NSHC Threat Research Lab
Document No. TR-CTI2025072302

Trend Report of Ransomware Activities in 2024

Cyber Threat Intelligence Report

July 2025

NSHC Inc.

- **twitter.com/nshcthreatrecon**
- **service@nshc.net**

Table of Contents

- Do not share — The content of this work is provided only to specific customers of information service. Therefore, sharing this content without permission is prohibited.
- Non-disclosure agreement — This work is provided under a non-disclosure agreement (NDA), and violation of this agreement may result in legal consequences.
- Caution — Other copyright-related matters, including actions permitted under this license, must be confirmed with the information service provider before use.

序論

ランサムウェアは、システム内のデータを暗号化したりアクセスを制限したりした後、それを復号化する代価として金銭を要求するサイバー攻撃の手法であり、さまざまな産業分野を対象に継続的な被害が発生しているようです。ランサムウェアは単純なデータ暗号化から進化し、盗んだ情報の公開を脅迫したり、複数のチャネルを利用した心理的圧力をかけたりするなど、攻撃手法が徐々に高度化しており、攻撃者は組織的かつ体系的な形で活動しています。

NSHC 脅威分析研究所は、このようなランサムウェアを含む様々なサイバー脅威の流れを分析し、実際の攻撃に使用された技術やツール、インフラなどを整理して脅威インテリジェンスを分析しています。これらの分析結果に基づき、本報告書は 2024 年の 1 年間に観測されたランサムウェア攻撃の全般的な特徴と構成要素を整理しようとしています。

特に被害が集中した国や産業群の分布、最初の侵入方法のタイプと利用割合、攻撃者が繰り返し悪用した脆弱性、侵入後の攻撃活動に使用されたオープンソースおよびフリーウェアツール、交渉および情報漏洩チャネルの運営構造と匿名インフラの利用方法、支払い要求時に使用された暗号通貨の種類および支払い誘導方法などを項目ごとに分析することで、攻撃者の活動展開方法と運営体系を段階的に記述している。

本報告書は、2024 年に分析されたランサムウェアを利用したハッキンググループに関連する脅威データの分析結果を総合的に扱っており、セキュリティ実務者、インテリジェンス分析者、政策決定者が脅威対応戦略を策定する際に実質的に活用できるように構造化された情報を提供することを目的としています。

攻撃対象

1. 攻撃対象国

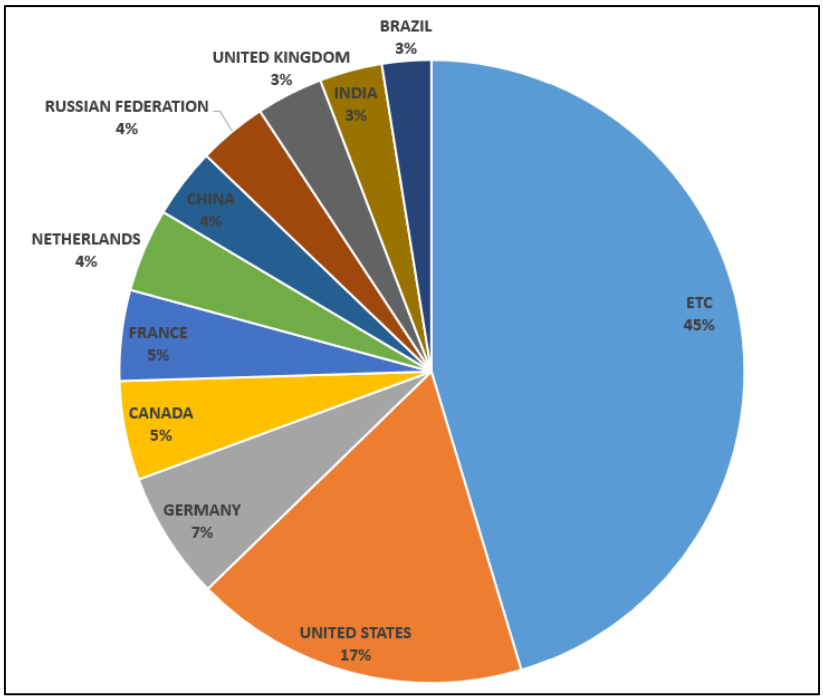
2024 年の 1 年間に発生したランサムウェア被害事例を国別に分類した結果、アメリカが全体被害の 17%で最も高い割合を占めました。これは、アメリカ国内の多数の産業群、豊富なデジタルインフラ、そして高価値データを保有する機関がランサムウェア組織の主要な標的となっていることを示唆しています。続いて、ドイツ（7%）、カナダ（5%）、フランス（5%）、中国（4%）、オランダ（4%）、ロシア（4%）、イギリス（3%）、インド（3%）、ブラジル（3%）などの国でも比較的高い被害が報告されました。

特にヨーロッパ諸国の被害割合が目立っており、これは製造、金融、物流などの主要産業を中心にデジタル化が活発に進んでいることや、EU の GDPR など厳格な情報保護規制により被害事例が透明に

報告されているためと解釈される。中国、ロシアなど自国内で攻撃と防御が混在している国々も被害統計に含まれている点は注目に値する。

興味深い点は、全体の被害の 45%がその他の国（ETC）に属しているという事実です。これは、ランサムウェア攻撃が特定の国にのみ集中しているのではなく、世界中に広範囲に拡散していることを意味します。特に、セキュリティインフラが比較的未整備であったり、被害事例の共有文化が弱い東ヨーロッパ、東南アジア、南米の国々も攻撃対象になっていることを示唆しています。

また、インドやブラジルのように IT インフラが急速に成長している国々も多く被害を受けており、新興デジタル国家に対するセキュリティ体制の強化の必要性が浮上しています。結論として、ランサムウェアは特定の産業や国家に限定されず、デジタル依存度が高いすべての国や組織が潜在的な標的となるグローバルな脅威であることが今回の統計を通じて確認できます。



[図 1: 攻撃対象国]

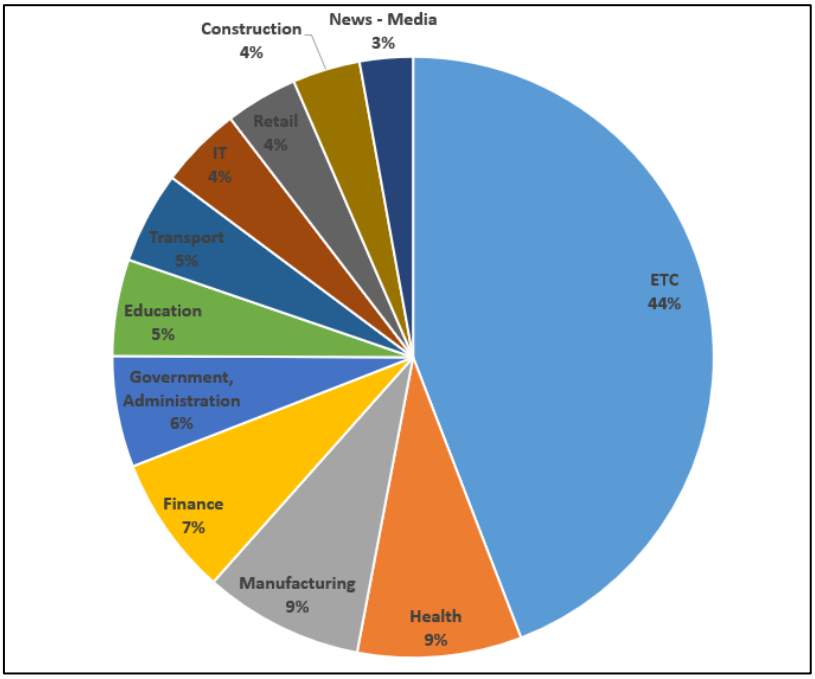
2. 攻撃対象産業群

2024 年の 1 年間にランサムウェアの被害を受けた産業群を分析した結果、医療（Health）と製造（Manufacturing）分野がそれぞれ 9%で最も高い被害率を示しました。医療産業は患者情報や診療システムなどの機密データを扱うため、攻撃が発生した際には業務麻痺に伴う危機対応の圧力から金銭を支払う可能性が高く、攻撃者の主要な標的となっています。製造分野は生産自動化システムの中断が直接的な被害につながるため、業務継続性の観点から被害規模が大きく、攻撃者が産業用システム（ICS/SCADA）を狙う傾向が続いています。

その他にも、金融（7%）、政府/行政（6%）、教育（5%）、運輸（5%）、IT（4%）、流通（4%）、建設（4%）、メディア（3%）などの産業分野でも多くの被害が発生しました。金融と政府部門は、それぞれ高価値の情報資産や公共サービス基盤システムを保有しているため、攻撃者にとって戦略的価値が高いです。教育機関の場合、VPN やメールアカウントを奪取して内部ネットワークに侵入する戦術がよく利用されており、IT および運輸分野は最近、サプライチェーン攻撃の主要なターゲットとなっています。

特に注目すべき点は、全体の被害の 44%がその他の産業群（ETC）に属している点です。これは、伝統的な主要産業だけでなく、法律、物流、農業、公共施設など多様な分野に攻撃が拡散していることを意味します。このように、ランサムウェアは特定の産業に限定されず、すべての産業群を脅かす全方位的な脅威として作用しており、攻撃者は RaaS（Ransomware-as-a-Service）モデルを通じて産業に特化した精密なターゲティング戦略を強化しています。

結論として、各組織は自社の産業特性と資産構造に適した産業別のセキュリティ戦略の策定が求められており、特に業務の継続性確保、バックアップ復旧体制、脅威インテリジェンスに基づく検出体制の強化が重要な対応課題として浮上しています。



[図 2: 攻撃対象産業群]

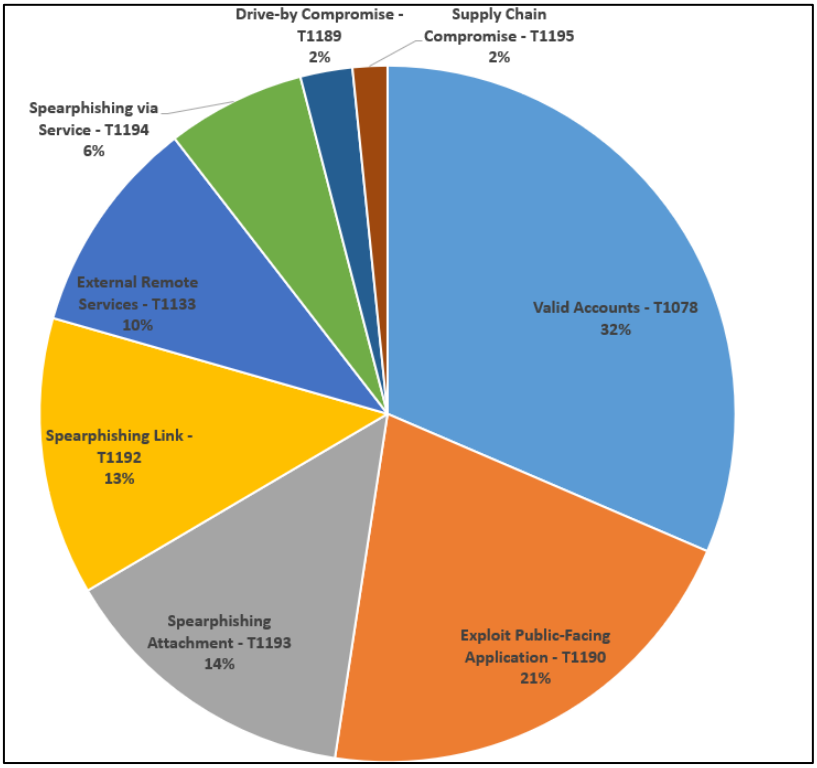
攻撃技術

攻撃者はランサムウェア攻撃のために様々な攻撃技術を使用して目標システムに侵入し、データを暗号化した後、攻撃対象に復号化の費用を要求します。この過程で使用される技術には、システムの脆

弱性を悪用したり、オープンソースやフリーウェアツールを利用する方法が含まれます。以下の本文では、2024 年の 1 年間に攻撃者が活用した主要な攻撃技術について述べます。

1. 最初の侵入

2024 年、ランサムウェアグループが利用した最初の侵入手段の分析結果によると、「有効なアカウント（Valid Accounts）」戦術が全体の 32%を占め、最も高い割合を示しました。これは、盗まれたまたは再利用された資格情報を通じて既存のアカウントで内部システムにアクセスする方法が主要な戦略として定着していることを示しています。VPN、RDP、クラウドベースの資産など、リモートアクセスポイントが増加した環境では、有効なアカウントの確保が初期侵入から権限拡張まで迅速に進むことができ、検知回避および内部移動の面で攻撃者に高い効率性を提供します。
2 番目に高い割合を占めた戦術は「外部に公開されたアプリケーションの悪用（Exploit Public-Facing Application）」で、全体の 21%を記録しました。この戦術は、外部からアクセス可能なウェブサービス、アプリケーション、認証インターフェースなどを対象としており、脆弱性だけでなく、誤った設定、認証回避、機能の露出など、さまざまな攻撃ポイントを利用して初期侵入を試みる方法です。アプリケーションが外部と直接接続されている構造的特性上、攻撃者は認証なしでアクセス可能なインターフェースを優先的に探索し、自動化ツールを通じて多数のシステムを同時にスキャンし攻撃するのに利用できます。管理されていない、または長期間放置されたシステムでは、この戦術が成功する可能性が高く、攻撃者はこれを通じて追加の侵入経路の確保や権限昇格によって戦術を拡張します。
メールを媒介とした侵入戦術も全体で少なからぬ割合を占めていた。「添付ファイルベースのスピアフィッシング（Spearphishing Attachment）」は全体の 14%、「リンクベースのスピアフィッシング（Spearphishing Link）」
「)」は 13%で、合計 27%を記録しました。添付ファイルを基にした戦術は、文書ファイルやスクリプトを含む悪性ファイルをユーザーに実行させる方法であり、リンクを基にした戦術は、メール本文内の URL を通じて外部の悪性ページに誘導する構造で構成されています。
「ドライブバイ感染（Drive-by Compromise）」と「サプライチェーン攻撃（Supply Chain Compromise）」はそれぞれ 2%という低い割合を記録しました。これらの戦術は初期侵入手段として利用される場合が限られており、構成と実行において一定レベル以上の事前準備やアクセス条件が求められる特性があります。戦術選択時に効率性と汎用性が重要な要素として作用する環境では、相対的に複雑度が高い方法は低い割合につながったと解釈されます。
全体的に見て、有効なアカウント戦術を通じた初期侵入が目立つ中で、公開されたアプリケーションの悪用戦術とソーシャルエンジニアリング技術の戦術が依然として併用されていると分析される。



[図 3: 初期侵入戦術の統計]

2. 脆弱性

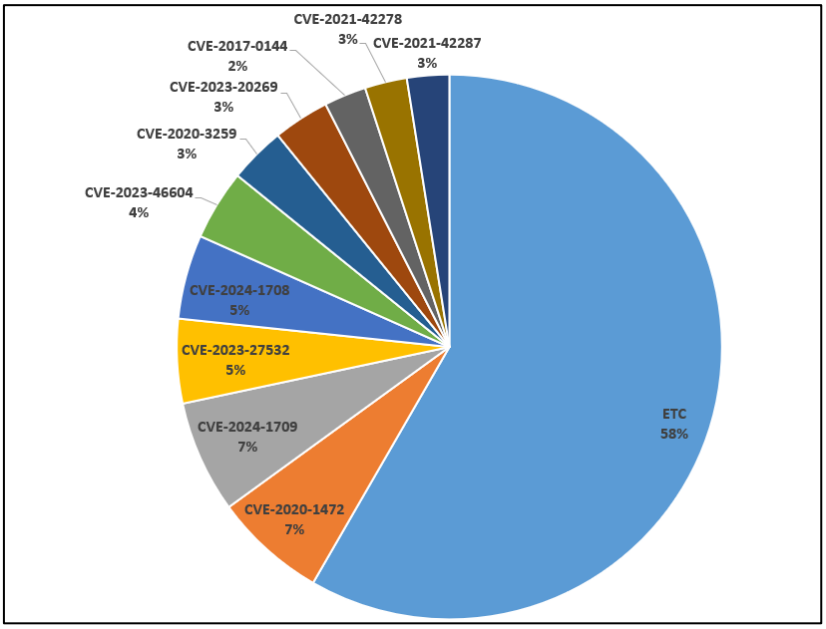
2024 年のランサムウェア攻撃で利用された脆弱性の分析結果、攻撃者が好む技術的アプローチが組織内部のセキュリティ構造と密接に関連していることが明らかになった。

最も高い割合を記録した脆弱性は、それぞれ 7%を占めた CVE-2020-1472（Zerologon ドメインコントローラー権限奪取脆弱性）と CVE-2024-1709（Windows Hyper-V リモートコード実行脆弱性）です。CVE-2020-1472 は、Windows 環境の Netlogon プロトコルを悪用して認証なしにドメインコントローラーの権限を奪取でき、組織全体を掌握する強力な攻撃手段として悪用されました。CVE-2024-1709 は、Hyper-V 機能が有効化された Windows Server および Windows 10/11 環境で、攻撃者が仮想マシン（VM）を通じてホストシステムでリモートコード実行を行うことを可能にする脆弱性であり、仮想化基盤インフラを運用する組織が主要なターゲットとなります。

その後に続く CVE-2023-27532（Veeam バックアップソリューション認証回避脆弱性）と CVE-2024-1708（Microsoft 環境認証パス回避脆弱性）はそれぞれ 5%を記録しました。Veeam 製品の脆弱性は、攻撃者が認証なしで TCP 9401 ポートを通じてバックアップサーバーにアクセスし、バックアップ設定および資格情報を盗むために悪用され、被害者の復旧能力を遮断して交渉の圧力手段として利用されます。CVE-2023-46604（Apache ActiveMQ RCE 脆弱性）は 4%と確認されており、Java ベースのメッセージブローカーシステムで操作されたメッセージを通じて任意のコードを実行できる構造で、アクセス制御が不十分な環境で高い脅威となります。

CVE-2021-42278 および CVE-2021-42287 は、それぞれ Windows Server の Active Directory 環境で発生する脆弱性であり、これらを連携して悪用することで、一般ユーザーアカウントを通じてドメイン管理者権限を奪取することができます。これらの脆弱性は Kerberos チケット偽造攻撃によく利用され、自動化侵入ツールに統合されて攻撃効率が高まっています。CVE-2020-3259（Cisco ASA 情報漏洩脆弱性）はセッショントークンを通じて認証を回避することが可能であり、CVE-2023-20269 は VPN 環境で認証回避を許可する構造で、リモートアクセスポイントが多い組織を狙うのに使用されます。

CVE-2017-0144（EternalBlue SMBv1 RCE 脆弱性）は 2%と低い割合ですが、依然としてパッチが適用されていない旧式のシステムを狙った攻撃に使用されています。全体の 58%は「その他（ETC）」に分類され、さまざまなオープンソースの脆弱性やベンダー特化の欠陥が含まれます。これは攻撃者が特定の CVE 一つに依存せず、環境や条件に応じてさまざまな脆弱性を併用しながら侵入戦略を展開していることを示しています。



[図 4: 脆弱性統計]

脆弱性	脆弱性のタイプ	脆弱性のターゲット
CVE-2020-1472	Privilege Escalation Vulnerability	Microsoft Netlogon
CVE-2020-3259	Information Disclosure Vulnerability	Cisco Adaptive Security Appliance (ASA)
CVE-2021-21972	Remote Code Execution Vulnerability	VMware vCenter Server
CVE-2021-22005	Remote Code Execution Vulnerability	VMware vCenter Server
CVE-2021-34527	Remote Code Execution Vulnerability	Microsoft Windows Print Spooler
CVE-2021-42278	Privilege Escalation Vulnerability	Microsoft Active Directory

CVE-2021-42287	Privilege Escalation Vulnerability	Microsoft Active Directory
CVE-2021-44228	Remote Code Execution Vulnerability	Apache Log4j
CVE-2022-1388	Remote Code Execution Vulnerability	F5 BIG-IP iControl REST
CVE-2022-24521	Privilege Escalation Vulnerability	Microsoft Common Log File System Driver
CVE-2022-26134	Remote Code Execution Vulnerability	Atlassian Confluence Server / Data Center
CVE-2022-29464	Arbitrary File Upload Vulnerability	WSO2 API Manager / Identity Server
CVE-2022-41040	Server-Side Request Forgery Vulnerability	Microsoft Exchange Server
CVE-2022-42475	Remote Code Execution Vulnerability	Fortinet FortiOS SSL VPN
CVE-2022-47966	Remote Code Execution Vulnerability	Zoho ManageEngine Products (Apache Santuario)
CVE-2023-20263	Remote Code Execution Vulnerability	Cisco IP Phone 8800 and 7800 Series
CVE-2023-20269	Authentication Bypass Vulnerability	Cisco ASA and FTD Software
CVE-2023-22069	Privilege Escalation Vulnerability	Oracle Database Server
CVE-2023-22515	Authentication Bypass Vulnerability	Atlassian Confluence Server / Data Center
CVE-2023-22518	Improper Authorization Vulnerability	Atlassian Confluence Server / Data Center
CVE-2023-22524	Remote Code Execution Vulnerability	Atlassian Confluence Mobile Plugin
CVE-2023-27532	Information Disclosure Vulnerability	Veeam Backup & Replication
CVE-2023-27997	Remote Code Execution Vulnerability	Fortinet FortiOS and FortiProxy
CVE-2023-28252	Privilege Escalation Vulnerability	Microsoft Common Log File System Driver
CVE-2023-29300	Privilege Escalation Vulnerability	Microsoft Win32k
CVE-2023-34362	SQL Injection Vulnerability	Progress MOVEit Transfer
CVE-2023-3519	Remote Code Execution Vulnerability	Citrix ADC and Gateway
CVE-2023-36884	Remote Code Execution Vulnerability	Microsoft Office and Windows HTML
CVE-2023-38203	Remote Code Execution Vulnerability	Adobe ColdFusion
CVE-2023-38831	Arbitrary Code Execution Vulnerability	WinRAR
CVE-2023-41265	Authentication Bypass Vulnerability	Ivanti EPMM
CVE-2023-41266	Command Injection Vulnerability	Ivanti EPMM
CVE-2023-46604	Remote Code Execution Vulnerability	Apache ActiveMQ
CVE-2023-46747	Remote Code Execution Vulnerability	F5 BIG-IP TMUI
CVE-2023-48365	Remote Code Execution Vulnerability	JetBrains TeamCity

CVE-2023-48788	Remote Code Execution Vulnerability	ConnectWise ScreenConnect
CVE-2023-4966	Information Disclosure Vulnerability	Citrix NetScaler ADC and Gateway
CVE-2024-1708	Improper Access Control Vulnerability	ConnectWise ScreenConnect
CVE-2024-1709	Path Traversal Vulnerability	ConnectWise ScreenConnect
CVE-2024-1800	Improper Authorization Vulnerability	Apple iOS, iPadOS, macOS
CVE-2024-1853	Privilege Escalation Vulnerability	Apple iOS, iPadOS, macOS
CVE-2024-21762	Command Injection Vulnerability	Fortinet FortiOS SSL VPN
CVE-2024-21887	Command Injection Vulnerability	Ivanti Connect Secure / Policy Secure
CVE-2024-23113	Remote Code Execution Vulnerability	Ivanti Connect Secure / Policy Secure
CVE-2024-23897	Arbitrary File Read Vulnerability	Jenkins
CVE-2024-24919	Path Traversal Vulnerability	Check Point Security Gateway
CVE-2024-26169	Privilege Escalation Vulnerability	Microsoft Windows Error Reporting Service
CVE-2024-27198	Authentication Bypass Vulnerability	JetBrains TeamCity
CVE-2024-27199	Authentication Bypass Vulnerability	JetBrains TeamCity
CVE-2024-3400	Command Injection Vulnerability	Palo Alto Networks PAN-OS (GlobalProtect)
CVE-2024-37085	Remote Code Execution Vulnerability	Progress MOVEit Transfer
CVE-2024-40711	Remote Code Execution Vulnerability	Microsoft Windows Hyper-V
CVE-2024-40766	Remote Code Execution Vulnerability	Microsoft Message Queuing (MSMQ)
CVE-2024-4358	Remote Code Execution Vulnerability	Adobe ColdFusion
CVE-2024-4577	Remote Code Execution Vulnerability	PHP CGI (Windows)
CVE-2024-50623	Remote Code Execution Vulnerability	Oracle WebLogic Server
CVE-2024-55956	Remote Code Execution Vulnerability	Cleo Harmony, VLTrader, LexiCom (version < 5.8.0.24)

[表 1: List of Vulnerabilities Related to Ransomware Attacks in 2024]

3. オープンソースおよびフリーウェア

2024 年のランサムウェアグループが攻撃戦術に利用したオープンソースおよびフリーウェアツールの分布を見ると、攻撃者がもはや独自のツールセットにのみ依存せず、既存の広く使用されている公開ツールを組み合わせて利用する傾向が明確に現れている。

全体で最も高い割合である 6%を記録したツールはコバルトストライク（Cobalt Strike）で、元々はペネトレーションテスト用に設計された商用ツールですが、クラック版が広範囲に流布され、様々なサイバー犯罪グループによって積極的に悪用されています。特に、ビーコン（Beacon）を活用した持続的な接続維持、コマンド実行、ファイルのアップロードおよびダウンロード、ラテラルムーブメント（Lateral movement）機能などが精巧に構成されており、侵害後の戦術遂行の中枢ツールとして位置づけられています。

続いて、PsExec（5%）とミミカッツ（Mimikatz）（5%）は、長い間さまざまな攻撃者によって悪用されてきた代表的な Windows ベースのツールである。

PsExec はシステム内部で権限昇格やリモートコマンドの実行を行うことができ、ラテラルムーブメント（Lateral movement）の過程で頻繁に利用され、攻撃者が追加のペイロードを配布または実行するのに役立ちます。

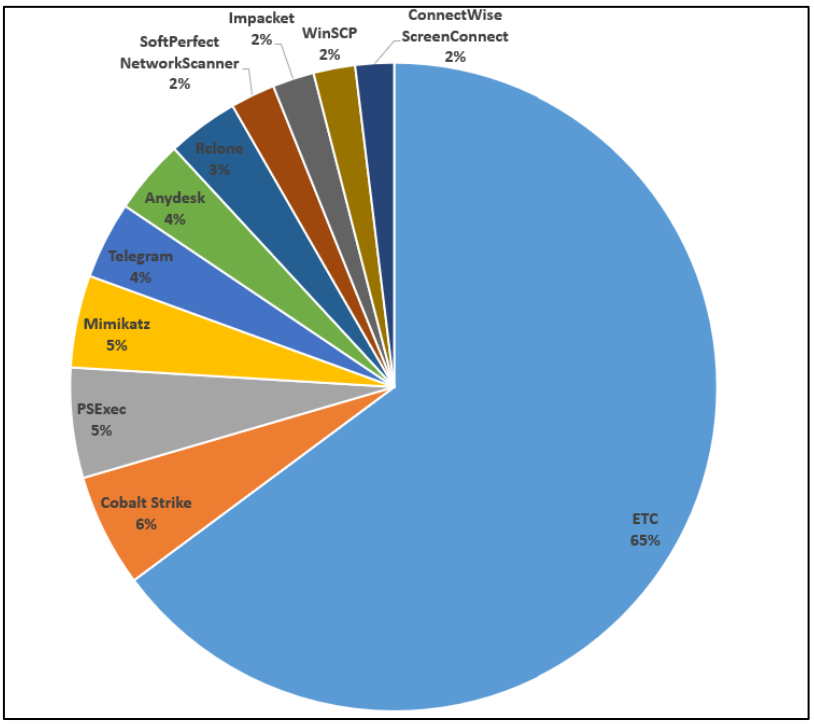
ミミカツは、認証情報のダンプ、トークンの窃取、Kerberos チケットの偽造などの機能を備えたツールで、ドメイン内のアカウント情報を収集し、内部権限の拡大と持続的な制御の確保に非常に効果的に使用されます。両方のツールは合法的なセキュリティ分析の目的にも使用されるため、EDR や検出システムを回避するための偽装戦術と併用されることが多いです。

テレグラム(Telegram)(4%)、アニーデスク(Anydesk)(4%)、Rclone(3%)は、C2 チャネルまたはデータ窃取の過程で利用されるツールであり、攻撃者の隠蔽性とリアルタイム制御能力を同時に満たすことに焦点が当てられています。

テレグラム（Telegram）はアクセスしやすいメッセージングプラットフォームであり、被害者との連絡手段として利用されたり、C2 サーバー手段として利用されたりするようです。メッセージの暗号化とユーザー間の直接通信構造は、検出回避に有利に働き、別途インフラを必要とせずに運用可能である点から、攻撃者が好むツールの一つに分類されます。

AnyDesk は GUI ベースのリモート制御ツールであり、攻撃者が取得した認証情報を使用してシステムにアクセスし、ファイルの閲覧、ディレクトリの探索、コマンドの実行などの操作を行うために使用されます。ユーザーセッション内で実行され、外見上は正常なリモート作業と区別が難しいため、検出が遅れる可能性があります。

Rclone はクラウドベースのストレージサービスと連携して大量のデータを外部に流出させるのに適しており、ログを生成せずにバックグラウンドで実行できるため、追跡を回避するのに有利です。



[図 5: オープンソースおよびフリーウェアの統計]

ツール	ツールの機能
Cobalt Strike	侵入テストフレームワーク
PsExec	Windows リモートコマンド実行ツール
Mimikatz	Windows 認証情報ダンピングツール
Telegram	メッセージングアプリケーション
Anydesk	リモートデスクトップソフトウェア
Rclone	クラウドファイル同期ツール
SoftPerfect NetworkScanner	ネットワーク情報スキャンツール
Impacket	プロトコルパケット作成・送信ツール
WinSCP	SFTP ベースのファイル転送ツール
ConnectWise ScreenConnect	リモートデスクトップソフトウェア

[表 2: オープンソースとフリーウェアのトップ 10]

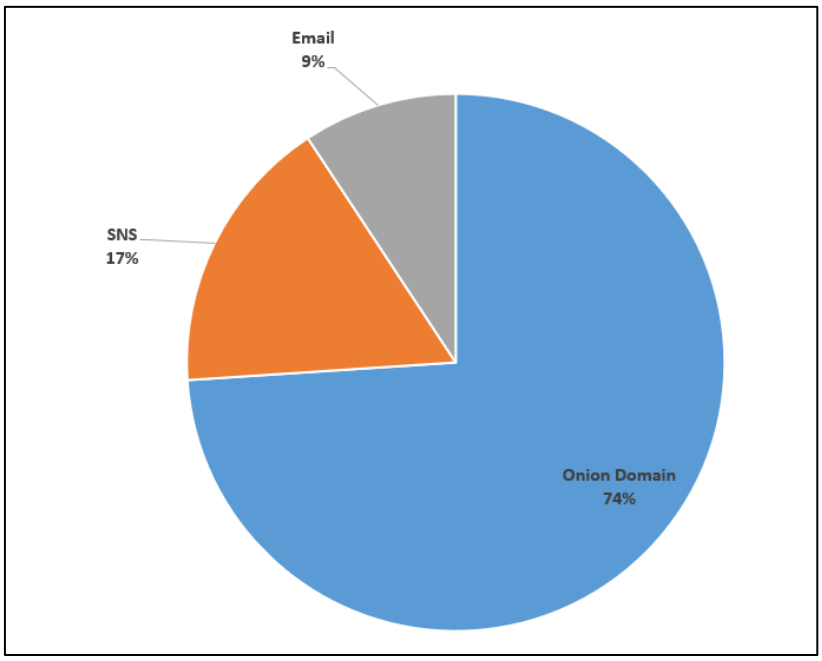
攻撃者のデジタル運用資産

攻撃者は被害者がランサムウェア感染の事実を認識し、復号化費用を支払えるように、感染システム内にランサムノート（Ransom Note）を生成します。このランサムノートには通常、攻撃者との連

絡手段、復号化費用の支払い方法、そして暗号通貨ウォレットアドレスなどのデジタル運用資産情報が含まれています。
本報告書では、攻撃者のデジタル運用資産を連絡網、送金手段、運用チャネルなどに分類し、攻撃者がランサムウェア活動を管理したり金銭的要求を実行する際に使用したネットワークおよび金融情報を中心に分析しました。

1. 攻撃者運用インフラ

2024 年、ランサムウェアグループが被害者との交渉、情報漏洩、金銭要求などに利用した運用インフラのタイプを分析した結果、オニオンドメイン（Onion Domain）に基づくインフラの絶対的な利用度が明確に示された。
全体の事例のうち 74%を占めたこのタイプは、Tor ネットワーク上でアクセス可能なドメイン、すなわちダークウェブ（Dark Web）インフラを意味し、攻撃者の立場から位置の隠蔽性、アクセス制御、追跡回避の面で最適化された特性を提供します。
これらのドメインは、被害者専用の交渉ページ、流出情報掲載サイト、支払い案内ページなどとして定型化されて使用され、多くの被害者は攻撃直後にその onion サイトへのアクセスを誘導されるのが一般的です。いくつかのグループは追跡を回避するために、複数ドメインの運用や定期的なドメインの変更方法を採用することもあります。
一方、SNS（ソーシャル・ネットワーキング・サービス）基盤のインフラは全体の 17%を占めており、一部のランサムウェアグループが運営インフラの補完手段として選択する事例と解釈される。Telegram、Twitter（X）、Mastodon、VK などの主要プラットフォームは、独自のインフラがなくてもアカウントを開設するだけで情報の投稿が可能である点から、簡便性とアクセス性の面で利点を提供する。これらの SNS チャンネルは、被害事実に関する簡単な言及や通知、または攻撃グループの一般的な主張やメッセージ伝達などの用途で利用される場合があり、迅速な露出が必要な状況で補助的な情報流通の窓口として限定的に使用される傾向が見られる。
一方、メールベースのインフラの活用割合は 9%に過ぎないことが明らかになった。これは、ランサムウェアグループが直接的な交渉経路としてメールを選択するケースが限られていることを意味し、全体の戦術構造内で主要なチャネルではなく補助的な用途で使用されていることを示唆している。メールは技術的に構築が簡単で、対象に合わせた配信が可能という利点があるが、相対的に接触可能性の不確実性、インフラ運用の持続性不足、一貫した交渉フローの維持の難しさなど、多くの実務的制約が存在する。特に、組織内部で受信されたメールへのアクセス権が制限されている場合や、メッセージがフィルタリングまたは内部プロセスによって遅延する可能性があるため、被害者の迅速な反応を促すには適していないチャネルと見なされていると分析されている。



[図 6: インフラの種類]

1) オニオンドメイン

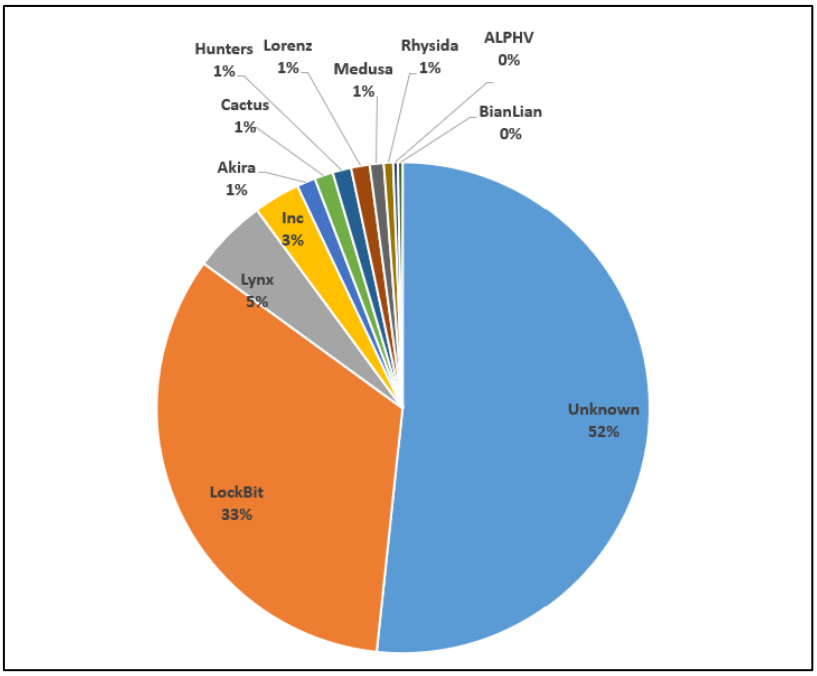
2024 年のランサムウェアグループのオニオンドメインを基盤とした運用インフラを分析した結果は、実際のランサムウェアハッキング活動で使用されたオニオンドメインアドレスを基準にグループ名を識別する方式で導き出された。

本分析は、各ドメインのページ構造、漏洩情報の掲載形式、交渉メッセージの言語と構成、運営スケジュールなどの定性的要素を総合的に検討し、該当ドメインが特定のグループに属するかどうかを判断する手続きを経ました。明確な識別子がないまま運営されている場合や、グループ間の類似性が高く判別が難しい場合には「Unknown」と分類されました。

その結果、運営主体が明確に識別できない、または技術的分析だけでは追跡が難しいドメインが全体の半分以上を占めることが判明し、全体の分析対象ドメインのうち 52%が「Unknown」と分類されました。これは、攻撃インフラの識別が単一の基準では難しいこと、そして一部のドメインが固定されたグループ名やシグネチャなしで運営されている特性と関連しています。

一方、識別が明確に行われたグループの中では、LockBit が最も顕著な割合を占めていました。全体のドメインの 33%を占有する LockBit は、2020 年に活動を開始して以来、様々なバージョンのアップデートを通じて技術的高度化と運営の精緻化を続けてきた代表的なランサムウェアグループです。彼らは、オニオンドメインを基盤とした流出データ公開ポータルや、被害者専用の交渉ページなどを独立した構成要素として体系化して活用しており、これを通じて被害者の応答率を高め、交渉の圧力水準を調整する戦略を実行しています。特に LockBit は RaaS モデルを基盤に、多数のパートナー攻撃者がそれぞれ異なる侵入手段、交渉方式、流出戦術を個別に適用できるよう支援しており、一つのグループが運営する単一ドメイン内でも異なる攻撃様相が現れる特徴を持っています。

これ以外にも、Lynx（5%）と Inc（3%）は全体の中でそれぞれ中位レベルの割合を占めるグループとして現れた。両グループとも上位グループに比べると活動割合は低いが、一定水準以上の攻撃頻度を示し、統計に含まれている点で注目する必要がある。



[図 7: オニオンドメインアドレスに基づくランサムウェアグループの分布状況]

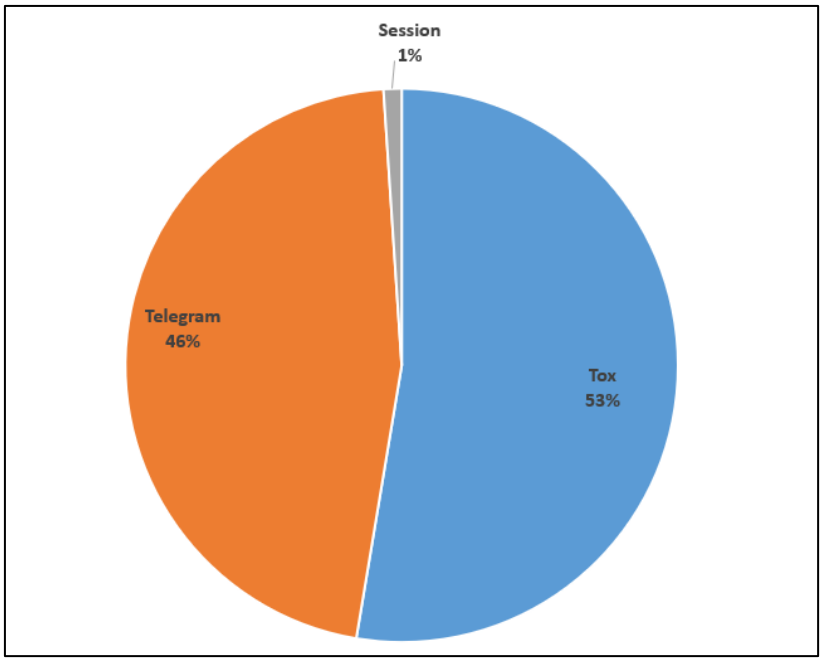
2) ソーシャルメディア

2024 年、ランサムウェア組織が被害者との交渉、コミュニケーション、支払い案内などに利用したメッセンジャープラットフォームの分布を見てみると、匿名性とセキュリティを両立する経路を優先的に選択する傾向が見られます。最も高い割合を占めたメッセンジャーはトックス（Tox）で、全体の 53%を記録しました。Tox は中央サーバーを経由せず、ユーザー間で直接接続される P2P（ピア・ツー・ピア）方式で動作し、アカウント作成時に電話番号やメールアドレスの入力が不要で、メッセージ履歴もサーバーに保存されないため、高いレベルの匿名性と追跡回避性を提供します。

2 番目に高い割合を示したプラットフォームはテレグラムで、全体の 46%を占めました。テレグラムはメッセンジャー機能のほかに、チャンネル運営、ファイル共有、ボット連携など多様な機能を提供しており、交渉手段だけでなく、流出情報の公開や内部通知などにも使用されています。テレグラムはデスクトップとモバイルの両方でアクセスしやすく、非公開チャットの開設やメッセージの自動削除などの機能も備えているため、攻撃者にとって有用なツールとして活用されています。

一方、セッション(Session)メッセンジャーは全体の 1%と非常に低い割合を示しました。セッションはシグナル(Signal)プロトコルを基に、トーア(Tor)ネットワークを組み合わせたメッセンジャーで、IP の露出を防ぎ、ユーザー識別子を非公開にする機能を提供します。

このような分布は、攻撃者が単に匿名性だけを考慮しているのではなく、運用の安定性、被害者へのアクセス性、機能性などを総合的に考慮してメッセンジャープラットフォームを選択していることを示している。



[図 8: ランサムウェアグループが活用したソーシャルメディア]

3) メールアドレス

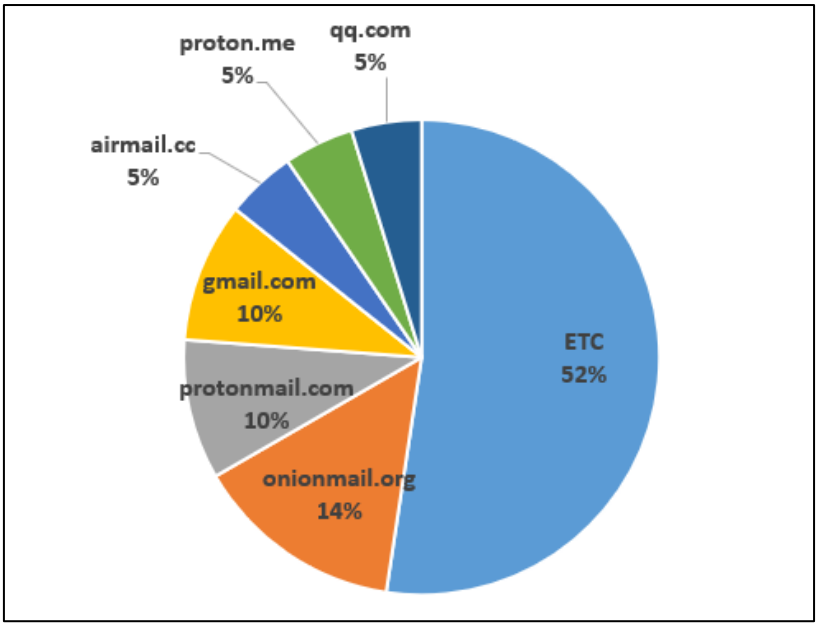
2024 年にランサムウェア組織が被害者との連絡手段として使用したメールドメインの分布を見てみると、特定のサービスに集中するのではなく、匿名性、アクセスのしやすさ、運用の利便性などを考慮して、様々なドメインを併用する傾向が確認されます。

最も高い割合を占めたメールドメインは「onionmail.org」で、全体の 14%を記録しました。該当ドメインはアカウント作成時に身元確認手続きがなく、メールサーバーの運営主体が比較的不明確であるため、攻撃者が匿名性を維持できるという特徴があります。

その後に続くドメインは protonmail.com と gmail.com で、それぞれ 10%の割合を示しました。ProtonMail はエンドツーエンドの暗号化機能を提供し、匿名での登録が可能であるため、攻撃者のコミュニケーション手段としてよく利用されています。一方、Gmail は広範な使用率と知名度、広く使用されているメールアドレスであることから、検出回避や被害者の信頼を得る手段として使用される事例が観察されています。

以下のドメインもそれぞれ 5%ずつ出現しました：airmail.cc、proton.me、qq.com。Airmail は登録手続きが簡単で匿名アカウントの使用が可能です。proton.me は Proton サービスの新しいドメインで、同じセキュリティ構造を持っています。qq.com は中国を拠点とするメールサービスで、一部

の攻撃者が別途登録手続きなしでアカウントを作成したり、既存のアカウントを利用して被害者との連絡手段として使用したと考えられます。
一方、その他（ETC）ドメインが全体の 52%を占め、最も大きな割合を占めました。該当項目には、独自ドメインを基にした自社メール、非標準メールサーバー、一時的なメールアドレスなどが含まれると見られ、識別が難しいドメインの使用が徐々に増加している様子です。これは、攻撃者が匿名性の維持とセキュリティ検知の回避を目的に、メールドメインを多様化していることを示しています。

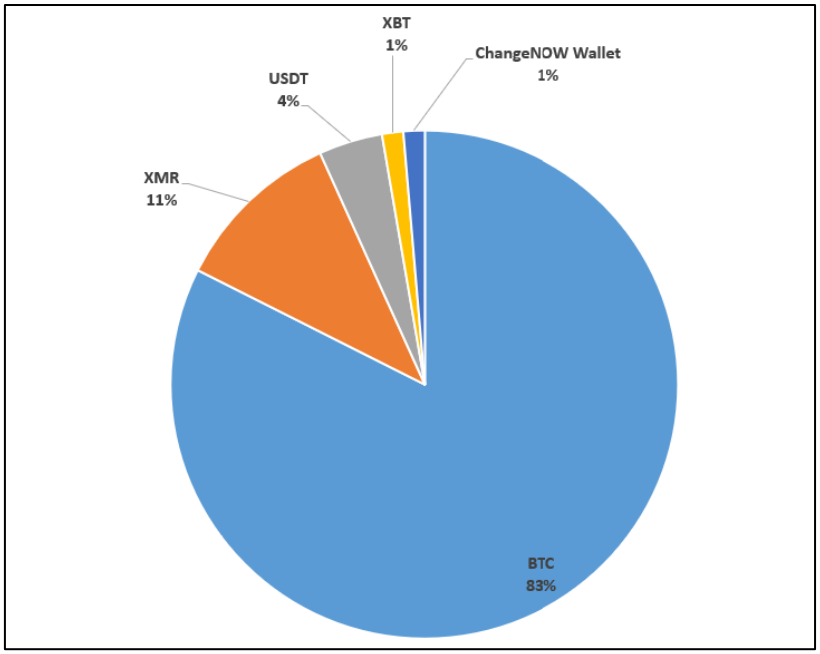


[図 9: ランサムウェア攻撃者のメールドメインアドレス]

2. 暗号通貨

2024 年基準でランサムウェアグループが被害者に復号化の代価として要求した暗号通貨の分布を見ると、ビットコイン（BTC）の使用割合が 83%で最も高くなっていることがわかりました。
ビットコインは、グローバルな流通性と取引所へのアクセスのしやすさ、被害者側の認知度が高いため、一般的な支払い手段として利用されています。
モネロ（XMR）は全体の 11%を占めており、リング署名、ステルスアドレス、コンフィデンシャルトランザクションなどの匿名性技術が適用された暗号通貨で、送信者や受信者のウォレットアドレスや取引金額が外部に露出しない構造を持っています。このような特性により、一部のグループは XMR を単独で要求したり、BTC と併用して使用しています。特に交渉中に支払い手段を変更したり、特定の条件で選択肢として案内する方法が確認されました。
USDT は全体の 4%を記録しており、米ドルに固定された価値を持つステーブルコインという特性上、金額換算が明確で価格変動による混乱を減らせる点で選ばれた事例が存在します。

XBT(1%)はビットコインの通貨コードであり、一部のサービスでは BTC と同様に使用されます。ChangeNOW Wallet（1%）は、多数の暗号通貨を受け取ることができる両替プラットフォームベースのアドレスであり、特定の資産に限定されない支払い方法を考慮した構成に見えます。このような分布は、匿名性、両替の利便性、被害者へのアクセス性など、さまざまな要素が支払い手段の選択に影響を与えていることを示しており、単一通貨の要求よりも状況に応じた並行または選択的な暗号通貨の使用が継続的に確認されています。



[図 10: 暗号通貨の統計]

結論

2024 年のランサムウェア攻撃は、技術構成要素、運用方式、インフラ活用など様々な側面で構造化された様相を示しました。攻撃者は単一のアプローチや単純な暗号化行為にとどまらず、初期侵入から交渉や金銭要求までの全過程を体系的に実行しました。これは各戦術が独立した単位ではなく、相互に連携した戦略的手続きとして機能していることを示しています。

攻撃対象は特定の産業や国に限定されず、広範囲に設定されており、その中でも特に医療、製造業、金融、公共行政部門で高い割合が確認されました。

国別では、アメリカ、ドイツ、フランス、カナダなどの事例が相対的に多く、それ以外にも様々な国で被害が発生し、地政学的な境界を超える攻撃の様相が明らかになった。これは、標的の選定が復旧の感度、情報資産の価値、セキュリティインフラのレベルなど、様々な要素を総合的に考慮して決定された可能性を示唆している。

侵入段階では、有効なアカウントの使用頻度が最も高く、これは攻撃者が認証手続きを回避して合法的なユーザーのように内部システムにアクセスする方法が戦術的に有利であることを反映しています

。これに加えて、公開アプリケーションの脆弱性、添付ファイル・リンクを基にしたスピアフィッシング、リモートアクセスツール（RDP、VPN など）の悪用も併用され、外部資産やユーザーの行動に依存する侵入経路が多数活用されました。
侵入後、Cobalt Strike、PSExec、Mimikatz、Rclone などのツールが繰り返し使用され、Telegram、AnyDesk、Tox は内部制御および攻撃者と被害者間の通信手段として共に活用されました。
攻撃者はデータ流出および交渉のために.onion ドメインを基盤としたダークウェブインフラを構築し、流出掲示サイトと支払い案内ページを運営しました。被害者との直接交渉には、テレグラムまたはトックスメッセンジャーが使用され、一部のケースでは SNS チャンネルを通じて流出の事実を外部に知らせたり予告する方法が確認されました。メールは補助的な連絡手段として限定的に活用され、全体のインフラは匿名性の確保、情報流通の制御、心理的圧迫の誘導という目的に合わせて構成されていました。
決済手段としてはビットコインが最も広く使用されており、一部の攻撃者は匿名性が強化されたモネロや為替変動がないテザーを併せて要求することもありました。被害者に馴染みのある決済手段を最初に案内した後、特定の条件に応じて暗号通貨の交換を要求する方法も一部の事例で確認されました。
このような点を総合すると、2024 年のランサムウェア攻撃は、単発的な侵害行為ではなく、侵入、内部活動、交渉、支払いに至るすべての過程を包括する組織的な構造で機能しています。各段階は個別の実行ではなく、戦略的な流れの中で有機的に結びついており、これは完結した犯罪モデルとしての機能を備えた脅威のタイプであることを示しています。したがって、今後の対応戦略の策定においては、技術的な防御とともに攻撃者の運用構造に対する体系的な理解が並行して行われるべきです。

ランサムウェア事故事例

2024 年に大衆メディアを通じて知られたランサムウェア事故の事例は約 20 件と確認されている。

1. 2024年1月の事故事例

Cybercriminals Target Toronto Zoo in Massive Data Breach
https://nationalcioreview.com/articles-insights/extra-bytes/cybercriminals-target-toronto-zoo-in-massive-data-breach/
2024 年 1 月、カナダのトロント動物園が Akira ランサムウェアグループの攻撃を受けました。これにより、1989 年から在職している現職および元職員、一部のボランティアの社会保障番号、生年月日、住所、電話番号などの機密個人情報が流出しました。また、2000 年から 2023 年 4 月までに入場券やメンバーシップを購入した訪問者と会員の名前、メールアドレス、住所、電話番号、クレジッ

トカードの最後の 4 桁と有効期限などの取引情報も含まれていました。さらに、数十年にわたって蓄積された野生動物保護研究データが失われ、動物園の研究活動に深刻な打撃を与えました。

January 2024 Cyberattack on Lurie Children's Hospital Affects 792K Individuals
https://www.hipaajournal.com/january-2024-cyberattack-on-lurie-childrens-hospital-affects-792k-individuals/
2024 年 1 月、アメリカのシカゴに位置する Ann & Robert H. Lurie Children's Hospital がランサムウェア攻撃を受けました。これにより、電子健康記録システム（EHR）や MyChart 患者ポータルなどの主要な IT システムが停止し、約 79 万 2 千人の患者の個人情報が流出する被害が発生しました。病院は手動記録手続きに切り替えて診療を続け、システムの復旧には約 4 か月を要しました。

Ransomware Attack Cost LoanDepot $27 Million
https://www.securityweek.com/ransomware-attack-cost-loandepot-27-million/
2024 年 1 月、アメリカのモーゲージ貸付業者 LoanDepot が ALPHV/BlackCat ランサムウェアグループの攻撃を受けました。これにより、約 1,690 万人の顧客の名前、生年月日、住所、メールアドレス、電話番号、社会保障番号、金融口座情報などの機密個人情報が流出し、オンラインアカウントへのアクセスと支払いサービスが数週間中断される被害が発生しました。会社はこの事件により約 2,700 万ドルの費用を支出し、被害を受けた顧客に対して 2 年間の信用モニタリングおよび身元盗難防止サービスを提供しました。

The Veolia Ransomware attack in early 2024
https://sigasec.com/the-veolia-ransomware-attack-in-early-2024/
2024 年 1 月、アメリカの水および廃水処理企業である Veolia North America が Black Basta ランサムウェアグループの攻撃を受けました。この攻撃により、Municipal Water 部門のバックエンドシステムとサーバーが停止し、一部の顧客がオンライン料金支払いシステムの利用に遅延を経験しました。また、少数の個人情報が流出し、流出したデータにはパスポート、運転免許証のスキャン、人的資源関連文書、法人車両リース文書などが含まれていました。Veolia は即座に防御措置を講じ、法執行機関および第三者のフォレンジック専門家と協力して事件を調査しています。水および廃水処理の運営には影響がなかったと発表しました。

2. 2024年2月の事故事例

Ransomware attack has cost UnitedHealth $872 million; total expected to surpass $1 billion
https://therecord.media/ransomware-unitedhealth-costs-billions-still-climbing

2024 年 2 月、アメリカの医療保険企業である UnitedHealth Group の子会社、Change Healthcare が ALPHV/BlackCat ランサムウェアグループの攻撃を受けました。これにより、保険請求および決済システムが停止し、アメリカ全土の医療サービス提供者が深刻な運営の混乱を経験し、患者は薬の処方や診療を受けるのに困難を感じました。また、約 1 億 9 千万人の患者個人情報が流出し、アメリカ史上最大規模の医療データ流出事件として記録されました。この事件により、UnitedHealth Group は 2024 年の 1 年間で約 309 億ドルの損失を被りました。

How the ransomware attack at Change Healthcare went down: A timeline
https://techcrunch.com/2025/01/27/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/
2024 年 2 月、アメリカのヘルスケア技術企業である Change Healthcare を対象に、ALPHV/BlackCat ランサムウェアグループの攻撃が発生しました。これにより、保険請求および決済システムが停止し、アメリカ全土の医療サービス提供者が深刻な運営の支障をきたし、患者は薬の処方や診療を受けるのに困難を経験しました。また、約 1 億 9 千万人の患者個人情報が流出し、アメリカ史上最大規模の医療データ流出事件として記録されました。

3. 2024年3月の事故事例

Panera Bread likely paid a ransom in March ransomware attack
https://www.bleepingcomputer.com/news/security/panera-bread-likely-paid-a-ransom-in-march-ransomware-attack/
2024 年 3 月、アメリカのファーストフードチェーンであるパネラブレッドを対象にランサムウェア攻撃が発生しました。これにより、内部 IT システム、電話、POS システム、ウェブサイト、モバイルアプリなどの主要システムが 1 週間にわたり停止し、電子決済やメンバーシップポイントの積み立てが不可能になるなど、店舗運営に深刻な支障が生じました。また、現職および元職員の名前や社会保障番号などの機密性の高い個人情報が流出し、パネラブレッドはハッカーからデータを削除するという保証を受けて身代金を支払ったとされています。

Hoya Corporation: Ransomware Attack Timeline
https://www.cm-alliance.com/cybersecurity-blog/hoya-corporation-ransomware-attack-timeline
2024 年 3 月末、日本の光学製品メーカーである Hoya Corporation を対象にランサムウェア攻撃が発生しました。この攻撃は Hunters International グループによって行われ、約 2TB に及ぶデータ（約 170 万件のファイル）が盗まれました。これにより、Hoya の生産および注文処理システムが停止し、一部の事業部門で IT システム障害が発生しました。攻撃者はデータの復号化と流出防止を条

件に、1,000 万ドルの身代金を要求しました。また、約 6,500 件の従業員および家族の個人情報が流出し、そこには従業員番号、名前、銀行口座情報、給与データ、身分証情報などが含まれていました。

VNDirect cyberattack causes big splash on stock market

https://vir.com.vn/vndirect-cyberattack-causes-big-splash-on-stock-market-109873.html

2024 年 3 月、ベトナムの証券会社 VNDirect を対象にランサムウェア攻撃が発生しました。これにより、オンライン証券取引システムが停止し、ハノイおよびホーチミン証券取引所は VNDirect のデリバティブおよび債券取引を一時的に中断しました。この事件により、VNDirect の株価が約 4%下落し、ホーチミン証券取引所の取引量が 10%減少するなど、金融市場に影響を与えました。

4. 2024年4月の事故事例

Snowflake Data Breach: What Happened and How to Prevent It

https://www.strongdm.com/what-is/snowflake-data-breach

2024 年 4 月から 6 月の間に、クラウドデータプラットフォームであるスノーフレーク（Snowflake）を使用する約 165 の組織を対象に大規模なサイバー攻撃が発生しました。この攻撃はサイバー犯罪グループ UNC5537（別名 ShinyHunters）によって行われ、情報窃取型のマルウェアを通じて収集されたアカウント情報を利用し、多数の顧客アカウントに不正アクセスが行われました。その結果、Ticketmaster、Santander Bank、Advance Auto Parts、Neiman Marcus などの主要企業の顧客データが流出し、流出したデータはダークウェブで販売されました。特に Ticketmaster の場合、5 億 6 千万件の顧客情報が流出し、イベントおよびチケットサービスに支障をきたしました。

MediSecure breach: implications for health care services and patients

https://insightplus.mja.com.au/2024/37/medisecure-breach-implications-for-health-care-services-and-patients/

2024 年 4 月、MediSecure を対象にランサムウェア攻撃が発生しました。これにより、約 1,290 万人の個人および医療情報が流出し、会社は財政的な困難の末に清算手続きを進める被害が発生しました。

5. 2024年6月の事故事例

Synnovis cyber attack – statement from NHS England

https://www.england.nhs.uk/2024/06/synnovis-cyber-attack-statement-from-nhs-england/

2024 年 6 月、イギリスのロンドン南東部地域にある NHS 病院を対象にランサムウェア攻撃が発生しました。この攻撃は、病院の病理学検査サービスを提供する Synnovis を標的にしました。その結果、King's College Hospital や Guy's and St Thomas' NHS Foundation Trust などで 1,600 件以上の手術と外来診療がキャンセルされ、血液検査や輸血サービスにも深刻な支障が生じました。また、患者の名前、生年月日、NHS 番号、検査履歴などの機密個人情報が流出し、ダークウェブに公開されました。このような被害により、NHS は患者に対し、緊急でない場合は病院訪問を控えるよう要請しました。

CDK Global Ransomware: What Happened and How It Impacted Businesses
https://www.blackfog.com/cdk-global-ransomware-attack/
2024 年 6 月、北米地域の約 15,000 の自動車ディーラーにサービスを提供する CDK Global が BlackSuit ランサムウェア攻撃を受けました。これにより、ディーラー管理システム（DMS）、顧客関係管理（CRM）ツールなどの主要システムが麻痺し、多くのディーラーが手作業に切り替えるなど、運営に深刻な支障が生じました。また、CDK Global は攻撃者に約 2,500 万ドル相当のビットコインを支払ったとされており、これにより約 6 億ドル以上の経済的被害が発生しました。

Indonesia won’t pay an $8 million ransom after a cyberattack compromised its national data center
https://apnews.com/article/indonesia-ransomware-attack-national-data-center-213c14c6cc69d7b66815e58478f64cee
2024 年 6 月、インドネシアの仮設国家データセンター（PDN）を対象に Brain Cipher ランサムウェア攻撃が発生しました。これにより、200 以上の中央および地方政府機関のデジタルサービスが中断され、特に主要空港の自動出入国審査システムが麻痺し、手動検査が行われるなどの混乱が生じました。攻撃者は約 800 万ドルの身代金を要求しましたが、インドネシア政府はこれを支払わずに対応しました。その後、ハッカーグループは謝罪とともに復号キーを無料で提供しました。この事件は、インドネシア政府のサイバーセキュリティ体制の不備とバックアップシステムの不足を露呈する契機となりました。

Cleveland City Hall confirms it was hit with ransomware attack
https://www.cleveland.com/metro/2024/06/cleveland-city-hall-confirms-it-was-hit-with-ransomware-attack.html
2024 年 6 月、アメリカのオハイオ州クリーブランド市庁舎を対象にランサムウェア攻撃が発生しました。これにより、市庁舎と一部の市庁部門が約 2 週間閉鎖され、出生・死亡証明書の発行、建築許可、各種市民サービスなどの重要な行政サービスが中断される被害が発生しました。クリーブランド市はランサム要求に応じず、FBI とオハイオ州防衛軍サイバー予備軍の支援を受けてシステム復旧作業を進めました。市庁舎は 6 月 20 日から限定的に市民サービスを再開しました。

6. 2024年7月の事故事例

OneBlood Notifies Individuals Affected by July 2024 Ransomware Attack

https://www.hipaajournal.com/oneblood-ransomware-attack/

2024 年 7 月、アメリカのフロリダに本社を置く非営利の血液寄付機関である OneBlood がランサムウェア攻撃を受けました。これにより、IT システムが中断され、血液の収集、検査、配布作業が手動に切り替わり、約 350 の病院への血液供給が遅延し、病院は緊急血液不足プロトコルを実施しなければなりませんでした。また、攻撃者は寄付者の名前や社会保障番号などの機密個人情報を含むデータを盗みました。OneBlood は被害者に対して 12 ヶ月間のクレジットモニタリングおよび身元盗難防止サービスを提供しました。

7. 2024年10月の事故事例

CASIO Ransomware Attack

https://www.loughtec.com/casio-cyber-attack

2024 年 10 月、日本の電子機器メーカーであるカシオを対象に Underground ランサムウェアグループの攻撃が発生しました。これにより、約 8,500 人の従業員、ビジネスパートナー、顧客の個人情報が流出し、内部システムが一時的に停止する被害が発生しました。流出した情報には、従業員の名前、メールアドレス、生年月日、家族情報、税識別番号などが含まれており、顧客の場合は配送先住所、電話番号、購入履歴などが含まれていました。カシオは身代金の要求に応じず、日本の個人情報保護委員会および海外の規制機関にこの事件を報告しました。また、被害者に個別に連絡し、状況を案内しています。

8. 2024年11月の事故事例

Starbucks forced to pay its baristas manually because of a ransomware attack on third-party software

https://edition.cnn.com/2024/11/25/tech/starbucks-ransomware-attack

2024 年 11 月、スターバックスを対象にランサムウェア攻撃が発生しました。これにより、従業員の勤務スケジュール管理や給与処理システムに障害が発生し、手作業に切り替えるなど、一部の運営上の不便が生じました。

Schneider Electric data breach by Hellcat Ransomware Gang

https://www.sangfor.com/blog/cybersecurity/schneider-electric-data-breach-hellcat-ransomware-gang

2024 年 11 月、フランスのエネルギー管理および自動化企業であるシュナイダーエレクトリック（Schneider Electric）を対象に Hellcat ランサムウェアグループの攻撃が発生しました。これにより約 40GB のデータが流出し、攻撃者は 12 万 5 千ドルの身代金を要求しました。

9. 2024年12月の事故事例

Brain Cipher Ransomware Attack: Alleged 1TB Data Breach at Deloitte UK

https://www.sangfor.com/blog/cybersecurity/brain-cipher-ransomware-attack-deloitte-uk-1tb-data-breach

2024 年 12 月、イギリスの会計およびコンサルティング企業であるデロイト UK を対象に、Brain Cipher ランサムウェアグループによる攻撃が発生しました。これにより約 1TB の圧縮データが盗まれ、攻撃者はセキュリティプロトコル違反の証拠、顧客契約書、内部セキュリティツールの情報を含むデータを公開すると脅迫しました。デロイトは、この事件が自社のシステムではなく外部の顧客システムに関連していると主張し、自社のシステムは影響を受けていないと述べました。

Recommendation

NSHC ThreatRecon チームは様々な目的のハッキンググループ(Threat Actor Group) 活動を分析し、組織内部のセキュリティチームがハッキング活動における被害をさらに減らせるように共通的に確認できる攻撃技術(technique)における MITRE ATT&CK の脅威緩和(Mitigations)項目を次のようにまとめた。

1. 脆弱性保護（Exploit Protection)

ソフトウェアのエクスプロイト(Exploit)発生を誘導したり、発生の可能性を探知及びブロックするために脆弱性保護(Exploit Protection)のソリューション使用の検討が必要

- エクスプロイト(Exploit)の動作の緩和のため、 WDEG(Windows Defender Exploit Guard)及び EMET(Enhanced Mitigation Experience Toolkit)の使用の検討が必要
- エクスプロイトのトラフィックがアプリケーションに辿り着くことを防止するため、Web アプリケーションのファイアウォール使用の検討が必要

2. 脆弱性のスキャニング（Vulnerability Scanning)

外部に漏出したシステムの脆弱性を定期的に検査し、致命的な脆弱性が見つかった場合、速やかにシステムをパッチする手続きの検討が必要

- 潜在的に 脆弱なシステムを新たに識別するため、定期的な内部ネットワークの検査の検討が必要
- 公開となった脆弱性における持続的なモニタリングの検討が必要
- 実際のハッキンググループ(Threat Actor Group)が使用した脆弱性におけるセキュリティ強化案件の検討が必要
- このレポートの“Appendix”には実際の 実際のハッキンググループ(Threat Actor Group)が使用した履歴がある脆弱性の情報が含まれている

3. セキュリティ認識教育（User Training)

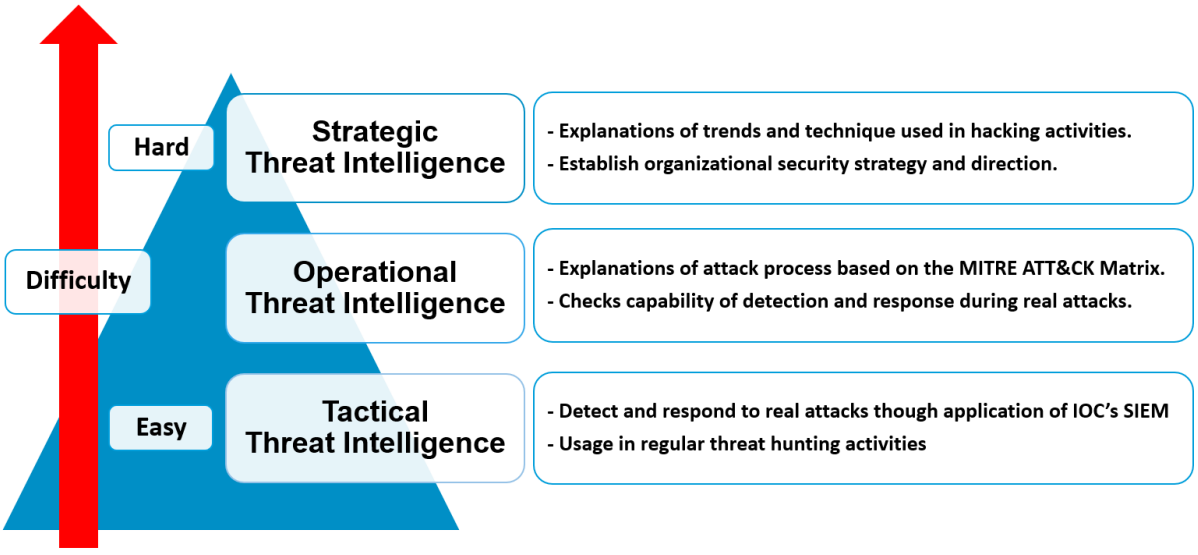
実際のハッキング及び侵害事故の事例を通じて注意すべきの状況について全社員が認知できるようにセキュリティ認識教育の検討が必要

- ソーシャルエンジニアリング(Social Engineering)技法とスピアフィッシング(Spear Phishing)E-Mail を識別できる教育の検討が必要

- ユーザーと管理者が多数のアカウントに同一なパスワードを使用しないように資格証明情報の管理の重要性における教育の検討が必要
- システムに保存したパスワードの危険性における教育の検討が必要
- リポジトリにデータを保存する時に注意すべきの事項における教育の検討が必要
- ブラウザの悪性の拡張プログラムが実行されないようにブラウザ管理における教育の検討が必要
- SMS、通話履歴、連絡先リストなどの敏感な情報のアクセス権限を要請する Android アプリケーションについて注意喚起できるような教育の検討が必要
- 非公式ページからアプリケーションをダウンロードしないように教育の検討が必要

4. 脅威インテリジェンスプログラム(Threat Intelligence Program)

ハッキンググループが使用しているマルウェアハッシュ(Hash)、IP 及びドメイン(Domain)情報を含む IOC(Indicator of Compromise)が見つかった場合、通知を送信するように探知の設定の検討が必要



- IPS、IDS 及びファイアウォールのようなネットワークセキュリティ装備のログから IOC と同一な通信 IP が見つかった場合
- 組織内部の DNS サーバー、ウェブゲートウェイ(Web Gateway)及びプロキシ(Proxy)ウェブ関係のシステムのログから IOC と同一なドメインが見つかった場合
- EDR(Endpoint Detection and Response)のようなエンドポイントセキュリティソリューションのログから PC 及びサーバーから IOC と同一なファイルハッシュ(Hash)が存在する場合

- 組織内部の様々なシステムのログを収集する SIEM(Security Information Event Management)から設定したユーズケース(Use Case)とルール(Rule)に IOC と同一なファイルハッシュ、IP 及びドメインが存在する場合*

5. ネットワークにおける脅威緩和

1) ネットワーク侵入防止（Network Intrusion Prevention)

組織のネットワークにアクセスする悪意的なトラフィックを事前にブロックするために侵入探知システム(Intrusion Detection System, IDS)及び侵入防止システム(Intrusion Prevention System, IPS)の使用の検討が必要

- ネットワークレベルからハッキンググループの攻撃活動を緩和するため AitM(Adversary in the Middle)のトラフィックパターンが識別できる侵入探知システム(Intrusion Detection System, IDS)及び 侵入防止システム(Intrusion Prevention System, IPS)の使用の検討が必要
- マルウェアが組織の内部ネットワークにアクセスしたり実行したりすることを防止するため、ホスト型の侵入防止システム(HIPS, Host Intrusion Prevention System)、アンチウイルス(Anti-Virus)などのソリューションの使用の検討が必要

2) ネットワーク細分化（Network Segmentation)

組織の重要なシステム及び資産を隔離するため、ネットワークを物理的及び論理的ネットワークで分割し、セキュリティコントロール及びサービスがそれぞれの下位のネットワークごとに提供できるようにネットワーク細分化(Network Segmentation)の使用の検討が必要

- DMZ(Demilitarized Zone)及び別のホスティングインフラを使用して外部/内部ネットワークを分離する政策の使用の検討が必要
- ハッキンググループのターゲットになりやすい組織の重要なシステム及び資産を識別し、無断アクセス及び変造から該当のシステムを隔離し、保護する政策の使用の検討が必要
- ネットワークのファイアウォールの構成から必要なポートとトラフィック以外は通信できないようにブロックする政策の検討が必要
- ネットワークプロキシ、ゲートワイ及びファイアウォールを使用して内部システムにおける直接的な遠隔アクセスを拒否する政策の使用の検討が必要
- 侵入の探知、分析及び対応システムは別のネットワークから運営するように検討が必要

6. ユーザーアカウントの脅威緩和

1) 多要素認証 (Multi-factor Authentication)

組織の資産にアクセスできるパスワードが漏洩された場合＝にもハッキンググループがアクセスすることを防止するため、複数の段階で認証段階を構成する多要素認証(MFA, Multi-Factor Authentication)の使用の検討が必要

2) アカウント使用政策 (Account Use Policies)

アカウントのセキュリティ設定に関した政策設定の検討が必要

- 企業の内部から業務用として活用している Windows PC のログインユーザーアカウントのパスワードを英語のアルファベットの大文字、小文字及び記号を含んでなるべく 8 桁以上で設定するように検討が必要
- Windows のアクティブディレクトリ(Active Directory)として構成された環境では、グループ政策(Group Policy)通じて企業の内部ネットワークに繋がる Windows PC のゆーあーアカウントのパスワードを英語のアルファベットの大文字、小文字及び記号を含んでなるべく 8 桁以上で設定するように構成し、3 か月ごとにパスワードが変更されるように政策使用の検討が必要
- 承認済みではないデバイスもしくは外部の IP からログインを防ぐよう、条件付きアクセス政策使用の検討が必要
- パスワードが推測されることを防ぐため、いくつかの回数のログイン失敗のあと、アカウントを凍結する政策使用の検討が必要

3) 特権アカウント管理 (Privileged Account Management)

アカウント資格証明によるリスクを最少化するため、管理者のアカウント及び権限が割り当てられた一般アカウントに関しての管理の検討が必要

- リモートデスクトッププロトコル(Remote Desktop Protocol, RDP)を通じてログインできるグループリストからローカル管理者(Administrators)グループを取り除くことについて検討が必要
- 管理者のアカウント及び権限が割り当てられた一般のアカウントの間、資格証明の重複防止のための政策の検討が必要
- 低い権限レベルのユーザーが高いレベルのサービスを作ったり、実行できないように権限設定の検討が必要
- 資格証明の悪用による影響を最少化するため、サービスアカウントにおける権限の制限する政策の検討が必要

7. エンドポイントの脅威緩和

1) ソフトウェアアップデート(Update Software)

エンドポイント(Endpoint)及びサーバーの OS とソフトウェアが最新バージョンでアップデートされているか確認が必要であり、特に外部に漏出されたシステム及供給網の公的に繋がる恐れがあるファイルの配布システム(Deployment Systems)における定期的なアップデートの検討が必要

2) OSの構成（Operating System Configuration)

ハッキンググループの晒された技術における被害を緩和するため、OS の構成の検討が必要

- NTLM(New-Technology LAN Manager)ユーザー認証プロトコル、Wdigest 認証無効化の検討が必要
- 業務及び運営に不要な場合、リムーバブルメディアを許容せず、制限する政策の検討が必要
- 署名済みではないドライバーがインストールされないよう、制限する政策の検討が必要

3) アプリケーション確認及びサンドボックス(Application Isolation and Sandboxing)

すでにハッキンググループが奪取した権限及び資格証明を通じてほかのプロセス及びシステムにアクセスすることを制限するため、アプリケーション隔離及びサンドボックスの使用の検討が必要

4) 実行防止（Execution Prevention)

システムからマルウェアの実行を防ぐため、実行ファイル及びスクリプト実行のコントロールの検討が必要

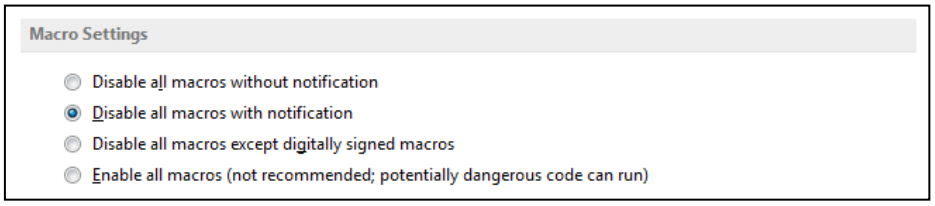
- 信頼できないファイルの実行を防止し、マルウェアの識別及びブロックするため、Windows アプリケーションのコントロールツールの使用の検討が必要
- ファイルが実行されるように許容するか、拒否するルールを作り、このファイルが実行できるユーザー及びグループを指定できる Windows のアップロッカー(AppLocker)の使用の検討が必要

5) 機能の無効化及びプログラムの削除（Disable or Remove Feature or

Program)

攻撃者の濫用を事前に防ぐため、潜在的に脅威となる恐れがある機能の無効化及びプログラムの削除の検討が必要

- Windows のシステムにインストールされている MS Office のセキュリティ設定の中、「マクロ設定」を「すべてのマクロを表示しない(通知表示)」の基本設定を変更できなくして、アクティブディレクトリ(Active Directory)から GPO Group Policy Object)の設定の上、配布する検討が必要



- DCOM(Distributed Component Object Model)の無効化の検討が必要
- 特定のシステムから MSHTA.exe が起動しないように検討が必要
- WinRM(Windows Remote Management)サービスの無効化の検討が必要
- 不要な自動実行機能の無効化の検討が必要
- ローカルパソコンのセキュリティ設定及びグループ政策から LLMNR(Link-Local Multicast Name Resolution)及びネットバイオス(NetBIOS)の無効化の検討が必要
- ローカルパソコンのセキュリティ設定及びグループ政策から LLMNR(Link-Local Multicast Name Resolution)及びネットバイオス(NetBIOS)の無効化の検討が必要
- PHP の eval()のようなウェブ技術の特定した関数を無効化する検討が必要

6) コード署名 (Code Signing)

信頼できないファイルの実行を防ぐため、コード署名情報を確認する政策設定の検討が必要

- 署名済みではないスクリプトの実行を防ぐパワーシェル(PowerShell)の政策設定の検討が必要
- 署名済みではないファイルの実行を防ぐ政策設定の検討が必要
- 署名済みではないサービスドライバーの登録及び実行を防ぐ政策設定の検討が必要

7) アンチウイルス (Antivirus)

マルウェアのダウンロード及び実行を通じたサイバー脅威を防止するため、これを探知しつつブロックできるアンチウイルス(Antivirus)の使用の検討が必要

- マルウェアのダウンロード及び実行の対応のため、ホスト型侵入防止システム(HIPS, Host Intrusion Prevention System)及びアンチウイルス(Anti Virus)などのソリューション使用の検討が必要

8) エンドポイントからの行為を防止 (Behavior Prevention on Endpoint)

エンドポイント(EndPoint)から潜在的な脅威になりやすい悪性行為が発生しないよう、事前に防止するために行為防止(Behavior Prevention)機能使用の検討が必要

- 信頼できないファイルの実行を防止するため、ASR(Attack Surface Reduction)ルールの有効化の検討が必要
- ファイルの署名が一致しないなど、潜在的な脅威になりやすいファイルを識別及び探知できるエンドポイント(EndPoint)ソリューション使用の検討が必要
- プロセスインジェクション(Process Injection)のような攻撃技術を探知及びブロックするため、行為防止(Behavior Prevention)機能使用の検討が必要

9) ハードウェア設置の制限 (Limit Hardware Installation)

USB デバイス及びリムーバブルメディアを含む承認済みではないハードウェアの使用を制限したり、ブロックしたりする政策を検討

- ¥承認済みではないハードウェアの使用を制限したり、ブロックするようにエンドポイントのセキュリティ構成及びモニタリングエージェントの使用の検討が必要

10) 企業モバイル政策 (Enterprise Policy)

モバイルデバイスの動作をコントロールするための政策設定のため、 EMM(Enterprise Mobility Management)/MDM(Mobile Device Management)システムの使用の検討が必要

- Android デバイスの業務文書及び内部システムのアクセスは制限付きの業務領域のみでアクセスできるように政策設定の検討が必要
- iOS からエンタープライズ配布用証明書で署名し、App Store ではないほかの手段から伝わってきた悪性アプリケーションをユーザーがインストールできないよう、プロフィールの制限設定の検討が必要

LEGAL DISCLAIMER

NSHC (NSHC Pte. Ltd.) takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuations. NSHC Research services are limited publications containing valuable market information provided to a selected group of customers. Our customers acknowledge, when ordering or downloading our publications

NSHC Research Services are for customers' internal use and not for general publication or disclosure to third parties. No part of this Research Service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, contact us. **service@nshc.net**

This document contains information that is the intellectual property of NSHC Inc. and Red Alert team only. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of NSHC. Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied.

NSHC.

NSHC disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of NSHC.