提供

Trellix ADVANCED RESEARCH CENTER

脅威レポート

2023 年 2 月

目次

2022 年第 4 四半期の脅威の概要

2022 年の最後の数か月間も、攻撃者は依然として手ごわい敵でした。それに対抗するために、Trellix Advanced Research Center では、数百人の選り抜きのセキュリティ アナリストおよび研究者のチームに、さらに多くの脅威情報リソースを提供しました。

「つまり、私たちは脅威インテリジェンスを次のレベルに高めたのです。それは、よりシンプルなセキュリティで、SecOps の混乱を落ち着かせるためです。より少ないストレスで、セキュリティ成果を向上させるためです。脅威は進化し続けています。そして、皆さんも進化し続けることができます。」

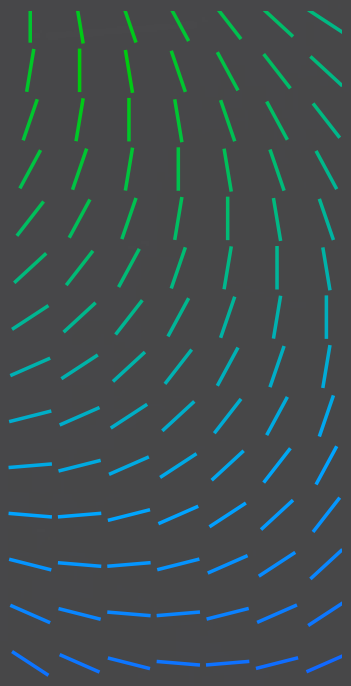
本レポートでは、前四半期に流行した攻撃者、ファミリー、キャンペーン、好まれた手法を業界屈指のラインナップで紹介しています。しかし、それだけではありません。情報源を拡張して、ランサムウェアのリーク サイトやセキュリティ業界のレポートからもデータを取得しています。また、Trellix のリソースの増加に伴い、ネットワーク セキュリティ、クラウド インシデント、エンドポイント インシデント、セキュリティ運用を扱った新しいコンテンツを含む脅威研究のカテゴリも増えています。

前回の脅威レポート以降、Trellix Advanced Research Center は、世界各地で研究と調査を行ってきました。そこでは、第 4 四半期のウクライナを標的としたサイバー攻撃の大幅な増加と Gamaredon との関連性が指摘されています。また、61,000 の脆弱なオープンソース プロジェクトにパッチを適用し、2023 年の脅威予測で、新たな年の過去にない攻撃に関するインサイトを公開しました。

これらの脅威レポートの向上によって得られた以下の概要は、お客様やセキュリティ業界が脅威の結果をより実感できるようにするために、Trellix Advanced Research Center が行っている取り組みを示す例となっています。

ランサムウェア

- 第 4 四半期に最も影響力のあったランサムウェア グループとして LockBit 3.0 が突出していることに関する分科会の調査
- ランサムウェアが米国を中心に世界的に流行し続けている
- 産業財・サービスを含むセクターを標的としたランサムウェア



国民国家

- 政府機関や運輸業を含むセクターを標的とした国家ぐるみの手口
- 国民国家による活動の影響を受ける、米国に拠点を置く企業

Living Off the Land (環境寄生)

- Trellix Advanced Research Center のハンティング手法により、流行中の Cobalt Strike に関する幅広いインサイト
- 中国のクラウド プロバイダーでホストされている多数の Cobalt Strike Team のサーバー
- 報告されたキャンペーンで最も多く見られた OS バイナリの上位 10 個のうち、約半数を占めている Windows Command Shell

攻撃者

- 中国、北朝鮮、ロシアが、攻撃が流行している国の上位にランクイン

メール セキュリティの傾向

- 世界的なサッカー大会期間中に観察された、アラブ諸国における大量の悪意のあるメール
- なりすましの手口や、ビッシングでよく使われる企業テーマを含む、フィッシング詐欺やビッシングのキャンペーン

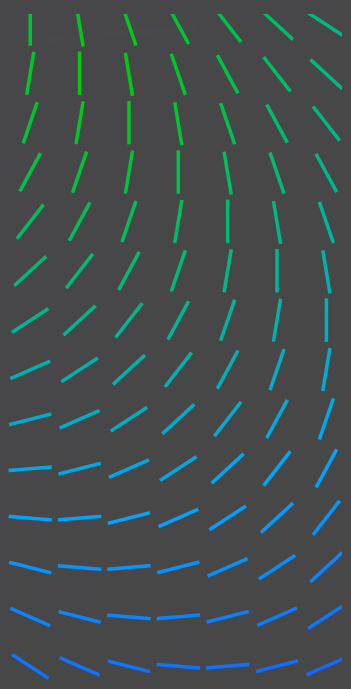
ネットワーク セキュリティ

- 四半期の最も影響力があり、重要で、関連性の高い攻撃、WebShell、ツール、および手口

Trellix XDR を活用したセキュリティ運用テレメトリ

- 一般的なセキュリティ 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 に対応した手法と検出
- 上位の手法と検出

2022 年第 4 四半期の脅威の概要



Threat Intelligence 責任者からの手紙

弊社の Advanced Research Center チームは、今年を締めくくる 2022 年第 4 四半期データの最初の脅威レポートを紹介できることを嬉しく思います。本レポートは、流行中のランサムウェアのリークサイトや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インサイトに加え、弊社の製品センサー アレイからの新しいデータを加えるなど、絶えず進化を続けています。Trellix では、お客様を不正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。攻撃者とその動機は決して止まることなく、より多面的になっているからです。地政学的および経済から見た先行きが複雑かつ不透明感が増す中で、グローバルな脅威インテリジェンスの必要性が高まっています。

世界的には、ウクライナ紛争による経済不安から、1970 年代以来の大規模なエネルギー価格ショックが発生し、世界経済に大きな打撃を与えています。ヨーロッパでの戦争の再発は、EU の安全保障・防衛に対するアプローチや、特にサイバー空間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っています。また、米政権は、地政学的な競争への対応、重要インフラストラクチャの保護、外国による情報操作や干渉への対処の必要性を認識していました。SolarWinds、Hafnium、ウクライナ、その他の出来事により、政権と議会は、国家のコミットメントと過去の米国政府の仕事に大きく立脚した新しいセキュリティ標準と資金調達について、超党派の行動を促しました。では、こうした不確実性は、企業のサイバーセキュリティ、公的・私的機関、民主主義の価値観にどのような影響を及ぼしているのでしょうか。

前四半期に、弊社のチームは、サイバーは政治的、経済的、領土的野心のために積極的に使用されるスパイ活動、戦争、虚偽情報の分野での国家戦略だと考えました。ウクライナにおける戦争では、新しい形態のサイバー攻撃も出現し、ハクティビストは、サイトの改ざん、情報の漏洩、DDoS (分散型サービス拒否) 攻撃の実行に精通し、より大胆になりました。その一方で、従来型のサイバー攻撃は続いています。フィッシング詐欺など、個人を騙し、操って機密情報や個人情報を流出させるソーシャル エンジニアリングの手口は、依然として流行しています。

ランサムウェアは、世界中の多くの組織を悩ませ続けています。COVID-19 のパンデミック時に観察されたように、サイバー犯罪者は危機と不確実性の時期に素早く利益を得ようとします。脅威の状況が進化するにつれて、私たちの研究も進化していきます。私たちの使命は、製品の有効性を常に改善し、実用的な情報をステークホルダーに提供することで、最も重要なものを確実に守ることにあります。本レポートでは、私たちの仕事が Trellix Advanced Research Center のメンバー全員にとっていかに重要であるかをご理解いただけるでしょう。私たちのチームには、ひとつひとつのプロジェクトに丁寧に心をこめて取り組んでいない研究者や専門家はいません。

この拡張レポートに対するご意見や、私たちのチームにもっと掘り下げてほしい分野があれば、私またはチーム @TrellixARC に Twitter でご連絡ください。そして、4 月にサンフランシスコで開催される RSA で多くの皆さんにお会いできることを楽しみにしています。

John Fokker
Threat Intelligence 責任者

方法

Trellix のバックエンド システムは、四半期ごとの脅威レポートのデータとして使用するテレメトリを提供しています。私たちは、テレメトリと、脅威に関するオープンソースのインテリジェンスや、ランサムウェア、国民国家の活動といった流行している脅威に関する独自調査を組み合わせて分析しています。

テレメトリを話題にするとき、感染ではなく、検出がその焦点になります。検出は、ファイル、URL、IP アドレス、その他の指標を弊社のいずれかの製品が検出し、弊社に報告したときに記録されます。

たとえば、本物のマルウェア サンプルを展開する有効性試験フレームワークを利用する組織が増加しています。この使用法は検出として表示されますが、感染でないことは明らかです。

テレメトリの誤検知を分析し、フィルタリングするプロセスは常に開発中であり、以前のエディションと比較すると、新たな脅威カテゴリが発生する可能性があります。

また、より多くの Trellix 組織チームがこの四半期レポートに貢献することで、新たな脅威カテゴリが追加されるでしょう。

大切なのは、お客様のプライバシーです。それは、テレメトリやお客様のセクターおよび国へのマッピングを行う際に重要です。国によって顧客ベースが異なるため、数字で見ると増えているように見えるかもしれませんが、もっと詳しくデータを調べる必要があります。たとえば、弊社のデータでは、電気通信セクターが常に高いスコアを記録しています。しかし、必ずしもこのセクターが多く狙われているというわけではありません。電気通信セクターには、企業が購入できる IP アドレス空間を所有する ISP プロバイダーも含まれています。それはどういう意味でしょうか? ISP の IP アドレス空間からの送信は電気通信セクターでの検出と見なされますが、異なるセクターで稼働している ISP クライアントからのものである可能性があります。

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されたさまざまなインサイトを提供します。この情報は、脅威の状況をよりよく把握し、監視バイアスを減らすために複数のソースから収集されており、2022 年第 4 四半期に最も影響力のあったランサムウェア ファミリーを判断するのに役立ちます。
最初のソースは定量的なソースで、ランサムウェアの IOC と Trellix の顧客テレメトリの相関から抽出されたランサムウェア キャンペーンの統計が描かれています。2 つ目は定性的なソースで、セキュリティ業界が発行するさまざまなレポートを Threat Intelligence グループが厳しく吟味・分析・分析した結果が示されています。最後に、3 つ目のソースは新しいカテゴリで、さまざまなランサムウェア グループの「リーク サイト」から集められたランサムウェア被害レポートのセットで構成されます。これらは正規化・強化を経て、最後に分析され、結果が匿名化の上、提供されます。

こうしてさまざまな視点を提供することで、現在の脅威の状況を構成しているパズルの多くのピースを提供することを目的としています。しかし、それぞれに制約があるため、どれも十分とは言えません。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るわけでもありません。また、すべての被害者が強要されてリーク サイトに掲載されるわけでもありません。しかし、異なる視点を組み合わせることで、さまざまな脅威をよりよく理解し、自らの盲点を減らすことができます。

情報に基づく判断は、潜在的な欠点や盲点を考慮しながら、ソースからの定量的・定性的なデータを組み合わせることで得られます。

2022 年第 4 四半期のランサムウェアのハイライト

第 4 四半期の最も影響力のあるランサムウェア グループ : LockBit 3.0

Trellix のさまざまなソースを観察した結果、2022 年第 4 四半期に最も影響力のあったランサムウェア 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 の重要な地位は、次のような特徴に基づいています。

3 位 Trellix のグローバル センサーから得られたランサムウェア テレメトリ分析によると、LockBit 3.0 は、四半期に最も多く見られたランサムウェア グループの中で第 3 位でした。

2 位 Threat Intelligence グループが収集した各種キャンペーンを分析した結果、LockBit 3.0 はセキュリティ業界による報告が最も多かったランサムウェア グループの中で、Cuba ランサムウェアと並んで第 2 位にランクインしました。

1 位 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たのは、LockBit 3.0 のリーク サイトでした。LockBit は、被害者を名指しで脅迫することでしきりに圧力をかけようとします。

2022 年第 4 四半期の LockBit のカテゴリと調査結果をさらに紹介します。

2022 年第 4 四半期の LOCKBIT 3.0 の影響を受けたセクター

29%

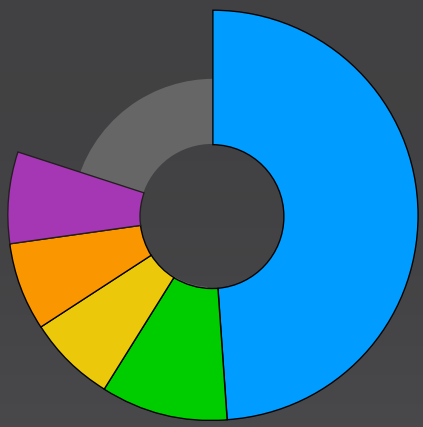
LockBit 3.0 の被害者リーク サイトによると、2022 年第 4 四半期に LockBit 3.0 の影響を最も多く受けたセクターは、産業財・サービスでした。

- 産業財・サービス
- 小売業
- テクノロジー
- ヘルスケア
- 建築・資材
- 人的財貨・家財
- 政府機関

2022 年第 4 四半期の LOCKBIT 3.0 の影響を受けた企業の国

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 LockBit 3.0 の影響を最も多く受けた企業の国は、米国 (49%)、次いで英国となっています。



- 米国
- 英国
- カナダ
- フランス
- ブラジル

LockBit 3.0 のツールおよびエクスプロイト

LOCKBIT 3.0 によって悪用されたことが判明している脆弱性

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

LOCKBIT 3.0 によって使用された悪意のあるツール

Amadey	Hakops
Blister	Neshta
BloodHound	SocGholish
Cobalt Strike	StealBit
Grabff	WinPEAS

LOCKBIT 3.0 によって使用され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	Process Monitor	WMIC
GMER	Netsh	Rundll32	RCLONE
MegaSync	Nltest		

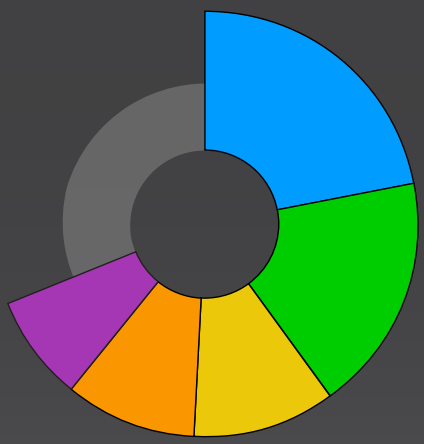
テレメトリの視点から見たランサムウェア

以下の統計は、弊社のテレメトリと Threat Intelligence ナレッジ ベースとの相関関係に基づいています。分析段階を受けて、選択した時間のデータからキャンペーンを特定し、その特徴を抽出します。表示される統計は、キャンペーンの統計であり、検出そのものではありません。弊社のグローバル テレメトリによると、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に属する侵害の痕跡 (IoC) が確認されました。確認されたキャンペーンで最も多く見られたランサムウェア ファミリーと、それぞれのツールや手法は、以下のとおりです。同様に、確認されたキャンペーンによる影響が特に大きかった国とセクターは、以下のとおりです。

2022 年第 4 四半期に最も多く見られたランサムウェア ファミリー

22%

2022 年第 4 四半期に最も多く見られたランサムウェア ファミリーは、Cuba でした。Zeppelin は Vice Society によって多用されました。Yanluowang の通信リークについては、こちらをお読みください。



- Cuba
- Hive
- LockBit
- Zeppelin
- Yanluowang

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多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 グループによって最も多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 グループによって使用されたことが最も多く観察された MITRE-ATT&CK 手法

1.	影響を与えるためのデータ暗号化	17%
2.	システム情報検出	11%
3.	PowerShell	10%
4.	イングレス ツール転送	10%
5.	Windows Command Shell	9%

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多用された悪意のないツール

21%

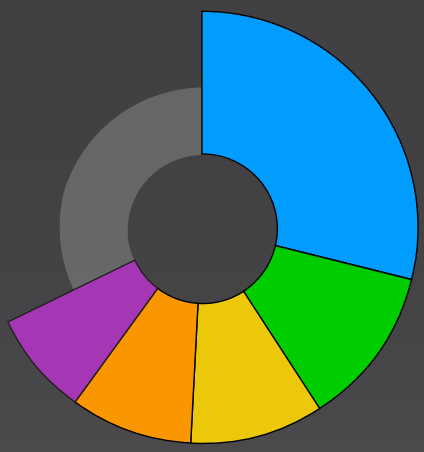
2022 年第 4 四半期にランサムウェア グループによって最も多用された悪意のないツールは、Cmd でした。

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

2022 年第 4 四半期にランサムウェア グループから最も影響を受けた国

29%

Trellix テレメトリによると、2022 年第 4 四半期にランサムウェア グループから最も多く影響を受けた国は、米国でした。

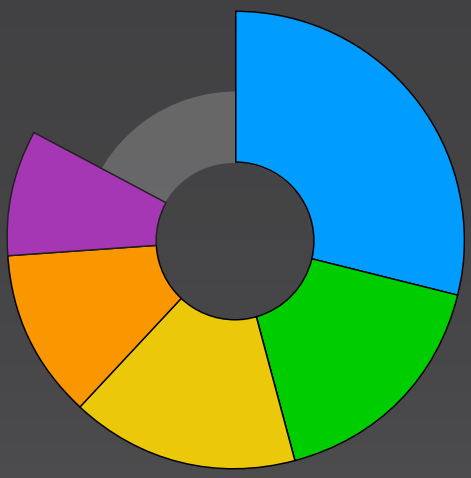


- 米国
- 中国
- カタール
- 日本
- インドネシア

2022 年第 4 四半期にランサムウェア グループから最も影響を受けたセクター

29%

Trellix テレメトリによると、2022 年第 4 四半期にランサムウェア グループから最も多く影響を受けたセクターは外部委託 & ホスティングでした。これは、ランサムウェアのリーク サイトに記載されている被害者の平均的な組織の規模と関連があります。これらの組織は、多くの場合、独自の割り当てられた IP ブロックを持たず、サード パーティのホスティング プロバイダーに依存しているという特徴があります。



- 外部委託 & ホスティング
- 銀行 / 金融 / ウェルス マネジメント
- 政府機関
- 卸売業
- 医薬品

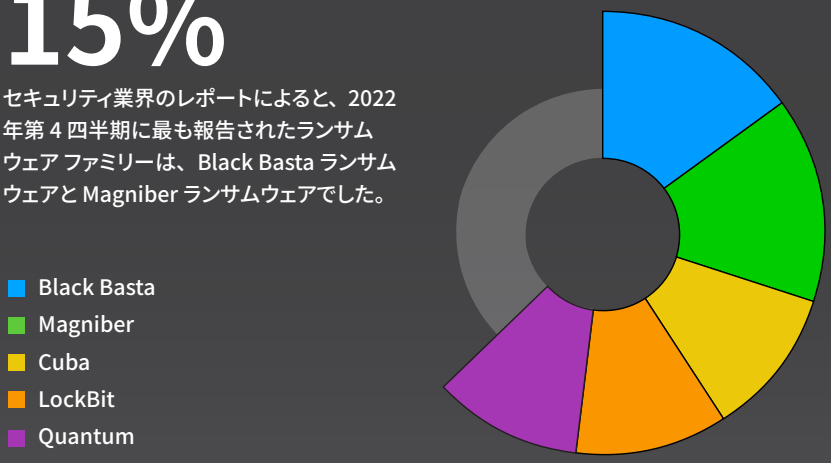
セキュリティ業界で報告されたランサムウェア

以下の統計は、公的報告書および社内調査に基づいています。なお、すべてのランサムウェア インシデントが報告されるわけではありません。多くのランサムウェア ファミリーはしばらくの期間、活動を続けており、当然ながら特定の四半期における新規ファミリーよりも注目度は低くなります。こうした基準に従って、これらのメトリックスは、セキュリティ業界が四半期に最も影響力があり、関連性があると判断したランサムウェア ファミリーを示しています。

2022 年第 4 四半期に最も多く報告されたランサムウェア ファミリー

15%

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 ファミリーは、Black Basta ランサムウェアと Magniber ランサムウェアでした。



2022 年第 4 四半期のランサムウェア ファミリーが使用した上位の攻撃手法

19%

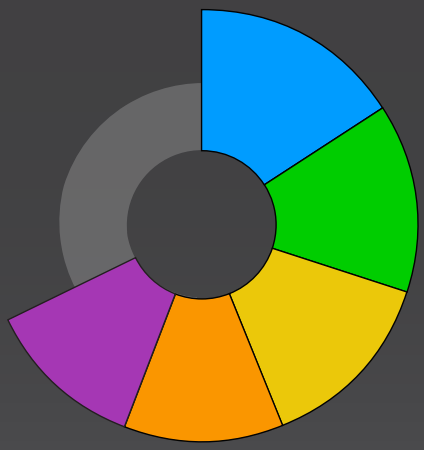
セキュリティ業界のレポートによると、2022 年第 4 四半期に最も報告されたランサムウェア ファミリーの攻撃手法は、「影響を与えるためのデータ暗号化」でした。

1.	影響を与えるためのデータ暗号化	19%
2.	Windows Command Shell	11%
3.	システム情報検出	10%
4.	イングレス ツール転送	10%
5.	PowerShell	10%

2022 年第 4 四半期のランサムウェア ファミリーの標的となった上位セクター

16%

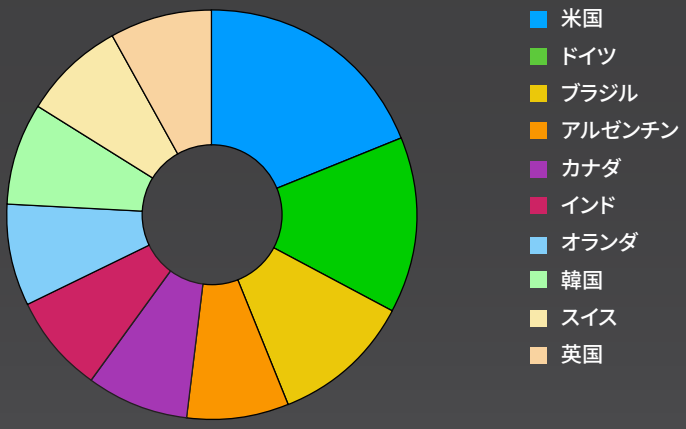
セキュリティ業界のレポートによると、2022 年第 4 四半期に最も多くランサムウェア ファミリーの標的となったセクターは、医療でした。



2022 年第 4 四半期に最も多くランサムウェア ファミリーの標的となった国

19%

セキュリティ業界のレポートによると、2022 年第 4 四半期に最も多くランサムウェア ファミリーの標的となった国は、米国でした。



2022 年第 4 四半期にランサムウェア ファミリーによって使用された 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 四半期のランサムウェア ファミリーによって使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 ファミリーによって最も多く使用された悪意のあるツールは、Cobalt Strike でした。

1.	Cobalt Strike	44%
2.	QakBot	13%
3.	IcedID	9%
4.	BURNTCIGAR	7%
5.	Carbanak SystemBC	7% 7%

2022 年第 4 四半期のランサムウェア ファミリーによって使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 ファミリーによって最も多く使用された悪意のないツールは、PowerShell でした。

1.	PowerShell	21%
2.	Cmd	18%
3.	Rundll32	11%
4.	VSSAdmin	10%
5.	WMIC	9%

2022 年第 4 四半期ランサムウェアの「リーク サイト」被害者レポート

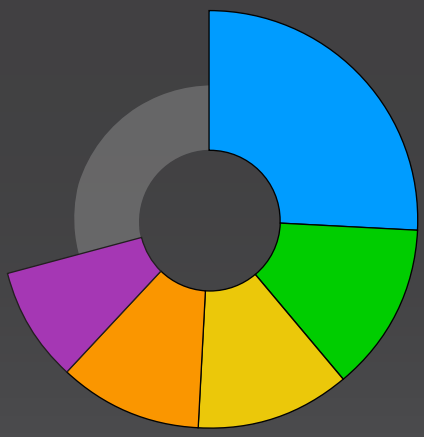
このセクションのデータは、さまざまなランサムウェア グループの「リーク サイト」を収集して作成されたものです。ランサムウェア グループは、これらの Web サイトに被害者の情報を公開することで、被害者を脅迫します。交渉が難航したり、被害者がランサムウェア グループの期限までに身代金の支払いを拒んだ場合、ランサムウェア グループは被害者から盗んだ情報を公開します。弊社では、オープンソース ツールの RansomLook を使用してさまざまな投稿を収集し、そのデータを内部処理して正規化・補強し、被害者分析結果を匿名で提供しています。

なお、各リーク サイトでは、すべてのランサムウェア被害者が報告されているわけではありません。多くの被害者が身代金を支払っており、その場合は報告されていません。これらのメトリックスは、ランサムウェア グループが脅迫や報復を行った被害者の指標であり、被害者の合計と混同しないようにする必要があります。

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 四半期にそれぞれのリーク サイトで最も多くの被害者を報告したランサムウェア グループ上位 10 個のうち、LockBit 3.0 が 26% を占めました。

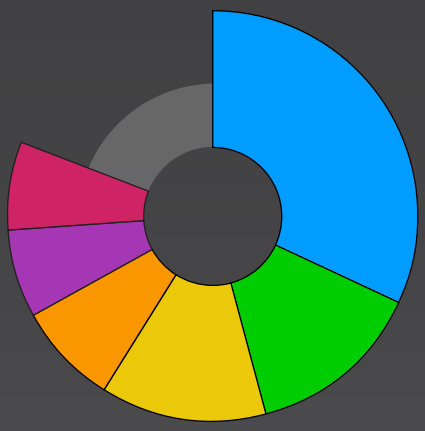


- LockBit 3.0
- ALPHV
- Royal
- Black Basta
- Cuba

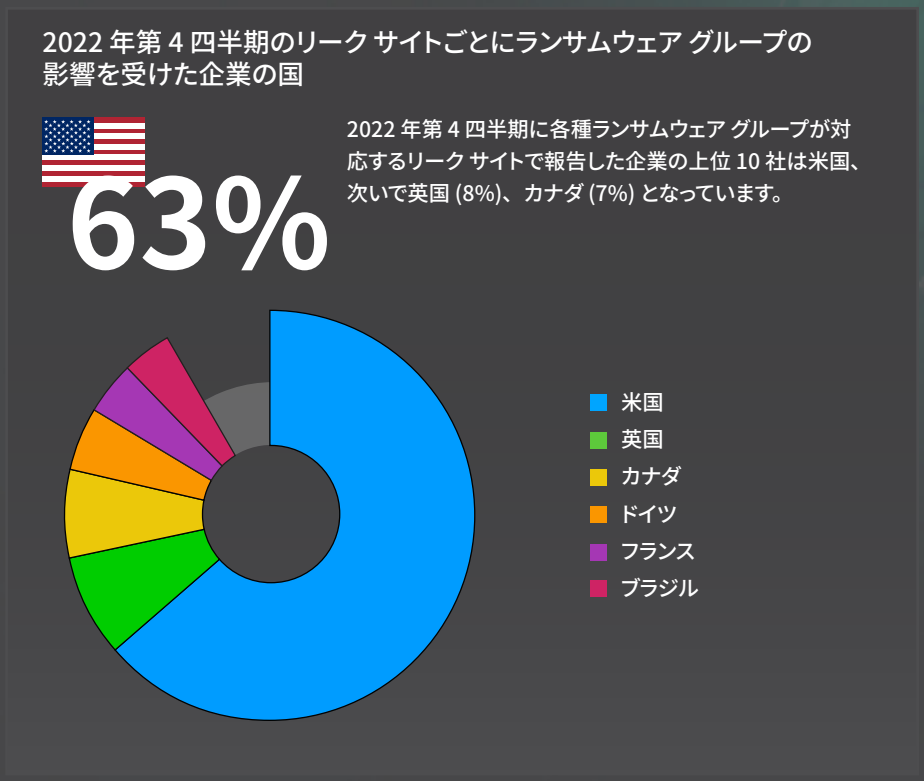
2022 年第 4 四半期のリーク サイトごとにランサムウェア グループの影響を受けたセクター

32%

2022 年第 4 四半期にリーク サイトごとにランサムウェア グループの影響を最も多く受けた業界は、産業財・サービスでした。産業財・サービスとは、主に建設や製造に使用されるすべての物質的製品と無形サービスを指します。



- 産業財・サービス
- 小売業
- テクノロジー
- 建築・資材
- ヘルスケア
- 政府機関



国民国家に関する 2022 年第 4 四半期の統計

このセクションでは、国民国家グループの活動に関して収集したインサイトを提供します。この情報は、脅威の状況をよりよく把握し、監視バイアスを減らすために複数のソースから収集されています。まず、国民国家グループの IOC と Trellix の顧客テレメトリの相関から抽出された統計を描いています。2 つ目に、セキュリティ業界が発行し、Threat Intelligence グループが厳しく吟味・解析・分析したさまざまなレポートから得られたインサイトを提供します。

2022 年第 4 四半期の国民国家による攻撃のハイライト

- 米国とドイツでは、国民国家からの攻撃が大幅に増加しました。
- 第 4 四半期の国民国家による攻撃で、中国とベトナムが登場します。

グローバル テレメトリの視点から見た国民国家による攻撃の統計

これらの統計は、弊社のテレメトリと Threat Intelligence ナレッジ ベースとの相関関係に基づいています。分析段階を受けて、選択した期間のデータからキャンペーンを特定し、その特徴を抽出します。表示される統計は、キャンペーンの統計であり、検出そのものではありません。さまざまなログの集約、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、Threat Intelligence ナレッジ ベースとの高度な相関により、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。

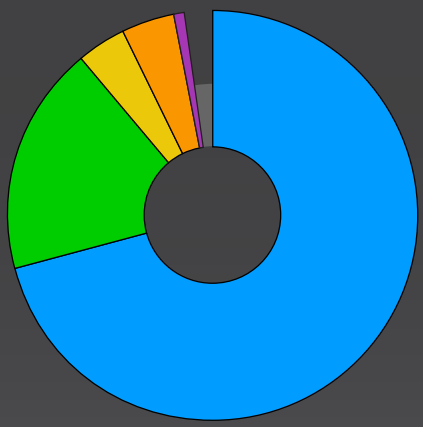
弊社のグローバル テレメトリによると、APT (Advanced Persistent Threat) グループによる複数のキャンペーンに関連する侵害の痕跡 (IoC) が確認されました。確認されたキャンペーンで最も多く見られた攻撃者の国と攻撃者、およびそれぞれのツールや手法は、以下のとおりです。同様に、確認されたキャンペーンによる影響が特に大きかった国とセクターに関するデータは、以下のとおりです。

国民国家に関するテレメトリ情報

2022 年第 4 四半期の国民国家の活動の背後にある攻撃者の最も多い国

71%

2022 年第 4 四半期の国民国家の活動の背後にある攻撃者の最も多い国は、中国でした。

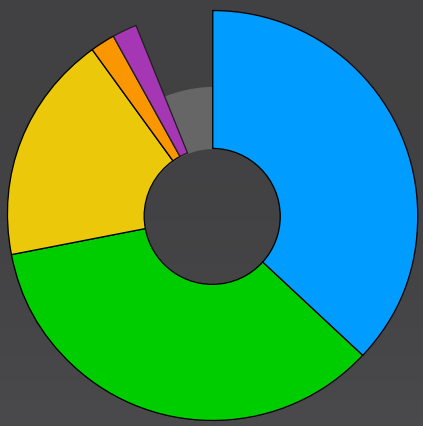


- 中国
- 北朝鮮
- ロシア
- イラン
- レバノン

2022 年第 4 四半期に最も多く見られた攻撃者グループ

37%

国民国家テレメトリーによると、2022 年第 4 四半期に最も多く見られた攻撃者グループは、Mustang Panda でした。



- Mustang Panda
- UNC4191
- Lazarus
- MuddyWater
- Kimsuky

2022 年第 4 四半期の国民国家の活動で最も多用された 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 / 情報	12%
4.	Windows Command Shell	11%
5.	レジストリ Run キー / スタートアップ フォルダー	10%

2022 年第 4 四半期に国民国家の活動で最も多用された悪意のあるツール

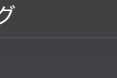
1.	PlugX	24%
2.	BLUEHAZE	23%
3.	DARKDEW	23%
4.	MISTCLOAK	23%
5.	JSX リモート アクセス型トロイの木馬	2%

2022 年第 4 四半期に国民国家の活動で最も多用された悪意のないツール

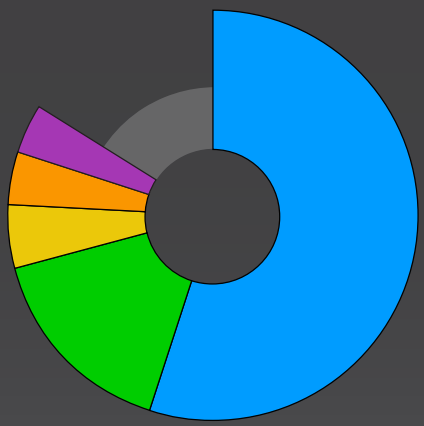
1.	Rundll32	22%
2.	Cmd	19%
3.	Reg	17%
4.	Ncat	12%
5.	Regsvr32	6%

2022 年第 4 四半期に国民国家の活動から最も影響を受けた国

55%



2022 年第 4 四半期に国民国家の活動から最も多く影響を受けた国は、米国でした。

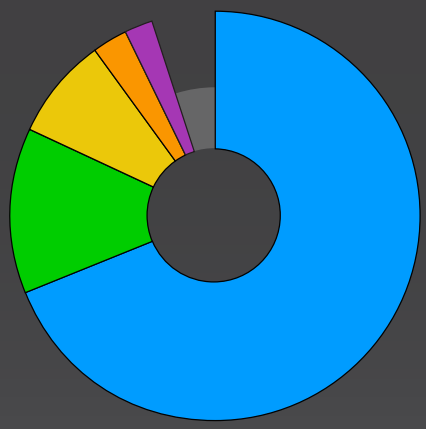


- 米国
- ベトナム
- インド
- ドイツ
- 中国

2022 年第 4 四半期に国民国家の活動から最も影響を受けたセクター

69%

2022 年第 4 四半期の国民国家の活動から最も多く影響を受けたセクターは、運輸業でした。



- 運輸業
- エネルギー / 石油 & ガス
- 卸売業
- 小売業
- 銀行 / 金融 / ウェルス マネジメント

2022 年第 4 四半期の公的報告書による国民国家インシデント

これらの統計は、公的報告書および社内調査に基づいており、顧客ログからのテレメトリに基づくものではありません。なお、すべての国民国家インシデントが報告されるわけではありません。多くのキャンペーンは、既知の同じ TTP に従っているため、あまり興味深い報告ではありません。業界では、攻撃者が新しいことを試したり、失敗したりするような新しいキャンペーンが選ばれる傾向があります。これらのメトリックスは、2022 年第 4 四半期に業界が有意義で関連性があると判断したものを示しています。

2022 年第 4 四半期に国民国家のキャンペーンの報告で最も多かった攻撃者の国

37%

2022 年第 4 四半期に公に報告された国民国家のキャンペーンのうち、中国を起源とするものの割合。

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 四半期に国民国家の活動の報告で最も多く見られた攻撃者

33%

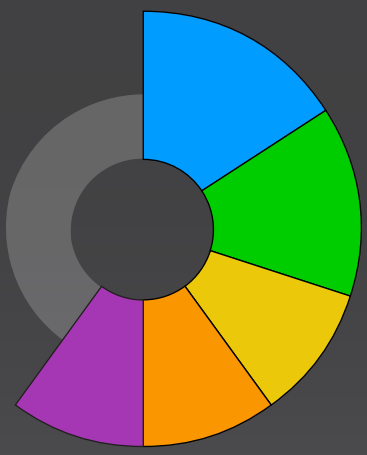
2022 年第 4 四半期の国民国家の活動の報告で最も多く見られた攻撃者は、Lazarus でした。

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

2022 年第 4 四半期に報告された国民国家のキャンペーンで最も標的となった国

16%

2022 年第 4 四半期に報告された国民国家のキャンペーンで最も標的となった国は、米国でした。

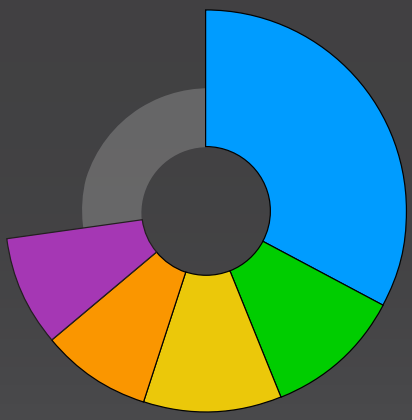


- 米国
- 英国
- パキスタン
- ロシア
- ウクライナ

2022 年第 4 四半期に報告された国民国家のキャンペーンで最も標的となったセクター

33%

2022 年第 4 四半期に報告された国民国家のキャンペーンで最も標的となったセクターは政府機関で、次いで軍機関 (11%)、通信 (11%) となっています。



- 政府機関
- 軍機関
- 電気通信
- エネルギー
- 金融

2022 年第 4 四半期に報告された国民国家のキャンペーンで使用された最も一般的な悪意のあるツール

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

2022 年第 4 四半期に国民国家のキャンペーンで使用された最も一般的な悪意のないツール

1.	Cmd	32%
2.	Rundl132	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民国家のキャンペーンで使用された最も一般的な MITRE ATT&CK 手法

1.	イングレス ツール転送	13%
2.	システム情報検出	13%
3.	難読化されたファイル / 情報	12%
4.	Web プロトコル	11%
5.	ファイル / 情報の難読化解除 / デコード	11%

2022 年第 4 四半期に報告された国民国家のキャンペーンでの悪用が観察された脆弱性

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 Living off the Land (環境寄生) およびサードパーティ ツール

Trellix Insights Global Threat Intelligence プラットフォームによる監視と追跡により、2022 年第 4 四半期の脅威の状況について、以下の情報が収集および可視化されました。

2022 年第 4 四半期の LOLBIN (環境寄生) のハイライト

- Living Off the Land (環境寄生) は、最初のアクセス、実行、検出、持続、そして影響まで、一貫してその役割を果たします。
- 2022 年第 4 四半期のデータでは、Windows Command Shell または PowerShell を介して実行されるコマンドおよびスクリプト手法が最もよく利用 (悪用) される傾向が続いていることを示しています。

- サイバー犯罪者による利用は、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広まっています。

また、脅威の状況で偶然出くわす新参者、一発屋、スクリプト キディなども、人気のある悪用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、気づかれないようにして、スーパーコンピュータ「ギブソン」をハッキングしたり、脆弱性を悪用したりしようとしています。

Living off the Land (環境寄生) の技術は、最初のアクセス、実行、検出、持続、そして影響まで、一貫して悪意のあるタスクを実行するために利用 (悪用) されています。2022 年第 4 四半期を通じて収集されたデータによると、Windows Command Shell を介してコマンドおよびスクリプト手法が実行される傾向が続いており、PowerShell が最もよく利用 (悪用) される手法であることがわかります。

2022 年第 4 四半期に最も多く見られた OS バイナリ

47%

2022 年第 4 四半期に最も多く見られた 10 個の OS バイナリのうち、Windows Command Shell が 47% とほぼ半数を占め、PowerShell (32%)、Rundl32 (27%) がそれに続きます。

1.	Windows Command Shell	47%
2.	PowerShell	32%
3.	Rundl32	27%
4.	Schtasks	23%
5.	WMI	21%

サイバー犯罪者による利用は、熟練した APT (Advanced Persistent Threat)、金銭目的のグループ、油断のないハクティビストなどの攻撃者の間で広まっています。

Trellix Insights プラットフォームで処理された、攻撃者が Windows バイナリを利用したイベントは、情報窃取、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のマルウェアを展開することにつながりました。MSHTA、WMI、WScript などのバイナリが実行され、攻撃者が管理するリソースから追加ペイロードを取得した可能性があります。

2022 年第 4 四半期の上位サードパーティ 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.	エクスプロイト後のツール	20%
4.	ネットワーク検出	16%
5.	AD 検出	10%

リモート アクセスや管理などのツールは、常に攻撃者が悪用するツールの上位に挙がりますが、セキュリティ実務者が使用するツールも悪意のある目的のために悪用され続けています。攻撃者は、キープアライブビーコンを開始したり、漏えいを自動化したり、標的の情報を収集・圧縮したりするためにこれらを使用することがあります。

無料のオープンソースのツールの中では、ソフトウェア パッカーが攻撃者によって悪用されています。これは、悪意あるコンテンツを含むように正規のソフトウェアを再パッケージ化したり、検出を回避しようとしてマルウェアをパックしたり、分析を妨げたりするために利用されています。

2022 年第 4 四半期の Cobalt Strike に関するインサイト

Advanced Research Center の Threat Intelligence 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手法を組み合わせることで、流行中の Cobalt Strike Team サーバー (Cobalt Strike C2) の利用状況をモニターしています。収集された Cobalt Strike ビーコンを分析する中で明らかになった注目すべきインサイトは、以下のとおりです。

15%
トライアル COBALT STRIKE ライセンス

流行が確認された Cobalt Strike ビーコンのうち、トライアル Cobalt Strike ライセンスを持つものは 15% に過ぎません。このバージョンの Cobalt Strike には、このポスト エクスプロイト フレームワークの既知の機能のほとんどが含まれています。しかし、"tell" を追加し、転送中の暗号化を解除することで、セキュリティ製品でペイロードを容易に検出できるようにしています。

87%
RUNDLL32.EXE

Rundll32.exe は、セッションを生成し、エクスプロイト後のジョブを実行するために使用されるデフォルトのプロセスで、確認されたビーコンの 87% で検出されました。

5%
ホスト HTTP ヘッダー

観測された Cobalt Strike ビーコンの少なくとも 5% は、ホスト Http ヘッダーを使用しており、Cobalt Strike でドメイン フロンティングを容易にするオプションとなっています。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 (CDN) を悪用する手法です。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 接続の下に隠します。

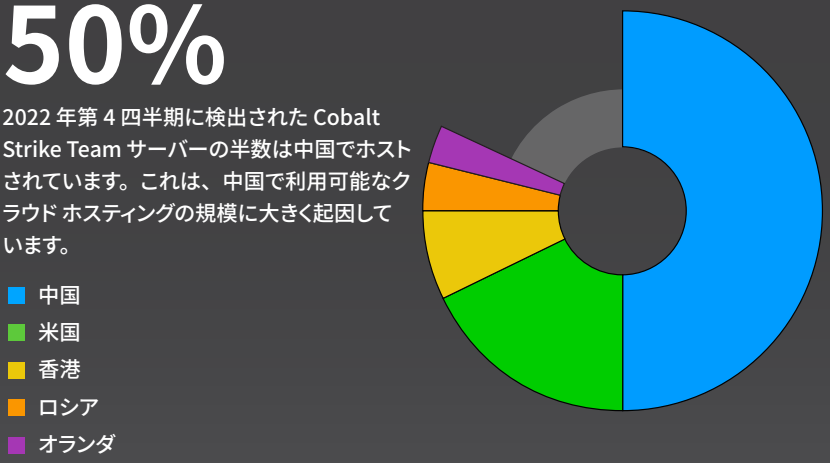
22%
DNS ビーコン

DNS ビーコンは、確認された Cobalt Strike ビーコンの 22% を占めています。このペイロード タイプは、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 チーム サーバーに通信を戻し、その活動を隠蔽します。

2022 年第 4 四半期の COBALT STRIKE TEAM サーバーをホストしている上位の国

50%

2022 年第 4 四半期に検出された Cobalt Strike Team サーバーの半数は中国でホストされています。これは、中国で利用可能なクラウド ホスティングの規模に大きく起因しています。



2022 年第 4 四半期の GOOTLOADER

Gootloader はモジュール型のマルウェアで、「GootKit」または「GootKit Loader」として識別される別のマルウェアと同じ意味で言及されることがあります。Gootloader マルウェアの現在のモジュール型機能は、REvil、Kronos、Cobalt Strike、Icedid などの追加のマルウェア ペイロードを配布するために使用されています。

最近のイベントでは、Gootloader は、検索エンジン最適化 (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ために使用される危険なサイトや偽サイトに、無防備なユーザーを誘導していたことが確認されています。しかし、この手法では、無防備なユーザーがアーカイブを開いてコンテンツを実行し、Windows Scripting Host 経由で悪意のある JS コードを実行することが必要です。それが成功すると、Gootloader は C2 通信を開始し、追加のマルウェアを取得します。

Gootloader は、登録者に提供される疑わしい Malware as a Service (MaaS) として、攻撃者が複数の追加ペイロードをロードできるようにするため、Gootloader は企業環境に重大な脅威をもたらします。

弊社は、Gootloader の内部トラッカーを使用して、2022 年 11 月 18 日に流行していることが発見された最新の亜種を確認し、2022 年 11 月 13 日時点で休止している古い亜種を目撃しました。最新の亜種に対する修正は以下のとおりです。

- レジストリ操作機能の削除
- リモート ネットワークへのリクエストを 3 から 10 URL に増加
- CScript で PowerShell スクリプトを直接呼び出す機能
- すべてのユーザー ログオンの永続性

Gootloader の追跡プロセス

Gootloader の新しい亜種は、複数の難読化層を使用して進化しています。解凍後に入れ子状になった各ステージは、その前のステージからロードされた変数を使用するため、分析が困難になります。YARA ハンティング作業によって収集されたサンプルは、静的な JavaScript および PowerShell アナライザに供給され、リモート Command and Control (C&C、C2) サーバーや固有の ID 署名などの IOC を抽出します。これらの IOC を使用して、流行中の Gootloader の特定のインスタンスを特定し、追跡することができます。

抽出された Gootloader IOC の処理として、Trellix の URL レピュテーションチームのデータベースに照会が行われ、悪意のあるドメイン、侵害されている可能性がある正規のドメイン、分析を阻害するためのおとりとして使用されている正規のドメインが特定されます。

Gootloader に関するテレメトリ情報

表示される統計情報は、抽出された IOC とお客様のログの相関から特定されたキャンペーンの統計であり、検出そのものではありません。Gootloader の場合、検出のほとんどがドメインのヒットに基づくものです。Gootloader はおとりのドメインを使用するため、表示された統計情報は、中レベルの信頼度で悪意があると解釈されるべきです。

2022 年第 4 四半期に GOOTLOADER による被害が最も多かった国

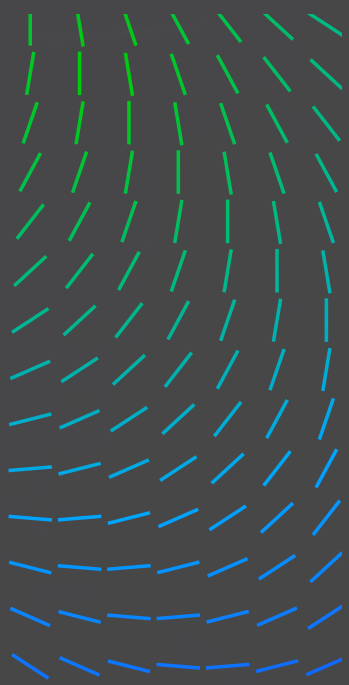
37%

2022 年第 4 四半期に Gootloader による被害が最も多かった国は、米国でした。

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 によって使用された最も一般的な MITRE ATT&CK 手法

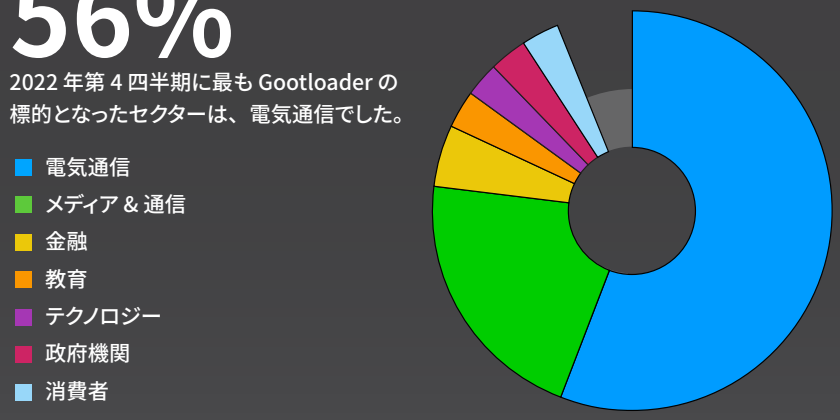
1. ファイル / 情報の難読化解除 / デコード
2. JavaScript
3. 難読化されたファイル / 情報
4. PowerShell
5. プロセス ハロウイング



2022 年第 4 四半期に最も多く GOOTLOADER の標的となったセクター

56%

2022 年第 4 四半期に最も Gootloader の標的となったセクターは、電気通信でした。



2022 年第 4 四半期に Gootloader によって使用された最も一般的な MITRE ATT&CK 手法

ファイル / 情報の難読化解除 / デコード

JavaScript

難読化されたファイル / 情報

PowerShell

プロセス ハロウイング

リフレクティブ コード ローディング

レジストリ Run キー / スタートアップ フォルダー

Rundll32

スケジュール タスク

2022 年第 4 四半期の脆弱性インテリジェンス

脆弱性ダッシュボードは、最新の影響度の高い脆弱性の分析を照合したものです。分析とトリアージは、Trellix Advanced Research Center の脆弱性に関する業界専門家によって行われます。これらの研究者はリバース エンジニアリングや脆弱性分析を専門とし、最新の脆弱性と、攻撃者がそれをどのように攻撃に利用しているかを継続的にモニターし、修復策を指導しています。この簡潔で高度な専門的アドバイスにより、ノイズからシグナルをフィルタリングし、組織に影響を及ぼす可能性のある最も重要な脆弱性に焦点を当て、迅速に対応することが可能になります。

2022 年第 4 四半期の脆弱性インテリジェンスのハイライト

41%

2022 年第 4 四半期にユニークな CVE によって影響を受けた脆弱な製品およびベンダーの 41% を Lanner が占めています。

29%

IAC-AST2500A ファームウェア バージョン 1.10.0 は、2022 年第 4 四半期に製品で使用された CVE として最も多く報告されています。

2022 年第 4 四半期の最も影響力のある脆弱性を含む製品、ベンダー、CVE

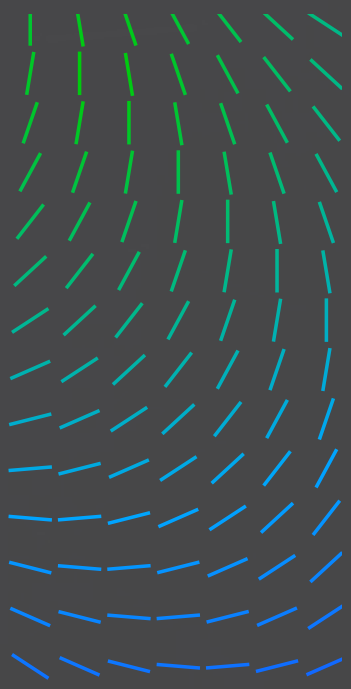
1.	Lanner	41%
2.	Microsoft	19%
3.	BOA	15%
4.	Oracle	8%
5.	Apple Chrome Citrix Fortinet Linux	各 5%

2022 年第 4 四半期に報告された製品別の CVE

29%

IAC-AST2500A ファームウェア バージョン 1.10.0 は、2022 年第 4 四半期に製品で使用された CVE として最も多く報告されており、次いで BOA サーバー (10%)、IAC-AST2500A (6%)、Exchange (6%) となっています。

報告された CVE 製品	ユニーク CVE
IAC-AST2500A、ファームウェア バージョン 1.10.0	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 まで	1
Oracle Access Manager、11.1.2.3.0、12.2.1.3.0、12.2.1.4.0	1
MacOS	1
Linux Kernel 5.15.61 以前	1
Internet Explorer	1



報告された CVE 製品	ユニーク CVE
FortiOS (sslvpnd)	1
Citrix ADC/Citrix Gateway	1
Chrome、108.0.5359.94/.95 以前のバージョン	1
BOA サーバー、Boa 0.94.13	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

メールのセキュリティに関する 2022 年第 4 四半期の傾向

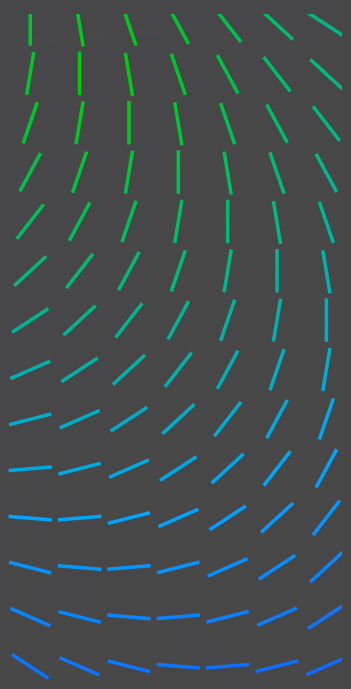
メールのセキュリティの統計は、全世界のお客様のネットワークに展開されている複数のメール セキュリティ アプライアンスから生成されたテレメトリに基づいています。検出ログを集計して分析し、以下の調査結果が作成されました。

メールのセキュリティに関する 2022 年第 4 四半期の傾向のハイライト

100% アラブ諸国における悪意のあるメールの量は、8 月と 9 月に比べ、10 月は 100% 増加していることが観察されました。

40% 最も多く利用されたマルウェア戦術は Qakbot で、アラブ諸国を標的としたキャンペーンの 40% を占めました。

42% 2022 年第 4 四半期に悪意あるメールの影響を最も多く受けたセクターは電気通信で、業界を標的とした悪意のあるメールキャンペーンの 42% を占めました。



87% 2022 年第 4 四半期に最も多く見られた攻撃方法の中で、悪意のある URL を使用したフィッシング詐欺メールが群を抜いていました。

64% なりすましのヒット数は、2022 年第 3 四半期から第 4 四半期にかけて 64% 増加しました。

82% CEO へのすべての詐欺メールのうち、無料メール サービスを利用して送信されたものの割合。

78% すべてのビジネス メール詐欺 (BEC) 攻撃のうち、一般的な CEO のフレーズが使われていたものの割合。

142% 2022 年第 4 四半期はビッシング攻撃が目立ち、2022 年第 3 四半期から 142% 増加しました。

2022 年第 4 四半期に最も多く見られたメール マルウェアの戦術

40%

2022 年第 4 四半期に最も多く見られたメール マルウェアの戦術は、Qakbot でした。

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 フィッシング詐欺の標的となった製品およびブランド

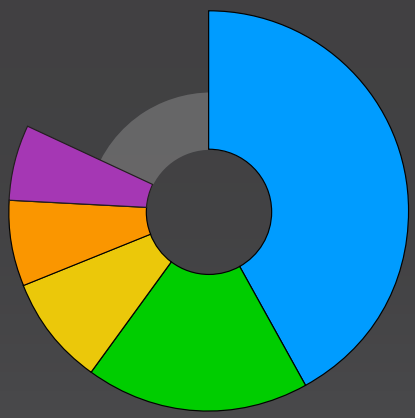
1.	一般	62%
2.	Outlook	13%
3.	Microsoft	11%
4.	Ekinet	8%
5.	Cloudfare	3%

2022 年第 4 四半期に悪意のあるメールの影響を最も受けたセクター

42%

2022 年第 4 四半期に悪意のあるメールの影響を最も受けたセクターは、電気通信でした。

- 電気通信
- 政府機関
- 教育
- 金融
- サービス / コンサルティング



メールのなりすましに関する 2022 年第 4 四半期の傾向のハイライト

82% CEO へのすべての詐欺メールのうち、無料メール サービスを利用して送信されたものの割合。

78% すべてのビジネス メール詐欺 (BEC) 攻撃のうち、一般的な CEO のフレーズが使われていたものの割合。

64% CEO などのビジネス リーダーになりすました悪意のあるメールの、2022 年第 3 四半期から第 4 四半期にかけての増加割合。

2022 年第 4 四半期に BEC 攻撃で使用された CEO のフレーズとして上位に挙げられるもの :

「急ぎの仕事があります。」

「仕事の指示を口頭で伝えたいので、今すぐ携帯電話の番号を教えてください。」

「電話番号を送ってください。すぐに済ませてほしい仕事があります。」

「携帯電話の番号を送ってください。テキストメッセージで指示を送ります。急ぎの仕事です。」

「携帯電話の番号を見直して確認し、私からのテキストメッセージを読んでください。」

「私からのメールは届きましたか？耳寄りな案件があります」

2022 年第 4 四半期のなりすましの比較

64% なりすましのヒット数は、2022 年第 3 四半期から第 4 四半期にかけて 64% 増加しました。

2022 年第 4 四半期のフィッシング詐欺キャンペーンに関するインサイト

詐欺や窃取に利用されることが増えている Web ホスティング プロバイダー

第 4 四半期には、正規の Web ホスティング プロバイダーを利用した詐欺行為やクレデンシャルの窃取が増加していることが観察されました。主に悪用されたサービス プロバイダーは 3 つあります。それは、dweb.link、ipfs.link、translate.goog です。また、ekinet、storageapi_fleek、selcdn.ru といった他のサービス プロバイダー ドメインからの量も増えていることがわかりました。攻撃者は、フィッシング詐欺ページをホストし、フィッシング対策エンジンをバイパスするために、新しい人気のあるホスティング サービスを継続的に使用しています。攻撃者が正規の Web ホスティング プロバイダーを利用することに関心を持つようになった理由の 1 つは、これらのサービスが正規のファイルをホストしてコンテンツを共有することを主な目的としているため、どの検出システムによってもブラックリスト化されないということです。

フィッシング詐欺メールで最も多く使われた攻撃方法

87%

2022 年第 4 四半期に最も多く見られた攻撃方法の中で、悪意のある URL を使用したフィッシング詐欺メールが群を抜いていました。

1.	URL	87%
2.	添付ファイル	7%
3.	ヘッダー	6%

2022 年第 4 四半期の悪用度の高い WEB ホスティング プロバイダー

154%

2022 年第 4 四半期に最も悪用された Web ホスティング プロバイダーは Dweb でしたが、第 3 四半期から第 4 四半期にかけて最も大きな増加を示したのは、Google Translate でした (154%)。

1.	Dweb	81%
2.	Ipfs	17%
3.	Google Translate	10%

2022 年第 4 四半期にフィッシング攻撃で最も多く使われた回避手法

63%

2022 年第 4 四半期に最も突出していたのは、302 リダイレクト ベースの回避でした。

- 第 4 四半期に地理情報ベースの回避型フィッシング攻撃が大幅に増加しました。
- 第 4 四半期には、Captcha ベースの攻撃も増加しました。

2022 年第 4 四半期のビッシングに関するインサイト

ビッシングはフィッシング詐欺の一種で、主にメール、テキスト メッセージ、電話、ダイレクト チャット メッセージを使用して、被害者が攻撃者とつながるように誘導するように設計されています。

142%

2022 年第 4 四半期はビッシング攻撃が目立ち、2022 年第 3 四半期から 142% 増加しました。

85%

無料メール サービスは、ビッシングを利用する悪質な攻撃者がよく利用する手段となっています。弊社が検出した 2022 年第 4 四半期のビッシング攻撃の大部分 (85%) は、無料メール サービスを利用して送信されていました。

第 4 四半期にビッシング キャンペーンで使用されたテーマとしては、**Norton、McAfee、Geek Squad、Amazon、PayPal** が最も一般的でした。

2022 年第 4 四半期のネットワーク セキュリティ

Trellix ARC のネットワーク研究チームは、お客様を脅かすネットワーク ベースの攻撃の検出とブロックに焦点を当てています。偵察、初期侵害、C2 通信、横移動の TTP など、キルチェーンのさまざまな領域を検証します。いくつかのテクノロジーを組み合わせた強みを利用して、未知の脅威をより的確に検出するための可視性を実現しています。

2022 年第 4 四半期にネットワーク セキュリティに対して使用された最も一般的な MITRE ATT&CK 手法

- T1083 - ファイル / ディレクトリ検出
- T1573 - 暗号化されたチャネル
- T1020 - 自動持ち出し
- T1210 - リモート サービス エクスプロイト
- T1569 - システム サービス
- T1059 - コマンド / スクリプト インタープリター : Windows Command Shell
- T1047 - Windows Management Instrumentation
- T1087 - アカウント検出
- T1059 - コマンド / スクリプト インタープリター
- T1190 - 公開アプリケーション エクスプロイト

2022 年第 4 四半期に外部向けサービスに対する影響が最も大きかった攻撃

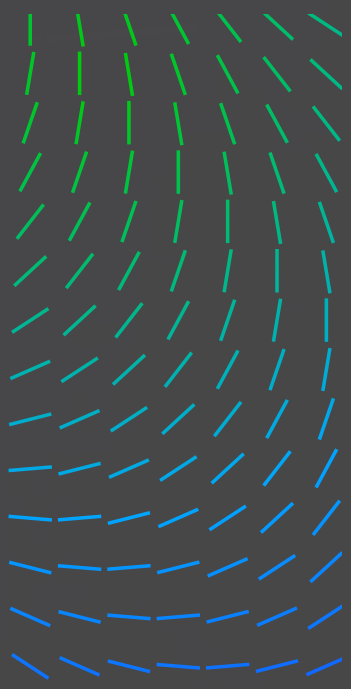
顧客環境に対する潜在的なしきい値を見つけるために外部向けマシンを探査するネットワーク スキャンが、日常的に数多く行われています。古いエクスプロイトは、パッチが適用されていないシステムを常に探しています。

- ファイル /etc/passwd アクセス試行検出
- 可能性のあるクロスサイト スクリプティング攻撃
- SIPVicious セキュリティ スキャナー
- 検出された Nmap スキャナー トラフィック
- スキャン活動 - Shellshock、Web サーバーの探査
- Bash リモート コードの実行 (Shellshock) HTTP CGI (CVE-2014-6278)
- Oracle WebLogic CVE-2020-14882 リモート コードの実行の脆弱性
- 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 コードの実行

2022 年第 4 四半期にネットワークの最初の足掛かりとして使用された最も重要な WebShell

脆弱な Web サーバーの制御を試みるために、以下の WebShell が使用されることが一般的に確認されています。

- 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時に最も関連のあるツール、手法、手順

脆弱な Web サーバーの制御を試みるために、以下の WebShell が使用されることが一般的に確認されています。

SCShell や PSExec のような古い脆弱性やツールの使用など、攻撃者が横移動の際に使用する TTP が大量に確認されています。

- SCshell: サービス マネージャーを利用したファイルレスの横移動
- Windows WMI リモート プロセス コール
- SMB 経由の WMIEXEC による 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 試行
- Apache Log4j CVE-2021-44228 RCE
- リモート ドメイン / エンタープライズ管理者アカウントの列挙
- 不審な PowerShell 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 ファイル内での列挙コマンドの検出
- SMB PSEXEC アクティビティ

Trellix XDR を活用したセキュリティ運用テレメトリ

この統計は、弊社の顧客ベースのさまざまなセンサーから生成されたテレメトリに基づいています。検知ログを集計して分析し、以下のセクションを作成しました。

2022 年第 4 四半期に最も影響の大きかったセキュリティ インシデント

以下のセクションは、2022 年第 4 四半期に最も多く発生したセキュリティ アラートを示しています。

EXPLOIT - LOG4J [CVE-2021-44228]

OFFICE 365 ANALYTICS [異常ログオン]

OFFICE 365 [許可されたフィッシング詐欺]

EXPLOIT - FORTINET [CVE-2022-40684]

EXPLOIT - APACHE SERVER [CVE-2021-41773 - 試行]

WINDOWS ANALYTICS [ブルートフォース成功]

EXPLOIT - ATLASSIAN CONFLUENCE [CVE-2022-26134]

EXPLOIT - F5 BIG-IP [CVE-2022-1388 試行]

2022 年第 4 四半期に最も多く使用された MITRE ATT&CK 手法

1.	公開アプリケーション エクスプロイト (T1190)	29%
2.	アプリケーション層プロトコル : DNS (T1071.004) フィッシング詐欺 (T1566)	14% 14%
3.	アカウント操作 (T1098.001) ブルートフォース (T1110) Web 閲覧による感染 (T1189) ユーザー実行 : 悪意のあるファイル (T1204.002) 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 四半期の上位のログ ソース分布

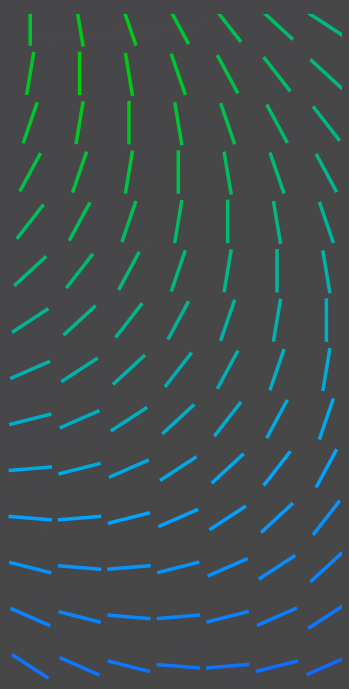
1.	ネットワーク	40%
2.	メール	27%
3.	エンドポイント	27%
4.	ファイアウォール	6%

2022 年第 4 四半期の観察されたエクスプロイト

2022 年第 4 四半期に最も多く観察されたエクスプロイト

30% 2022 年第 4 四半期に最も多く観察されたエクスプロイトは、Log4j でした。

1.	Log4j (CVE-2021-44228)	30%
2.	Fortinet (CVE-2022-40684)	16%
3.	Apache Server (CVE-2021-41773)	15%
4.	Atlassian Confluence (CVE-2022-26134)	14%
5.	F5 Big-IP (CVE-2022-1388 試行)	13%
6.	Microsoft Exchange (ProxyShell エクスプロイト試行)	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する中で、クラウド インフラへの攻撃は常に増加しています。Gartner 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。

2022 年第 4 四半期のテレメトリを分析する際に、以下のことが観察されました。

- AWS に関連する検出は、AWS がクラウド市場の主要なリーダーとしての地位を確立しているためと考えられます。
- ほとんどの攻撃は、ブルートフォース / パスワードスプレー攻撃による有効なアカウントへの初期アクセスに集中しており、それがクラウドの攻撃対象における初期感染ベクトルであることを示しています。
- 企業アカウントの大半が多要素認証を有効にしているため、ブルートフォース攻撃に成功すると、敵は MFA プラットフォームに到達し、MFA 関連の検出が急増しました。

以下のセクションでは、弊社の顧客ベースにおけるクラウドベースの攻撃テレメトリ データの内訳を、さまざまなクラウド プロバイダー別に簡単に説明します。

2022 年第 4 四半期の AWS に関する MITRE ATT&CK 手法の分布

1.	有効なアカウント (T1078)	18%
2.	クラウド コンピューティング インフラストラクチャ変更 (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 (T1110) 防衛策阻害 (T1562)	各 6%

2022 年第 4 四半期の AZURE に関する上位 MITRE ATT&CK 手法

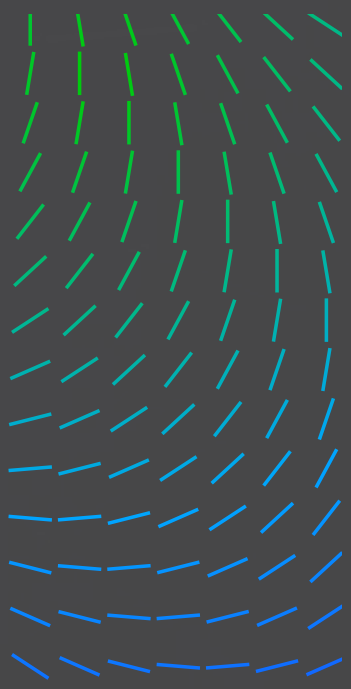
1.	有効なアカウント (T1078)	23%
2.	多要素認証 (T1111)	19%
3.	ブルートフォース (T1110)	14%
4.	プロキシ (T1090)	14%
5.	アカウント操作 (T1098)	5%

2022 年第 4 四半期の MITRE ATT&CK 手法別の上位 AWS 検出

MITRE 手法	ルール
アカウント操作 (T1098)	IAM アイデンティティに添付された AWS 特権ポリシー 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 AWS Analytics API キーの異常な使用状況 AWS GuardDuty 異常なユーザー行動 AWS GuardDuty 匿名アクセス権付与
防衛策阻害 (T1562)	AWS CloudTrail ポリシーの CloudTrail への変更 AWS CloudTrail 証跡の削除
ファイル内の認証情報 (T1552.001)	AWS 秘密鍵が盗まれる可能性があることをアラートで通知
クラウド コンピューティング インフラストラクチャ 変更 (T1578)	AWS CloudTrail S3 バケットの削除 AWS CloudTrail S3 バケット ACL の配置 AWS CloudTrail オブジェクト ACL の配置

2022 年第 4 四半期の MITRE ATT&CK 手法別の上位 AZURE 検出

MITRE ATT&CK 手法	ルール
有効なアカウント (T1078)	Azure AD 危険なサインイン いつもと違う場所からの Azure ログイン アカウントによる Azure ログインが 60 日間見られない
ブルートフォース (T1110)	Azure 多要素認証の失敗 Azure ポータルに対するブルートフォース攻撃をグラフで表示 分散型パスワード クラックの試行をグラフで表示
多要素認証 (T1111)	Azure MFA は詐欺警告のため拒否 Azure MFA はユーザーがブロックされたため拒否 Azure MFA は詐欺コードのため拒否 Azure MFA は詐欺アプリのため拒否
外部リモート サービス (T1133)	Tor ネットワークから Azure にサインイン
アカウント操作 (T1098)	Azure 異常ユーザーのパスワードリセット



2022 年第 4 四半期の GCP に関する MITRE ATT&CK 手法の分布

1.	有効なアカウント (T1078)	36%
2.	API による実行 (T0871)	18%
3.	アカウント検出 (T1087.001) アカウント操作 (T1098) 防衛策阻害 (T1562) クラウド コンピューティング インフラストラクチャ変更 (T1578) リモート サービス (T1021.004)	各 9%

2022 年第 4 四半期の MITRE ATT&CK 手法別の上位 GCP 検出

MITRE ATT&CK 手法	ルール
有効なアカウント (T1078)	GCP サービス アカウントの作成 GCP Analytics 異常なアクティビティ GCP サービス アカウント キーの作成
リモート サービス (T1021.004)	GCP ファイアウォール ルールは、ssh ポートのすべてのトラフィックを許可
アカウント操作 (T1098)	GCP 組織の IAM ポリシー変更
アカウント検出 (T1087.001)	アラート [“gcps net user”]
Transfer Data to Cloud Account (T1527)	GCP ロギング シンクの変更
クラウド コンピューティング インフラストラクチャ変更 (T1578)	GCP 削除からの保護の無効化

レポートおよびリサーチ

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

Trellix Advanced Research Center によって特定された最も影響力のある最新の脅威を追跡するには、以下のリソースをご覧ください。

TWITTER

Trellix ARC

The 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、脅威を取り巻く環境全体の中で、新たな手法、トレンド、攻撃者の最前線に立っています。全世界のセキュリティ運用チームの主要なパートナーである Trellix Advanced Research Center は、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コンテンツを提供することで、弊社の最新 XDR プラットフォームを支えています。

Trellix について

Trellix は、サイバー セキュリティの将来と気持ちのこもった業務を再定義するグローバル企業です。今日の最も高度な脅威に直面している組織は、弊社のオープンでネイティブな eXtended Detection and Response (XDR) プラットフォームを使用することにより、業務の保護と耐久性に自信を持つことができます。Trellix は、広範なパートナー エコシステムとともに、機械学習と自動化を通じて技術革新を加速させ、生きたセキュリティによって 40,000 以上の企業や政府機関のお客様を支援しています。詳細は https://www.trellix.com/ja-jp/index.html をご覧ください。

詳細は、Trellix.com もご確認ください。

Trellix について

Trellix は、サイバーセキュリティの将来を再定義するグローバル企業です。今日の最も高度な脅威に直面している組織は、弊社のオープンでネイティブな eXtended Detection and Response (XDR) プラットフォームを使用することにより、業務の保護と耐久性に自信を持つことができます。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、機械学習と自動化を通じて技術革新を加速させ、40,000 以上の企業や政府機関のお客様を支援しています。

072022-05