サイバーセキュリティレポート

2024.10

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

© NTT Security Holdings

目次

【1 ページサマリー】 2
1. 中国系ハッカーグループ Salt Typhoon が米国の大手 ISP を攻撃 3
1.1. 概要 3
1.2. Salt Typhoon の攻撃について 3
1.3. Typhoon ハッカーの名称について 4
1.4. 中国の関心とハッキング活動について 5
1.5. まとめ 5
2. フィッシング詐欺の今～どのように成功させようとするのか 6
2.1. 概要 6
2.2. フィッシングサイトにアクセスさせないための対策 6
2.3. 手の込んだフィッシングメールからの誘導の例 6
3. 加速するゼロデイ脆弱性の悪用 9
3.1. 概要 9
3.2. 統計情報の推移 9
3.3. 2024 年のリモートアクセス製品への攻撃 11
3.4. 中国によるゼロデイ脆弱性の収集から悪用まで 11
3.5. まとめ 12

© NTT Security Holdings

【1 ページサマリー】

当レポートでは 2024 年 10 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『中国系ハッカーグループ Salt Typhoon が米国の大手 ISP を攻撃』

- 中国系ハッカーグループの Salt Typhoon（別名「FamousSparrow」、「GhostEmperor」、「APT40」）が、8 か月以上にわたり米国のインターネットサービスプロバイダー（ISP）に侵入していたことを、The Wall Street Journal（WSJ）が 2024 年 9 月から 11 月の現在まで複数回にわたり報じている。
- Salt Typhoon は、米国政府の高官が使用する携帯電話をハッキングし、数千回分の通話記録やテキストメッセージを入手していた。また、米国の法執行機関が、犯罪や安全保障に関して合法的に捜査を行うために使う監視システムにも不正アクセスしていた可能性が指摘されている。
- 米国以外の国でも同様の活動が行われていることが懸念される。インフラ企業へのハッキングであるため官民合わせて対応を行う必要がある。

第 2 章『フィッシング詐欺の今～どのように成功させようとするのか』

- 被害が相次ぐフィッシング詐欺の対策として、迷惑メールフィルタリング等によりフィッシングサイト URL の検知が行われている。
- 検知によりフィッシングメールと判定されるのを回避するため、フィッシングサイトの URL をメールに直接記さない手法がしばしば用いられてきたが、最近は更に手の込んだものになっている。
- フィッシングメールからフィッシングサイトへの誘導として、QR コードや、URL の特殊な構文の使用、検知対象外の正規サイトを経由させるアクセスといった手法が用いられている。

第 3 章『加速するゼロデイ脆弱性の悪用』

- サイバーセキュリティ組織の Mandiant が公開した 2023 年に悪用された脆弱性に関する分析レポートから、ゼロデイ脆弱性の悪用の割合が増加しており、悪用開始までの期間が短縮されている傾向が判明した。
- 2024 年に入ってからも、国家支援型の攻撃グループを中心に、リモートアクセス製品のゼロデイ脆弱性を悪用した攻撃が多数見られている。
- 攻撃者が悪用する脆弱性の中で、ゼロデイ脆弱性は高い比率を占めており、ゼロデイ攻撃が行われる前提で、一つの機器が突破されても大きなインシデントにつながらない多層防御態勢を構築・維持することが求められている。

© NTT Security Holdings

1. 中国系ハッカーグループ Salt Typhoon が米国の大手 ISP を攻撃

1.1. 概要

中国系ハッカーグループの Salt Typhoon（ソルト・タイフーン［別名「FamousSparrow」、「GhostEmperor」、「APT40」］）が、8 か月以上にわたり米国のインターネットサービスプロバイダー（ISP）に侵入していたとして、The Wall Street Journal（WSJ）が 2024 年 9 月から 11 月の現在まで、複数回にわたり報じている。Salt Typhoon は米政府関係者らが使用する携帯電話をハッキングしたとされる他、米国の法執行機関が使用する監視システムにも不正アクセスしていた可能性が指摘されている。

Salt Typhoon は 2020 年から活動しており、スパイ活動とデータ窃取、特にネットワークトラフィックの傍受に重点を置いている。主な標的は北米や東南アジアである[1, 2, 3]。

1.2. Salt Typhoon の攻撃について

【米国の ISP への侵入】[1, 2, 3]

WSJ によると、Salt Typhoon は米国の大手 ISP に侵入し、膨大なインターネットトラフィックの収集を試みたとされる。被害に遭った ISP として、Verizon Communications、AT＆T、Lumen Technologies が挙げられている。Salt Typhoon はこれらの顧客である大多数の米国人の電話データにアクセスできる状態にあったようだが、実際に選ばれたターゲットは、数十人の政治家および国家安全保障に関係する人物に限定されていたとみられる。また、同グループは侵害した ISP を経由して、米国の法執行機関が犯罪や安全保障に関する調査のために使用する監視システムにも数か月にわたってアクセスした可能性があり、これは米国の重大な国家安全保障リスクに相当する。グループは ISP のトラフィック処理の大部分を担う Cisco ルーターを悪用した可能性もあり（Cisco はこれを否定）、捜査当局はその調査を進めている。

さらに、Salt Typhoon は一般的なインターネットトラフィックや、米国と緊密に情報を共有する他国の通信会社にもアクセスしていたとの情報もある。

---

[1] 出典：THE WALL STREET JOURNAL『China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack』
https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835

[2] 出典：THE WALL STREET JOURNAL『U.S. Wiretap Systems Targeted in China-Linked Hack』
https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b

[3] 出典：THE WALL STREET JOURNAL『China Hack Enabled Vast Spying on U.S. Officials, Likely Ensnaring Thousands of Contacts』
https://www.wsj.com/politics/national-security/china-hack-enabled-vast-spying-on-u-s-officials-likely-ensnaring-thousands-of-contacts-1340ba4a

© NTT Security Holdings

【トランプ次期大統領もハッキングの標的に】[4, 5, 6]

Salt Typhoon は、安全保障を担当する米政府高官や政治家の携帯電話の回線に侵入し、数千回の通話記録やテキストメッセージの記録を入手していたこともわかっている。また、米大統領選を前に、トランプ次期大統領候補とバンス上院議員（次期副大統領候補）の携帯電話でのやり取りも盗聴していた。他にハッキングの標的となった電話所有者のリストには、民主党の次期大統領候補ハリス氏（現副大統領）の選挙スタッフやバイデン政権当局者、米議会有力者などが含まれていた。

本件については捜査が継続中であるが、米国の安全保障当局は、中国のハッキングの目的は選挙の妨害ではなく、情報収集であると見ている。そして例えば、中国が AI を駆使して盗んだデータを分析し、何百万人ものアメリカ人の精巧なソーシャルマップ（人物や組織の社会的な関連やつながりを視覚的に示すツール）の作成を目指しているのではないか、といった懸念が生じている。

1.3. Typhoon ハッカーの名称について

マイクロソフトは、世界中のサイバー攻撃に対する調査を支援しており、脅威アクターには気象に関する名前を付けて分類している。「Typhoon（台風）」という単語を含むグループ名（およびその活動）は中国政府が背後にあるとされる一部のキャンペーンを意味する。ちなみに他の国家の場合、イランには「Sandstorm」（砂嵐）、ロシアには「Blizzard」（吹雪）というニックネームを割り当てている[7]。

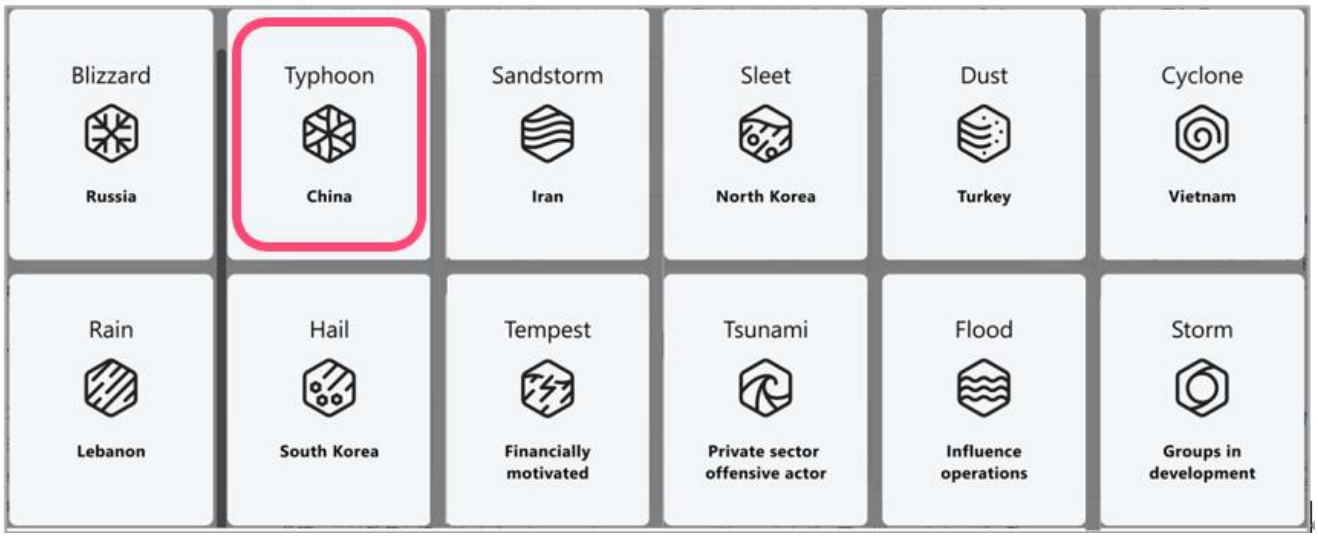

図 1 マイクロソフトによる脅威アクターの名称の分類[8]

---

[4] 出典：THE WALL STREET JOURNAL『U.S. Officials Race to Understand Severity of China's Salt Typhoon Hacks』
https://www.wsj.com/politics/national-security/u-s-officials-race-to-understand-severity-of-chinas-salt-typhoon-hacks-6e7c3951

[5] 出典：THE WALL STREET JOURNAL『China Hack Enabled Vast Spying on U.S. Officials, Likely Ensnaring Thousands of Contacts』
https://www.wsj.com/politics/national-security/china-hack-enabled-vast-spying-on-u-s-officials-likely-ensnaring-thousands-of-contacts-1340ba4a

[6] 出典：読売新聞『中国系ハッカー集団「ソルト・タイフーン」、米安全保障担当の高官らの携帯電話回線に侵入か』
https://www.yomiuri.co.jp/world/20241106-OYT1T50073/

[7] 出典：Microsoft『Microsoft が脅威アクターに名前を付けする方法』
https://learn.microsoft.com/ja-jp/defender-xdr/microsoft-threat-actor-naming

[8] 出典：Microsoft『Microsoft が脅威アクターに名前を付けする方法』
https://learn.microsoft.com/ja-jp/defender-xdr/microsoft-threat-actor-naming

© NTT Security Holdings

1.4. 中国の関心とハッキング活動について

中国は以前から、産業や軍事に関する情報窃取を行っているが、現在は特に、米国の重要インフラのシステムへの侵入に高い関心を持っている。有名な中国系ハッカーグループの Volt Typhoon は、その代表格とみられている。このグループは水処理システムや空港、ガスパイプラインなどの重要インフラのシステムに侵入後、LotL（Living Off The Land:侵入先に既に存在する機能を悪用する攻撃。新たなマルウェアをインストールしないため、見つかりにくい）と呼ばれるステルス技術を使いながらスパイ活動を行う。それは将来、台湾有事等が発生した場合、サイバー攻撃により社会的な混乱を引き起こすことで、米国が行う他国への支援活動を妨害することを意識していると思われる。Volt Typhoon については、今年 1 月、侵入の足掛かりとして脆弱な SOHO ルーター等をハッキングしていたことについて、米政府が対策を講じたことを発表していた [2]。なお、中国国家から支援を受けている Volt Typhoon が米国の重要インフラにサイバー攻撃を仕掛けているという米国の主張に対し、これを中国政府は「虚偽情報」であると否定している[9]。今回の Salt Typhoon は、このような中国が関連する一連のハッキング活動の最新のものと考えられている。

他にも、「BGP ハイジャック」と呼ばれる手法でのハッキングについても、中国は疑われている。これは、ISP 間の接続でよく使用される BGP（Border Gateway Protocol）の技術を悪用し、インターネット上のトラフィックが中国を経由するよう、通信経路を不正に変更して情報を窃取する攻撃である。米政府は、中国の国営電気通信企業である中国電信（チャイナ・テレコム）がこれまでに少なくとも 6 回にわたって米国のインターネットトラフィックを中国が受信できるように経路変更していたことを警戒し、今年 9 月、ネットワークでのデータ通信経路に関するセキュリティを高めるよう連邦機関に要請を出している[10]。

1.5. まとめ

中国が米国の国家安全保障に関わる情報や要人の通話データ等の入手に成功していたというニュースは衝撃的である。米国以外の国でも同様の活動が行われていることが懸念される。インフラ企業へのハッキングであるため官民合わせて対応を行う必要がある。

[9] 出典：中国国際放送局『中国のサイバーセキュリティ機関 米政府機関によるボルト・タイフーンの虚偽情報を全面的に解析』
https://japanese.cri.cn/2024/07/08/ARTIFofPCj4BA1b8LeYESGQz240708.shtml

[10] 出典：Reuters『White House asks agencies to step up internet routing security efforts』
https://www.reuters.com/world/us/white-house-asks-agencies-step-up-internet-routing-security-efforts-2024-09-03/

© NTT Security Holdings

2. フィッシング詐欺の今～どのように成功させようとするのか

2.1. 概要

フィッシング詐欺の被害が止まらない。金融機関やショッピングサイト等を騙ったメールや SMS によって誘導されたフィッシングサイトで、銀行口座やクレジットカード口座情報を詐取される被害が続いている。フィッシング攻撃者はこれまでも、本物のメールやサイトをコピーする等の手法で被害者を欺いてきたが、さらに最近は、検知をかいくぐることを狙った、手の込んだ手法のフィッシングが目立っている。

2.2. フィッシングサイトにアクセスさせないための対策

フィッシングメール対策として、メールや SMS を受信した際の迷惑メールフィルタリングが挙げられる[11]。フィルタリングでは、送信元の判定等に加え、文中にある URL がフィッシングサイトであるかの検知が行われている[12]。検知の処理では主に、フィッシングサイトの URL を収集したブロックリストが用いられている。ブロックリストには、ユーザーからの報告や自動化されたスキャンツール等によって収集・判定されたフィッシングサイトの URL が集められている[13]。

さらに、ブロックリスト等のフィッシングサイトの検知情報を基にして、フィッシングサイトをホスティングしているサーバー管理者に対し、サイト停止を依頼するテイクダウン活動が、公的機関やセキュリティ会社等により行われている[14]。

しかし、これらの取り組みによって無効化されても、新しいフィッシングサイトが次から次へと立ち上げられており、イタチごっこの様相を呈している。

2.3. 手の込んだフィッシングメールからの誘導の例

フィッシング攻撃者はしばしば、フィッシングサイトの URL をメール文にそのまま記載しない手法を用いる。これは上記のような検知からフィッシングサイトを隠すことを狙ったものである。特に最近は、以下のように手の込んだフィッシング手法が確認されている。

---

[11] 出典：フィッシング対策協議会『利用者向け フィッシング詐欺対策ガイドライン 2024 年度版』
https://www.antiphishing.jp/report/consumer_antiphishing_guideline_2024.pdf

[12] 出典：迷惑メール対策推進協議会『迷惑メール白書 2022-2024』
https://www.dekyo.or.jp/soudan/data/anti_spam/whitepaper/2022-2024/wp2022-2024.pdf

[13] 出典：ASCII.jp『電子メールのセキュリティ技術 その 1 不正なメールサーバーを「RBL」で排除しよう』
https://ascii.jp/elem/000/000/689/689619/

[14] 出典：フィッシング対策協議会『フィッシング対策ガイドライン 2024 年度版』
https://www.antiphishing.jp/report/antiphishing_guideline_2024.pdf

© NTT Security Holdings

【QR コードから誘導する「クイッシング」】

本文中に URL が記されておらず、代わりにアクセス先として QR コードを読み取りアクセスすることを促すフィッシングメールが確認されている（図 2）[15]。指示通りにアクセスすると、フィッシングサイトが表示される。

このような QR コードを使用したフィッシングは“quishing”（クイッシング）と呼ばれている[16]。メールフィルタリングによる URL 文字列のチェックを回避するため、画像でアクセス先を表示するクイッシングを用いるようになったと考えられる。

2023 年に、Microsoft 社のサービスの認証確認メールに偽装したクイッシングが、英語圏で急増した[17]。金融機関や宅配業者に偽装した日本語のフィッシングメールでもクイッシングが盛んになっており、8 月にはフィッシング対策協議会が注意喚起を発表した[18]。

図 2 QR コードが記載された フィッシングメールの例 （フィッシング対策協議会の注意喚起より引用）

【Basic 認証の URL 構文の利用】

ブラウザー等での簡易な認証の仕組みとして Basic 認証がある。Basic 認証では自動的にログインできるよう、予め URL に ID とパスワードの文字列を埋め込んでおくことができる。近年は目にすることがほとんど無くなった古い構文である。

この構文を応用した手法が、今年の 8 月頃から日本語のフィッシングメールで数多く確認されている[19]。メールには、ID とパスワードの入る部分に、正規サイトのドメイン名が入った URL が記載されている（図 3）。実際には、アクセス先のサイトには Basic 認証が無く、ID とパスワードの部分は不要であり、正規サイトのドメイン名はアクセスに関係ないノイズ情報となっている。この手法は、メール受信者の目視確認や検知をかく乱し、正規サイトの URL と誤認させることを狙ったもの[20]と考えられる。

---

[15] 出典：フィッシング対策協議会『ニュース | 緊急情報 | QR コードから誘導するフィッシング（2024/08/28)』 https://www.antiphishing.jp/news/alert/qr_20240828.html

[16] 出典：Sophos『From QR to compromise: The growing “quishing” threat』 https://news.sophos.com/en-us/2024/10/16/quishing/

[17] 出典：Microsoft Security Blog『How Microsoft Defender for Office 365 innovated to address QR code phishing attacks』 https://www.microsoft.com/en-us/security/blog/2024/11/04/how-microsoft-defender-for-office-365-innovated-to-address-qr-code-phishing-attacks/

[18] 出典：フィッシング対策協議会『ニュース | 緊急情報 | QR コードから誘導するフィッシング（2024/08/28)』 https://www.antiphishing.jp/news/alert/qr_20240828.html

[19] 出典：インプレス 窓の杜『こんなの絶対騙される……古い URL 形式を使った巧妙な詐欺リンクの偽装方法が話題に-やじうまの杜』 https://forest.watch.impress.co.jp/docs/serial/yajiuma/1620057.html

[20] 出典：A-p0c Blog『Phishing with HTTP Basic Authentication Syntax』 https://apoc.work/2023/03/21/phishing-with-http-basic-authentication-syntax

© NTT Security Holdings

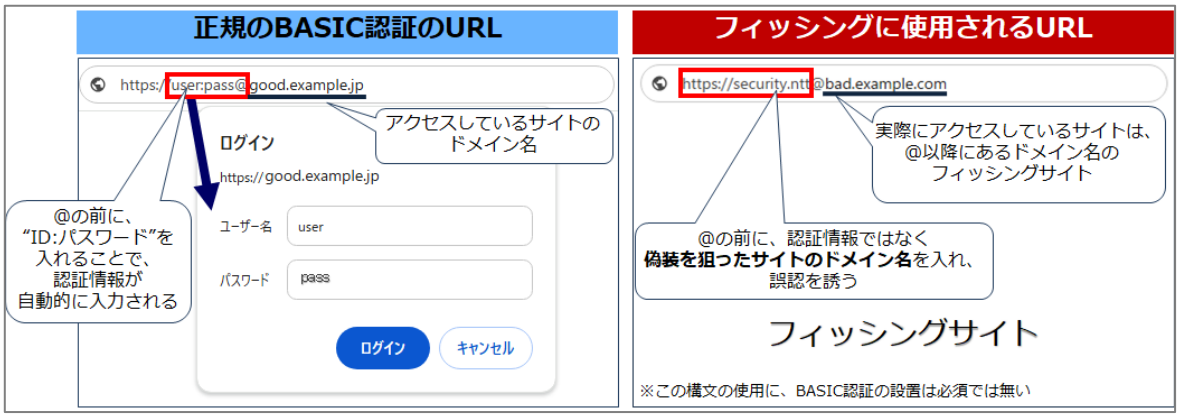

図 3 Basic 認証用の URL 構文を利用したカモフラージュ

【Google 翻訳の利用】

Google 翻訳は、翻訳したいページの URL を指定するとページをまるごと取りこんで翻訳する、ウェブサイト翻訳機能を提供している。この機能を利用したフィッシング攻撃が確認されている。

フィッシング攻撃者はまず、フィッシングサイトを作成する。加えて、アクセスするとフィッシングサイトへと転送するリダイレクト専用のサイトも作成する。そしてフィッシングメールに、アクセスすると Google 翻訳がリダイレクトサイトを翻訳する URL を記載する。これにより、アクセスの流れにおいては Google 翻訳のサイトを経由するのみでフィッシングサイトに誘導することが出来る（図 4）。

この手法は、正規サイトである Google 翻訳は検知されにくいこと、また、リダイレクトサイトを Google 翻訳に読み込ませることで検知から秘匿し、テイクダウン等を困難にすること等が狙いと考えられる。日本語のフィッシングメールへの使用は 2022 年 4 月頃には知られており[21]、今年の 9 月頃から使用がさらに盛んになっている。

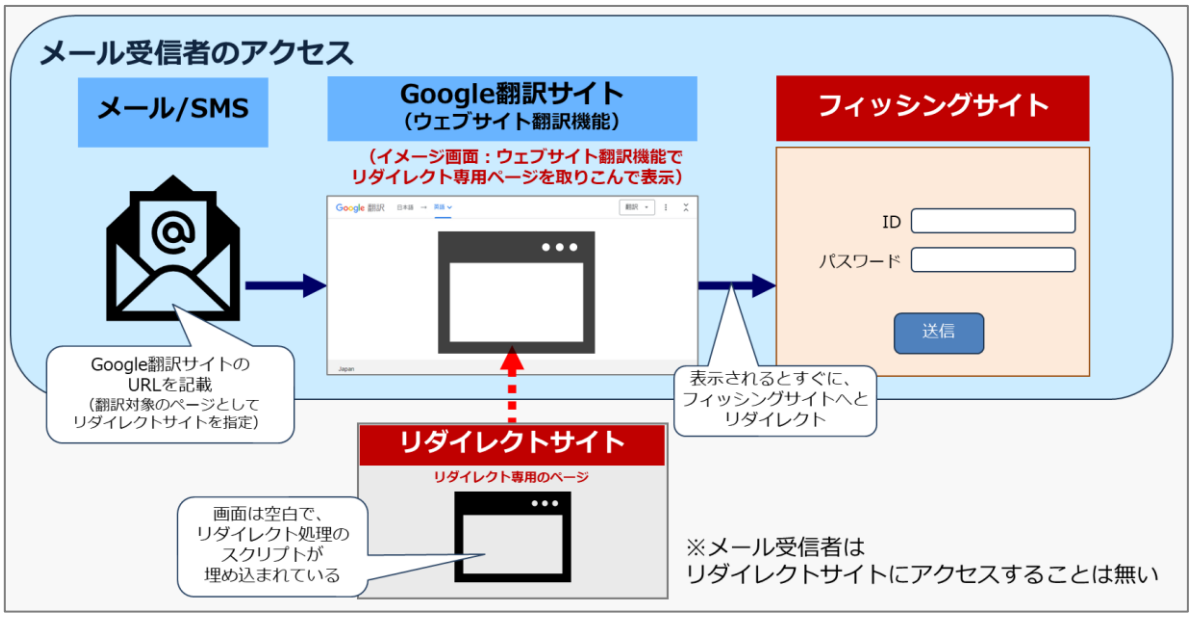

図 4 Google 翻訳を利用したフィッシングのフロー

[21] 出典：フィッシング対策協議会『ニュース | 緊急情報 | au をかたるフィッシング（2022/04/12)』
https://www.antiphishing.jp/news/alert/au_20220412.html

© NTT Security Holdings

3. 加速するゼロデイ脆弱性の悪用

3.1. 概要

10 月 16 日、Google Cloud のサイバーセキュリティ組織である Mandiant が、2023 年に悪用された脆弱性に関する分析レポートを公開した。ゼロデイ攻撃（脆弱性の公開や、脆弱性を修正するパッチの提供の前に実行される攻撃）が増えていると言われているが、このレポートはそれを客観的に示すことになった。本稿ではレポートの概要を紹介するとともにその背景について述べる。

3.2. 統計情報の推移

Google Mandiant の分析レポート「How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends」によると、2023 年に悪用された脆弱性について、以下の 2 つの特徴が明らかになっている[22]。

- 悪用が観測された脆弱性に占めるゼロデイ脆弱性（公開されていない／修正プログラムが提供されていない脆弱性）の割合は、2022 年以前は 60%前半で推移していたが、2023 年は 70%に上昇した。
- 脆弱性が公開されてから悪用が開始されるまでの期間は平均で 5 日間であり、これは前年の統計の 6 分の 1 以下であった。

【悪用された N デイ脆弱性に対するゼロデイ脆弱性の割合増加】

悪用が観測された N デイ脆弱性(修正パッチが公開されている脆弱性)とゼロデイ脆弱性の比率は、図 5 のように推移している。なお、「N デイ」（N 日）とは、修正パッチが公開されてからパッチ適用までに経過する期間を意味する。

2022 年以前は悪用が観測された脆弱性全体に占めるゼロデイ脆弱性の比率は 60%前半で推移していたが、2023 年は 70%に上昇した。この上昇は、N デイ脆弱性の悪用件数の変化によるものではない。ゼロデイ脆弱性の悪用件数は年々増加傾向[23]にあり、図 6 に示した通り、2022 年に一旦減少した[24]ものの、2023 年は 97 件となり、前年に比べて 76%の増加が見られた[25]。

97 件の内 61 件は、モバイル機器、OS、ブラウザーのようなエンドユーザー向け製品の脆弱性だった。特徴的なのは、複数の製品に共通で使用されるサードパーティ製のコンポーネント・ライブラリの脆弱性の増加である。1 つの脆弱性への攻撃手法を開発することで複数の製品をターゲットにできるため、攻撃者にとっては効率がよく、このような脆弱性は積極的に利用されていると考えられる。

残りの 36 件は、エンタープライズ向けの製品の脆弱性だった。この中には、セキュリティ製品・機器が多く含まれる。ネットワー

---

[22] 出典：Google Cloud Blog『How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends』https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023

[23] 出典：Google Cloud Blog『Zero Tolerance: More Zero-Days Exploited in 2021 Than Ever Before』https://cloud.google.com/blog/topics/threat-intelligence/zero-days-exploited-2021

[24] 出典：Google Cloud Blog『Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace』https://cloud.google.com/blog/topics/threat-intelligence/zero-days-exploited-2022

[25] 出典：Google『We're All in this Together: A Year in Review of Zero-Days Exploited In-the-Wild in 2023』https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf

© NTT Security Holdings

ク境界（組織の内部ネットワークと外部のネットワークとの境界）で稼働するそのような製品・機器への攻撃に成功すると、これをターゲット組織への初期侵入経路として利用できるため、攻撃者にとっては優先的な攻撃対象となっていると見られる。

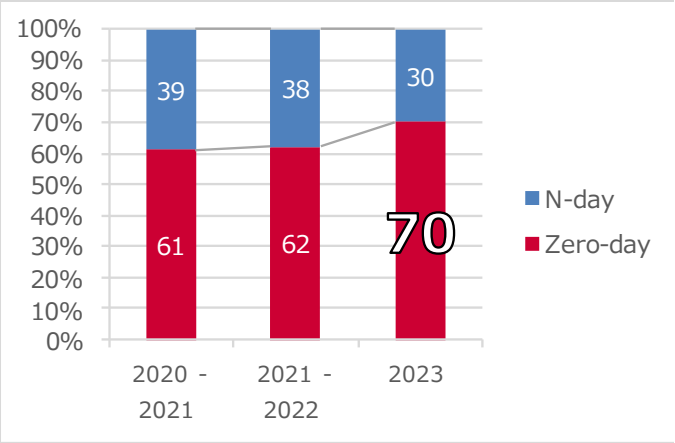

図 5 悪用された脆弱性に占めるゼロデイ・N デイの比率
(数値は Mandiant のレポート [22] より引用)

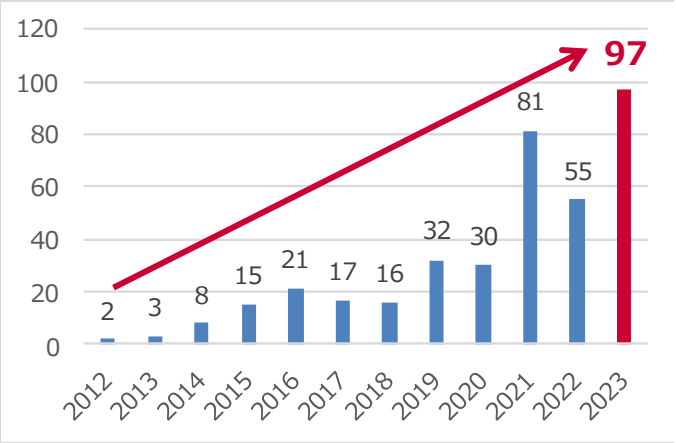

図 6 ゼロデイ脆弱性が悪用された件数の推移
(数値は Mandiant のレポート [22, 23, 24] より引用)

【脆弱性公開から悪用開始までの期間の短縮】

脆弱性が公開されてから悪用が開始されるまでの期間は、年々短縮している（図 7)。

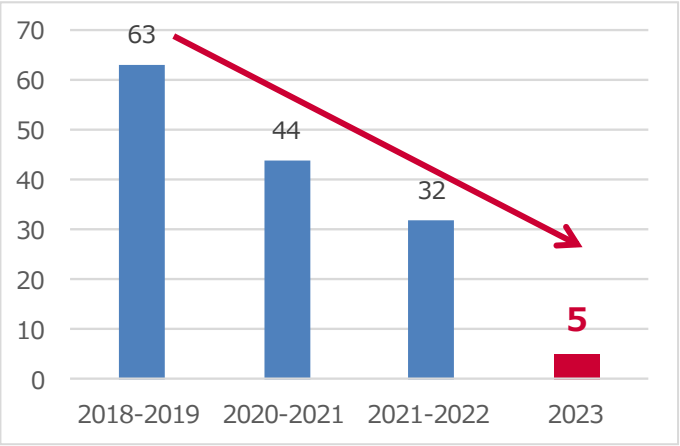

図 7 脆弱性の公開から悪用開始までの日数
(数値は Mandiant のレポート [22] より引用)

2018~2019 年には悪用開始まで平均 63 日かかっていたが、2023 年には平均 5 日となった。前年の平均 32 日と比較しても、6 分の 1 以下に短縮している。防御側の検出能力向上やパッチ適用の迅速化に対抗するために、攻撃者はそれを上回る早さで脆弱性の悪用を開始している。

この大幅な期間短縮は、2022 年後半から爆発的に普及した生成 AI の登場と時期を同じくしている。攻撃者は生成 AI

© NTT Security Holdings

を活用することで、ゼロデイ脆弱性の発見から攻撃コードの生成までを効率的に行い[26]、攻撃開始までの期間を短縮していると考えられる。

3.3. 2024 年のリモートアクセス製品への攻撃

2024 年に入ってからも、引き続きゼロデイ脆弱性の悪用は続いており、特に、直接の攻撃経路となりうる VPN などリモートアクセス製品の脆弱性は攻撃者にとって格好の対象となっている。

図 8 は、2024 年 1 月から 10 月までに発生したリモートアクセス製品への攻撃をまとめたもので、黄枠部分は、ゼロデイ攻撃で使用された脆弱性である。様々なベンダーのリモートアクセス製品が攻撃対象となっており、多くは国家支援型の攻撃グループによるものであることが判明している。

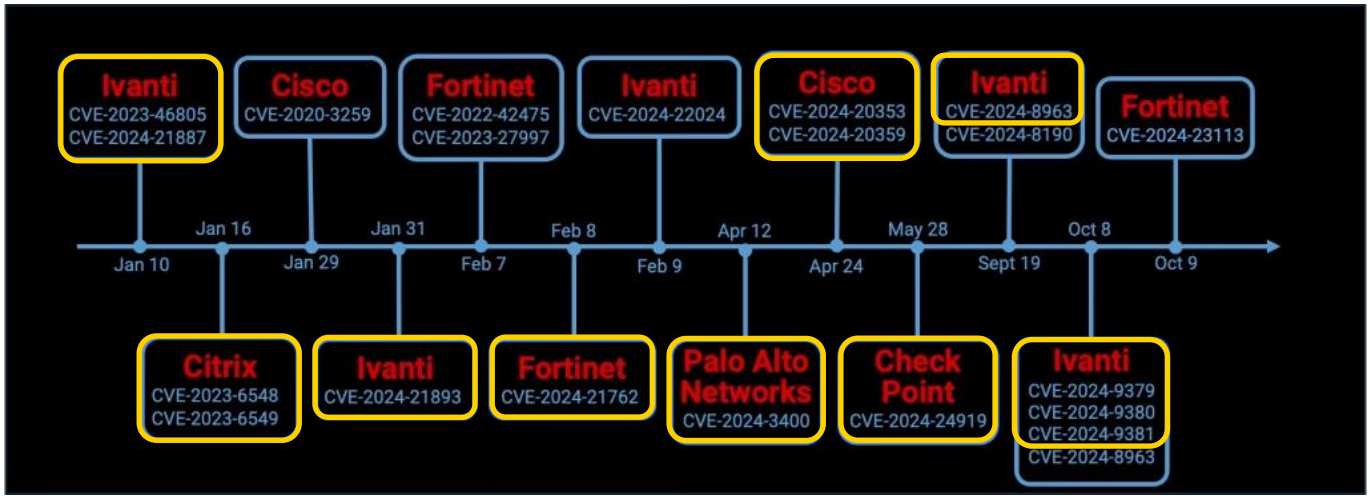

図 8 2024 年 1 月~10 月のリモートアクセス製品の脆弱性悪用のタイムライン（黄枠は当社加工）[27]

なお、図 8 の脆弱性のうち、Ivanti の CVE-2024-22024 と CVE-2024-9381 を除く全てが、CISA の KEV（既知の悪用された脆弱性カタログ）に掲載されている。

3.4. 中国によるゼロデイ脆弱性の収集から悪用まで

国家支援型の攻撃グループによる脆弱性の悪用は後を絶たない。その中でも、中国の国家支援型の攻撃グループのゼロデイ脆弱性の悪用件数は 2023 年には 12 件となっており、他国の国家支援型の攻撃グループによるゼロデイ脆弱性の悪用件数の合計よりも高い値となっている [25]。

中国は国家の取り組みとして、中国国内で大規模なハッキングコンテストを複数開催し、バグバウンティプログラム(バグ・脆弱性の発見者に報酬を支払う制度)も整備することで[28]、自国内でサイバーセキュリティ分野の優秀な人材を育成し、採用する

[26] 出典：Barracuda blog『5 Ways cybercriminals are using AI: Malware generation』
https://blog.barracuda.com/2024/04/16/5-ways-cybercriminals-are-using-ai--malware-generation

[27] 出典：HACKMAGEDDON『CVEs Targeting Remote Access Technologies』
https://www.hackmageddon.com/2024/04/22/cves-targeting-remote-access-technologies/

[28] 出典：Atlantic Council『Capture the (red) flag: An inside look into China's hacking contest ecosystem』
https://www.atlanticcouncil.org/in-depth-research-reports/report/capture-the-red-flag-an-inside-look-into-chinas-hacking-contest-ecosystem/

© NTT Security Holdings

エコシステムを構築している。育成した優秀な人材の活用先の 1 つとして、教育機関を中心とした研究コミュニティが存在し、脆弱性についても研究している。

研究コミュニティによる脆弱性の研究結果は、2021 年 9 月に施行された「ネットワーク製品セキュリティ脆弱性管理規定」(网络产品安全漏洞管理规定 [Regulations on the Management of Network Product Security Vulnerabilities])によって公表を規制されることがある。規制された脆弱性情報は、セキュリティベンダーだけでなく、中国政府からのサイバー攻撃を請け負う組織にも共有されていると考えられている[29]。実際、中国独自の脆弱性データベース CNVD は、近年、新規掲載数の減少が見られ、脅威度の高い脆弱性は遅れて掲載されることがある。そして、その中には、中国の国家支援型の攻撃グループに悪用されたものも含まれていた[30]。

3.5. まとめ

攻撃者はゼロデイ脆弱性を効率的に見つける手段や体制を整えており、今後悪用される脆弱性の中でも、引き続きゼロデイ脆弱性は高い比率を占める可能性が高い。ゼロデイ攻撃が行われる前提で、一つの機器が突破されても大きなインシデントにつながらない多層防御態勢を構築・維持することが求められている。

以上

[29] 出典：Sophos News『Pacific Rim: Inside the Counter-Offensive—The TTPs Used to Neutralize China-Based Threats』https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/

[30] 出典：Atlantic Council『Sleight of hand: How China weaponizes software vulnerabilities』https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/

© 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

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

© NTT Security Holdings