Presented by

Trellix ADVANCED RESEARCH CENTER

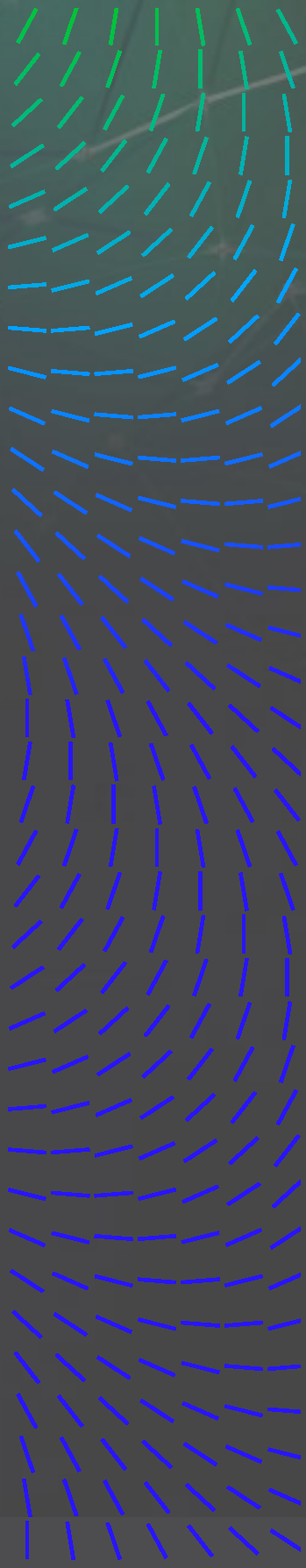
# THE THREAT REPORT

February 2023

脅威レポート

# TABLE OF CONTENTS





## 2022年第4四半期の脅威の概要

2022年最後の四半期も脅威アクターの攻撃の手が緩むことはなく、Trellix Advanced Research Centerでは、数百人の精鋭セキュリティアナリストと研究者のチームに、さらに多くの脅威インテリジェンスリソースを追加することで対抗しています。

「別の言い方をすると、私たちは脅威インテリジェンスをさらにワンランク上のレベルへと引き上げました。今までよりもシンプルなセキュリティでSecOpsの混乱を和らげ、セキュリティの負担を減らしつつ、より成果を向上させるために。脅威は進化を続けています。そして、私たちも進化し続けるのです。」

このレポートでは、2022年第4四半期に業界で最も蔓延した攻撃者、脅威ファミリー、攻撃キャンペーン、よく利用されている攻撃手法の情報を皆様に提供してします。しかし、それだけではありません。Trellixは利用するランサムウェアのリークサイトやセキュリティ業界のレポートからデータを収集し、ソースを拡大しました。Trellixのリソースが増えるにつれ、ネットワークセキュリティ、クラウドインシデント、エンドポイントインシデント、セキュリティオペレーションをカバーする新たなセクションなど、脅威研究領域も拡大しています。

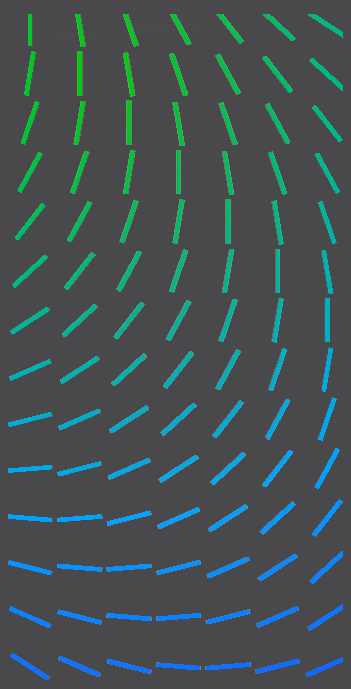
Trellix Advanced Research Centerは、前回の脅威レポート以降、2022年第4四半期にウクライナを標的としたサイバー攻撃の大幅な増加に関連するサイバー犯罪集団「Gamaredon」に関する調査や、61,000件の脆弱なオープンソースプロジェクトのパッチ適用、2023年の脅威予測による新年の新たな攻撃に関する洞察の発表など、世界各地で調査と発見に取り組んでいます。

これらの脅威レポートの改善点から得られた以下の概要は、顧客やセキュリティ業界が脅威に対してより高い成果を上げられるよう、Trellix Advanced Research Centerがどのように取り組んでいるかを例示しています。

**ランサムウェア**

- 2022年第4四半期に最も影響を及ぼしたランサムウェアグループとして顕著であった「LockBit 3.0」に関するブレイクアウト調査
- 米国を中心に、世界中で蔓延を続けているランサムウェア
- 産業材・サービスなどのセクターを狙うランサムウェア





**国家主導の活動**

- 政府、運輸・海運などのセクターを標的とする国家主導の活動
- 国家主導の活動によって影響を受けた米国拠点企業

**環境寄生**

- Trellix Advanced Research Centerのハンティング手法を使用し、野生のCobalt Strikeに関するインサイトを拡大
- 中国系クラウドプロバイダーにホストされているCobalt Strikeチームの非常に多くのサーバー
- 報告されたキャンペーンで最も蔓延した上位トップ10のOSバイナリのうち、Windowsコマンドシェルがほぼ半数を独占

**攻撃者**

- 中国、北朝鮮、ロシアが、最も活発に活動していた攻撃者の拠点国の上位にランクイン

**メールセキュリティの傾向**

- サッカーワールドカップの開催期間中にアラブ諸国で急増した悪質なメール
- フィッシングおよびビッシングのキャンペーンに関する洞察（なりすましの手口、ビッシングで多用されている企業テーマなど）

**ネットワークセキュリティ**

- 2022年第4四半期に最も影響が大きく、重要であり、そして関連性が高かった攻撃、WebShell、ツール、手法について

**Trellix XDRによるセキュリティオペレーションの遠隔観測**

- 蔓延しているセキュリティアラート、エクスプロイト、ログソース、MITRE ATT&CK 手法
- クラウドインシデント
- Azure、AWS、GCPで確認された手法と検出結果の内訳
- 主な手法と検出結果について



## Trellix脅威インテリジェンス責任者からのご挨拶

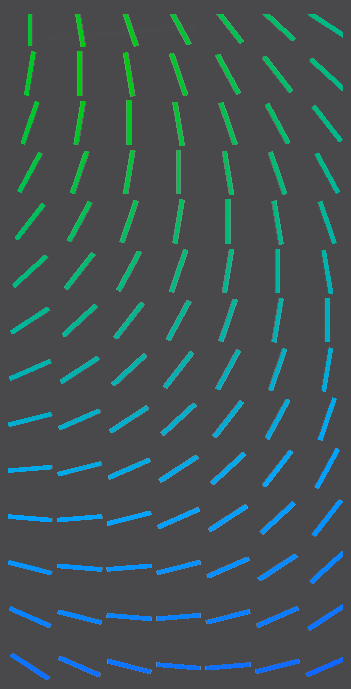
Trellix Advanced Research Centerチームは、2022年第4四半期に関する今年初めての脅威レポートを紹介し、1年を締めくくることができ大変うれしく思います。このレポートでは、ランサムウェアのリークサイトや実際のインフラストラクチャの追跡など他のデータソースから得られた洞察に加え、当社製品群のセンサーから収集した新たなデータを組み合わせることで、継続的に進化していることがお分かりいただけると思います。攻撃者やその動機に決して終わりはなく、それらがより多面的になっている状況の中、Trellixは、お客様を悪から守るというミッションに粘り強く取り組んでいます。地政学的、経済的な見通しは依然として複雑であり、不確実性を増しているため、グローバル脅威インテリジェンスの必要性が高まっています。

世界レベルでは、ウクライナでの戦争が招いた経済的な不確実性が、1970年代以来となる大規模なエネルギー価格の高騰を引き起こし、世界経済に大きな打撃を与えています。また、欧州で再び戦争が勃発したことは、EUの安全保障と防衛に対するアプローチや、特にサイバースペースにおける自国の利益を守る能力を疑問視する人々への警鐘にもなりました。米政権も、地政学的な競争への対応、重要インフラの保護、外国からの情報操作や干渉に対処する必要性を認識しています。SolarWindsやHafniumのイベント、またウクライナ戦争などの出来事がきっかけとなり、米国の政権と議会は連携して、過去の米国政府が打ち出してきた国家公約や取り組みを大幅に上回る、新たなセキュリティ基準と予算に向けて行動を起こしています。それでは、この不確実性は、私たちのビジネス、公共・民間機関におけるサイバーセキュリティ、そして民主主義的な価値観に、どのような影響を及ぼしているのでしょうか。

2022年第3四半期、Trellix Advanced Research Centerチームは、政治的、経済的、領土的な利益を目的とした諜報活動、戦争、（悪意を伴う）情報騒乱の領域における政治的手段として、サイバーが積極的に利用されていることを確認しました。ウクライナ戦争では、新しい形態のサイバー攻撃が出現し、ハクティビストの知識レベルが上がり、サイトの改ざん、情報漏洩、DDoS攻撃がより大胆に実行されています。その一方で、従来型のサイバー攻撃も続いています。フィッシングのような、個人を騙して機密情報や個人情報を漏洩させるソーシャルエンジニアリングの手口は、依然として蔓延したままです。

ランサムウェアは引き続き世界中の多くの組織を悩ませています。新型コロナウイルス感染症のパンデミック禍に見られたように、サイバー犯罪者は、危機と不確実性の時代から利益を得ようと迅速に行動しています。脅威の状況が進化すれば、私たちの調査も進化します。Trellixは、引き続き弊社の製品の有効性を常に向上させ、最も重要なものを確実に保護できるよう、関係者の皆様にアクションに結び付く実用的なインテリジェンスを提供することに全力を注ぐことを使命としていきます。





このレポートから、Trellix Advanced Research Centerのメンバー、一人ひとりにとって、私たちの取り組みが如何に重要なものであるかをご理解いただけると考えています。当チームのすべての研究者や専門家が誠心誠意、一つひとつのプロジェクトに向き合っています。

今回の拡張版レポートに関するご意見をお寄せください。また、本レポートでご覧になりたいテーマがありましたら、お気軽に私または当チームのTwitter（@TrellixARC）までご連絡ください。また、4月にサンフランシスコで開催されるRSAで、多くの方にお会いできることを楽しみにしております。

ジョン・フォッカー（John Fokker）
脅威インテリジェンス責任者

## 調査方法

Trellixは、Trellixのバックエンドシステムから提供される遠隔観測で報告された情報を用いて、四半期脅威レポートを作成しています。Trellixは、この情報をランサムウェアや国家主導の活動などの一般的な脅威に関するオープンソースのインテリジェンス、そして私たち独自の調査結果と組み合わせて活用しています。

遠隔観測とは、感染ではなく検出のことを指します。ファイル、URL、IPアドレスなどの痕跡がプロダクトのいずれかにより検知され報告された場合に、検出として記録されます。

例えば、Trellixは、実際のマルウェアサンプルを展開する有効性試験のフレームワークを使用する組織が増加していることを認識しています。このように展開されたマルウェアサンプルは検出として表示されますが、間違いなく感染ではありません。

遠隔測定における偽陽性の分析とフィルタリングのプロセスは絶えず進歩しているため、過去のエディションと比較した場合に、結果として新しい脅威のカテゴリが追加される可能性があります。

また、Trellixの社内でこの四半期レポートに寄与するチームが増えた場合にも、新たな脅威カテゴリが追加されることになります。

お客様のプライバシーは重要です。これは、遠隔観測やお客様の業種および国へのマッピングでも重要になります。国ごとに顧客基盤が異なるため、数字では増えているように見えることもありますが、解説はデータを掘り下げてみなければなりません。例えば私たちのデータでは、通信業界で高いスコアが記録されることがありますが、必ずしも同業界が標的になりやすいことを示しているわけではありません。通信業界には、企業が購入できるIPアドレス空間を所有するISPプロバイダも含まれています。これはどういうことかというと、

ISPのIPアドレス空間からの送信は通信業界での検出と見なされますが、別の業種で稼働しているISPクライアントからのものである可能性があるのです。

## 2022年第4四半期のランサムウェア

このセクションでは、ランサムウェアグループの活動に関して収集したさまざまなインサイトを提供します。この情報は、脅威の状況をより正確に把握し、観測バイアスを低減するほか、2022年第4四半期に最も影響を与えたランサムウェアファミリーについて判断できるよう、複数のソースから収集されています。1つは定量的なデータソースで、ランサムウェアのIoC（侵害の痕跡）とTrellixのお客様の遠隔観測との相関分析に基づいて抽出された、ランサムウェアキャンペーンに関する統計データを示しています。2つ目は定性的なデータソースで、セキュリティ業界から発表されたさまざまなレポートに対して、Trellixの脅威インテリジェンスグループが精査、解析、分析を行った結果を示しています。最後の3つ目は新しいデータソースのカテゴリであり、さまざまなランサムウェアグループの「リークサイト」から収集したランサムウェア被害者の情報を正規化し、エンリッチ化して、そして最終的に匿名化されたバージョンとして提供し、分析した結果を示すものです。

これらの異なる視点を提供することで、現在の脅威の状況を明らかにするために多くの手がかりをもたらすことを目指しています。ソースにもそれぞれの限界があり、十分なものではありません。インターネットに接続されているすべてのシステムのログにアクセスできる人はいませんし、すべてのセキュリティインシデントが報告されているわけでも、すべての被害者が強請（ゆす）られたり、リークサイトに掲載されたりしているわけでもありません。しかし、さまざまな視点を組み合わせれば、私たちが抱えている盲点を減らしつつ、さまざまな脅威に関する理解を深められるようになります。

十分な情報に基づいた判断とは、潜在的な難点や盲点を考慮しながら、各種ソースから取得した定量データと定性データを組み合わせることによって、生み出されるものです。

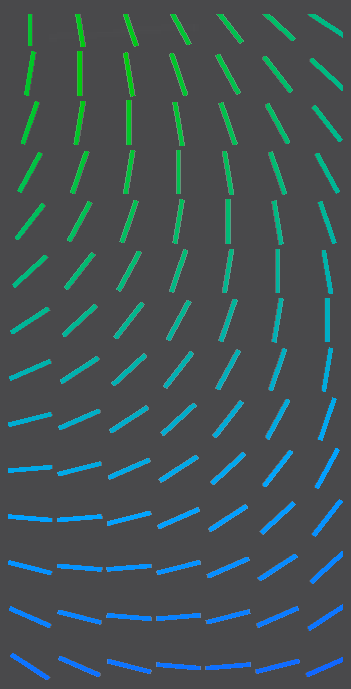
## 2022年第4四半期のランサムウェアに関するハイライト

### 2022年第4四半期に最も影響を及ぼしたランサムウェアグループ「LockBit 3.0」

Trellixのさまざまなソースを観測した結果、2022年第4四半期に最も影響を及ぼしたランサムウェアグループはLockBit 3.0であると結論づけることができます。LockBit 3.0の影響の大きさは、以下の点に基づいています。

**3位** Trellixのグローバルセンサーから収集したランサムウェアに関する遠隔観測の分析結果によると、LockBit 3.0は、2022年第4四半期に最も蔓延したランサムウェアグループにおいて、3位にランクインしています。





**2位** Trellixの脅威インテリジェンスグループが収集したさまざまなキャンペーンの分析結果によると、 LockBit 3.0は、Cubaランサムウェアと並び、セキュリティ業界で最も報告されたランサムウェアグループにおいて2位にランクインしています。

**1位** LockBit 3.0のリークサイトは、2022年第4四半期にランサムウェアグループの中で、最も多くの被害者が報告されました。LockBit 3.0は、被害者名の公表により被害者に圧力をかけることに最も固執したグループといえます。

2022年第4四半期のLockBit 3.0に関するその他のカテゴリと所見は、以下の通りです。

### 2022年第4四半期に最もLOCKBIT 3.0の影響を受けた上位トップ10のセクター

# 29%

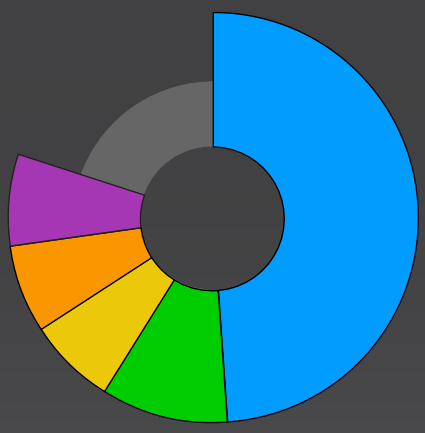
LockBit 3.0の被害者リークサイトによると、2022年第4四半期に最もLockBit3.0の影響を受けたセクターは、産業財・サービスとなっています。

- 産業材・サービス
- 小売
- テクノロジー
- ヘルスケア
- 建設＆資材
- 私財・家財
- 政府

### 2022年第4四半期に最もLOCKBIT 3.0の影響を受けた企業の国別トップ10

# 49%

LockBit 3.0の被害者リークサイトによると、2022年第4四半期に最もLockBit 3.0の影響を受けたのは米国を企業（49%）で、英国の企業がこれに続いています。



- 米国
- 英国
- カナダ
- フランス
- ブラジル

## LockBit 3.0のツールとエクスプロイト

### LockBit 3.0によって悪用されることが判明した脆弱性

| |
|---|
| CVE-2018-13379 |
| CVE-2020-0787 |
| CVE-2021-20028 |
| CVE-2021-34473 |
| CVE-2021-34523 |

### LockBit 3.0が利用した悪意のあるツール

| | |
|---|---|
| Amadey | Hakops |
| Blister | Neshta |
| BloodHound | SocGholish |
| Cobalt Strike | StealBit |
| Grabff | WinPEAS |

### LockBit 3.0が利用した悪意のないツール

| | | | |
|---|---|---|---|
| BCDEdit | MiniDump | NSIS | Schtasks.exe |
| Cmd | MpCmdRun.exe | PCHunter | VSSAdmin |
| Fltmc.exe | Mshta | PowerShell | wevtutil |
| Fsutil | Mstsc | プロセスモニター | WMIC |
| GMER | Netsh | Rundll32 | RCLONE |
| MEGASYNC | Nltest | | |

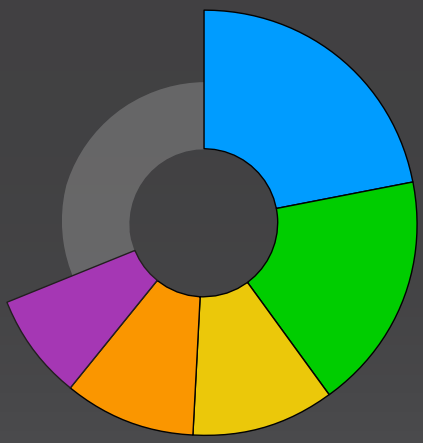
## Trellixの遠隔観測に基づくランサムウェアの状況

以下の統計データは、Trellixの遠隔測定と脅威インテリジェンスのナレッジベースとの相関分析に基づいています。Trellixは、分析の段階を経て、選択された期間のデータから一連のキャンペーンを洗い出し、それらの特徴を抽出しています。以下に示されている統計データはキャンペーンに関するものであり、検出そのものに関する統計データではありません。弊社のグローバル遠隔測定は、さまざまなランサムウェアグループによる複数のキャンペーンのIoCを示していました。以下のランサムウェアファミリーや各ランサムウェアファミリーのツールと手法は、特定されたキャンペーンで最も利用されていたファミリー、並びにそのツールと手法を示すものです。同様に、それに続く国やセクターは、特定されたキャンペーンの影響を最も受けた国およびセクターであることを示しています。

## 2022年第4四半期に最も蔓延したランサムウェア

# 22%

2022年第4四半期に最も蔓延したランサムウェアファミリーは、Cubaとなっています。Vice SocietyグループがZeppelinを多く利用していました。Yanluowangによる通信漏洩の詳細については、こちらをご覧ください。




## 2022年第4四半期にランサムウェアグループによって最も広く利用された悪意のあるツール

# 41%

2022年第4四半期にランサムウェアグループに最も広く利用された悪意のあるツールは、Cobalt Strikeでした。

| | | |
|---|---|---|
| 1. | Cobalt Strike | 41% |
| 2. | Mimikatz | 23% |
| 3. | BURNTCIGAR | 13% |
| 4. | VMProtect | 12% |
| 5. | POORTRY | 11% |

## 2022年第4四半期にランサムウェアグループによる利用が最も確認されたMITRE ATT&CK手法

| | | |
|---|---|---|
| 1. | 事業に影響を及ぼすデータ暗号化 | 17% |
| 2. | システム情報の検出 | 11% |
| 3. | PowerShell | 10% |
| 4. | 侵入ツールの送り込み | 10% |
| 5. | Windowsコマンドシェル | 9% |

## 2022年第4四半期に最もランサムウェアグループに利用された悪意のないツール

# 21%

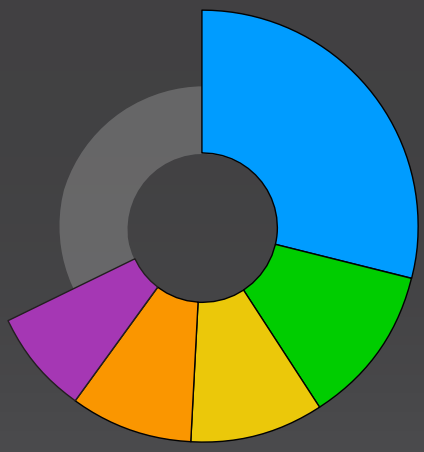
2022年第4四半期に最もランサムウェアグループに利用された悪意のないツールは、Cmdです。

| | | |
|---|---|---|
| 1. | Cmd | 21% |
| 2. | PowerShell | 14% |
| 3. | Net | 10% |
| 4. | Reg | 8% |
| 5. | PsExec | 8% |

## 2022年第4四半期に最もランサムウェアグループの影響を受けた国

29%

Trellixの遠隔測定によると、2022年第4四半期に最もランサムウェアグループの影響を最も受けた国は米国でした。

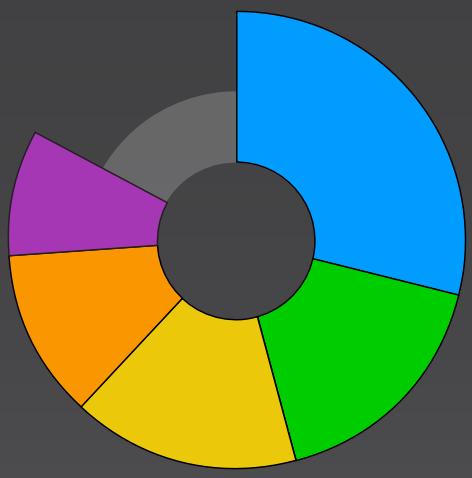


- 米国
- 中国
- カタール
- 日本
- インドネシア

## 2022年第4四半期に最もランサムウェアグループの影響を受けたセクター

29%

Trellixの遠隔測定によると、2022年第4四半期に最もランサムウェアグループの影響を受けたセクターは、アウトソーシング＆ホスティングとなっています。このデータは、ランサムウェアのリークサイトに掲載される被害者の平均的な組織規模と相関関係があり、これらの組織の多くは、独自のIPアドレスブロックが割り当てられておらず、サードパーティーのホスティングプロバイダを利用している傾向があります。



- アウトソーシング＆ホスティング
- バンキング/金融/ウェルスマネジメント
- 政府
- 卸売
- 製薬



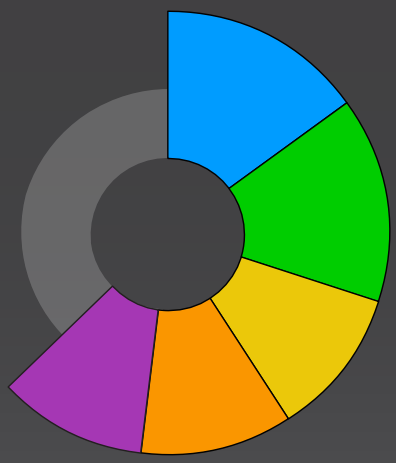
## セキュリティ業界から報告されたランサムウェア

以下の統計データは、公開されているレポートや社内調査に基づく統計データに基づいています 。すべてのランサムウェアインシデントが報告されているわけではないことにご注意ください。多くのランサムウェアファミリーはしばらくの間活動したのち、当然のことながら、特定の四半期に新たに登場したファミリーよりも注目度が下がっていきます。
これらの基準に従って、以下のランサムウェアファミリーに関する指標は、セキュリティ業界が2022年第4四半期に最も影響力があり、関連性が高いと判断したものとして示されています。

### 2022年第4四半期に最も報告されたランサムウェア

# 15%

セキュリティ業界の公開レポートによると、2022年第4四半期に最も報告されたランサムウェアファミリーは、Black BastaとMagniberでした。



- Black Basta
- Magniber
- Cuba
- LockBit
- Quantum

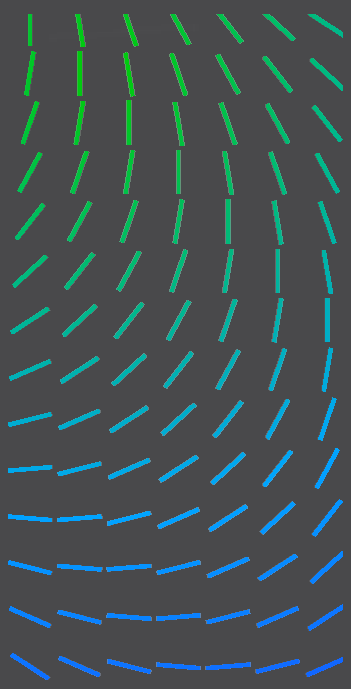
### 2022年第4四半期に最も報告されたランサムウェアファミリーの攻撃手法

# 19%

セキュリティ業界のレポートによると、2022年第4四半期に最も報告されたランサムウェアファミリーの攻撃手法は、データの暗号化となっています。

1. 事業に影響を及ぼすデータ暗号化 19%
2. Windowsコマンドシェル 11%
3. システム情報の検出 10%
4. 侵入ツールの送り込み 10%
5. PowerShell 10%

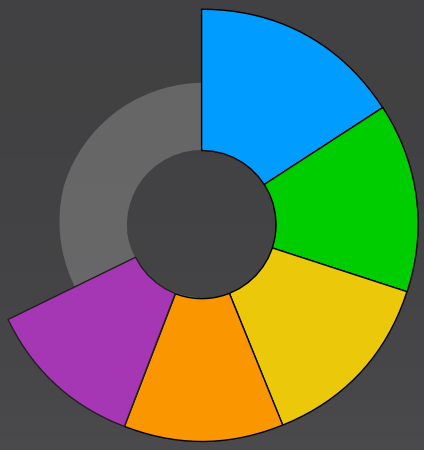




## 2022年第4四半期に最もランサムウェアファミリーの標的とされたセクター

# 16%

セキュリティ業界のレポートによると、2022年第4四半期に最もランサムウェアファミリーの標的とされたのは、ヘルスケア部門となっています。



- ヘルスケア
- 金融
- 政府
- 製造
- 運輸

## 2022年第4四半期に最もランサムウェアファミリーの標的とされた国

# 19%

セキュリティ業界のレポートによると、2022年第4四半期に最もランサムウェアファミリーの標的とされた国は、米国となっています。

- 米国
- ドイツ
- ブラジル
- アルゼンチン
- カナダ
- インド
- オランダ
- 韓国
- スイス
- 英国

## 2022年第4四半期に最もランサムウェアファミリーに利用されたCVE

| | | |
|---|---|---|
| 1. | CVE-2021-31207 | 16% |
| | CVE-2021-34474 | 16% |
| | CVE-2021-34523 | 16% |
| 2. | CVE-2021-34527 | 13% |
| 3. | CVE-2021-26855 | 9% |
| | CVE-2021-27065 | 9% |

### 2022年第4四半期にランサムウェアファミリーに利用された悪意のあるツール

# 44%

セキュリティ業界のレポートによると、2022年第4四半期に報告されたランサムウェアファミリーに最も利用された悪意のあるツールは、Cobalt Strikeとなっています。

| | | |
|---|---|---|
| 1. | Cobalt Strike | 44% |
| 2. | QakBot | 13% |
| 3. | IcedID | 9% |
| 4. | BURNTCIGAR | 7% |
| 5. | Carbanak<br>SystemBC | 7%<br>7% |

### 2022年第4四半期にランサムウェアファミリーに利用された悪意のないツール

# 21%

セキュリティ業界のレポートによると、2022年第4四半期に報告されたランサムウェアファミリーに最も利用された悪意のないツールは、PowerShellとなっています。

| | | |
|---|---|---|
| 1. | PowerShell | 21% |
| 2. | Cmd | 18% |
| 3. | Rundll32 | 11% |
| 4. | VSSAdmin | 10% |
| 5. | WMIC | |

## 2022年第4四半期にランサムウェアの「リークサイト」に掲載された被害者

このセクションのデータは、さまざまなランサムウェアグループの「リークサイト」をスクレイピングしてコンパイルされたものです。ランサムウェアグループは、これらのWebサイトで被害者に関する情報を公開することで、被害者を恐喝します。
ランサムウェアグループは、被害者との交渉が停滞した場合、あるいは提示する期限までに被害者が身代金の支払いを拒んだ場合に、被害者から盗んだ情報を公開します。Trellixでは、ransomlookというオープンソースのツールで収集したさまざまな掲載情報を内部処理して正規化し、結果をエンリッチ化して、匿名化されたバージョンでの被害者に関する分析データを提供しています。

重要な点として、すべてのランサムウェア被害者が各リークサイトに掲載されるわけではありません。多くの被害者は、身代金を支払うことで掲載を逃れています。これらの指標は、ランサムウェアグループが恐喝または報復を実行した被害者に関するものであり、被害者の総数と混同しないようにご注意ください。

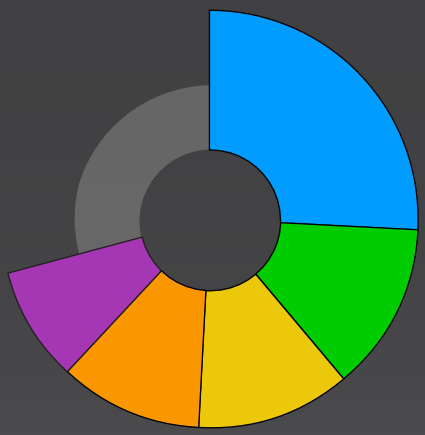


## 2022年第4四半期に最も多くの被害者を報告したランサムウェアグループ

# 26%

2022年第4四半期に各リークサイトに最も多くの被害者を報告したランサムウェアグループは、LockBit 3.0でした。同グループが報告した被害者が、上位トップ10のランサムウェアグループから報告された全被害者の26%を占めています。

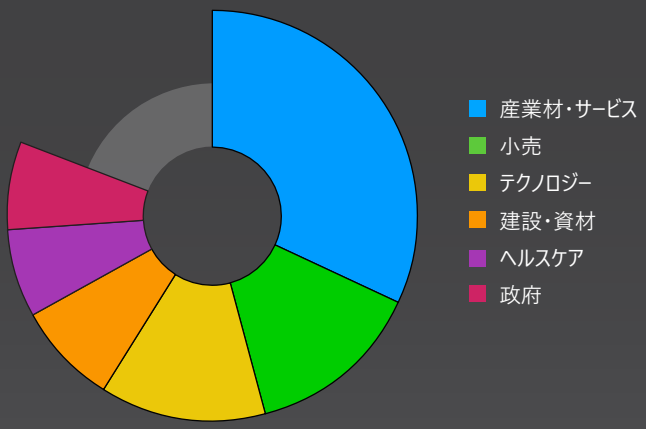
- LockBit 3.0
- ALPHV
- Royal
- Black Basta
- Cuba



## 2022年第4四半期にランサムウェアグループの各リークサイトの影響を最も受けたセクター

# 32%

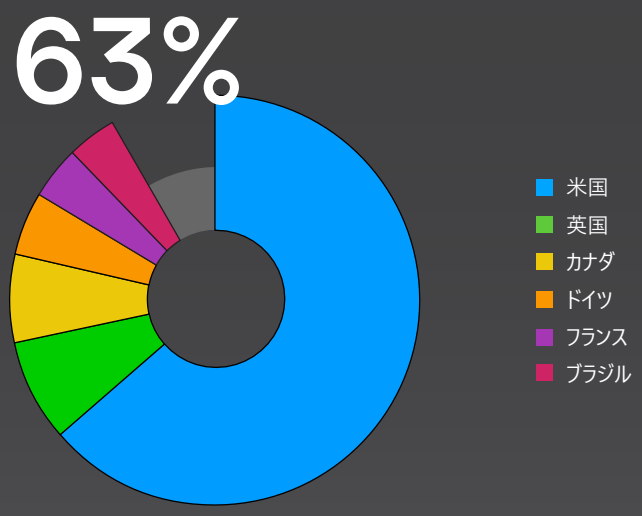
2022年第4四半期にランサムウェアグループの各リークサイトの影響を最も受けたセクターは、産業材・サービスとなっています。産業材・サービスのセクターには、主に建設や製造に使用される、あらゆる資材および材料製品と無形のサービスが含まれます。






**2022年第4四半期に最もランサムウェアグループの各リークサイトの影響を受けた企業の国別トップ10**

63%が米国に拠点を置く企業、これに続き、英国 (8%) とカナダ (7%) が、影響を受けた企業の国の上位でした。




## 2022年第4四半期の国家主導の活動に関する統計データ

このセクションでは、国家主導の活動に関して収集したインサイトを提供しています。この情報は、脅威の状況をより正確に把握しつつ、観測バイアスを減らせるように複数のソースから収集されています。まずは、国家主導のグループのIoCとTrellixのお客様の遠隔観測との相関分析から抽出した統計データを図示します。次に、セキュリティ業界から発表され、そしてTrellixの脅威インテリジェンスグループによって精査、解析、分析が行われたさまざまなレポートから得たインサイトを提供します。

## 2022年第4四半期の国家主導の活動に関するハイライト

- 米国とドイツで国家主導の攻撃が大幅に増加
- 2022年第4四半期、中国とベトナムが最も国家主導の攻撃を受けた国としてランキングに浮上

## Trellixのグローバル遠隔観測に基づく国家主導の活動に関する統計データ

これらの統計データは、Trellixの遠隔観測と脅威インテリジェンスのナレッジベースとの相関分析に基づいています。Trellixでは、分析の段階を経て、選択された期間のデータから一連のキャンペーンを洗い出し、それらの特徴を抽出しています。以下に示されている統計データはキャンペーンに関するものであり、検出そのものに関する統計データではありません。さまざまな方法によるログの集約、お客様に

よる脅威シミュレーションフレームワークの使用、そして脅威インテリジェンスのナレッジベースとのハイレベルな相関関係により、データは必要な基準を満たすように手動でフィルタリングされます。

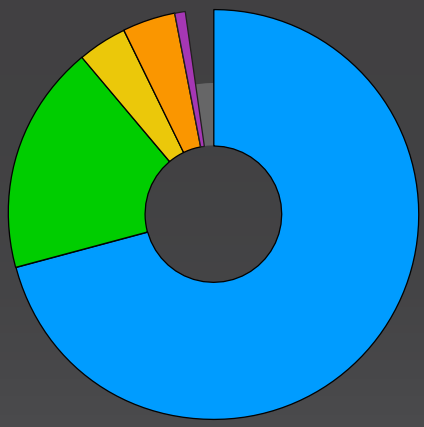
弊社のグローバル遠隔観測は、持続的標的型攻撃（APT）グループによる複数のキャンペーンのIoCを示していました。以下は、特定されたキャンペーンにおいて、最も活発に活動していた攻撃者が拠点とする国や攻撃者のグループ、並びに最も広く利用されていた攻撃者たちのツールや手法を示したものです。同様に、国やセクターに関するデータも、特定されたキャンペーンの影響を最も受けている国やセクターを示しています。

## 国家主導の活動に関する遠隔観測に基づくインサイト

### 2022年第4四半期に国家主導の活動の背後にある、最も活発に活動していた攻撃者の拠点国

**71%**

2022年第4四半期に国家主導の活動を背後にして、最も活発に活動していた攻撃者の拠点国は、中国となっています。

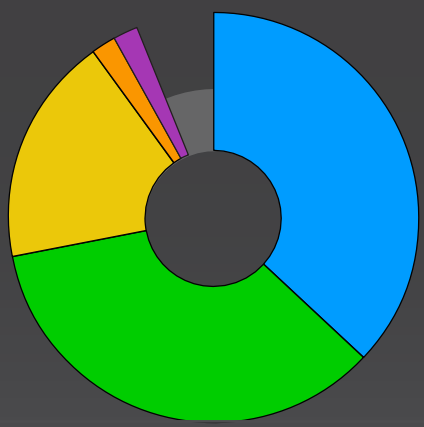


- 中国
- 北朝鮮
- ロシア
- イラン
- レバノン

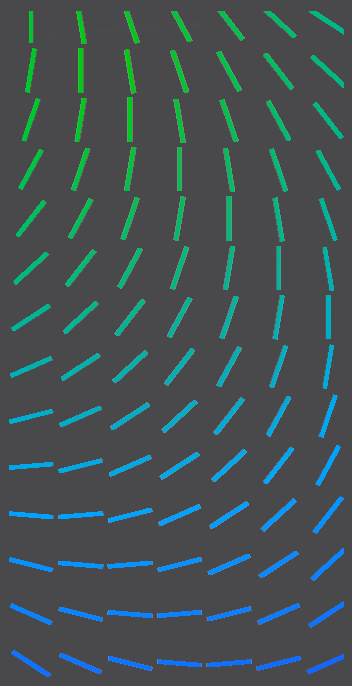
### 2022年第4四半期に最も活発に活動していた攻撃者グループ

**37%**

国家主導の活動に関する遠隔観測によると、2022年第4四半期に最も活発に活動していた脅威アクターグループは、Mustang Pandaとなっています。



- Mustang Panda
- UNC4191
- Lazarus
- MuddyWater
- Kimsuky



## 2022年第4四半期に国家主導の活動に最もよく利用されたMITRE ATT&CK手法

| | | |
|---|---|---|
| 1. | DLL サイドローディング | 14% |
| 2. | Rundll32 | 13% |
| 3. | 難読化されたファイルまたは情報 | 12% |
| 4. | Windowsコマンドシェル | 11% |
| 5. | レジストリ実行キー/スタートアップフォルダ | 10% |

## 2022年第4四半期に国家主導の活動に最もよく利用された悪意のあるツール

| | | |
|---|---|---|
| 1. | PlugX | 24% |
| 2. | BLUEHAZE | 23% |
| 3. | DARKDEW | 23% |
| 4. | MISTCLOAK | 23% |
| 5. | JSX を悪用した遠隔操作ウイルスのツール（RAT） | 2% |

## 2022年第4四半期に国家主導の活動に最もよく利用された悪意のないツール

| | | |
|---|---|---|
| 1. | Rundll32 | 22% |
| 2. | Cmd | 19% |
| 3. | Reg | 17% |
| 4. | Ncat | 12% |
| 5. | Regsvr32 | 6% |

## 2022年第4四半期に最も国家主導の活動の影響を受けた国

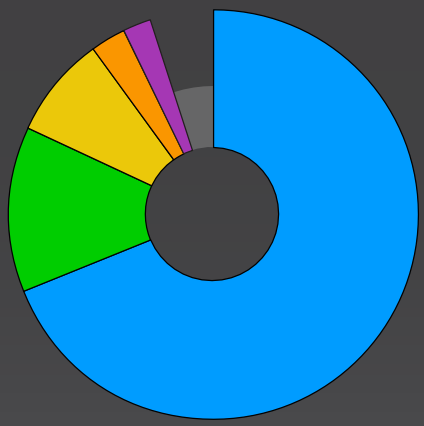
55%

2022年第4四半期に最も国家主導の活動の影響を受けた国は、米国となっています。

### 2022年第4四半期に最も国家主導の活動の影響を受けたセクター

# 69%

2022年第4四半期に最も国家主導の活動の影響を受けたセクターは、運輸・海運となっています。



- 運輸・海運
- エネルギー/石油・ガス
- 卸売
- 小売
- バンキング/金融/ウェルスマネジメント

## 2022年第4四半期に公開されているレポートによる国家主導のインシデント

以下の統計データは、公開されているレポートや社内調査に基づいています。お客様のログから取得した遠隔観測に基づくデータではありません。すべての国家主導のインシデントが報告されているわけではないことにご注意ください。多くのキャンペーンは、既知のTTP（戦術・技術・手順）に倣った、報告の重要性が低いものです。セキュリティ業界は、攻撃者が何らかの新しいことを試みたり、また失敗したりするような、より斬新なキャンペーンを取り上げる傾向にあります。これらの指標は、2022年第4四半期の期間にセキュリティ業界が鋭いインサイトと実際の問題との関連性を見出した情報を示したものです。

### 2022年第4四半期に最も報告された国家主導の攻撃者の拠点国

# 37%

2022年第4四半期に公表された国家主導のキャンペーンの37%が、中国を拠点とする攻撃者によるものでした。

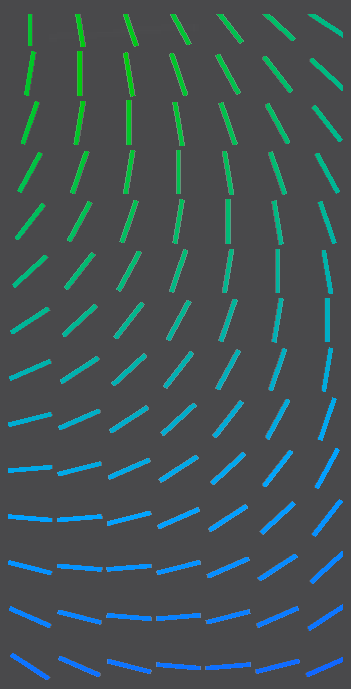
| | | |
|---|---|---|
| 1. | 中国 | 37% |
| 2. | 北朝鮮 | 24% |
| 3. | イラン | 1% |
| 4. | ロシア | 1% |
| 5. | インド | 1% |

### 2022年第4四半期に最も活動が報告された国家主導の攻撃者グループ

# 33%

2022年第4四半期に最も活発な活動が報告された国家主導の攻撃者はLazarusとなり、全体の33%を占めています。

| | | |
|---|---|---|
| 1. | Lazarus | 33% |
| 2. | Mustang Panda | 17% |
| 3. | APT34<br>APT37<br>APT41<br>COLDRIVER<br>Patchwork<br>Polonium<br>SideWinder<br>Winnti Group | 各 1% |

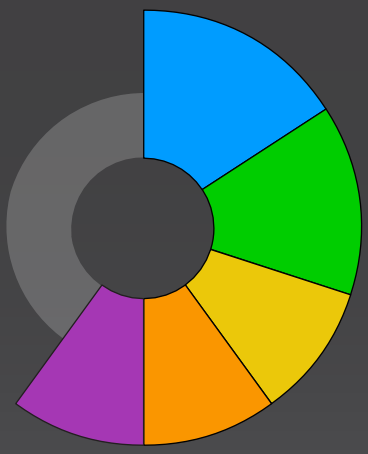


## 2022年第4四半期に報告された国家主導のキャンペーンにおいて最も標的とされた国

# 16%

2022年第4四半期に報告された国家主導のキャンペーンにおいて最も標的とされた国は、米国となっています。

- 米国
- 英国
- パキスタン
- ロシア
- ウクライナ

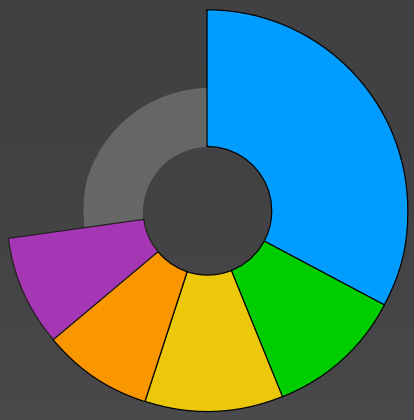


## 2022年第4四半期に報告された国家主導のキャンペーンにおいて最も標的とされたセクター

# 33%

2022年第4四半期に報告された国家主導のキャンペーンにおいて最も標的とされたセクターは政府となり、軍部（11%）、通信（11%）セクターがこれに続いています。

- 政府
- 軍部
- 通信
- エネルギー
- 金融



## 2022年第4四半期に報告された国家主導のキャンペーンで最もよく選ばれた悪意のあるツール

| | | |
|---|---|---|
| 1. | PlugX | 22% |
| 2. | Cobalt Strike | 17% |
| 3. | Metasploit | 13% |
| 4. | BlindingCan | 9% |
| 5. | Scanbox<br>ShadowPad<br>ZeroCleare | 各 9% |

## 2022年第4四半期の国家主導のキャンペーンで最もよく選ばれた悪意のないツール

| | | |
|---|---|---|
| 1. | Cmd | 32% |
| 2. | Rundll32 | 20% |
| 3. | PowerShell | 14% |
| 4. | Reg | 8% |
| 5. | Schtasks.exe | 7% |

**2022年第4四半期に報告された国家主導のキャンペーンで最もよく選ばれたMITRE ATT&CK手法**

| | | |
|---|---|---|
| 1. | 侵入ツールの送り込み | 13% |
| 2. | システム情報の検出 | 13% |
| 3. | 難読化されたファイルまたは情報 | 12% |
| 4. | Webプロトコル | 11% |
| 5. | 難読化解除/ファイルまたは情報の解読 | 11% |

### 2022年第4四半期に報告された国家主導のキャンペーンでの悪用が確認された脆弱性

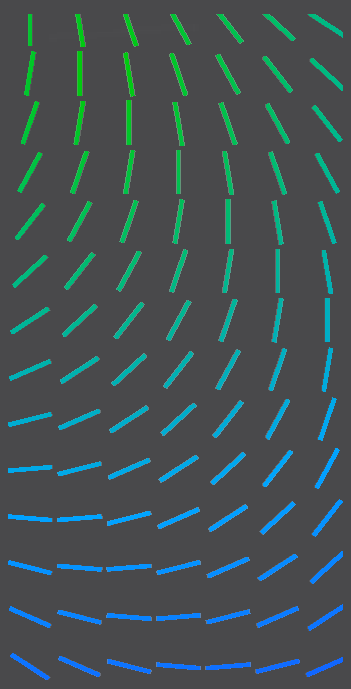
| | |
|---|---|
| CVE-2017-11882 | CVE-2020-17143 |
| CVE-2021-44228 | CVE-2021-21551 |
| CVE-2018-0802 | CVE-2021-26606 |
| CVE-2021-26855 | CVE-2021-26857 |
| CVE-2021-27065 | CVE-2021-26858 |
| CVE-2021-34473 | CVE-2021-28480 |
| CVE-2021-34523 | CVE-2021-28481 |
| CVE-2015-2545 | CVE-2021-28482 |
| CVE-2017-0144 | CVE-2021-28483 |
| CVE-2018-0798 | CVE-2021-31196 |
| CVE-2018-8581 | CVE-2021-31207 |
| CVE-2019-0604 | CVE-2021-40444 |
| CVE-2019-0708 | CVE-2021-45046 |
| CVE-2019-16098 | CVE-2021-45105 |
| CVE-2020-0688 | CVE-2022-1040 |
| CVE-2020-1380 | CVE-2022-30190 |
| CVE-2020-1472 | CVE-2022-41128 |
| CVE-2020-17141 | |

## 2022年第4四半期の環境寄生とサードパーティーツール

Trellix Insights や Trellix Global Threat Intelligenceのプラットフォームでの観測と追跡を通じて、2022年第4四半期の脅威の状況に関する以下のインテリジェンスと可視性を取得しました。

### 2022年第4四半期の環境寄生に関するハイライト

- 環境寄生は、初期アクセスから、実行、探索、持続、影響に至るフェーズにおいて引き続き役割を担っている
- 2022年第4四半期のデータでは、Windowsコマンドシェルまたは PowerShellを介して実行されるコマンドやスクリプトの手法が最も一般的に利用（悪用）される傾向が続いていることを示している



・サイバー犯罪者による（環境寄生の）利用は、熟練したAPT、金銭目的のグループ、ハクティビストなどの攻撃者の間で蔓延している

たまたま脅威情勢に現れた新参の攻撃者、単発的な攻撃者、スクリプトキディも、一般的な侵入ツールのフレームワークに組み込まれた既存のバイナリを利用して、（手法は未熟ではありながら）気づかれることなくスーパーコンピューターのハッキングや、脆弱性の悪用を試みています。

環境寄生型の手口は、初期アクセスから、実行、探索、持続、影響に至るまでのフェーズで、不正なタスクを実行するために利用（悪用）され続けています。2022年第4四半期を通じて収集されたデータによると、最も一般的に利用（悪用）されている手法として、Windowsコマンドシェルを介してコマンドおよびスクリプトが実行される傾向が続いていることが分かります。

### 2022年第4四半期に最も蔓延したOSバイナリ

**47%**

2022年第4四半期に最も蔓延した上位10種のOSバイナリのうち、Windowsコマンドシェルがその半数近く（47%）を占めており、次にPowerShell（32%）、Rundll32（27%）が続いています。

| | | |
|---|---|---|
| 1. | Windows コマンドシェル | 47% |
| 2. | PowerShell | 32% |
| 3. | Rundll32 | 27% |
| 4. | Schtasks | 23% |
| 5. | WMI | 21% |

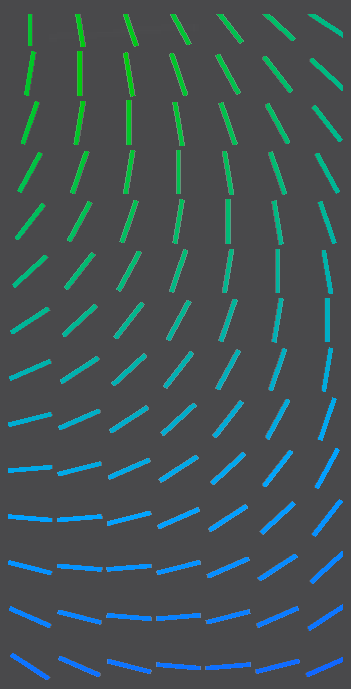
サイバー犯罪者による（環境寄生の）利用は、熟練したAPT、金銭目的のグループ、目的意識の高いハクティビストなどの脅威アクターの間で蔓延しています。

Trellix Insightsのプラットフォームで処理されたイベントから、攻撃者がWindowsバイナリを利用し、情報窃取型マルウェア、遠隔操作ウイルス（リモートアクセス型トロイの木馬）、ランサムウェアなどの追加マルウェアの展開に繋がっていました。

MSHTA、WMI、WScriptなどのバイナリは、攻撃者の制御下にあるリソースから追加のペイロードを取り込むために実行された可能性があります。

### 2022年第4半期に最も蔓延したサードパーティーツール

| | | |
|---|---|---|
| 1. | リモートアクセス ツール | 58% |
| 2. | ファイル転送 | 22% |
| 3. | Post Exploitation （侵入後）ツール | 20% |
| 4. | ネットワーク検出 | 16% |
| 5. | ADの検出 | 10% |



リモートアクセスツールや制御ツールは、常に攻撃者が最も悪用しているツールの上位にランクインしていますが、セキュリティ担当者向けのツールが悪意を持って使われる状況も続いています。攻撃者はキープアライブビーコンを作動開始させ、データ持ち出し（抽出）の自動化、標的情報の収集や圧縮を行うために、これらのツールを使用する可能性があります。

無料かつオープンソースツールのうち、攻撃者がソフトウェアパッカーを悪用し、悪意のあるコンテンツを含めせて正規のソフトウェアを再パッケージ化したり、検出の回避や分析の妨害を目的としてマルウェアを圧縮（パック）したりしていることが確認されました。

## 2022年第4四半期のCOBALT STRIKEに関するインサイト

Trellix Advanced Research Centerの脅威インテリジェンスグループは、ペイロードとインフラストラクチャのハンティング法を組み合わせることで、Cobalt Strikeを悪用しているグループが現在も使用しているCobalt Strike Team Server（Cobalt Strike C2サーバ）の使用状況を監視しています。以下のセクションでは、収集したCobalt Strikeビーコンを分析中に判明した特筆すべきインサイトを提示します。

### 15%
**評価版COBALT STRIKEの割合**

現在も使用されているCobalt Strikeのビーコンのうち、Cobalt Strikeの評価ライセンスを持っていたビーコンはわずか15%でした。評価版のCobalt Strikeには、このポストエクスプロイト（侵入後）のフレームワークのよく知られている機能がほとんど含まれています。
しかし、「tells」を追加することで、セキュリティプロダクトがペイロードの検出が容易にするための転送中の暗号（ペイロードエンコーダ）が削除されます。

### 5% Host HTTP ヘッダー

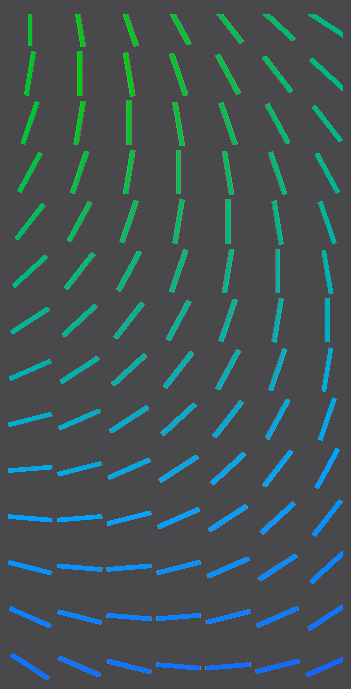
観測されたCobalt Strikeのビーコンのうち、少なくとも5%は、Host Httpヘッダーを使用していました。このHost Httpヘッダーのオプションは、Cobalt Strikeによるドメインフロンティングを容易にするものです。ドメインフロンティングとは、複数のドメインをホストするコンテンツデリバリーネットワーク（Content Delivery Networks；CDN）を悪用する手法であり、攻撃者は、悪意のあるWebサイトへのHTTPSリクエストを、正規のWebサイトへのTLS接続の中に忍ばせます。

### 22% DNSビーコン

確認されたCobalt Strike ビーコンのうち、DNSビーコンが22%を占めていました。このタイプのペイロードは、DNSクエリを介して、ドメインの権威サーバーである攻撃者のCobalt Strike Team Serverに応答を返すことで、脅威活動を隠蔽します。

### 87%
**RUNDLL32.EXE**

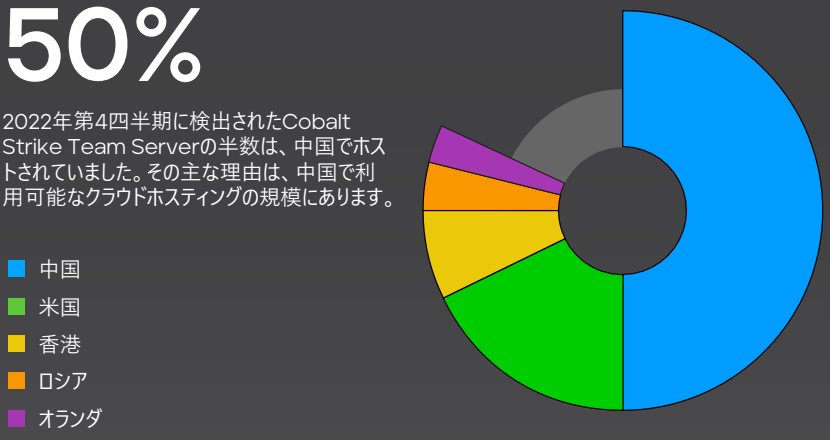
確認されたビーコンの87%から、セッションを生成し、ポストエクスプロイト（侵入後）のジョブを実行するために使われるデフォルトプロセスであるRundll32.exeが見つかりました。



**2022年第4四半期に最もCobalt Strike Team Serverを
ホストしていた国**

# 50%

2022年第4四半期に検出されたCobalt Strike Team Serverの半数は、中国でホストされていました。その主な理由は、中国で利用可能なクラウドホスティングの規模にあります。




## 2022年第4四半期の GOOTLOADER

Gootloaderとはモジュール式のマルウェアで、折に触れて、別のマルウェアとして識別されている「GootKit」または「GootKit Loader」とほとんど同じ意味で言及されることがあります。現在、Gootloaderマルウェアのモジュール機能は、REvil、Kronos、Cobalt Strike、Icedidといった追加のマルウェアのペイロードを配布するために利用されています。

最近の事例では、Gootloaderが検索エンジンの最適化（SEO）を利用して、JS（JavaScript）ファイルのペイロードを含むアーカイブファイルをホストする侵害されたサイトまたは偽のサイトに、疑いを持たないユーザーを誘導していることが確認されました。ただし、この手法では、その何ら疑いを持たないユーザーにアーカイブを開かせ、コンテンツを実行させる必要があり、それによって、Windowsスクリプトホストを介して悪意のあるJSコードを実行されます。JSコードの実行に成功すると、GootloaderはC2通信を開始し、追加のマルウェアを取り込みます。

Gootloaderは、そのため攻撃者が複数の追加ペイロードを取り込むことができるように、利用者に提供されている「サービスとしてのマルウェア（MaaS）」である疑いがあります。そのため、企業環境にとって重大な脅威をもたらすことになります。

Trellixは社内のGootloaderトラッカーを利用し、2022年11月18日に実際に確認した最近の亜種の正体を特定したほか、2022年11月13日の時点で古い亜種が活動を停止していることを確認しました。最新の亜種では、以下の変更が行われています。

- レジストリ操作機能の削除
- リモートネットワーク接続リクエスト数を3個から10 個のURLに増加

・Cscriptを介してPowerShellスクリプトを直接呼び出す機能

・すべてのユーザーログオンの持続性

### TrellixのGootloader追跡プロセス

Gootloaderの新亜種は、複数の難読化レイヤーを使用して進化しています。解凍（アンパック）後のネスト化されたステージは、それよりも前のステージで読み込まれた変数を使用するため、分析が一層難しくなっています。弊社のYARAハンティング活動を通じて収集されたサンプルは、JavaScriptとPowerShellの静的分析に取り込まれ、リモートコマンド＆コントロール（C&C、C2）サーバーやユニークIDを持つシグネチャなどのIoCを抽出します。これらのIoCを使用し、広く出回っているGootloaderのインスタンスを特定して、追跡することができます。

抽出されたGootloaderのIoCは、TrellixのURLレピュテーションチームのデータベースに照会（クエリー）され、悪意のあるドメイン、侵害された可能性のある正規のドメイン、そして分析の妨害を目的としたおとり（デコイ）として使用されている正規のドメインが特定されるように処理されます。

### Gootloaderの遠隔観測に基づくインサイト

以下に示されている統計データは、抽出したIoCとTrellixのお客様のログとの相関分析によって特定されたキャンペーンに関するものであり、検出そのものに関する統計データではありません。Gootloaderの場合、検出の大多数は、ドメインへの攻撃に基づいくものです。Gootloaderはおとりドメインを使用しているため、示されている統計データは中程度の信頼度で悪意のあるものとして検出されたと解釈してください。

#### 2022年第4四半期に最もGootloaderの被害を受けた国

**37%**

2022年第4四半期に最もGootloaderの被害を受けた国は、米国となっています。

| | |
|---|---|
| 1. 米国 | 37% |
| 2. イタリア | 19% |
| 3. インド | 11% |
| 4. インドネシア | 9% |
| 5. フランス | 5% |

#### 2022年第4四半期にGootloaderで最もよく選ばれたMITRE ATT&CK手法

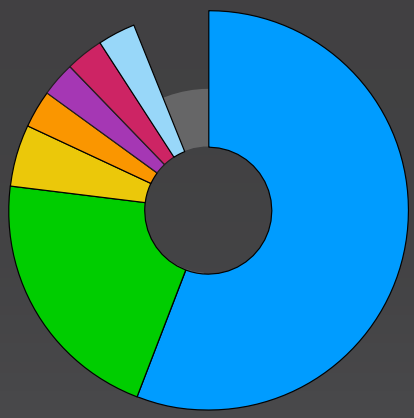
1. 難読化解除/ファイルまた情報の解読
2. JavaScript
3. 難読化されたファイルまたは情報
4. PowerShell
5. プロセスハロウイング

### 2022年第4四半期に最もGootloaderの標的とされたセクター

# 56%

2022年第4四半期に最もGootloaderの
標的とされたセクターは、通信となっています。

- 通信
- メディア&コミュニケーション
- 金融
- 教育
- テクノロジー
- 政府
- 消費者



### 2022年第4四半期にGootloaderが最も利用したMITRE攻撃手法

難読化解除/ファイルまたは情報の解読

JavaScript

難読化されたファイルまたは情報

PowerShell

プロセスハロウイング

反射型コード読み込み

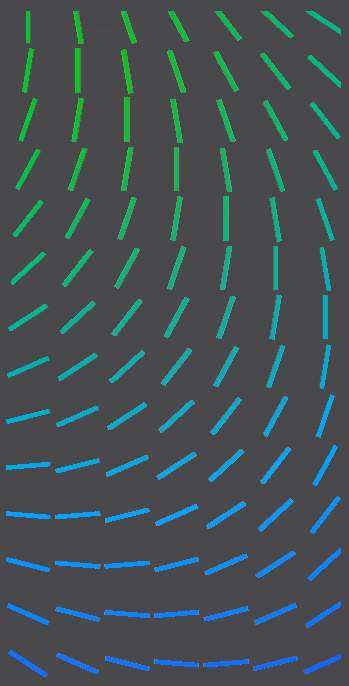
レジストリ実行キー/スタートアップフォルダ

Rundll32

スケジュール設定されたタスク

## 2022年第4四半期の脆弱性に関するインテリジェンス

Trellixの脆弱性ダッシュボードは、最新かつ影響度の高い脆弱性の分析データを照合してします。分析とトリアージは、Trellix Advanced Research Centerの脆弱性に関する専門家が実施します。
リバースエンジニアリングと脆弱性分析を専門とするこれらの研究者は、最新の脆弱性と、攻撃者がどのようにこれらの脆弱性を利用して攻撃を行うのかを継続的に監視し、是正ガイダンスを提供します。この簡潔ながら技術的に高度な専門的アドバイスにより、ノイズから脅威の兆候を洗い出し、組織に影響を及ぼす可能性のある最も影響度の高い脆弱性に焦点を当て、迅速に対応することが可能になっています。



## 2022年第4四半期の脆弱性インテリジェンスに関するハイライト

**41%**

2022年第4四半期に脆弱なプロダクトおよびベンダーに影響を与えた固有のCVEのうち、41%がLannerの脆弱性となっています。

**29%**

2022年第4四半期に最もCVEの利用が報告された製品は、Lanner IAC-AST2500Aのファームウェアのバージョン1.10.0でした。

### 2022年第4四半期に最も影響を及ぼした脆弱なプロダクト、ベンダー、CVE

| | | |
|---|---|---|
| 1. | Lanner | 41% |
| 2. | Microsoft | 19% |
| 3. | BOA | 15% |
| 4. | Oracle | 8% |
| 5. | Apple<br>Chrome<br>Citrix<br>Fortinet<br>Linux | 各 5% |

### 2022年第4四半期にCVEが報告された製品

**29%**

2022年第4四半期に使用された製品のうち、最もCVEが報告されたのは、Lanner IAC-AST2500Aのバージョン1.10.0のファームウェアとなり、次いでBOA Serverが10%、Lanner IAC-AST2500Aが6%、Exchangeが6%となっています。

| CVEの利用が報告された製品 | 固有のCVE数 |
|---|---|
| Lanner IAC-AST2500Aのバージョン1.10.0のファームウェア | 9 |
| BOAサーバー | 3 |
| Exchange | 3 |
| IAC-AST2500A | 2 |
| tvOS | 1 |
| iPadOS | 1 |
| iOS | 1 |
| Windows | 1 |
| Safari | 1 |
| SQLite 3.40.0 を含む、それ以前のバージョン | 1 |
| Oracle Access Manager のバージョン11.1.2.3.0、12.2.1.3.0、12.2.1.4.0 | 1 |
| MacOS | 1 |
| Linux Kernel の5.15.61以前のバージョン | 1 |
| Internet Explorer | 1 |



| CVEの利用が報告された製品 | 固有のCVE数 |
|---|---|
| FortiOS（sslvpnd） | 1 |
| Citrix ADC/Citrix Gateway | 1 |
| Chrom の108.0.5359.94/.95以前のバージョン | 1 |
| BOAサーバーのBoa 0.94.13のバージョン | 1 |

### 2022年第4四半期に報告されたCVE

CVE-2022-1786
CVE-2022-26134
CVE-2022-27510
CVE-2022-27518
CVE-2022-31685
CVE-2022-32917
CVE-2022-32932
CVE-2022-33679
CVE-2022-34718
CVE-2022-35737
CVE-2022-3602
CVE-2022-3786
CVE-2022-37958
CVE-2022-40684
CVE-2022-41040
CVE-2022-41080
CVE-2022-41082
CVE-2022-41128
CVE-2022-41352
CVE-2022-42468
CVE-2022-42475
CVE-2022-4262
CVE-2022-42856
CVE-2022-42889
CVE-2022-43995
CVE-2022-46908
CVE-2022-47939

## 2022年第4四半期のメールセキュリティの傾向

メールセキュリティに関する統計データは、世界中のお客様のネットワークに展開されている複数のメールセキュリティアプライアンスから生成された遠隔測定に基づいています。以下のセクションでは、検出ログを集計・分析した調査結果を提示しています。

### 2022年第4四半期のメールセキュリティの傾向に関するハイライト

**100%**

2022年10月、アラブ諸国における悪意のあるメールの量は、同年8月、9月と比較して100%増加していることが確認されました。

**40%**

アラブ諸国を標的としたキャンペーンのうち、最も利用されたマルウェアの手口は「Qakbot」で全体の40%を占めています。

**42%**

2022年第4四半期に最も悪意のあるメールの影響を受けたセクターは通信となり、各種業界を標的としたすべての悪意のあるメールキャンペーンのうち、42%を占めています。



**87%** 2022年第4四半期に最も広く利用された攻撃ベクトル（経路）のうち、悪意のあるURLを利用したフィッシングメールが87 %となり、圧倒的多数を占めています。

**64%** 2022年第3四半期から第4四半期にかけて、なりすまし攻撃が64%の増加となっています。

**82%** 全てのCEO詐欺メールのうち、 82%が無料のメールサービスを利用して送信されています。

**78%** 全てのビジネスメール詐欺（BEC）による攻撃のうち、78%がCEOが一般的に使用するフレーズが使われています。

**142%** 2022年第4四半期はビッシング攻撃が顕著となり、2022年第3四半期に比べ、142%の増加となっています。

### 2022年第4四半期に最も蔓延したメールマルウェア

**40%**

2022年第4四半期に最も蔓延したメールマルウェアは、「Oakbot」となっています。

| | | |
|---|---|---|
| 1. | Qakbot | 40% |
| 2. | Emotet | 26% |
| 3. | Formbook | 26% |
| 4. | Remcos | 4% |
| 5. | QuadAgent | 4% |

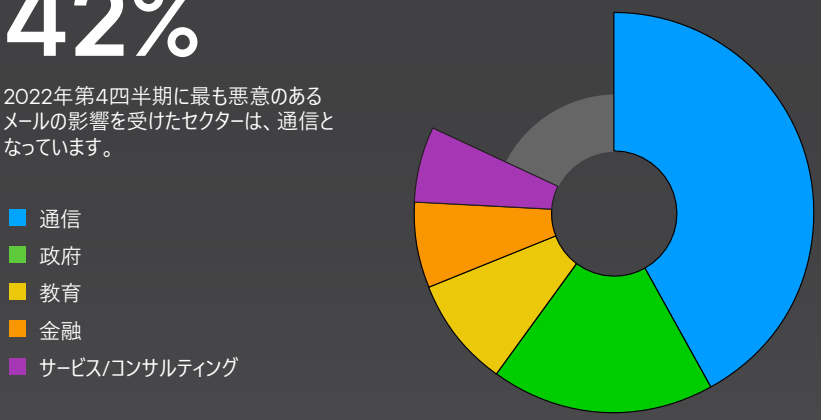
### 2022年第4四半期に最もメールフィッシング攻撃の標的とされた製品やブランド

| | | |
|---|---|---|
| 1. | 商標登録なし | 62% |
| 2. | Outlook | 13% |
| 3. | Microsoft | 11% |
| 4. | Ekinet | 8% |
| 5. | Cloudfare | 3% |

### 2022年第4四半期に最も悪意のあるメールの影響を受けたセクター

**42%**

2022年第4四半期に最も悪意のあるメールの影響を受けたセクターは、通信となっています。



## 2022年第4四半期のなりすましメール（Email Impersonation）の傾向に関するハイライト

**82%** 全てのCEO詐欺メールのうち、 82%が無料のメールサービスを利用して送信されています。

**78%** 全てのビジネスメール詐欺（BEC）による攻撃のうち、78%がCEOが一般的に使用するフレーズが使われています。

**64%** 2023年第3四半期から第4四半期にかけて、CEOなどのビジネスリーダーを装った悪意のあるメールが64%増加しています。

## 2022年第4四半期にBEC攻撃で使われたCEOのフレーズ：

"I need you to carry out a task for me immediately."

"I need you to get a task done so kindly forward me your cell phone number."

"Send me your phone number, You need to get something done for me right now."

"Please send me your cell number and keep an eye out for my text. I need a task completed."

"Please review and confirm your cellphone number and keep a lookout to my text for instructions."

"Did you receive my previous email? I have a Profitable deal for you."

### 2022年第4四半期のなりすましに関する比較データ

**64%** 2022年第3四半期から第4四半期にかけて、なりすまし攻撃が64％増加しました。



## 2022年第4四半期のフィッシングキャンペーンに関するインサイト

### 詐欺や窃盗にWebホスティングプロバイダを使用するケースが増加

2022年第4四半期、正規のWebホスティングプロバイダを利用した、ユーザーに対する詐欺やユーザーの認証情報の窃盗が増加が確認されました。主にdweb.link、ipfs.link、translate.googという3つのサービスプロバイダが悪用されていました。また、ekinet、storageapi_fleek、selcdn.ruといった他のサービスプロバイダのドメインが悪用されたケースも多数確認しています。前述したこれらのドメインのような、他のサービスプロバイダのドメインもいくつか確認しました。攻撃者は、フィッシングページをホストとし、またアンチフィッシングエンジンを回避するために、新しく普及しているホスティングサービスを利用する傾向が続いています。

**フィッシングメールで最も利用された攻撃ベクトル**

**87%**

2022年第4四半期にフィッシングメールで最も利用された攻撃ベクトルは悪意のあるURLで、圧倒的多数を占めていました。

| | |
|---|---|
| 1. URL | 87% |
| 2. 添付 | 7% |
| 3. ヘッダー | 6% |

攻撃者が正規のWebホスティングプロバイダの利用に強い関心を示すようになってきた理由の1つには、これらのサービスは正規ファイルのホストし、コンテンツを共有することを主な目的としているため、どの検知システムのブラックリストにも登録できないことが挙げられます。

**2022年第4四半期に最も悪用されたWebホスティングサービス**

**154%**

2022年第4四半期に最も悪用されたWebホスティングプロバイダはDwebですが、第4四半期に最も増加の伸びが高かったのはGoogle翻訳で、第3四半期と比較して154％の増加となっています。

| | |
|---|---|
| 1. Dweb | 81% |
| 2. Ipfs | 17% |
| 3. Google翻訳 | 10% |

**2022年第4四半期にフィッシング攻撃で最も利用された回避型の手法**

**63%**

2022年第4四半期に最も顕著であった回避型の手法は、302リダイレクトをベースとするものとなっています。

- 2022年第4四半期、地理情報をベースとした回避型の手法によるフィッシング攻撃が大幅に増加
- 2022年第4四半期中には、Captchaベースの攻撃も増加



## 2022年第4四半期のビッシングに関するインサイト

ビッシングとは、フィッシングの一種で、主に電子メール、テキストメッセージ、通話、ダイレクトチャットメッセージなどを使い、被害者の気を引いて、彼らを攻撃者に接続させるように仕組まれた攻撃です。

**142%** 2022年第4四半期はビッシング攻撃が顕著であり、2022年第3四半期と比較して142% の増加となっています。

**85%** ビッシングを用いる攻撃者は、無料のメールサービスを好んで利用しています。弊社が2022年第4四半期に検知したビッシング攻撃のうち、無料のメールサービスを利用して送信された攻撃が全体の85%にも上っていました。

2022年第4四半期のビッシングキャンペーンで最も多用されたテーマは、**Norton、McAfee、Geek Squad、Amazon、PayPal**でした。

## 2022年第4四半期のネットワークセキュリティ

Trellix ARCのネットワーク調査チームは、弊社のお客様を脅かすネットワークベースの攻撃を検知し、遮断することに焦点を当てています。私たちは、偵察、初期侵害、C2通信、また同様にラテラルムーブメント（横移動）などのTTPを含め、サイバーキルチェーンのさまざまな領域を綿密に調査しています。弊社は、統合により強化されたテクノロジーの強みを活かすことで、未知の脅威をより適切に検出するための可視性を確保しています。

### 2022年第4四半期にネットワークセキュリティへの対抗手段として最も利用されたMITRE ATT&CK手法

- T1083 - ファイルとディレクトリの検出
- T1573 - 暗号化されたチャネル
- T1020 - 自動化された持ち出し
- T1210 - リモートサービスの悪用
- T1569 - システムサービス
- T1059.003 - コマンドとスクリプトのインタープリタ：Windowsコマンドシェル
- T1047 - Windows Management Instrumentation（WMI）
- T1087 - アカウントの検出
- T1059 -コマンドとスクリプトのインタープリタ
- T1190 - 外部公開アプリケーションへのエクスプロイト



## 2022年第4四半期の外部向けサービスに最も影響を与えた攻撃

お客様の環境に対する潜在的な閾値を見つけるため、外部向けのマシーンをプローブ（探査）する多くのネットワークスキャンが毎日実行されています。古いエクスプロイトは、今もパッチが適用されていないシステムを探しています。

- ファイル/その他/パスワードへのアクセス試行の検出
- クロスサイトスクリプティング攻撃の可能性
- SIPViciousセキュリティスキャナー
- Nmapを使ったスキャンにてトラフィックを検出
- スキャン活動 - Shellshock、Webサーバーのプロービング
- Bashリモートコード実行（Shellshock）HTTP CGI (CVE-2014-6278)
- Oracle WebLogic CVE-2020-14882　リモートコード実行の脆弱性
- ディレクトリトラバーサルの試行
- Apache Struts 2 ConversionErrorInterceptor OGNLスクリプトインジェクション
- Apache Log4j CVE-2021-44228　リモートコード実行

## 2022年第4四半期にネットワークへアクセスする最初の足掛かりとして最も利用されたWebShell

脆弱なWebサーバーを操作しようとする場合には、一般的に以下のWebShellが利用されていることを確認しています。

- China Chopper WebShell
- JFolder WebShell
- ASPXSpy WebShell
- C99 WebShell
- Tux WebShell
- B374K WebShell / RootShellファミリー



## 2022年第4四半期のネットワーク侵入後に最も利用されたツール、手法、手順

脆弱なWebサーバーを操作しようとする場合に、以下のWebShellが利用されていることが一般的に確認されています。

攻撃者がラテラルムーブメント時に使用するTTPには、古い脆弱性やSCShellやPSExecのようなツールの利用が多く見られることが確認されています。

- SCshell: サービスマネージャーを利用したファイルレスのラテラルムーブメント
- Windows WMIのRemote Process Call （リモートプロセスの呼び出し）
- SMB上のWMIEXECを介したCMDシェルの呼び出し
- EternalBlueエクスプロイトの検出
- Microsoft SMBv3 CVE-2020-0796の試行
- Apache Log4j CVE-2021-44228のリモートコード実行（RCE）
- ドメイン/エンタープライズ管理者アカウントのリモートエミュレーション
- 不審なPowerShell Remoting（ PowerShellのリモート処理）
- WMICを使用した不審なネットワーク偵察
- バッチファイルで検出されたエミュレーションコマンド
- SMB PsEXEc Activity（SMBのPSExecを操作）

## Trellix XDRによるセキュリティオペレーションの遠隔観測

以下の統計データは、Trellixの顧客基盤に渡って展開されるさまざまなセンサーから生成された遠隔観測に基づいています。以下のセクションでは、検出ログを集計・分析した結果を提示してします。

2022年第4四半期に最も影響を及ぼしたセキュリティインシデント

2022年第4四半期に最も頻発したセキュリティアラートは、以下の通りです。

EXPLOIT - LOG4J [CVE-2021-44228]
（エクスプロイト - LOG4J [CVE-2021-44228]）

OFFICE 365 ANALYTICS [Abnormal Logon]

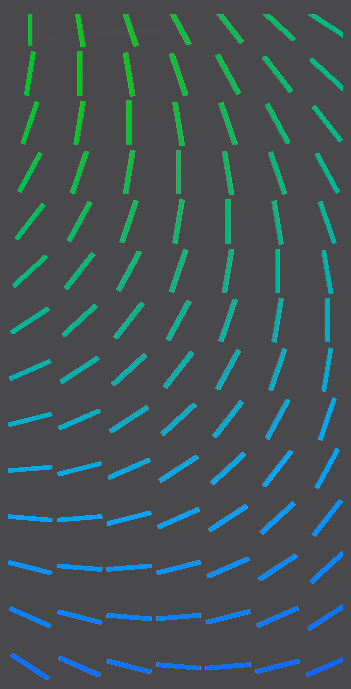
（OFFICE 365 Analytics [異常なログイン] ）

OFFICE 365 [Allowed Phish]
（OFFICE 365 [フィッシングの許可]）

EXPLOIT - FORTINET [CVE-2022-40684]
（エクスプロイト - FORTINET [CVE-2022-40684]）

EXPLOIT - APACHE SERVER [CVE-2021-41773 - Attempt]
（エクスプロイト – APACHEサーバー [CVE-2021-41773 – 試行]）





WINDOWS ANALYTICS [Brute Force Success]
（WINDOWS Analytics [ブルートフォース攻撃の成功] ）

EXPLOIT - ATLASSIAN CONFLUENCE [CVE-2022-26134]
（エクスプロイト - ATLASSIAN CONFLUENCE [CVE-2022-26134]）

EXPLOIT - F5 BIG-IP [CVE-2022-1388 Attempt]
（エクスプロイト - F5 BIG-IP [CVE-2022-1388の試行]）

### 2022年第4四半期に最も利用されたMITRE ATT&CK手法

| | | |
|---|---|---|
| 1. | 外部公開されたアプリケーションへの攻撃（T1190） | 29% |
| 2. | アプリケーションレイヤープロトコル：DNS （T1071.004） | 14% |
| 3. | フィッシング（T1566） | 14% |
| 4. | アカウント操作（T1098.001） | |
| 5. | ブルートフォース（総当たり攻撃） （T1110）<br>ドライブ・バイ・コンプロマイズ（ドライブバイ攻撃） （T1189）<br>ユーザー実行：悪意のあるファイル（T1204.002）<br>有効なアカウント：ローカルアカウント（T1078,003） | 各 7% |

### 2022年第4四半期に最も利用されたログソースの内訳

| | | |
|---|---|---|
| 1. | ネットワーク | 40% |
| 2. | メール | 27% |
| 3. | エンドポイント | 27% |
| 4. | ファイアウォール | 6% |

## 2022年第4四半期に観測されたエクスプロイト

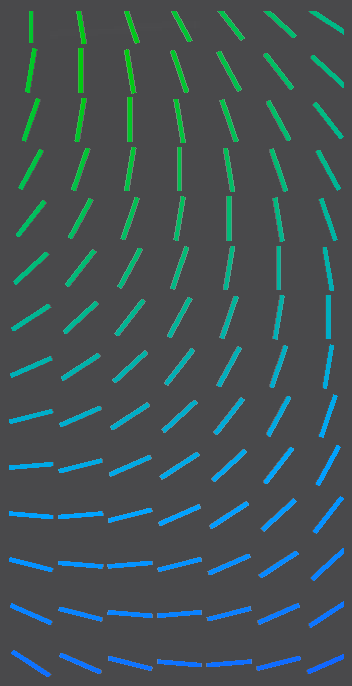
### 2022年第4四半期に最も蔓延したエクスプロイト

**30%**

2022年第4四半期に最も蔓延したエクスプロイトは、Log4jとなっています。

| | | |
|---|---|---|
| 1. | Log4j（CVE-2021-44228） | 30% |
| 2. | Fortinet（CVE-2022-40684） | 16% |
| 3. | Apacheサーバー（CVE-2021-41773） | 15% |
| 4. | Atlassian Confluence（CVE-2022-26134） | 14% |
| 5. | F5 Big-IP（CVE-2022-1388の試行） | 13% |
| 6. | Microsoft Exchange（ProxyShell エクスプロイトの試行） | 11% |





## 2022年第4四半期のクラウドインシデント

多くの企業がオンプレミスのインフラから移行している状況の中、クラウドインフラへの攻撃が絶えず増加しています。Gartner社のアナリストは、2025年までに85%以上の組織がクラウドファーストの原則を採用すると予測しています。

Trellixは、2022年第4四半期の遠隔観測を分析し、以下の点を確認しました。

- AWSでの検出が突出している理由は、AWSがクラウド市場で主要なリーダーとしての地位を確立しているためと推測される
- 大多数の攻撃は、ブルートフォース/パスワードスプレー攻撃で有効なアカウントへの初期アクセスを得ることに狙いを定めており、これがクラウド攻撃対象領域への初期感染経路になっている
- 多数の企業アカウントで多要素認証（MFA）が有効になっており、ブルートフォース攻撃に成功した攻撃者はMFAプラットフォームに到達（侵入）できるため、MFA関連の検出が急増する結果となっている

以下のセクションでは、クラウドプロバイダー別に、Trellixの顧客基盤におけるクラウドベースの攻撃に関する遠隔観測に基づくインサイトを簡潔に説明します。

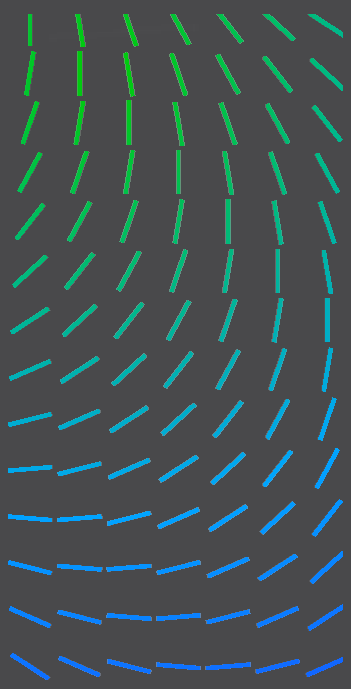
### 2022年第4四半期にAWSで最も検出されたMITRE ATT&CK手法の内訳

| | |
|---|---|
| 1. 有効なアカウント（T1078） | 18% |
| 2. クラウドコンピュートインフラストラクチャの改ざん（T1578） | 12% |
| 3. アカウント操作（T1098） | 9% |
| 4. クラウドアカウント（T1078.004） | 8% |
| 5. ブルートフォース攻撃<br>（総当たり攻撃）（T1110）<br>防御の妨害（T1562） | 各 6% |

### 2022年第4四半期にAzureで最も検出されたMITRE ATT&CK手法

| | |
|---|---|
| 1. 有効なアカウント（T1078） | 23% |
| 2. 多要素認証（MFA）（T1111） | 19% |
| 3. ブルートフォース攻撃（総当たり攻撃）（T1110） | 14% |
| 4. プロキシ（T1090） | 14% |
| 5. アカウント操作（T1098） | 5% |





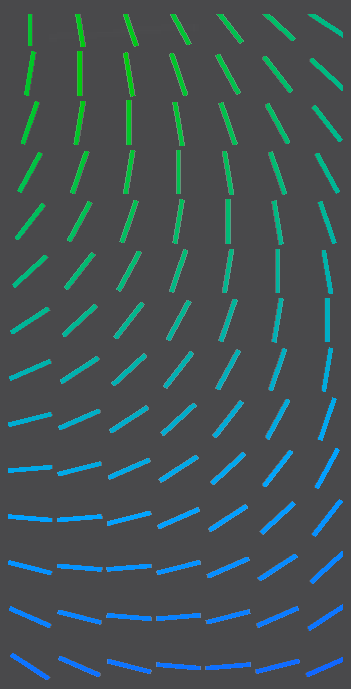
### 2022年第4四半期にAWSで最も検出されたMITRE ATT&CK手法

| MITRE手法 | ルール |
|---|---|
| アカウント操作（T1098） | AWS - IAM Identityにアタッチされた権限ポリシーの操作<br>AWS S3 - バケットポリシーの削除 |
| 有効なアカウント（T1078） | AWS Analyticsコンソールへの異常なログイン<br>AWS Analytics APIキーの異常な利用<br>AWS Guarddutyでの匿名ユーザーの振る舞い<br>AWS Guarddutyへの匿名アクセス権限の付与 |
| 防御の妨害（T1562） | AWS Cloudtrailのポリシーの変更<br>AWS Cloudtrailの証跡の削除 |
| ファイル内の認証情報（T1552.001） | AWSの秘密鍵が盗まれた可能性に関する警告 |
| クラウドコンピュートインフラストラクチャの改ざん（T1578） | AWS CloudtrailによるS3バケットの削除<br>AWS CloudTrailによるS3 バケットのACLの追加（プット）<br>AWS CloudtrailによるObject ACLの追加（プット） |

### 2022年第4四半期にAzureで最も検出されたMITRE ATT&CK手法

| MITRE ATT&CK手法 | ルール |
|---|---|
| 有効なアカウント（T1078） | Azure ADへの危険なサインイン<br>不自然な場所からのAzureへのログイン<br>60日以内にAzureへのログインがないアカウント |
| ブルートフォース攻撃（T1110） | Azureポータルに対するMicrosoft Graphを介したブルートフォース攻撃によるAzureへの認証に複数回失敗<br>Microsoft Graphを介した分散したパスワードクラッキングの試行 |
| 多要素認証の傍受（T1111） | 不正アラートを理由とするAzure MFAの拒否<br>ユーザーがブロックされていることを理由とするAzure MFAの拒否<br>不正コードを理由とするAzure MFAの拒否<br>不正アプリを理由とするAzure MFAの拒否 |
| 外部リモートサービス（T1133） | TorネットワークからAzureへのサインイン |
| アカウント操作（T1098） | Azureでの不自然なユーザーパスワードのリセット |





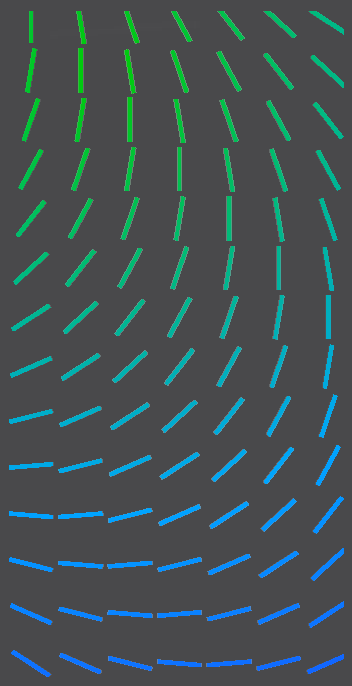
## 2022年第4四半期にGCPで検出されたMITRE ATT&CK手法の内訳

| | | |
|---|---|---|
| 1. | 有効なアカウント（T1078） | 36% |
| 2. | APIによる実行（T0871） | 18% |
| 3. | アカウントの検出（T1087.001）<br>アカウント操作（T1098） | |
| 4. | 防御の妨害（T1562）<br>クラウドコンピュートインフラストラクチャの改ざん（T1578）<br>リモートサービス：SSH（T1021.004） | 各 9% |

## 2022年第4四半期にGCPで最も検出されたMITRE ATT&CK手法

| MITRE ATT&CK手法 | ルール |
|---|---|
| 有効なアカウント（T1078） | GCPによるサービスアカウントの作成<br>GCP Analyticsによる異常な操作<br>GCPによるサービスアカウントキーの作成 |
| リモートサービス：SSH（T1021.004）<br>アカウント操作（T1098） | GCPファイアウォールがSSHポートのすべてのトラフィックを許可<br>GCP組織によるIAMポリシーの変更 |
| アカウントの検出（T1087.001） | アラート ["gcps net user"] |
| クラウドアカウントへのデータ転送（T1537） | GCPのロギングシンクの改ざん |
| クラウドコンピュートインフラストラクチャの改ざん（T1578） | GCPの削除保護の無効化 |





## 著者および研究者

Alfred Alvarado
Henry Bernabe
Adithya Chandra
Dr. Phuc Duy Pham
Sarah Erman
John Fokker
Lennard Galang
Sparsh Jain
Daksh Kapoor
Maulik Maheta
João Marques
Tim Polzer
Srini Seethapathy
Rohan Shah
Vihar Shah
Swapnil Shashikantpa
Shyava Tripathi
Leandro Velasco

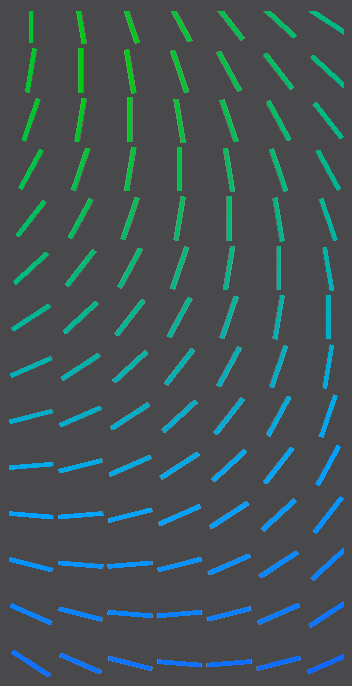
## リソース

以下の Trellix のリソースをご活用いただき、Trellix Advanced Research Centerによる最新の脅威や調査結果の把握にお役立てください。

### TWITTER

Trellix ARC





## TRELLIX ADVANCED RESEARCH CENTERについて

Trellix Advanced Research Centerは、サイバーセキュリティ業界で最も包括的な憲章を掲げ、あらゆる脅威の状況における新たな手法、傾向、そして攻撃者に対する最前線を担っています。Trellix Advanced Research Centerは、世界のセキュリティオペレーションチームの主要パートナーとして、セキュリティアナリストにインテリジェンスと最先端のセキュリティ情報を提供すると同時に、業界をリードするTrellixのXDRプラットフォームを強化しています。

## TRELLIXについて

Trellixは、サイバーセキュリティの未来を再定義するグローバル企業です。TrellixのオープンかつネイティブでXDR（Extended Detection and Response）プラットフォームは、現在最も高度な脅威に直面するお客様が業 務の保護や回復に確信を持って対応するための支えとなります。Trellixのセキュリティ専門家は、広範なパートナーエコシステムとともに、データサイエンスと自動化によりテクノロジーイノベーションを加速させ、4万を超える企業や政府機関のお客様の力となっています。詳しくは、www.trellix.comをご覧ください。



詳しくは、 Trellix.comをご覧ください。



072022-05