サイバーセキュリティレポート

2023.07

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

目次

【1 ページサマリー】

当レポートでは 2023 年 7 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『ランサムウェア攻撃で名古屋港の業務が停止に』

- 貨物取扱量が日本一の名古屋港にて、ランサムウェア攻撃により港の機能が停止に陥る重大なシステム障害が発生し、数日にわたりコンテナの積み下ろしができず物流が停滞した。
- 今回、名古屋港への攻撃を行ったのは、世界中で数多くの被害を出している「LockBit ランサムウェアグループ」とみられている。
- 今回の物流へのサイバー攻撃は日本経済へも影響を与えかねないものであり、このようなランサムウェアグループによる犯罪の防止に日本が率先して取り組むことが期待される。

第 2 章『米政府機関等の Outlook メールアカウント、中国の攻撃者によりハッキングされる』

- 7 月 12 日、Microsoft 社は中国系のハッカーとみられる攻撃者により、少なくとも 2 つの米政府機関を含む、世界中のおよそ 25 の組織の Outlook メールアカウントがハッキングを受けたことを公表した。
- Microsoft はこれまでの発表の中で、攻撃の発端となった署名キーが窃取された方法について明らかにしておらず、また、脆弱性を認めないような表現を用いていることもあり、専門家から批判を受けている。
- 高いセキュリティが要求される場合には、たとえ大手のクラウドサービスであっても利用者は任せきりにするのではなく、詳細なログ監視等を別途行う必要がある。

第 3 章『USB メモリを利用する APT 攻撃の増加』

- USB メモリをネットワーク内へのマルウェア感染拡大に利用する、中国やロシア等の国家を背景とした APT 攻撃の事例が多数確認されている。
- ネットワークから分離されているような重要なシステムを狙っていると考えられ、システム内へのマルウェアの送り込み、さらにマルウェア感染したシステムから他システムへの感染拡大や機密情報の持ち出しにも、USB メモリが利用されている。
- 組織で USB メモリを使用する場合は、外部からの持ち込みか内部限定での使用かを問わず全て、マルウェア感染の可能性を疑って対策を行うことが求められる。

1. ランサムウェア攻撃で名古屋港の業務が停止に

1.1. 概要

2023 年 7 月 4 日、名古屋港での貨物や設備の管理に使用する「**名古屋港統一ターミナルシステム**（**N**agoya **U**nited **T**erminal **S**ystem [以下、**NUTS**]）において、港の機能が停止に陥る重大なシステム障害が発生した。NUTS を管理する名古屋港運協会は、システム障害の原因がランサムウェアの感染であることを公表し、愛知県警が不正アクセス禁止法違反の疑いで捜査している[1]。

名古屋港は、**貨物量**、**輸出額**、**貿易黒字額**、利用者、また陸地部分の面積いずれも日本最大で、約二日半にわたりコンテナの搬出入ができなくなったことで現場は大混乱となった[2]。

図 1 名古屋港全景[3]

1.2. システム障害の経緯

被害を受けた NUTS は、名古屋港の 5 つのコンテナターミナル全てで使われている、コンテナの積み降ろしや運び出しなどを一元管理するシステムで、2023 年 1 月から新システムが全面稼働している。これにより、名古屋港は多数あるコンテナの配置状況等をリアルタイムで把握し、トラックのコンテナ搬出入等の計画をすぐに算出して作業を効率よく進めることができる。

障害が発生した 7 月 4 日朝、出勤した名古屋港運協会の職員がシステムの不具合に気付き、ダウンしているサーバー等の再起動を行ったが復旧しなかった。さらにプリンターが動き出し、冒頭に「LockBit Black Ransomware」と記載された、ランサムウェアの感染を通告する英語の脅迫文が 100 枚程出力された[4]。全サーバーのデータは暗号化されており、協会は警察にも相談したうえで、5 日正午にランサムウェアへの感染を公表した[5]。

---

[1] 出典：読売新聞オンライン『英語で「ランサムウェアに感染」、プリンターから１００枚印刷…名古屋港システム障害』
https://www.yomiuri.co.jp/national/20230705-OYT1T50220/

[2] 出典：名古屋港管理組合『日本一の名古屋港』
https://www.port-of-nagoya.jp/shokai/kohoshiryo/kids/1001074.html

[3] 出典：名古屋港管理組合『名古屋港の全容』
https://www.port-of-nagoya.jp/shokai/kohoshiryo/photogallery/photogallery/1001055.html

[4] 出典：朝日新聞 DIGITAL『プリンターは延々と英文はき出した サイバー被害の名古屋港、対策は』
https://www.asahi.com/articles/ASR7C5H87R7BOIPE003.html

[5] 出典：NHK 名古屋放送局『名古屋港にサイバー攻撃？ ランサムウエアの被害とは？』
https://www.nhk.or.jp/nagoya/lreport/article/001/44/

名古屋港運協会では、感染前のバックアップデータを元に復元作業を実施したが、システム復旧に至るまで相当な時間を要した。難航した要因として、バックアップデータを保存していたサーバーでもランサムウェアが検出され駆除が必要だったこと、別のシステム障害も発生し復旧が伸びたことが挙げられる[6]。

脅迫をしてきた攻撃者について同協会は、脅迫文に身代金額の記載はなく、攻撃者への連絡も行っていないと述べている。なお、このようなランサムウェア攻撃でよく見られる暴露サイトでの窃取情報の公開は、8 月 14 日時点で確認できていない。

システム障害の発生から復旧までの簡単な時系列は下記の通りである[7]。

【時系列】	
・7 月 4 日 06:30 頃	NUTS システムの作動停止を確認。同日のコンテナの搬出入が停止
・7 月 5 日 12:00 頃	名古屋港運協会がランサムウェア感染によるシステム障害を発表（第一報）
・7 月 6 日 07:15 頃	バックアップデータの復元が終了。別のシステム障害が発生
・7 月 6 日 14:15 頃	システム障害が解消。順次コンテナの搬出入作業が再開
・7 月 6 日 18:15 頃	全ターミナルで業務を再開

1.3. 被害状況

今回のサイバー攻撃により NUTS が停止した影響で、名古屋港では 2 日間で約 1 万 5 千本のコンテナの搬出入ができなくなる等の事態が生じ[8]、港周辺は待機するコンテナトレーラーで大渋滞となった。コンテナの搬出入が再開した後も、しばらくの間は完全復旧に向けて作業時間を通常より延ばす必要があったため、配送の遅延等が続いていた。

なお、名古屋港では自動車関係の部品なども多く扱っているが、トヨタやそのグループ会社は「在庫があるので、生産に影響は出ていない」としている[9, 10]。

本件については政府がセキュリティ対策を取りまとめることになり、7 月 31 日には国土交通省が第 1 回目の「コンテナターミナルにおける情報セキュリティ対策等検討委員会」を開催した[11]。

1.4. LockBit ランサムウェア について

今回の攻撃は、ロシア語圏に居住するメンバーを中心に構成され、最も活発に活動しているハッカー集団のひとつ「**LockBit ランサムウェアグループ**」**（以下、LockBit）**によるものと考えられている。LockBit のターゲットは金融、IT、製造業等が上

[6] 出典：日経 XTECH『バックアップからもマルウエア検出で復旧遅れ、名古屋港統一ターミナルシステム』
https://xtech.nikkei.com/atcl/nxt/news/18/15539/

[7] 出典：名古屋港運協会『NUTS システム障害の経緯報告』
https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf

[8] 出典：日経 XTECH『バックアップからもマルウエア検出で復旧遅れ、名古屋港統一ターミナルシステム』
https://xtech.nikkei.com/atcl/nxt/news/18/15539/

[9] 出典：NHK『名古屋港 システム障害「ランサムウエア」感染確認 復旧急ぐ』
https://www3.nhk.or.jp/news/html/20230705/k10014119091000.html

[10] 出典：東海テレビ『トレーラー運転手「仕事になりませんわ」名古屋港のシステム障害が 6 日朝復旧 コンテナ搬出入再開も大幅遅れ』
https://www.tokai-tv.com/tokainews/article_20230706_28617

[11] 出典：国土交通省『「コンテナターミナルにおける情報セキュリティ対策等検討委員会」を開催します』
https://www.mlit.go.jp/report/press/port02_hh_000189.html

位を占めており、全世界でこれまで 2 千以上の企業や団体、1 万 5 千人以上の個人に被害をもたらしたとされている[12]。LockBit が港を攻撃した事例は、2022 年 12 月のポルトガルのリスボン港以来、今回の名古屋港が二例目である[13]。

1.5. VPN 装置が侵入口か

名古屋港運協会では VPN 装置「FortiGate」を使用しており、今回の LockBit ランサムウェアはその FortiGate を経由して送り込まれた可能性が疑われている。VPN 装置はランサムウェアの主要な侵入経路として知られており、FortiGate のユーザーも過去に脆弱性を狙った侵入により大規模な被害に遭っている。同協会では最新の重大な脆弱性に対応する修正を適用しておらず[14]、セキュリティ運用体制に何らかの問題があった可能性が考えられる。

1.6. まとめ

この事件は、重要インフラのひとつである物流がサイバー攻撃で止まった国内初のケースとなった。今回は数日で復旧できたものの、長期化した場合、一般市民の生活はもちろんのこと日本経済へも多大な影響を与えかねなかった。サイバー攻撃を100%防ぐことはできないため、このような犯罪/テロ行為を行った者に相応の処罰を与えることが再発防止に有効と考えるが、残念ながらランサムウェア攻撃に対する日本での検挙はこれまで難航しているのが実態である。

一方、国際的には、重要インフラに対する攻撃は主権侵害に該当すると考えられており、犯人の逮捕や暴露サイトの閉鎖に取り組み、成功している事例もある。コロニアルパイプラインの事件では米国が外交的圧力でロシアのランサムウェアグループを検挙させた。そのようなグループの多くはロシア語圏を拠点としているため、現時点ではそれらが関与するサイバー犯罪を取り締まるのは困難であると考えられるが、ウクライナでの戦争が終結した後を見据えて、日本が国際社会と協力し、このような犯罪者を野放しにしない新たな枠組みを作れるよう率先して取り組むことに期待する。

[12] 出典：産経ニュース『ロシア拠点ハッカーに日本人　世界最大サイバー犯罪集団、幹部が主張　被害２千社、１万５千人』
https://www.sankei.com/article/20220905-KWCTLULU4VN4PPPYVSGWQKRVFU/

[13] 出典：TechFinitive『LockBit ransomware attackers target Japan's biggest port: but who's next?』
https://www.techfinitive.com/lockbit-ransomware-attackers-target-japans-biggest-port/

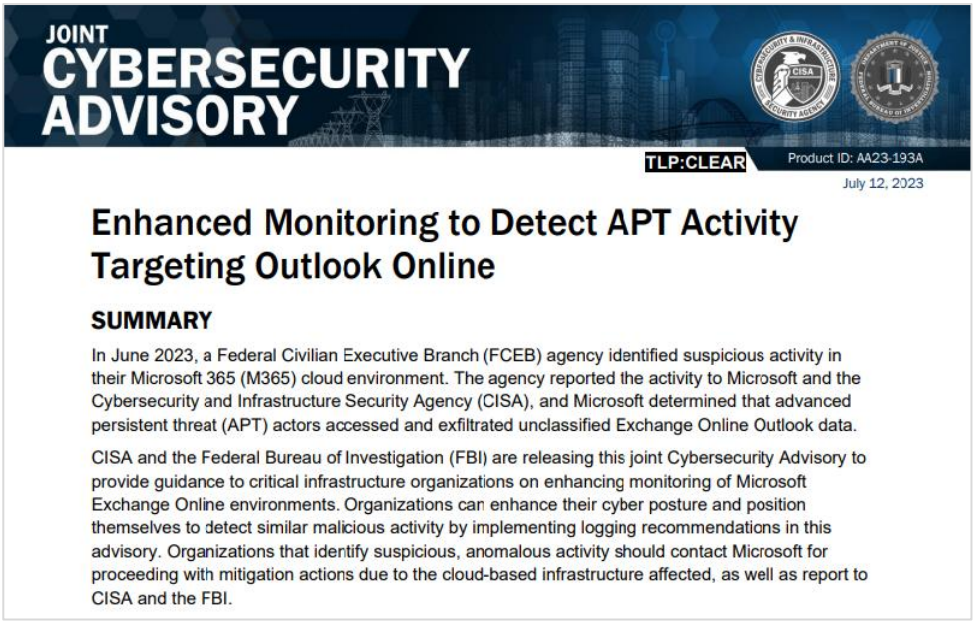
[14] 出典：読売新聞オンライン『名古屋港システム停止、脆弱なＶＰＮ狙われたか…最新「修正プログラム」適用せず無防備状態』
https://www.yomiuri.co.jp/national/20230727-OYT1T50215/

2. 米政府機関等の Outlook メールアカウント、中国の攻撃者によりハッキングされる

2.1. 概要

7 月 12 日、Microsoft 社は中国系のハッカーとみられる攻撃者により、少なくとも 2 つの米政府機関を含む、世界中のおよそ 25 の組織の Outlook メールアカウントがハッキングを受けたことを公表した[15, 16]。

事態を重く見た CISA（Cybersecurity and Infrastructure Security Agency）と FBI は同日、重要インフラ組織を対象とした文書を発表。監視を強化しこの攻撃を検知するための方法を説明した。


JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA23-193A

July 12, 2023

Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

SUMMARY

In June 2023, a Federal Civilian Executive Branch (FCEB) agency identified suspicious activity in their Microsoft 365 (M365) cloud environment. The agency reported the activity to Microsoft and the Cybersecurity and Infrastructure Security Agency (CISA), and Microsoft determined that advanced persistent threat (APT) actors accessed and exfiltrated unclassified Exchange Online Outlook data.

CISA and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory to provide guidance to critical infrastructure organizations on enhancing monitoring of Microsoft Exchange Online environments. Organizations can enhance their cyber posture and position themselves to detect similar malicious activity by implementing logging recommendations in this advisory. Organizations that identify suspicious, anomalous activity should contact Microsoft for proceeding with mitigation actions due to the cloud-based infrastructure affected, as well as report to CISA and the FBI.

図 2 本件に関する CISA と FBI 連名のセキュリティアドバイザリー[17]

Microsoft の発表によると、同社がこの攻撃に対し軽減策を適用して以降、さらなる不正アクセスを受けた証拠はない。しかし、攻撃の発端となった署名キー（後述）が窃取された方法について明らかにしておらず、また、脆弱性の存在を認めないような表現を用いていることもあり、不誠実であると専門家から批判を受けている[18]。

2.2. 事件発覚の経緯

6 月 16 日、米国務省は同省が利用している Microsoft のメールサービス「Exchange Online」のログに異常なデータア

[15] 出典：Bleeping Computer『Microsoft: Chinese hackers breached US govt Exchange email accounts』
https://www.bleepingcomputer.com/news/security/microsoft-chinese-hackers-breached-us-govt-exchange-email-accounts/

[16] 出典：Microsoft『Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email』
https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

[17] 出典：CISA『Enhanced Monitoring to Detect APT Activity Targeting Outlook Online』
https://www.cisa.gov/sites/default/files/2023-07/aa23-193a_joint_csa_enhanced_monitoring_to_detect_apt_activity_targeting_outlook_online_2.pdf

[18] 出典：Ars Technica『Microsoft takes pains to obscure role in 0-days that caused email breach』
https://arstechnica.com/security/2023/07/microsoft-takes-pains-to-obscure-role-in-0-days-that-caused-email-breach/

クセスを検知し、Microsoft に報告した[19, 20]。調査の結果、5 月 15 日からおよそ 1 か月の間、何者かによって、約 25 の組織の電子メールデータと、これらの組織に関連する個人のメールアカウントが不正アクセスされていたことが判明した。米商務省のアカウントも被害を受けており、トップのジーナ・レモンド商務長官も例外ではなかった[21]。

2.3. 攻撃とその実行者について

7 月 14 日、Microsoft は今回の攻撃の実行者と攻撃手法について説明したブログを公開した[22]。

【Storm-0558】

この攻撃は Microsoft が「Storm-0558」という名称で追跡している攻撃者によるものであった。Storm-0558 は、米国や欧州の政府機関等をターゲットとし、スパイ活動、データ窃取、資格情報へのアクセスを目的として活動しており、過去にはフィッシング攻撃等を行っている。中国を拠点とする攻撃者であると推定されており、その根拠の一つとして、Storm-0558 の 4 月から 7 月の活動パターンを観察したところ、中国での一般的な勤務時間帯と合致していたことをあげている（**図 3**）。

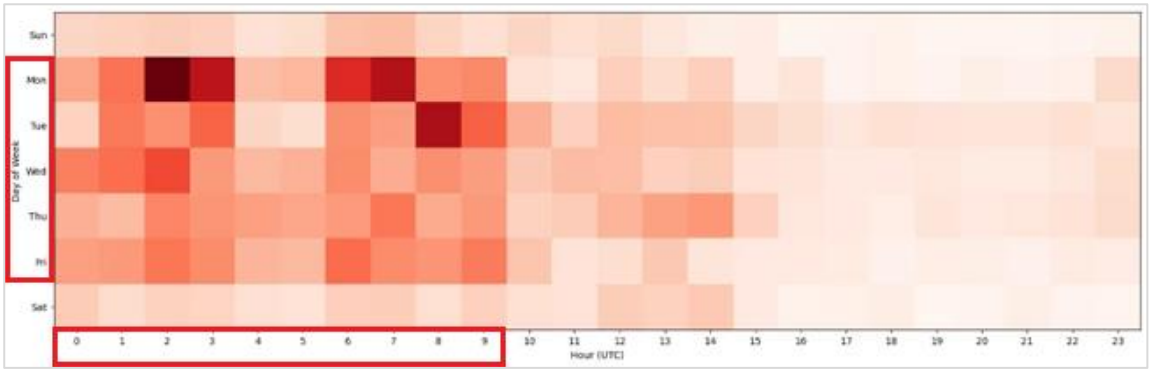


図 3 Storm-0558 の活動曜日（縦軸）・時間（横軸）（Microsoft のサイトより）
主に、月曜から金曜の UTC 0 時から 9 時（中国標準時午前 8 時から午後 5 時）に活動している

【攻撃手法について】

攻撃者は、まず、何らかの方法で取得した「Microsoft アカウント（MSA）署名キー」を利用して Web メール版 Outlook である Outlook Web Access（OWA）用のセキュリティトークンを偽造した。MSA 署名キーは、一般消費者向けのシステムで利用されるものであり、今回侵害された主に法人向けのクラウドサービス「Azure AD」用のキーとは別である。本来、これ

[19] 出典：Microsoft『Mitigation for China-Based Threat Actor Activity』
https://blogs.microsoft.com/on-the-issues/2023/07/11/mitigation-china-based-threat-actor/
[20] 出典：Reuters『Chinese hackers breached State, Commerce Depts, Microsoft and US say』
https://www.reuters.com/technology/chinese-hackers-accessed-government-emails-microsoft-says-2023-07-12/
[21] 出典：The Washington Post『Chinese hackers breach email of Commerce Secretary Raimondo and State Department officials』
https://www.washingtonpost.com/national-security/2023/07/12/microsoft-hack-china/
[22] 出典：Microsoft『Analysis of Storm-0558 techniques for unauthorized email access』
https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

らのキーとトークンは、それぞれのシステムの中でのみ有効である[23]。しかし、このトークン検証に問題があり、MSA 署名キーで偽造したトークンで Azure AD ユーザーになりすますことが可能であった。

また、OWA の API にも、過去に発行した古いトークンを示すことで新しいトークンを取得できるという問題があり、これを悪用し新しいトークンを不正に取得した攻撃者に、メールデータや添付ファイル等のデータを API 経由で窃取されてしまった。

2.4. Microsoft の発表に対する疑問

上記の Microsoft の発表や本件への対応について、メディアやセキュリティの専門家から疑問が呈されている。

【MSA 署名キーの取得方法】

セキュリティトークンの偽造に使用され、事の発端となった MSA 署名キーについては、単に「（攻撃者が）取得した」とだけブログに記載されている。具体的な取得方法は明記されておらず、この点について説明を求めたメディアにも回答していない。メディアからは、Microsoft 自身が侵入された可能性があるとの指摘もある[24]。

【脆弱性を認めない体質】

前述したようにトークン検証には、一般の消費者向けのキーで作成したトークンで法人向けの Azure AD にアクセスできるという脆弱性があったことになる。しかし、Microsoft はこれまでの発表で「脆弱性」や「ゼロデイ」といった表現を用いず、「問題」や「欠陥」といったあいまいな表現を利用し、ダメージコントロールに注力していると専門家は指摘している[25]。

また、こういった脆弱性が発覚した場合には CVE を活用して、利用者が脆弱性を識別、追跡できるようにしておくことが一般的だが、Microsoft はこれまでクラウドサービスについて脆弱性を認めたことがなく、CVE も発行していない[26]。

【Microsoft 自身の検知能力と顧客が負担するコスト】

前述のように、今回の攻撃は Microsoft 自身が気づいたものではなく、米国務省が検知したものである。また、検知には Microsoft と高額な契約をしている場合にのみ取得できる詳細なログが必要であり、標準的な契約で取得できるログは限定的で、今回の攻撃を検知するには不足していた[27]。つまり、Microsoft 側の欠陥で受けた攻撃について、顧客側が余分なコストをかけて検知する必要があった。

なお、7 月 19 日、Microsoft は詳細なログを取得する機能を、標準的な契約ユーザーに対しても開放した[28]。

---

[23] 出典：Microsoft『Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email』
https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

[24] 出典：The Stack『Microsoft clams up over critical Azure key breach, security incident as attackers breach US agencies』
https://www.thestack.technology/microsoft-msa-key-breach-mystery/

[25] 出典：TechCrunch『Microsoft lost its keys, and the government got hacked』
https://techcrunch.com/2023/07/17/microsoft-lost-keys-government-hacked/

[26] 出典：Ars Technica『Microsoft takes pains to obscure role in 0-days that caused email breach』
https://arstechnica.com/security/2023/07/microsoft-takes-pains-to-obscure-role-in-0-days-that-caused-email-breach/

[27] 出典：Reuters『Microsoft under fire after hacks of US State and Commerce departments』
https://www.reuters.com/technology/microsoft-under-fire-after-hacks-us-state-commerce-departments-2023-07-13/

[28] 出典：CISA『CISA and Microsoft Partnership Expands Access to Logging Capabilities Broadly』
https://www.cisa.gov/news-events/news/cisa-and-microsoft-partnership-expands-access-logging-capabilities-broadly

2.5. まとめ

信頼性の高さで知られる Microsoft のクラウドサービスが中国の攻撃者により侵害され、メールデータが窃取された。

情報インフラが基盤となる ICT 社会において、サイバーセキュリティのリスクは重要な問題である。そのため、被害に遭った組織・企業には、迅速にかつ透明性を持って情報開示することで、被害の連鎖を防ぎ、ステークホルダーへの説明責任を果たすことが求められる。今回の事案は世界市場をリードするクラウドサービス提供事業者で起きており、影響も大きいことから、なお一層の適切な開示を行うことが求められる。

また、高いセキュリティが要求される場合には、たとえ大手のクラウドサービスであっても利用者は任せきりにするのではなく、詳細なログ監視等を別途行う必要があることを、今回の一件は明らかにした。

3. USB メモリを利用する APT 攻撃の増加

3.1. 概要

2023 年 7 月に Mandiant 社は、マルウェア感染した USB メモリを使用する攻撃の検知が 2022 年下半期より 3 倍に増加したと発表した[29]。機密情報の窃取を狙った APT グループによる攻撃が大半を占めると、同社は分析している。

このようなサイバー攻撃者が使用するマルウェアは、システムへの侵入時、また侵入後の感染拡大や情報の持ち出しに USB メモリを使うよう作成されている。セキュリティが強固なシステムへの攻撃に、USB メモリの利用が有効とのサイバー攻撃者の思惑が窺える。

3.2. Mandiant 社が検知した攻撃例

USB メモリを利用する攻撃の検知例として Mandiant 社は、サイバー攻撃者による攻撃キャンペーンの例を紹介[29]している。

この攻撃キャンペーンでは、騙されたユーザーが USB メモリに仕込まれたマルウェアのインストーラーを実行すると、端末がマルウェアに感染する仕組みになっていた。マルウェアは感染後、システム内で他の機器にアクセスして機密情報を収集し、バックドアを設けてシステムの外への接続を試みる。さらに、感染したシステムにある他の USB メモリに、マルウェアのインストーラーを設置する機能が確認されている（図 4）[29]。これは USB メモリの接続先でマルウェアを自己増殖させるためとみられている。

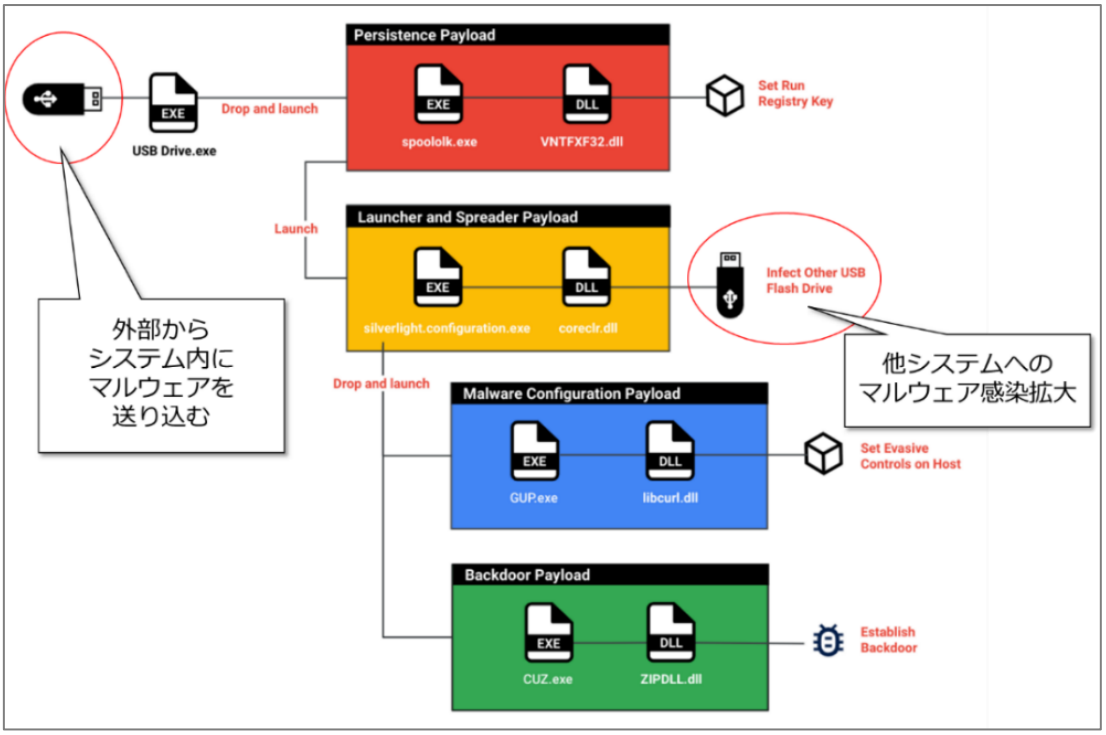


図 4 USB メモリを利用するマルウェアの感染の展開

(Mandiant 社作成の図に注釈を追加)

[29] 出典：Mandiant『The Spies Who Loved You: Infected USB Drives to Steal Secrets』
https://www.mandiant.com/resources/blog/infected-usb-steal-secrets

3.3. 攻撃経路に利用される USB メモリ

Mandiant 社以外でも昨年から今年にかけて、USB メモリを利用した、中国やロシア等の国家を後ろ盾とした APT グループによる攻撃キャンペーンが複数検知されている [30, 31, 32]。

これらの攻撃では、システム間を跨いでマルウェアを移動させるための攻撃経路として USB メモリが利用されている。経路は以下の 3 つに分類できる。

【外部からシステム内にマルウェアを送り込む経路として】 [33]

攻撃者は USB メモリを通して重要なシステムにマルウェアを感染させる。

攻撃者が郵送[34]等により従業員へと渡した USB メモリや、組織外の端末への接続でマルウェアに感染した USB メモリが、標的組織内に持ち込まれる。従業員がその USB メモリを端末に接続し、誤ってインストーラーを実行する等により（図 5）[30]、システム内でのマルウェア感染拡大が発生する。

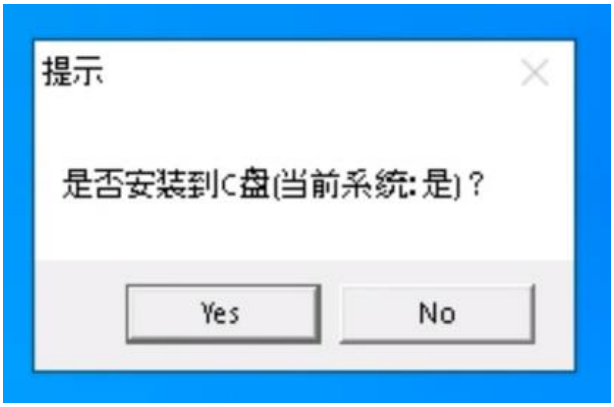


図 5 感染を狙った偽装プログラムのメッセージ

＜日本語訳：C ドライブにインストールしますか？
（現在のシステム：はい）＞

【マルウェアに感染したシステムからの感染拡大経路として】 [33]

感染したマルウェアはシステムに常駐し、USB メモリの接続状況を監視する。そして、新たに USB メモリが接続されたことを検知すると、その USB メモリへと自身をコピーする。感染した USB メモリがまた別のシステムへと接続されることで、マルウェア感染がシステム外に拡大する。これにより、最初に感染したシステムが標的のシステムではなくても、最終的に標的のシステムへと感染が到達する可能性がある。

---

[30] 出典：NTT セキュリティテクニカルブログ『USB メモリを起点とした FlowCloud を用いた攻撃について』
https://jp.security.ntt/tech_blog/102id0t

[31] 出典：Check Point Research『Beyond the Horizon: Traveling the World on Camaro Dragon's USB Flash Drives』
https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/

[32] 出典：Symantec Enterprise Blogs『Shuckworm: ロシアによるウクライナに対する 執拗なサイバーキャンペーンの裏側』
https://symantec-enterprise-blogs.security.com/blogs/japanese/shuckworm-roshianiyoruukurainaniduisuru-zhiaonasaihakiyanhennolice

[33] 出典：MITRE ATT&CK『Replication Through Removable Media, Technique T1091 – Enterprise』
https://attack.mitre.org/techniques/T1091/

[34] 出典：Recorded Future『FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware』
https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware

【マルウェアに感染したシステムからの情報流出経路として】[35]

USB メモリへのマルウェア感染時に、窃取した機密情報もコピーするマルウェアが確認されている[36]。これは、セキュリティが強固で情報を外部に送信することが困難なシステムから、USB メモリを通じてセキュリティが比較的緩い別のシステムに持ち出すことで、機密情報の外部送信の機会を狙ったものと考えられる。

3.4. なぜ攻撃経路として USB メモリが狙われているのか

重要なシステムは、ネットワーク分離や多層防御、標的型メールのフィルタリング等の対策で、外部からの侵入が困難になっている。そのようなセキュリティが強固なシステムでは、メンテナンス等の外部システムとの情報のやり取りにオンラインを避けるため、しばしば USB メモリが使われるが、サイバー攻撃者はその裏をかこうとしていると考えられる。

実際に、中国政府やロシア政府関連等の APT グループによる政府・民間を標的とした攻撃で、このような手法が複数確認されており、その中には日本の組織に関連した攻撃も含まれている（図 6）[29]。

図 6 中国政府系 APT グループによる
USB メモリを利用した攻撃の被害組織の分布

3.5. まとめ

昨今のサイバー攻撃者の活動から、組織における USB メモリの使用には、より一層の警戒が必要であることが明確になった。これまでは外部から持ち込まれる USB メモリは警戒されてきたが、今後は組織内でのみ使用する USB メモリについても同等に警戒し、マルウェアに感染している可能性があるという前提で運用する必要がある。

以上

[35] 出典：MITRE ATT&CK『Exfiltration Over Physical Medium: Exfiltration over USB, Sub-technique T1052.001』 https://attack.mitre.org/techniques/T1052/001/

[36] 出典：Kaspersky ICS CERT『Common TTPs of attacks against industrial organizations. Implants for gathering data』 https://ics-cert.kaspersky.com/publications/reports/2023/07/31/common-ttps-of-attacks-against-industrial-organizations-implants-for-gathering-data/

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