サイバーセキュリティレポート

2024.12

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 2024 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『CISA が BOD 25-01「クラウドサービスの安全な実践の実装」を発令』

- 2024 年 12 月 18 日、米国政府機関の CISA は、BOD 25-01「クラウドサービスの安全な実践の実装」を発令し、政府機関のクラウドのセキュリティ体制強化を指示した。
- 近年、政府機関におけるクラウド利用で被害が相次いでおり、その防止策として CISA はクラウド利用におけるセキュリティ対策の枠組みである SCuBA を進めてきた。今回の指令は、各政府機関が SCuBA を確実に実施するよう発令されたものである。
- BOD25-01 が推進する SCuBA の取り組みは今後、民間においてもクラウドセキュリティの参考にされていくと考えられる。

第 2 章『中国系ハッカーが Visual Studio Code を悪用したサイバー攻撃を実施』

- 中国に関係しているとみられるハッカーが、南ヨーロッパの大手 IT サービスプロバイダーを対象としたサイバースパイ活動「Operation Digital Eye」を展開していたことが明らかになった。
- このキャンペーンでは、Microsoft Visual Studio Code の機能を悪用して、怪しいトラフィックを正当なものに見せ、検出回避を狙っていた。このような正規のアプリケーションを悪用した攻撃を検出するための堅牢なメカニズムの開発は、今後、さらに重要な課題となると考えられる。
- サイバー諜報範囲を南ヨーロッパにまで広げている事から、中国は「一帯一路」構想の対象地域での経済的な優位性や影響力を確保しようとしているとみられる。

第 3 章『年末より相次ぐ日本へのサイバー攻撃』

- 2024 年末から年始にかけて、JAL、三菱 UFJ 銀行、りそな銀行、みずほ銀行、NTT ドコモなどにサイバー攻撃が相次ぎ、サービスに影響が出た。
- これらは関連性のある一連の攻撃キャンペーンであると考えられるが、現在までに攻撃者は特定されていない。
- 動機や実行力の観点から、今回のサイバー攻撃者の候補としてはロシアが考えられる。他にはこのタイミングでこのような攻撃を実行する有力な候補は見つからなかった。

1. CISA が BOD 25-01「クラウドサービスの安全な実践の実装」を発令

1.1. 概要

2024 年 12 月 18 日、米国政府のサイバーセキュリティを担当する CISA（サイバーセキュリティおよびインフラストラクチャセキュリティ庁）は、BOD 25-01「クラウドサービスの安全な実践の実装」（Implementing Secure Practices for Cloud Services）を発令した（図 1）[1]。

この指令で CISA は、政府機関（連邦文民行政部門（FCEB））に対し、CISA が推進するクラウド環境のセキュリティ対策である SCuBA（Secure Cloud Business Applications）を実施することを義務付けた。

図 1　CISA による BOD 25-01 発令

1.2. CISA の BOD 25-01 発令までの背景

【米国政府のクラウドを狙ったサイバー攻撃の被害】

近年、米国の政府機関では、クラウドへのサイバー攻撃による重大な被害が発生している。2020 年には、SolarWinds 社のクラウドサービス「Orion」にマルウェアが仕込まれ、約 18,000 の組織が影響を受けたことが判明した。攻撃者は Orion のアップデートに悪意のあるコードを埋め込むことで、政府機関や企業のネットワークに侵入し、機密情報を窃取していた。また、2023 年には中国の APT「Storm-0558」がアメリカ政府高官の電子メールを閲覧していたことが判明した。攻撃者は Windows の欠陥を利用して Microsoft の署名キーを窃取することにより、Exchange Online や Azure Active Directory のアカウントに不正アクセスを行っていた。

[1] 出典：CISA『BOD 25-01: Implementing Secure Practices for Cloud Services』
https://www.cisa.gov/news-events/directives/bod-25-01-implementing-secure-practices-cloud-services

これらの重大なサイバーセキュリティインシデントの原因分析等から、クラウド環境におけるセキュリティ制御の不適切な構成が問題視されるようになった。

【SCuBA プロジェクト】

上記のようなクラウド環境へのセキュリティ脅威に対抗するため、CISA は、SCuBA（Secure Cloud Business Applications）プロジェクトを開始した。このプロジェクトは、政府機関のクラウドビジネスアプリケーション環境を保護するためのガイダンス、およびクラウドを保護する能力の提供を目指すものである。[2]

SCuBA で CISA は、まず、セキュリティ上望ましいクラウドの構成のベースラインを定義している。ベースラインは、クラウドサービス利用者に向けた具体的なセキュリティ構成の推奨事項である。ここでの推奨事項としては、多要素認証（MFA）の強制といったアクセス制御、暗号化と保護を確実に行うデータ保護、異常な活動を迅速に検出するシステムの監視とログ管理といった対策が定められている[3]。なお、各組織の独自の要件やリスク許容度に合わせてベースラインは調整が可能である。そしてベースラインに沿った、一貫性があり管理しやすいクラウドセキュリティ構成を提示している。併せて、セキュリティ構成がベースラインに達しているか自動で評価するためのツールも提供されている。

各社のクラウド製品に合わせたベースラインとクラウドセキュリティ構成、評価ツールのセットを CISA は提供している。2022 年 10 月には Microsoft 365 用の「ScubaGear」、2023 年 12 月には Google Workspace 用の「ScubaGoggles」の提供を開始した。なお、これら以外のクラウド製品用のセットについても、CISA は順次追加していく意向を示している。

1.3. BOD 25-01「クラウドサービスの安全な実践の実装」

【CISA の「BOD」とは】

CISA の BOD（Binding Operational Directives）は「拘束力のある運用指令」の略称で、米国の政府機関に対してサイバーセキュリティの強化を義務付ける指令である。特定のセキュリティ対策を実施するための具体的な手順や期限を定めており、政府機関がサイバー脅威に対して迅速かつ効果的に対応できるようにすることを目的としている。政府機関に対して拘束力があり、政府全体のサイバーセキュリティの水準を高めることが、BOD 発令には期待されている。

【BOD 25-01 の指令内容】

2024 年 12 月に発令された BOD 25-01 は、政府機関のクラウドサービスにおけるセキュリティ強化を目的とした BOD の指令である。この指令では政府機関に対し、広く使用されている代表的な SaaS 製品について、SCuBA プロジェクトを利用したセキュリティ対策の実施を求めている[4]。対策で使用するツールのダウンロード元、ならびに評価ツールでの確認結果の報告先として、CISA はサイバーセキュリティ管理と報告のためのプラットフォーム「CyberScope」を設置しており（図 2）[5]、担当者はこのサイトを活用することで BOD 25-01 に対応することができる。

---

[2] 出典：CyberScoop『CISA delivers new directive to agencies on securing cloud environments』 https://cyberscoop.com/cisa-scuba-baselines-cloud-security-directive/

[3] 出典：CISA『Secure Cloud Business Applications (SCuBA) Project』 https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

[4] 出典：CISA『BOD 25-01: Implementation Guidance for Implementing Secure Practices for Cloud Services』 https://www.cisa.gov/news-events/directives/bod-25-01-implementation-guidance-implementing-secure-practices-cloud-services

[5] 出典：CISA『BOD 25-01: Implementation Guidance for Implementing Secure Practices for Cloud Services』 https://www.cisa.gov/news-events/directives/bod-25-01-implementation-guidance-implementing-secure-practices-cloud-services

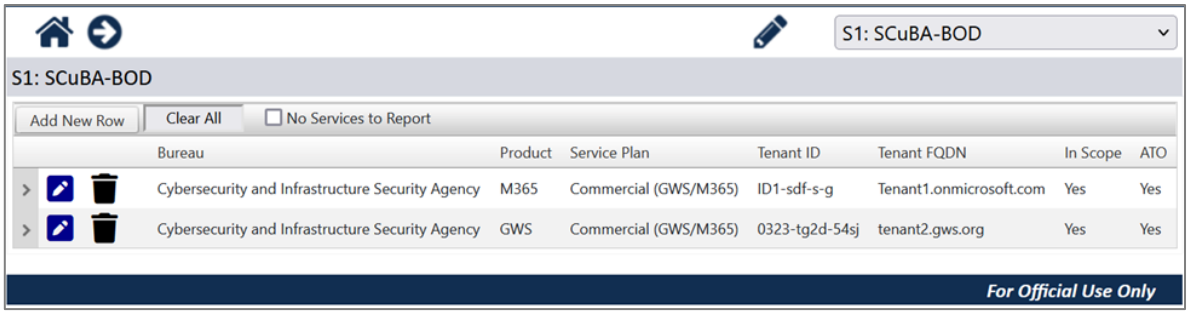

図 2　Cyber Scope のクラウド管理のユーザーインターフェース

まず求められる対応が、クラウド環境の特定である。自組織でクラウドサービスを使っているかを確認し、使用している場合はどのクラウドサービスを利用しているか特定することを求めている。

次に、セキュリティ評価ツールの導入である。ツールを使ってクラウド環境の安全性をチェックすることを求めている。SCuBA プロジェクトで開発されているセキュリティ評価ツールを、調査用端末にインストールし実行する事により、組織のクラウド環境が SCuBA の定めるベースラインを満たしているか確認することができる。例えば Microsoft 365 の使用を特定できた組織であれば、Microsoft 365 用の評価ツール「ScubaGear」を使用する[6]。このツールを使う事で、Microsoft 365 の構成設定を収集し、SCuBA セキュア構成ベースラインと比較したレポートを出力することができる（図 3）[7]。担当者はこのレポートを CISA に提出する。

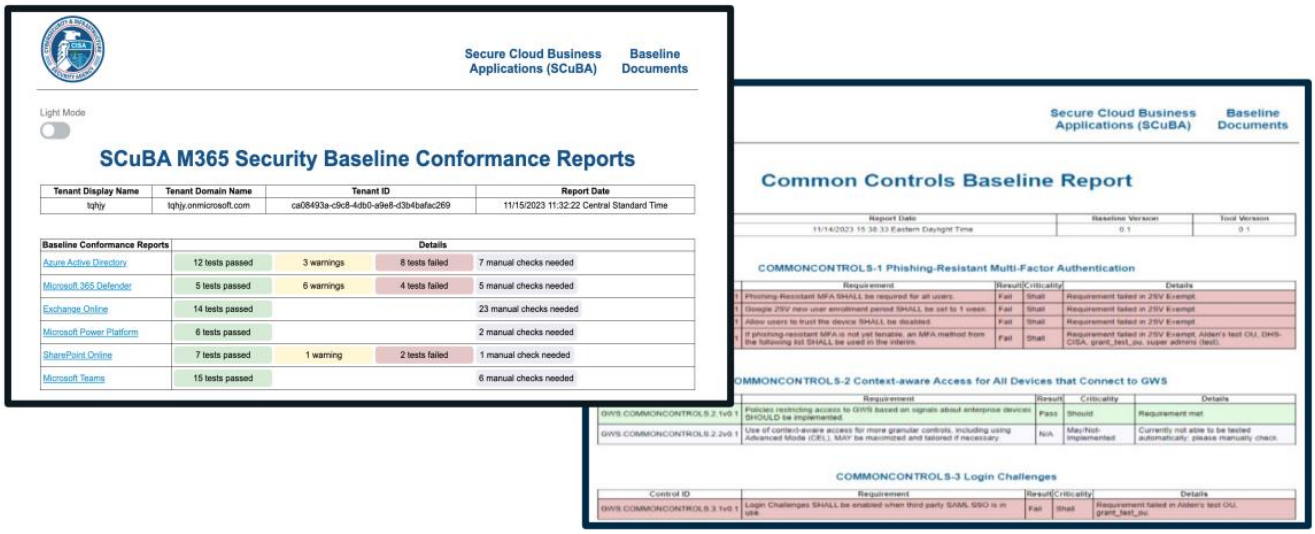

図 3　出力されるレポートのサンプル

そして、ベースラインとの比較後に求められるのが、セキュリティ基準の遵守である。CISA の定めるセキュリティ基準にクラウド環境を合わせるよう指示している。各組織には、SCuBA プロジェクトで定められている対策を実行し、ベースラインから逸脱している部分を修正することが求められている。

---

[6] 出典：GitHub『cisagov/ScubaGear』
https://github.com/cisagov/ScubaGear?tab=readme-ov-file

[7] 出典： NIST『CISA'S SCuBA OVERVIEW』
https://csrc.nist.gov/csrc/media/Presentations/2024/cisa-s-scuba-overview/5-CISAs_SCuBA_Overview-Mamika_Huynh.pdf

【BOD 25-01 のロードマップ】

CISA は指令の実行期限を定めている。クラウド環境の特定を 2025 年 2 月 21 日までに実施し、評価ツールを 2025 年 4 月 25 日までに導入することを求めている。なお今後、クラウド環境の特定は毎年第 1 四半期に実施し、評価ツールの結果については、ツールの自動レポート提出機能を有効にするか、手動での四半期ごとの報告が定められている。

さらに、必須となる全ての SCuBA のポリシー（BOD 25-01 発行時点で有効なポリシー）を、2025 年 6 月 20 日までに実装することも求めている。

【BOD 25-01 の発令の背景】

BOD 25-01 は特定の最近の脅威に焦点を当てて発令されたものではないが、APT やサイバー犯罪者の両方による最近の脅威活動に対応したものであると、CISA の担当者は説明している[8]。

1.4. まとめ

利便性に優れたクラウドサービスは、今や政府機関や企業にとって欠かせない存在である。一方で、攻撃者たちがクラウド環境をますます標的にするようになり、侵入するための戦術を進化させている。そのような中で浮き彫りになった、誤った設定や脆弱なセキュリティ制御による重大なリスクを CISA は指摘している。そして BOD 25-01 は、そのリスクを軽減させ、サイバー脅威に対する政府機関の回復力を高めるための重要なステップであると述べている[9]。

今回の指令で推進される SCuBA は、Microsoft 365 や Google Workspace といった具体的なクラウドサービスにおけるセキュリティ対策の実運用に対応しており、低レイヤーの話や一般論に留まる従来のクラウドのガイドラインとは一線を画したものと言える。クラウドに依存する状況でセキュリティ改善が必要であるのは、米国政府だけではなく他の多くの組織にとっても同様である。SCuBA のツールは GitHub で公開され民間でも利用可能な為、セキュリティ評価ツールでクラウドの構成設定を収集したり、ベースラインをセキュリティ監査の参考にしたりする等、今後、民間の組織でもクラウドセキュリティに活用されるようになっていくと考えられる。

[8] 出典：CyberScoop『CISA delivers new directive to agencies on securing cloud environments』 https://cyberscoop.com/cisa-scuba-baselines-cloud-security-directive/

[9] 出典：CISA『CISA Directs Federal Agencies to Secure Cloud Environments』 https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-secure-cloud-environments

2. 中国系ハッカーが Visual Studio Code を悪用したサイバー攻撃を実施

2.1. 概要

中国に関係しているとみられるハッカーが、南ヨーロッパの大手 IT サービスプロバイダーを対象としたサイバースパイ活動「Operation Digital Eye」を展開していたことが、2024 年 12 月 10 日に明らかとなった（図 4）。このキャンペーンでは、侵入先へのリモートアクセスを持続させるため、正規のアプリケーションである Visual Studio Code を悪用していた。自身の活動によって発生する不正なトラフィックを正規のアプリケーションによる動きに見せることで、検出を回避しようとしていたとみられる[10]。

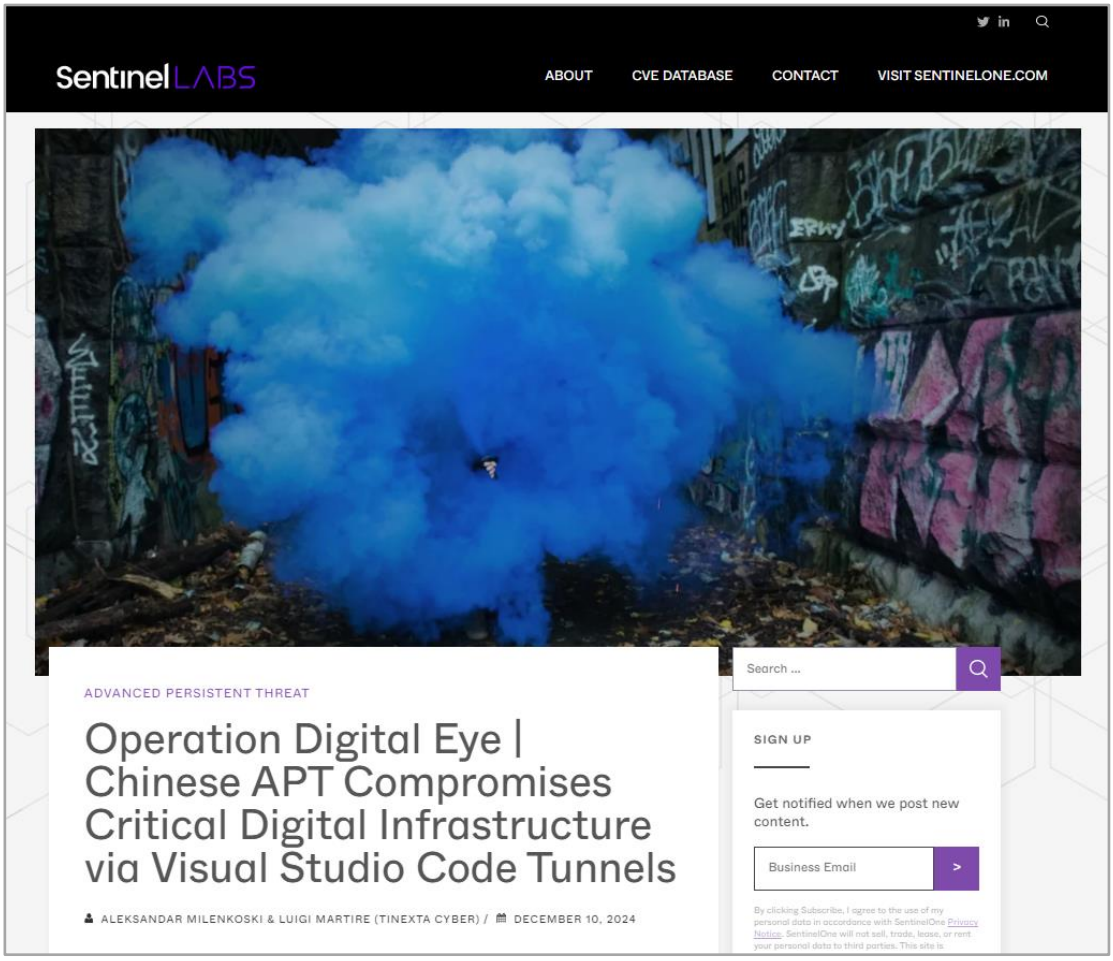

図 4 セキュリティ組織 SentinelLabs と Tinexta Cyber が発表した Operation Digital Eye についてのレポート[11]

[10] 出典：SentinelOne『Operation Digital Eye | Chinese APT Compromises Critical Digital Infrastructure via Visual Studio Code Tunnels』
https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

[11] 出典：SentinelOne『Operation Digital Eye | Chinese APT Compromises Critical Digital Infrastructure via Visual Studio Code Tunnels』
https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

2.2. Operation Digital Eye キャンペーンについて

【標的と攻撃者】[12]

「Operation Digital Eye」と名付けられた今回の攻撃作戦は、2024 年 6 月下旬から 7 月中旬にかけて、約 3 週間にわたって実施された。標的となったのは、南ヨーロッパの大手 IT サービスプロバイダー数社であり、これらは様々な業界の企業に向けて IT サービスの提供や管理を行っていた。

サイバー攻撃を実行したのは、中国国家の指示・支援を受けながら、標的に対して長期間にわたり高度で執拗な攻撃を行う APT（Advanced Persistent Threat）グループである可能性が高いことが、分析から推定されている。そして今回の作戦では、同グループが、標的組織に関係する下流のサプライチェーンをスパイしようとしていたと考えられている。

【一帯一路】

図 5 中国の一帯一路構想のイメージ図[13]

南ヨーロッパを攻撃対象地域としたのは、中国の戦略が背景にあるためと考えられる。中国の習近平国家主席は、シルクロード経済圏構想「一帯一路」（図 5）を 2013 年に打ち出している。これは中国を起点として、同国とその他の地域（ヨーロッパ・アジア・中東・アフリカ東岸）の間の物流ルートを、一帯（中央アジア経由の陸路）と一路（インド洋経由の海路）でつなぎ、中国政府の支援によるインフラ建設や、中国と対象地域の間での経済協力の促進を目指すものである。南ヨーロッ

[12] 出典：SentinelOne『Operation Digital Eye | Chinese APT Compromises Critical Digital Infrastructure via Visual Studio Code Tunnels』
https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

[13] 出典：Xinhuanet『Chronology of China's Belt and Road Initiative』
http://www.xinhuanet.com/english/2016-06/24/c_135464233.htm

パは、地中海の主要な港であるギリシャのピレウス港のような、インフラ投資先として価値のある拠点も擁しており、重要な産業へのアクセスを提供している。これらの地域へのサイバー攻撃には、戦略的な情報を収集し、「一帯一路」構想のように、中国が経済的な優位性を確保し、影響力を高めることを促進する狙いがあるのではないかと考えられる[14]。

【攻撃の実行】[15]

攻撃者はまず、標的のシステムからインターネットに接続されていた脆弱な Web サーバーに対して SQL インジェクション攻撃を実行することで、アプリケーションやデータベースサーバーへの侵入に成功した。続いて、それらのサーバー等へのアクセスを維持できるようにするため、PHP ベースの Web シェル（バックドア）をインストールし、認証情報収集、偵察等を行った。さらにネットワーク内の他のシステムにも侵害範囲を拡大させていった。アクセス維持には Visual Studio Code リモートトンネルも使われた。

【Visual Studio Code リモートトンネルの悪用】[16]

今回のキャンペーンでは、日常的なビジネスツールを利用するといった中国の APT グループとの類似性が確認された。中でも特徴的なのは、攻撃者が外部からサーバーに対しコマンドを出す際に、正規のアプリケーションである Visual Studio Code（VSCode）のリモートトンネル機能を利用している点である。Visual Studio Code は、Microsoft が開発した無料のテキストエディターで、リモートで開発作業ができる人気のツールである。また、リモートトンネルは、リモートにある PC などに対し、セキュリティで保護されたトンネルを介して接続する機能であるが、攻撃者がこれを悪用した場合、ネットワーク内にある PC などにより、リモートから任意のコマンドを実行したり、ファイルを操作したりする可能性がある。

セキュリティツールでの検出においては実行ファイルの署名がチェックされるが、Visual Studio Code リモートトンネルは Microsoft と Microsoft Azure（パブリッククラウドサービス）のネットワークシステムによって署名された実行ファイルを含んでいる。どちらも正当な署名とみなされ許可されるようになっているため、検出が難しい。外部との接続においても、GitHub アカウントや Azure サーバーでの認証を行うことから、不審な点が見えにくい。悪意ある活動を正当なものとして偽装することができる Visual Studio Code を利用したリモート接続は、ハッカーにとって魅力的なものとなっている。

なお今回の攻撃においては、データ抜き取りのフェーズに到達する前に不正活動が検出され、侵害は阻止された。

2.3. まとめ

今回のケースで、中国がサイバー諜報範囲を南ヨーロッパにまで広げていることが分かった。「一帯一路」構想を進める中国は、エリア内にある地域での経済的な優位性や影響力を確保しようとしているとみられる。

また、Operation Digital Eye キャンペーンでは、Microsoft Visual Studio Code の機能を悪用して、怪しいトラフィックを正当なものに見せ、検出回避を狙った。このような正規のアプリケーションを悪用した攻撃を検出するための、堅牢なメカニズムの開発は今後、さらに重要な課題となると考えられる。

---

[14] 出典：DARKREADING『Sprawling 'Operation Digital Eye' Attack Targets European IT Orgs』
https://www.darkreading.com/cyberattacks-data-breaches/operation-digital-eye-attack-targets-european-it-orgs

[15] 出典：SentinelOne『Operation Digital Eye | Chinese APT Compromises Critical Digital Infrastructure via Visual Studio Code Tunnels』
https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

[16] 出典：SentinelOne『Operation Digital Eye | Chinese APT Compromises Critical Digital Infrastructure via Visual Studio Code Tunnels』
https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

3. 年末より相次ぐ日本へのサイバー攻撃

3.1. 概要

2024 年末から年始にかけて、JAL、三菱 UFJ 銀行、りそな銀行、みずほ銀行、NTT ドコモ等において、外部から大量のデータが送付されたことによりサービスが中断するなどの被害が相次いだ。DDoS によるサイバー攻撃とみられているが、実行者についてはこれまでのところ特定されていない[17]。

図 6 JAL へのサイバー攻撃を伝える NHK ニュース[18]

3.2. サイバー攻撃について

12 月 26 日午前 7 時過ぎ、JAL でネットワーク障害が発生し、午後には復旧したが、欠航や運航遅延が発生した。また、同日午後、三菱 UFJ 銀行ではンターネットバンキングでログインできない不具合が発生した。29 日 21 時頃には、りそな銀行のアプリでつながりにくい状況が発生し、31 日にはみずほ銀行のオンラインバンキングが利用できない状況が発生した。年が明けて 1 月 2 日、NTT ドコモが提供するポータルサイト「goo」のサービス全般、スマートフォン決済アプリ「d 払い」の検索機能などにつながりにくい状況が発生した。これらの事象は外部から大量のデータを送りつけられたことにより発生しており、DDoS 攻撃を受けたとみられている。いずれも比較的短時間で復旧したが、各社の事業の重要なサービスに影響が及んだ。

[17] 出典：TECH+（テックプラス）『年末年始を狙う「DDoS 攻撃」、発生したシステム障害を時系列順に整理』
https://news.mynavi.jp/techplus/article/20250110-3104063/

[18] 出典：NHK『JAL にサイバー攻撃か 欠航や遅れも システム不具合は復旧』
https://www3.nhk.or.jp/news/html/20241226/k10014679271000.html

3.3. 攻撃者について

今回の攻撃はサイバー空間での戦争行為と捉えかねない、重要インフラへの連続した攻撃で、人々の生活にも大きな影響の出る恐れのある大胆不敵な犯行であることから、現在ある情報を元に攻撃者について分析を行う。

被害に遭ったのはいずれも著名な重要インフラ企業で、同様の被害が短い期間に相次いでおり、特定の IoT ボットが攻撃に使われた可能性を指摘する分析も出ていることから[19] 、関連性のある一連の攻撃キャンペーンであると考えられる。ただし、現時点までこの攻撃者を特定するような情報は報告されていない。攻撃者が犯行声明のようなことを実施しない限り、攻撃元を秘匿しやすい DDoS 攻撃においては、犯人を特定することは容易ではないため、以下は推測を交えていることを先にお断りする。

ここではサイバー攻撃者を大きく３つに分類して、それぞれにおいて本件に関わった攻撃者が存在する可能性について検討する。

【ハクティビスト】

ハッキングを通して自らの主張を広げようとするハクティビストの主要な攻撃手法は DDoS であり、今回の一連の攻撃と合致する。しかし、セキュリティ脅威動向を監視する当社の OSINT モニタリングチームで追跡している数百のハクティビストの中に、今回の攻撃に関する投稿を行っているアクターは見つかっていない。また、ハクティビストが今回の攻撃者だとすると世界中でニュースになるような大きな成果を上げているにもかかわらず、攻撃が成功した報告や自らの政治的主張を拡散しないことは考えにくい。このことから、ハクティビストが今回の攻撃に関与している可能性は極めて低いと考えられる。

【サイバー犯罪者】

この攻撃では情報窃取や身代金要求などは確認されていない。株価操作という狙いも考えられなくはないが、大金を儲けようとするとインサイダー取引の監視により検知されるので、正体が露見する可能性が高い。またそれ以上に、攻撃の一部は年末年始で株式市場が休業している期間に実行されている点が不自然である。攻撃者が攻撃の規模や労力に見合う収益を上げているとは考え難い。以上のことから金銭を目的としたサイバー攻撃を行う犯罪者は今回の攻撃には関与していないと考えられる。

逆に、今回の攻撃はサイバー犯罪者以外の嫌がらせや威圧を目的とした者の可能性が高いことが想起される。

【国家支援を受けたサイバー攻撃者】

国家の意思を実現するサイバー攻撃者の動向を読み解くには、支援者である国のサイバー戦略や外交政策などを分析する必要がある。

北朝鮮

高いサイバー攻撃能力を持つことが知られているが、近年は金銭目的の活動が多く、国連の報告書によると北朝鮮は外貨収入の半分をサイバー攻撃によって得ている。しかし、「サイバー犯罪者」の項で説明したとおり、金銭目的では今回の攻撃は説明がつかない。また、最近の北朝鮮と日本の外交関係は没交渉に近い状況が続いており、今回のサイバー攻撃に至るまでの期間に、何か特別な問題が日朝間に起きていたという情報は見当たらず、このタイミングで連続して日本に対して前例のない妨害活動を行う理由は見つからない。

[19] 出典：トレンドマイクロ『2024 年末からの DDoS 攻撃被害と関連性が疑われる IoT ボットネットの大規模な活動を観測』 https://www.trendmicro.com/ja_jp/research/24/l/iot-botnet-activity-ddos-attacks.html

中国

中国は安全保障や先端技術に関する情報窃取に力を入れてサイバー攻撃を行っていることが知られている。また、VoltTyphoon で知られている、台湾進攻に備えた重要インフラへの妨害準備と考えられる活動が、米国やその他の国々に対して行われていると報告されているが[20]、これまでのところ、実際にこのキャンペーンにおいて、サイバー攻撃により重要インフラへの妨害を行った形跡は発見されていない。加えて、JAL への攻撃の前日となる 12 月 25 日は日中外相会談が行われ、関係改善に向けた双方の意思が確認されている[21]。もし、この直後に日本にサイバー攻撃を繰り返し行ったとするならば、不自然であると考える。

ロシア

ロシアは、軍事攻撃や情報工作等と並行してサイバー攻撃を実施するハイブリッド戦争をドクトリンとして持ち、ウクライナ侵攻等を通して、世界で最もサイバー攻撃の実践を積み重ねていると考えられており、サイバー攻撃による妨害工作の実践も豊富である。

JAL への攻撃前日の 12 月 25 日、ロシアを刺激した可能性が疑われる動向があった。ウクライナのゼレンスキー大統領との電話会談にて石破首相が、ロシアの凍結資産を活用して 30 億ドルをウクライナに送金する用意があると伝えたと、海外メディアが報じていた[22]。また、昨年の 5 月 10 日に JR 東日本が正体不明のサイバー攻撃を受け、モバイル Suica に障害が発生したが[23]、その 3 日前には、プーチン大統領の大統領就任式に日本は出席しなかったということがあり[24, 25]、これについても関連が疑われる。

最近ヨーロッパでは、親ロシア派ハクティビストによるサイバー攻撃に加えて、ロシアの関与が疑われる放火、海底ケーブルの切断、侵入事件等が増えており、サイバーおよび物理の両空間でウクライナ支援国に対する破壊工作活動を過激化していると考えられている[26, 27]。

3.4. まとめ

動機や実行力の観点から、今回のサイバー攻撃者の候補としてはロシアが考えられる。他にはこのタイミングでこのような攻撃を実行する有力な候補は見つからなかった。但し、今後の新たな情報によって分析結果は変わる可能性があることは留意いた

[20] 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/

[21] 出典：NHK『日中外相会談 中国外相の来年早い時期の訪日・対話で一致』
https://www3.nhk.or.jp/news/html/20241225/k10014678341000.html

[22] 出典：The Odessa Journal『Japan will provide Ukraine with an additional $3 billion from frozen Russian assets』
https://odessa-journal.com/japan-will-provide-ukraine-with-an-additional-3-billion-from-frozen-russian-assets

[23] 出典：NHK『JR 東日本 モバイル Suica 障害 徐々に解消 “サイバー攻撃原因”』
https://www3.nhk.or.jp/news/html/20240510/k10014446081000.html

[24] 出典：ロイター『プーチン大統領の就任式、日本は出席せず＝林官房長官』
https://jp.reuters.com/markets/japan/funds/4X6QYMFHHZM6NLUJHBLTK6L5ZE-2024-05-07/

[25] 出典：The Odessa Journal『Japan will provide Ukraine with an additional $3 billion from frozen Russian assets』
https://odessa-journal.com/japan-will-provide-ukraine-with-an-additional-3-billion-from-frozen-russian-assets

[26] 出典：ロイター『コラム：欧州諸国、ロシア関与の破壊工作が急増 対応が急務』
https://jp.reuters.com/opinion/forex-forum/GKRHTRCQSRJIXE24RES6BKOSCM-2024-10-21/

[27] 出典：NHK『相次ぐ海底ケーブル損傷 ロシアの「ハイブリッド攻撃」か』
https://www3.nhk.or.jp/news/html/20250112/k10014691431000.html

だきたい。

また、この分析については様々な議論があると考えるが、現在、導入に向けて議論されている「能動的サイバー防御」を運用する場面においても、攻撃者を明確に特定することができない状況が発生することが想定される。どのようなプロセスや判断基準をもって攻撃者を特定するのかについて、これを機会に議論が深まることを期待したい。

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