サイバーセキュリティレポート

2024.06

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 2024 年 6 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『中国のサイバー攻撃者、脆弱性を悪用して 2 万台超の FortiGate へ侵入』

- 6 月 10 日、オランダ国立サイバーセキュリティセンター（NCSC）は、中国の国家支援を受ける攻撃者が実行したサイバー攻撃の範囲について、「これまで知られていたよりもはるかに大きい」と発表した。
- Fortinet の次世代ファイアウォール「FortiGate」においては、2022 年 12 月にゼロデイ脆弱性「CVE-2022-42475」が公表された。この時期に、バックドアを設けるマルウェア「COATHANGER（コートハンガー）」の設置を意図した、当脆弱性を悪用する大規模なゼロデイ攻撃が行われていたことが、今回の発表で明らかになった。
- 現時点での実際の被害件数は不明であり、今後、このバックドアを契機とした、さらなる被害が報告されることが想定される。

第 2 章『Snowflake を利用する複数の企業でデータ漏洩が発生』

- 6 月 2 日、データ管理・分析サービスを提供する Snowflake 社は、サイバー攻撃により複数の顧客企業からデータが漏洩したと発表した。
- 攻撃者は、Snowflake のシステムの脆弱性等を悪用したのではなく、自身で入手した認証情報を使用して、ターゲット企業が使用する Snowflake にログインし、情報を窃取したとみられている。被害を受けたアカウントでは、多要素認証が設定されておらず、認証情報だけでログインできる状態だった。
- クラウドベースのサービスを利用すると、セキュリティ対策をクラウドベンダーに任せられると考えがちだが、すべてを任せられるわけではない。安全に利用するためには、クラウド事業者との責任分界点を確認して、自らが管理すべき領域については適切な対策を施す必要がある。

第 3 章『企業が止まる、仮想サーバー環境への攻撃』

- 2024 年 6 月の KADOKAWA グループに対するランサム攻撃のように、全社的なシステム障害を引き起こす、プライベートクラウドと呼ばれる仮想サーバー環境へのランサム攻撃が近年増加している。
- 仮想サーバー環境内では、企業にとって重要なシステムのサーバーが多数稼働していることが多い。ランサム攻撃では、管理するハイパーバイザーを侵害することでそれらサーバーをまとめて攻撃するといったことが行われている。
- 企業は、企業全体の活動停止によって脅迫することを狙うランサム攻撃者を意識し、全社的なセキュリティ対策を行う必要がある。

1. 中国のサイバー攻撃者、脆弱性を悪用して 2 万台超の FortiGate へ侵入

1.1. 概要

6 月 10 日、オランダ国立サイバーセキュリティセンター（NCSC）は、中国国家の支援を受ける攻撃者によって過去に実行されたサイバー攻撃の範囲について、「これまで知られていたよりもはるかに大きい」と発表した[1]。

NCSC は今年の 2 月 6 日、オランダ軍事情報安全保障局（MIVD）及びオランダ一般情報安全保障局（AIVD）と協力し、Fortinet の次世代ファイアウォール「FortiGate」に侵入した後に使用されるバックドアツール「COATHANGER（コートハンガー）」について、調査報告を発表していた[2]。その後、更なる調査で 2022 年から 2023 年の数か月間にかけて、COATHANGER のインストールを意図したと考えられる中国からの攻撃により、世界中の 2 万台以上の FortiGate に不正アクセスがあったことが分かり、今回警告を発した。

1.2. 攻撃について

【オランダ軍への攻撃】[3, 4]

2023 年、中国の攻撃者が「FortiGate」の脆弱性「CVE-2022-42475」を悪用してオランダ軍のネットワークに侵入した。これは機密扱いではない研究開発用のもので、他のネットワークからは分離された環境でもあったため、利用者も 50 人未満と少なく影響は限定的であった。

しかし、オランダ軍事情報安全保障局（MIVD）とオランダ一般情報安全保障局（AIVD）は、そのインシデントの対応中に、これまで知られていなかったリモート操作型のトロイの木馬「COATHANGER（コートハンガー）」が使用されていたことを発見。今年 2 月にオランダ国立サイバーセキュリティセンター（NCSC） が COATHANGER についての調査結果を公開した。

[1] 出典：Nationaal Cyber Security Centrum『Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices』https://www.ncsc.nl/actueel/nieuws/2024/juni/10/aanhoudende-statelijke-cyberspionagecampagne-via-kwetsbare-edge-devices

[2] 出典：Nationaal Cyber Security Centrum『Nieuwe malware benadrukt aanhoudende interesse in edge devices』https://www.ncsc.nl/actueel/nieuws/2024/februari/6/nieuwe-malware-benadrukt-aanhoudende-interesse-in-edge-devices

[3] 出典：Nationaal Cyber Security Centrum『TLP:CLEAR MIVD AIVD Advisory COATHANGER』（ダウンロードページ）https://www.ncsc.nl/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear

[4] 出典：Ministerie van Defensie『MIVD onthult werkwijze Chinese spionage in Nederland』https://www.defensie.nl/actueel/nieuws/2024/02/06/mivd-onthult-werkwijze-chinese-spionage-in-nederland

Cybersecurity Advisory

9 February 2024

UNCLASSIFIED
TLP:CLEAR

Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT

This advisory is a joint publication of the MIVD and AIVD, the intelligence and security services of the Netherlands. An accompanying press release was published on the website of the Ministry of Defence of the Netherlands.

1. Overview

- The Ministry of Defence (MOD) of the Netherlands was impacted in 2023 by an intrusion into one of its networks. The effects were limited because of prior network segmentation.
- Incident response uncovered previously unpublished malware, a remote access trojan (RAT) designed specifically for Fortigate appliances. It is used as second-stage malware, and does *not* exploit a new vulnerability. Intelligence services MIVD & AIVD refer to the malware as COATHANGER based on a string present in the code.
- The COATHANGER malware is stealthy and persistent. It hides itself by hooking system calls that could reveal its presence. It survives reboots and firmware upgrades.
- MIVD & AIVD assess with high confidence that the malicious activity was conducted by a state-sponsored actor from the People's Republic of China.

limited because the victim network was segmented from the wider MOD networks.

The victim network had fewer than 50 users. Its purpose was research and development (R&D) of unclassified projects and collaboration with two third-party research institutes. These organizations have been notified of the incident.

2.1 Attribution

MIVD & AIVD assess with high confidence that the intrusion at the MOD, as well as the development of the malware described in this report, was conducted by a state-sponsored actor from the People's Republic of China.

MIVD & AIVD emphasize that this incident does not stand on its own, but is part of a wider trend of Chinese political espionage against the Netherlands and its allies.

図 1 オランダ国立サイバーセキュリティセンター（NCSC）が公開した COATHANGER についてのレポート[5]

【FortiGate の脆弱性「CVE-2022-42475」】

「CVE-2022-42475」は FortiOS の SSL-VPN 機能におけるヒープベースのバッファオーバーフローの脆弱性である。これは、認証されていない遠隔の第三者が、細工したリクエストを送信することで任意のコードやコマンドを実行できるものである。Fortinet はゼロデイ脆弱性の存在を 2022 年 12 月に公表し[6] 、翌月には、政府機関や関連団体を標的としたゼロデイ攻撃に悪用されていたことを発表した。この発表で、攻撃者は特定されなかったが、脆弱性の悪用によりトロイの木馬が設置されることは確認されていた[7]。その直後、Mandiant 社が、中国政府に関連する者が同脆弱性によるゼロデイ攻撃を行っていると発表した[8]。

今回（６月）の NCSC の発表においても、攻撃者を中国系としており、2022 年から 2023 年の脆弱性発表前後の数か月間にわたり、攻撃者が当脆弱性を悪用し、FortiGate にマルウェア「COATHANGER」をインストールする活動を行っていたことを伝えている。この活動により、世界中で 2 万台以上の FortiGate に対する不正アクセスが行われ、そのうち約 14,000 台がゼロデイ期間中に侵害の被害に遭っている。その中には西側諸国の政府、国際機関、防衛関連企業などが含

[5] 出典：Nationaal Cyber Security Centrum『TLP:CLEAR MIVD AIVD Advisory COATHANGER』（ダウンロードページ）
https://www.ncsc.nl/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-COATHANGER-tlp-clear

[6] 出典：FortiGuard Labs『Heap-based buffer overflow in sslvpnd』
https://www.fortiguard.com/psirt/FG-IR-22-398

[7] 出典：BleepingComputer『Fortinet: Govt networks targeted with now-patched SSL-VPN zero-day』
https://www.bleepingcomputer.com/news/security/fortinet-govt-networks-targeted-with-now-patched-ssl-vpn-zero-day/

[8] 出典：Google Cloud Blog (Mandiant)『Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475)』
https://cloud.google.com/blog/topics/threat-intelligence/chinese-actors-exploit-fortios-flaw?hl=en

まれていた。この被害状況から、中国のサイバースパイ活動がかなり広範囲であったことが分かる[9]。なお、当脆弱性を悪用した中国の攻撃者として、UNC3886 が確認されている[10]。同グループは、Fortinet や VMware 製品のゼロデイ脆弱性を悪用した攻撃を行うことで知られている。

【バックドア「COATHANGER」】[11]

攻撃者は脆弱な FortiGate を発見すると、脆弱性を利用してシステムへの侵入を試み、成功すると、リモート操作用のマルウェア「COATHANGER」を別のホストから標的のシステムにダウンロードさせる。COATHANGER はその後、攻撃者のコマンド＆コントロールサーバに接続し、バックドアとして機能する。

このマルウェアはシステムのリブートやファームウェアアップデートを行っても消えずにシステムに残り、攻撃者は標的へのアクセスを維持することができる。高いステルス性も備えており、システムコール（OS の機能を呼び出すために使用される関数）を傍受してマルウェアの検知を避ける機能が備わっている。NCSC はマルウェア検知ツール YARA で検出できるよう、COATHANGER の YARA ルールを、2 月に発表した論文で公開している。ただ、システム内で COATHANGER が見つかった場合、現時点では FortiGate のデバイスを初期化し、再度インストールと構築を実施するしかないと述べている。

COATHANGER の被害件数は不明だが、検出や削除が難しいという特徴がある故、攻撃者は依然として数多くの潜在的な標的にアクセスできる状態にあると考えられる。今後も世界中で攻撃対象が拡大され、情報窃取などの被害が発生する可能性が高いと NCSC は警告している[12]。

【ハッカー集団による中国への報復】

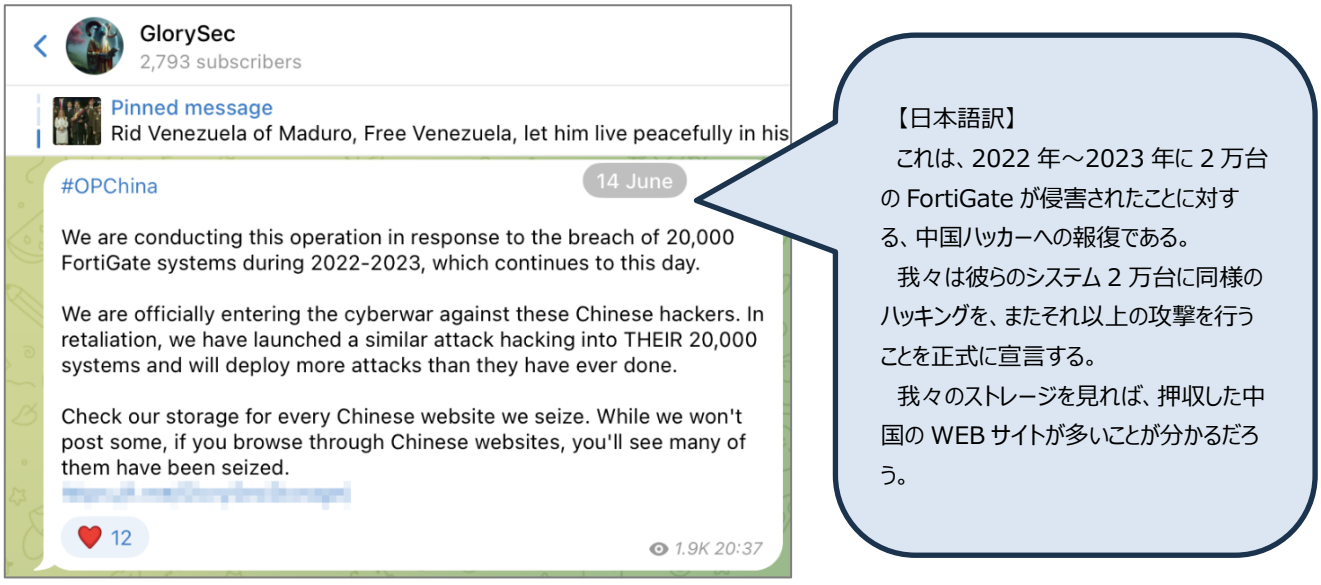

図 2 ハッカー集団 GlorySec が中国の攻撃者に対する報復を宣言した、テレグラムでの投稿

[9] 出典：Nationaal Cyber Security Centrum『Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices』https://www.ncsc.nl/actueel/nieuws/2024/juni/10/aanhoudende-statelijke-cyberspionagecampagne-via-kwetsbare-edge-devices

[10] 出典：Codebook『中国ハッカーUNC3886 の長期的なスパイ活動で使われる手法やマルウェアについて、Mandiant が解説』https://codebook.machinarecord.com/threatreport/33558/

[11] 出典：Nationaal Cyber Security Centrum『TLP:CLEAR MIVD AIVD Advisory COATHANGER』（ダウンロードページ）https://www.ncsc.nl/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-COATHANGER-tlp-clear

[12] 出典：Ministerie van Defensie『MIVD onthult werkwijze Chinese spionage in Nederland』https://www.defensie.nl/actueel/nieuws/2024/02/06/mivd-onthult-werkwijze-chinese-spionage-in-nederland

今回判明した 2 万台超の FortiGate への侵入に対する報復として、世界中で活動を展開しているハッカー集団「GlorySec」[13]が、今年の 6 月に中国へのサイバー戦争を宣言し、中国の攻撃者のシステムへの攻撃を開始したことをテレグラムで主張した。

1.3. まとめ

以前（２月）の NCSC の報告により、中国の APT グループと見られる攻撃者が本ゼロデイ脆弱性を悪用していたことが知られていたが、短期間に 2 万台を超えるシステムをバッファオーバーフローで侵害していたことは想定を大きく超えるものであった。現時点での実際の被害件数は不明であり、今後、このバックドアを契機とした、さらなる被害が報告されることが想定される。

[13] 出典：Medium『GlorySec and Indonesian Hackers: Conflict and Competition in Cyberspace』
https://medium.com/@harboot/glorysec-and-indonesian-hackers-conflict-and-competition-in-cyberspace-637743541f04

2. Snowflake を利用する複数の企業でデータ漏洩が発生

2.1. 概要

6 月 2 日、データ管理・分析サービスを提供する Snowflake 社（以降、社名は「Snowflake 社」、同社の提供するサービスは単に「Snowflake」と記載）は、サイバー攻撃により複数の顧客企業からデータが漏洩したと発表した[14]。この攻撃によって、スペインのサンタンデール銀行では最大 3,000 万人分の顧客情報を含むデータが窃取され、ハッカーフォーラムで売りに出された[15]。

2.2. Snowflake とは

Snowflake は、米国の Snowflake 社が提供するクラウドベースのデータ管理・分析サービスである。Amazon の AWS や Microsoft の Azure、Google の Google Cloud Platform といった主要なクラウドプロバイダー上で利用できる[16]。多くのファイル形式をサポートしており、異なるファイル形式をまたいだデータ分析や、データの自動圧縮、自動暗号化等をサポートしている。マスターカードや Adobe、ファイザー等、世界中で 9,800 社を超える企業に利用されている[17]。

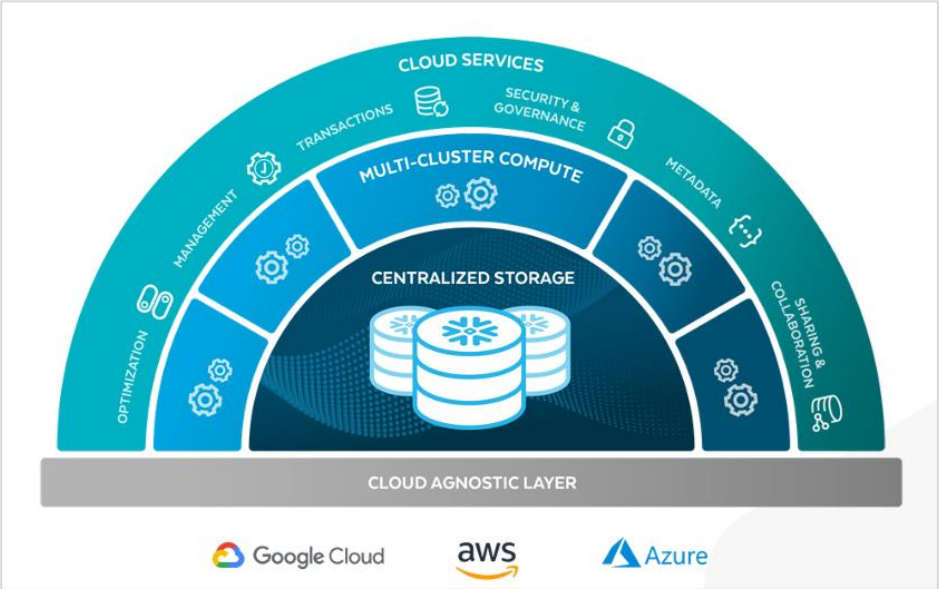

図 3 Snowflake のサービス概要図[18]

[14] 出典：Snowflake『SNOWFLAKE SECURITY HUB』
https://www.snowflake.com/en/resources/learn/snowflake-security-hub/

[15] 出典：ITPro.『Snowflake data breach claims spark war of words over culpability』
https://www.itpro.com/security/cyber-attacks/snowflake-data-breach-claims-spark-war-of-words-over-culpability

[16] 出典：Snowflake『8 Reasons to Build Your Cloud Data Lake on Snowflake』
https://www.snowflake.com/blog/snowflake-managed-data-lake-benefits/

[17] 出典：Help Net Security『The number of known Snowflake customer data breaches is rising』
https://www.helpnetsecurity.com/2024/06/10/snowflake-customer-data-breaches/

[18] 出典：Snowflake『SNOWFLAKE: ONE CLOUD DATA PLATFORM FOR ALL YOUR ANALYTICS NEEDS』
https://www.snowflake.com/en/resources/solution-brief/cross-region-and-cross-cloud-database-replication/

2.3. 事件について

【事件の発覚 サンタンデール銀行】

初めに攻撃に気づいたのはスペインに本社を置くサンタンデール銀行であった。同行が、米国メイン州の司法長官に提出した報告書によると、Snowflake とみられる外部システムへのハッキングが 4 月 17 日に発生し、同行は 5 月 10 日にこれを検知した[19]。同行の 12,786 人の従業員の名前、社会保険番号、銀行口座に関する情報等が漏洩した可能性がある。さらに、5 月 14 日に発表された同行の声明によると、従業員に関する情報だけではなく、スペイン、チリ、ウルグアイの顧客に関する情報も侵害された[20]。

【漏洩情報の販売】

5 月 30 日、世界最大級のハッカーフォーラム「Breachforums」に、当時、同フォーラムのオーナーであったハッカーグループ Shinyhunters がサンタンデール銀行の 3,000 万人分の顧客情報を含むデータを 200 万ドルで販売すると投稿した。この投稿で記載されている国名もスペイン、チリ、ウルグアイであり、前述のサンタンデール銀行の発表と一致していることから、Snowflake から盗まれた情報であるとみられている。

なお、この投稿よりも前の 5 月 24 日、別のハッカーフォーラム（ロシア系）に同様のデータを販売する旨の投稿があったが、Breachforums への投稿後に削除されている。この投稿も Shinyhunters によるものなのか等、詳細は不明である。

図 4 サンタンデール銀行の顧客情報を販売する Shinyhunters の投稿

[19] 出典：Office of the Maine Attorney General『Data Breach Notifications』
https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/64c7c259-76f1-4ad5-b4cc-aa49e0421716.html

[20] 出典：Santander『Statement』
https://www.santander.com/content/dam/santander-com/en/stories/contenido-stories/2024/statement.pdf

【攻撃について】

攻撃者は、自身で入手した認証情報を使用して、ターゲット企業が使用する Snowflake にログインし、情報を窃取したとみられている。これまでの調査で、使用された認証情報のうち約 8 割は以前からハッカー達の間で流通していたものであったことが確認されている[21]。古いものでは、2020 年に盗まれたと思われるものもあり、企業が当時と同じパスワードを使っていたために侵入されたケースもあった。また、攻撃を受けたそれらのアカウントでは、多要素認証が設定されていなかったため、攻撃者は認証情報だけでログインすることができた。

【その他の被害企業】

上述のサンタンデール銀行に続き、Shinyhunters によって Breachforums でデータ販売の投稿材料にされたチケット販売会社チケットマスター[22]で大きな被害が発生している。その他、自動車パーツ会社アドバンスオートパーツ[23]、百貨店大手のニーマン・マーカス[24]等が被害を公表している。Mandiant は、攻撃を受けた可能性のある約 165 の組織に警告を送ったと発表している。

2.4. Snowflake 社の対応

事件の発覚後、攻撃の原因として、脆弱性等、Snowflake のシステムの問題が疑われた Snowflake 社は、セキュリティ企業の Mandiant および CrowdStrike と共同で声明を出し、今回の攻撃は Snowflake の脆弱性やシステムの設定ミスによるものではなく、また、同社の現在および過去の従業員のアカウントが用いられたこともなかったと発表した[25, 26]。そして、顧客には多要素認証を使用し、安全な場所からのみのアクセスを許可するように設定することを呼び掛けた。

サイバー攻撃を受けた際に企業が顧客のパスワードを強制リセットすることは珍しいことではないが、今回、同社は攻撃に気づいた後もそういった対応を行わなかった。Snowflake 社が被害の拡大防止を図らなかったことについて、専門家は疑問を呈している[27]。なお、同社は IT 系メディアの取材に対し、「Snowflake の責任共有モデルでは、多要素認証の適用は顧客の責任である」と答えている[28]。

---

[21] 出典：Google Cloud Blog(Mandiant)『UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion』 https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

[22] 出典：BBC『Data allegedly stolen from 560 million Ticketmaster users』 https://www.bbc.com/news/articles/c899pz84d8zo

[23] 出典：UNITED STATES SECURITIES AND EXCHANGE COMMISSION『Form 8-K（Advance Auto Parts, Inc.）』 https://www.sec.gov/Archives/edgar/data/1158449/000115844924000162/aap-20240523.htm

[24] 出典：DARK READING『Neiman Marcus Customers Impacted by Snowflake Data Breach』 https://www.darkreading.com/cloud-security/nieman-marcus-customers-impacted-snowflake-data-breach

[25] 出典：Snowflake『SNOWFLAKE SECURITY HUB』 https://www.snowflake.com/en/resources/learn/snowflake-security-hub/

[26] 出典：Decipher（Cisco Duo Security）『SNOWFLAKE: CUSTOMER ACCOUNTS TARGETED IN 'IDENTITY-BASED ATTACKS'』 https://duo.com/decipher/snowflake-customer-accounts-targeted-in-identity-based-attacks

[27] 出典：TechCrunch『What Snowflake isn't saying about its customer data breaches』 https://techcrunch.com/2024/06/07/snowflake-ticketmaster-lendingtree-customer-data-breach/

[28] 出典：TechCrunch『Hundreds of Snowflake customer passwords found online are linked to info-stealing malware』 https://techcrunch.com/2024/06/05/snowflake-customer-passwords-found-online-infostealing-malware/

2.5. まとめ

クラウドベースのサービスを利用すると、セキュリティ対策をクラウドベンダーに任せられると考えがちだが、すべてを任せられるわけではない。Snowflake のような SaaS の場合、例えば、データセンターの物理的な保護や OS の更新といったセキュリティ対策はベンダーが実施するが、多要素認証の有効化や認証情報の管理、アクセス制限の設定等は利用者の責任で行う必要がある[29]。過去にも、システム側の欠陥ではなく、ユーザー組織の設定の不備や漏洩認証情報を利用した不正アクセスにより、Salesforce[30]や Office365[31]といった大手が運用しているクラウドサービスからもデータ漏洩事件が発生している。

総務省が、2022 年 10 月に公開した「クラウドサービス利用・提供における適切な設定のためのガイドライン[32]」では、クラウドサービス利用者側へ求める対策として、多要素認証の導入を「特に重要な設定項目」として強調しているほか、特定の IP アドレスからのみアクセス可能にする制御の設定や、ログの管理とモニタリングの実施等を推奨している。

ただし、多要素認証を導入すると、利便性の低下によりサイトの利用者が減ることもある。また、クラウドサービスの利用目的によっては厳重なアクセス制御を必要としない場合もある。そのため、利便性とクラウドサービスで扱う情報の重要性のバランスを考慮して、多要素認証の利用は推奨しても、ユーザーが選択するのが一般的である。

クラウドサービスを安全に利用するためには、クラウド事業者との責任分界点を確認して、自らが管理すべき領域については、用途に応じて適切な対策を施す必要がある。

---

[29] 出典：Microsoft『クラウドにおける共同責任』
https://learn.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility

[30] 出典：Krebs on Security『Many Public Salesforce Sites are Leaking Private Data』
https://krebsonsecurity.com/2023/04/many-public-salesforce-sites-are-leaking-private-data/

[31] 出典：ITmedia NEWS『三菱電機、新たに 1115 件の情報漏えい明らかに　中国経由で不正アクセス』
https://www.itmedia.co.jp/news/articles/2103/29/news130.html

[32] 出典：総務省『クラウドサービス利用・提供における適切な設定のためのガイドライン』
https://www.soumu.go.jp/main_content/000843318.pdf

3. 企業が止まる、仮想サーバー環境への攻撃

3.1. 概要

企業のネットワーク内に構築された仮想サーバー環境へのランサム攻撃が、近年増加している。多数の仮想サーバー（Virtual Machine [以降、VM と表記]）により重要なシステムを稼働させている企業も多く、ランサム攻撃を受けると企業活動に大きな影響が出る。

2024 年 4 月には複数の企業で、SEXi ランサムグループによる仮想サーバー環境への攻撃によって、全社的なシステム障害が相次いだ[33]。また、6 月の KADOKAWA グループに対するランサム攻撃でも、相当数の VM が利用不可能な状態になったことが発表[34]されている。

3.2. 仮想サーバー環境とランサム攻撃

【企業システムに採用される仮想サーバー環境】

自前で用意しているオンプレミス環境内に、「プライベートクラウド」と呼ばれる仮想サーバー環境を構築している企業が多くある。この環境内ではサーバーを仮想化した VM が多数集約され稼働している。VM の実体はサーバー内に保存されているファイルである。ハードウェアのサーバーでは手間のかかる、サーバーの作成/削除、複製や処理能力の増強等が、VM であればファイル単位で容易にできる。そのため、多数のサーバーを連携させ柔軟に運用することが求められる大規模なシステムにも対応可能である。また、プライベートクラウドは自前の環境で構築するため、独自性の高いシステムや、社外のクラウドに預けることが難しい機密情報を扱うシステム等に向いているとされる[35]。

一方でランサム攻撃者は、ビジネス上重要な情報を扱う大規模なシステムを人質とした多額の身代金要求を意図して、近年、企業内の仮想サーバー環境を攻撃対象にしていると考えられている[36]。

【攻撃ポイントとなるハイパーバイザー】

仮想サーバー環境に多数ある VM を集約して管理するサーバーが、**ハイパーバイザー**である（図 5）。2024 年 6 月、ランサムグループの BlackSuit は、日本の KADOKAWA グループへのランサム攻撃の犯行声明で、VMware ESXi（イーエスエックス・アイ）を侵害したことを示唆した。VMware ESXi は代表的なハイパーバイザーである[37]。

ランサム攻撃者は、仮想サーバー環境を効率よく攻撃するためハイパーバイザーを狙う。セキュリティ企業の Recorded

---

[33] 出典：DARK READING『SEXi Ransomware Desires VMware Hypervisors in Ongoing Campaign』
https://www.darkreading.com/threat-intelligence/sexi-ransomware-desires-vmware-hypervisors

[34] 出典：YouTube ニコニコ公式チャンネル / niconico『ニコニコのサービス停止に関するお詫びと今後について』
https://youtu.be/Kyz47Md9fCw?si=7XFlu71ynS4GMRKM&t=143

[35] 出典：NTT 東日本『プライベートクラウドとは？パブリッククラウド・オンプレミスと徹底比較！』
https://business.ntt-east.co.jp/content/cloudsolution/column-360.html

[36] 出典：DARK READING『'MichaelKors' Showcases Ransomware's Fashionable VMware ESXi Hypervisor Trend』
https://www.darkreading.com/cloud-security/-michaelkors-ransomware-fashionable-vmware-esxi-hypervisor

[37] 出典：日経クロステック（xTECH）『今さら聞けないブロードコムと VMware、基礎からライセンス問題まで 5 つの疑問』
https://xtech.nikkei.com/atcl/nxt/column/18/02864/060600001/

Future 社は、VMware ESXi を狙った攻撃が、2021 年から 2022 年にかけて 3 倍に急増したとレポートしている[38]。

よく行われる、ハイパーバイザーを使用したランサム攻撃の手法[39]は次の通り。まず、脆弱な VPN 等を介してターゲットの企業ネットワーク内に侵入した攻撃者は、ハイパーバイザーのアクセス権限を奪う。この際には、ハイパーバイザーに存在する脆弱性やネットワーク内で発見したアカウント情報等が利用される。そして、管理下にある複数の VM から情報を窃取したり、VM を暗号化したりする。さらに、VM のスナップショットを削除するといったことも行う。これにより、暗号化された VM ファイルをスナップショットから復旧することができなくなる。

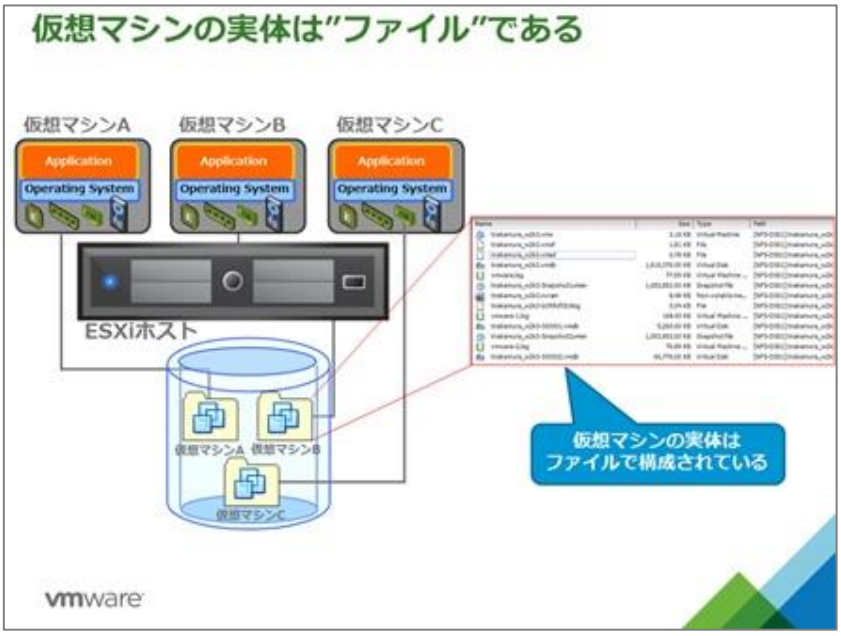

図 5 仮想サーバー環境のハイパーバイザー構成例（例：VMware ESXi） [40]

3.3. ハイパーバイザーへのランサム攻撃例

【ランサム事例①：SEXi ランサムグループ】

2024 年 4 月、VMware ESXi を攻撃するランサムグループ「SEXi ランサムグループ」による被害が相次いだ[41]。VMWare ESXi のみを標的とする事から、もじって「SEXi」と名乗っているとみられている。米国のファストフードチェーンの Panera Bread、米国のホテル会社の Omni Hotels、チリのホスティングプロバイダーの IxMetro Powerhost での被害が判明している。3 社いずれにおいてもランサム攻撃に起因する全社的なシステム障害が発生し、顧客サービスに関わるシステム（POS、予約システム、ホテルのドアロック等）まで停止した。IxMetro Powerhost では VM のバックアップもあったがそれも

[38] 出典：Recorded Future『In Before The Lock: ESXi』
https://www.recordedfuture.com/in-before-the-lock-esxi

[39] 出典：CrowdStrike『Hypervisor Jackpotting, Part 3: Lack of Antivirus Support Opens the Door to Adversary Attacks』
https://www.crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/

[40] 出典：VMware Japan Blog『新卒 SE 社員が贈る vSphere のキソ！第 1 回～ vSphere を俯瞰する～』
https://blogs.vmware.com/vmware-japan/2014/08/vsphere_kiso01.html

[41] 出典：BleepingComputer『The Week in Ransomware - April 5th 2024 - Virtual Machines under Attack』
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-5th-2024-virtual-machines-under-attack/

暗号化されたため、復旧が困難になった[42]。

【ランサム事例②：Akira ランサムグループ】

よく使われているため VMware ESXi での被害が多いが、それ以外のハイパーバイザーへの攻撃も確認されている。

2023 年に Sophos が検知した Akira ランサムグループの攻撃事例[43]では、Windows 系のハイパーバイザーである Hyper-V が悪用された。攻撃者はネットワークに侵入後、窃取した管理者アカウントを使用して Hyper-V を起動することにより、組織内の VM へのさらなるアクセス展開を試みていた。

3.4. まとめ

ランサム攻撃者だけではなく APT の攻撃者も、諜報活動をシステム内に広げる拠点を確保するために仮想サーバー環境への攻撃を行っており[44, 45]、利用している企業にとって仮想サーバー環境の保護は重要課題である。具体的には、VM を管理するハイパーバイザーにおける対策が主眼となる。ハイパーバイザーへのアクセス管理を多要素認証等で厳格にし、ネットワークトラフィックの監視を行うことで、ハイパーバイザーへの不正アクセスを防止する。また、ハイパーバイザーの脆弱性がしばしば攻撃に悪用されるため、ソフトウェアを最新化する等、脆弱性管理を行う[46]。加えて、仮想サーバー環境を攻撃されても被害の及ばないバックアップの確保や、バックアップから迅速に復元できる体制の構築を推奨する。

巨額の身代金を手に入れるという目的があるランサム攻撃者たちは、侵入後どうしたら大きな効果を上げられるかを考えて攻撃をデザインしている。企業の全体にわたる活動停止を引き起こすために仮想サーバー環境を攻略するという、今回紹介した手法はその一形態である。企業は、全社的な被害を狙う攻撃を意識したセキュリティ対策を経営課題とし、取り組む必要がある。

以上

[42] 出典：BleepingComputer『Hosting firm's VMware ESXi servers hit by new SEXi ransomware』
https://www.bleepingcomputer.com/news/security/hosting-firms-vmware-esxi-servers-hit-by-new-sexi-ransomware/

[43] 出典：Sophos『Akira, again: The ransomware that keeps on taking』
https://news.sophos.com/en-us/2023/12/21/akira-again-the-ransomware-that-keeps-on-taking/

[44] 出典：Medium(MITRE-Engenuity)『Infiltrating Defenses: Abusing VMware in MITRE's Cyber Intrusion』
https://medium.com/mitre-engenuity/infiltrating-defenses-abusing-vmware-in-mitres-cyber-intrusion-4ea647b83f5b

[45] 出典：Google Cloud Blog(Mandiant)『Cloaked and Covert: Uncovering UNC3886 Espionage Operations』
https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations

[46] 出典：VMware Japan Blog [TAM Blog]『ランサムウェアの脅威から仮想化基盤を守るには』
https://blogs.vmware.com/vmware-japan/2021/10/tam-blog-ransomware-resiliency.html

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：nsj-co-osint-monitoring@security.ntt