヤル Q2」が 25 年の歴史に幕、2 月末にサービス終了』
https://internet.watch.impress.co.jp/docs/news/637881.html

[22] 出典：Commsrisk『Elon Musk Says Twitter Lost $60mn a Year Because 390 Telcos Used Bot Accounts to Pump A2P SMS』
https://commsrisk.com/elon-musk-says-twitter-lost-60mn-a-year-because-390-telcos-used-bot-accounts-to-pump-a2p-sms/

© 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