2015

CISCO TALOS

YEAR IN REVIEW

2016

寺下 健一

CxO Advisor
Office of the CTO, CX, APJC

CISCO TALOS

About Talos

CISCO TALOS

グローバル脅威インテリジェンス

AIに支えられたサービス、最先端の研究およびインサイトを通じて、
世界中のネットワークをプロアクティブに防御

1日あたり
8,860億件以上の
セキュリティイベント分析

4,600万台以上の
デバイスから
情報を収集

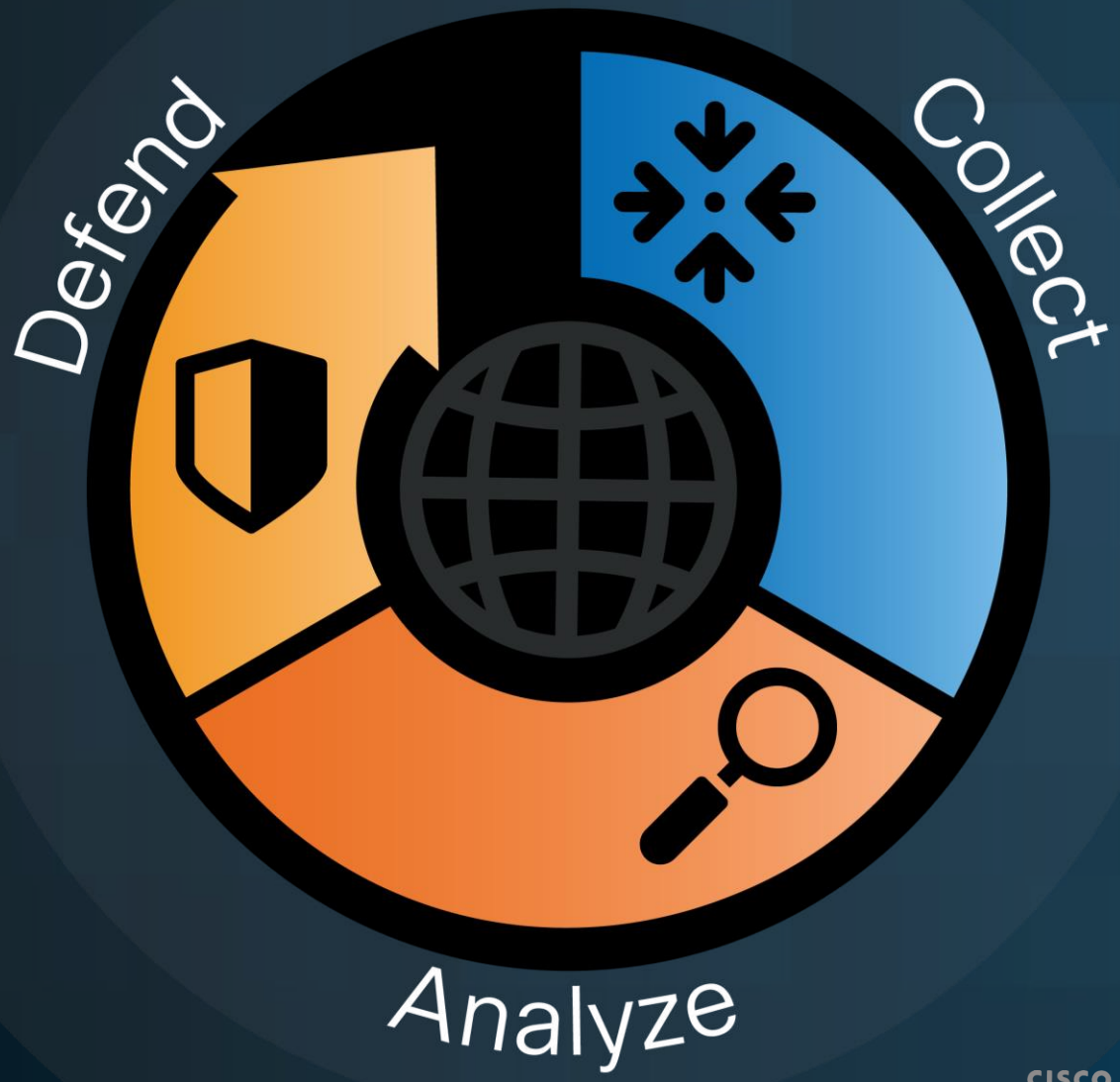
193カ国をカバー

46以上の言語
に対応

CISCO TALOS

Talosは包括的インテリジェンスによりCisco全体を支えています。

世界中のあらゆる顧客環境において、あらゆるイベントを、毎日継続的に対応しています



CISCO TALOS

About the Talos Year in Review

Cisco Talos 2025 Year in Reviewは、グローバルにおける攻撃者の活動を形作った戦術・技術・手順（TTP）を詳細に分析したレポートです。

本レポートは、Talosによる独自の脅威調査、エンドポイント、ネットワーク、電子メール環境にわたるCiscoの大規模なセキュリティテレメトリ、さらにCisco Talos Incident Response（Talos IR）が実施した実地調査に基づき、一貫して侵害につながった攻撃経路を特定しています。

分析対象には、以下の領域が含まれます：

- 実運用において最も多く悪用された脆弱性
- ネットワークおよびセキュリティインフラに対する継続的な標的化
- ランサムウェアのエコシステムの変化と攻撃手法（プレイブック）
- アイデンティティを起点とした侵害および認証情報の悪用
- フィッシングおよびソーシャルエンジニアリングの動向
- 国家支援型の攻撃キャンペーン
- 攻撃者のワークフローにおけるAIの運用的活用

Talos Year in Reviewは、防御側に対して、2025年における脅威アクターの大規模な活動実態を明確に示すとともに、これらのトレンドが今後の検知、セキュリティ強化、およびインシデント対応戦略にどのような意味を持つかを理解するために作成されています。

CISCO TALOS

攻撃者は2025年にどのように適応したのか

「Cisco Talos YEAR IN REVIEW」は、世界中の脅威アクターの活動を形作ったTTPを詳細に分析したものです。

分析領域

実際の攻撃活動において最も多く悪用された脆弱性

ネットワークおよびセキュリティ基盤に対する継続的な標的化

ランサムウェアエコシステムの変化と攻撃手法（プレイブック）

アイデンティティ中心の侵害と認証情報の悪用

フィッシングおよびソーシャルエンジニアリングの動向

国家支援型攻撃キャンペーン

攻撃者のワークフローにおけるAIの運用的活用

CISCO TALOS

主なトピック

1. 両極端な脆弱性攻撃 迅速性と持続性

2025年において、攻撃者は迅速に行動すると同時に、粘り強さも併せ持っていました。

大規模な脆弱性が新たに出現すると即座に動員する一方で、長年存在しているリスクの悪用も継続していました。

CISCO TALOS

2. アイデンティティ: 信頼の基盤としてのアーキテクチャ

攻撃者は、スケール、制御、信頼を支えるシステムを標的としていました。

アイデンティティを掌握することは、アクセスを掌握することを意味します。

アイデンティティはエンタープライズのコントロールプレーンとなっており、攻撃者はそれを認識していました。

CISCO TALOS

3. 影響拡大を狙った集中管理システムへの攻撃

攻撃者は、集中化されたインフラストラクチャ、管理プラットフォーム、および共有フレームワークに攻撃を集中させました。

これにより、環境全体にわたる侵害をスケールさせることが可能となりました。

脆弱性

脆弱性の悪用は、即時的であると同時に長期的でもあります。

Vulnerabilities Summary

1. React2Shellは、最も標的となった脆弱性になりました。
2. 悪用までのタイムラインは大幅に短縮されています。
3. 広範に組み込まれたフレームワークが、大きなリスクになっています。
4. 古い弱点の放置は、今なお確実に攻撃者の利益につながっています。

2025年において、攻撃者は新たに発見された脆弱性の武器化をかつてない速度で進める一方、深く組み込まれたレガシーな脆弱性の悪用も継続していました。リスクは均等に分布しているわけではなく、中央集約型システム、共有フレームワーク、およびサポート終了（EOL）機器が、業界全体にわたり不均衡に大きなリスクを生み出していました。

40%

標的とされた上位100件の脆弱性のうち、サポート終了（EOL）システムが対象だった割合

23%

ネットワーク機器に直接影響を与えた脆弱性の割合

32%

少なくとも10年以上前の脆弱性の割合

CISCO TALOS

最も多く標的とされた脆弱性トップ10

最も標的とされた脆弱性は、迅速性、規模、そして長年にわたり存在する弱点の継続的な悪用によって特徴づけられる脅威環境を反映しています。

Ranking	Vulnerability	Vendor/product
1	CVE-2025-55182	React Server Components (aka React2Shell)
2	CVE-2017-9841	PHPUnit
3	CVE-2025-49704	Microsoft SharePoint (aka ToolShell)
4	CVE-2025-49706	Microsoft SharePoint (aka ToolShell)
5	CVE-2025-53770	Microsoft SharePoint (aka ToolShell)
6	CVE-2025-53771	Microsoft SharePoint (aka ToolShell)
7	CVE-2013-0632	Adobe ColdFusion
8	CVE-2021-44228	Apache Log4J (aka Log4Shell)
9	CVE-2021-44832	Apache Log4J (aka Log4Shell)
10	CVE-2021-45046	Apache Log4J (aka Log4Shell)

CISCO TALOS

主要なポイント

1. レガシーシステムは依然として
攻撃に対して非常に脆弱である
2. フレームワークレベルの脆弱性は、
サプライチェーンの弱点を露呈させる
3. ネットワーク機器は主要な標的となっている
4. CVEの経過年数の分布は、
体系的なパッチ適用遅延を浮き彫りにしている

CISCO TALOS

セキュリティチームへのガイダンス

1. 重要な信頼または制御経路上に位置する高リスクなレガシーシステムを特定する。
2. アイデンティティ検証、アクセス管理、またはネットワークフロー制御を担う領域において、システム刷新を優先する。
3. システム刷新は即時かつ全面的である必要はなく、リスクに基づいて優先順位付けし、段階的に実施すべきである。
4. サポートされていないインフラを維持するコストは、置き換えコストをますます上回る傾向にある。

CISCO TALOS

AI

AIは攻撃と防御の双方を加速させている。

CISCO TALOS

AIは既存の攻撃手法を増幅している

主な観測事項

Augmentation
拡張

AIは主に、従来型攻撃の特定の工程を強化するために使用されています

Deception
欺瞞

AIにより、攻撃者は説得力の高いフィッシングメール、Webサイト、および誘導コンテンツを大規模に生成可能となっています

Democratization
民主化

AIは初心者攻撃者の参入障壁を下げる一方で、高度な攻撃者の能力をさらに拡張します

Impersonation
なりすまし

高度な攻撃者は、ディープフェイクやAI生成の人物像を用いて侵入を実現しています

CISCO TALOS

主要動向：エンタープライズAIエージェントの妨害

Talosが積極的に監視している動向：

- **Prompt injection** — AIシステムを操作し、機密情報を開示させる手法
- **Context poisoning** — AIモデルのデータ学習を改変し、応答を操作する手法
- **Jailbreaking** — 大規模言語モデルに組み込まれた安全対策を回避する技術
- **Data exfiltration** — エンタープライズデータにアクセス可能なAIシステムを欺く

CISCO TALOS

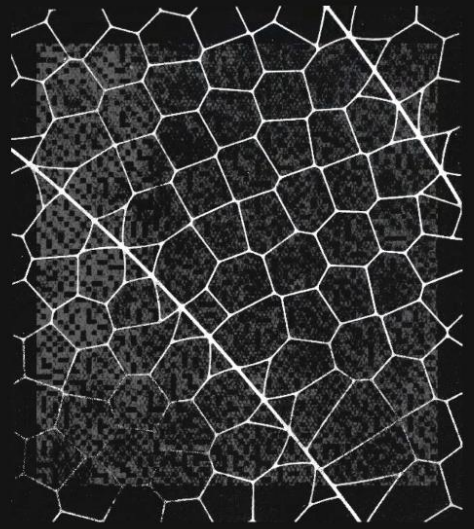
ANTHROP\C

Research Economic Futures Commitments Learn News Try Claude

Project Glasswing

Securing critical software for the AI era

Continue reading



aws ANTHROP\C BROADCOM

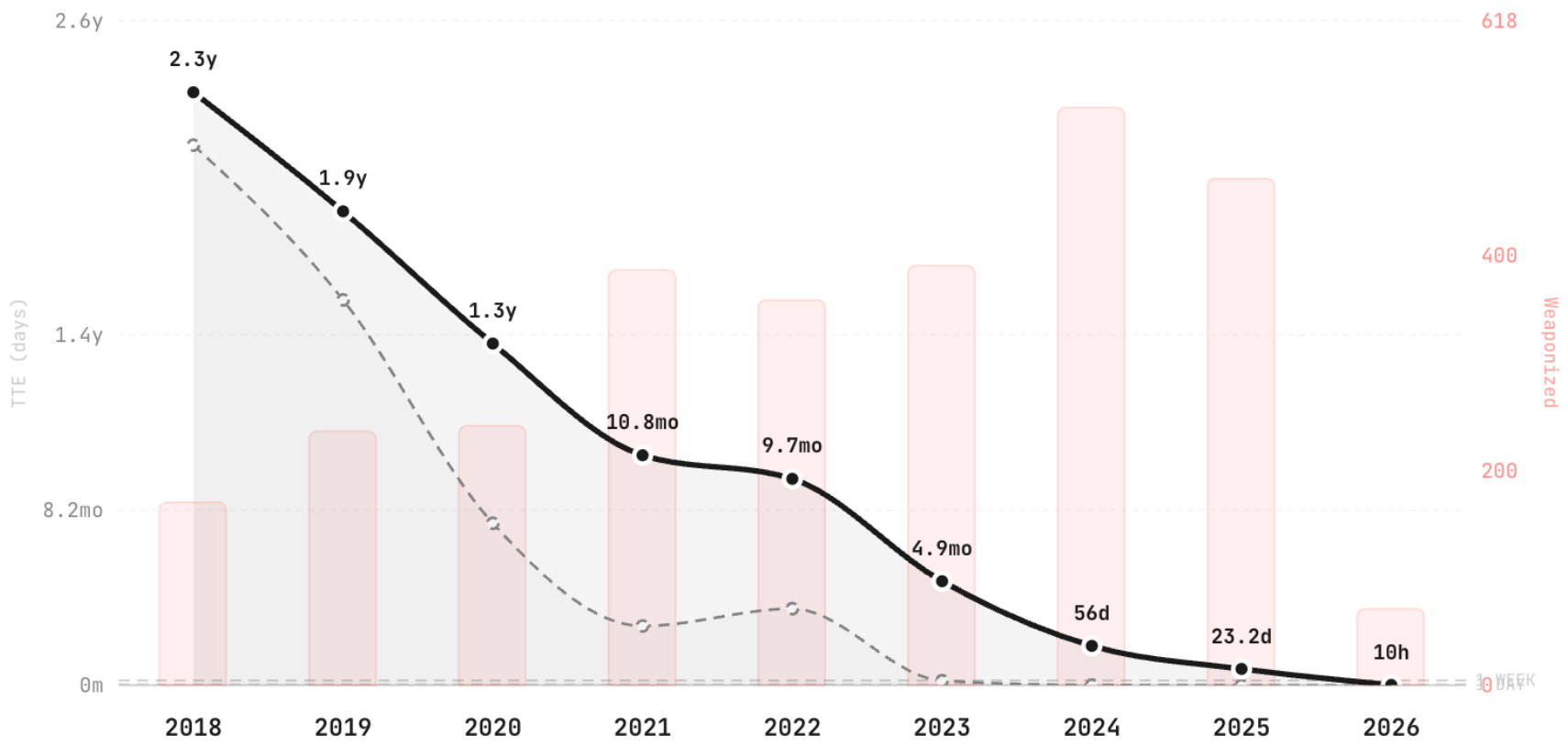
cisco CROWDSTRIKE Google JPMorganChase

THE LINUX FOUNDATION Microsoft NVIDIA paloalto NETWORKS

https://www.anthropic.com/glasswing

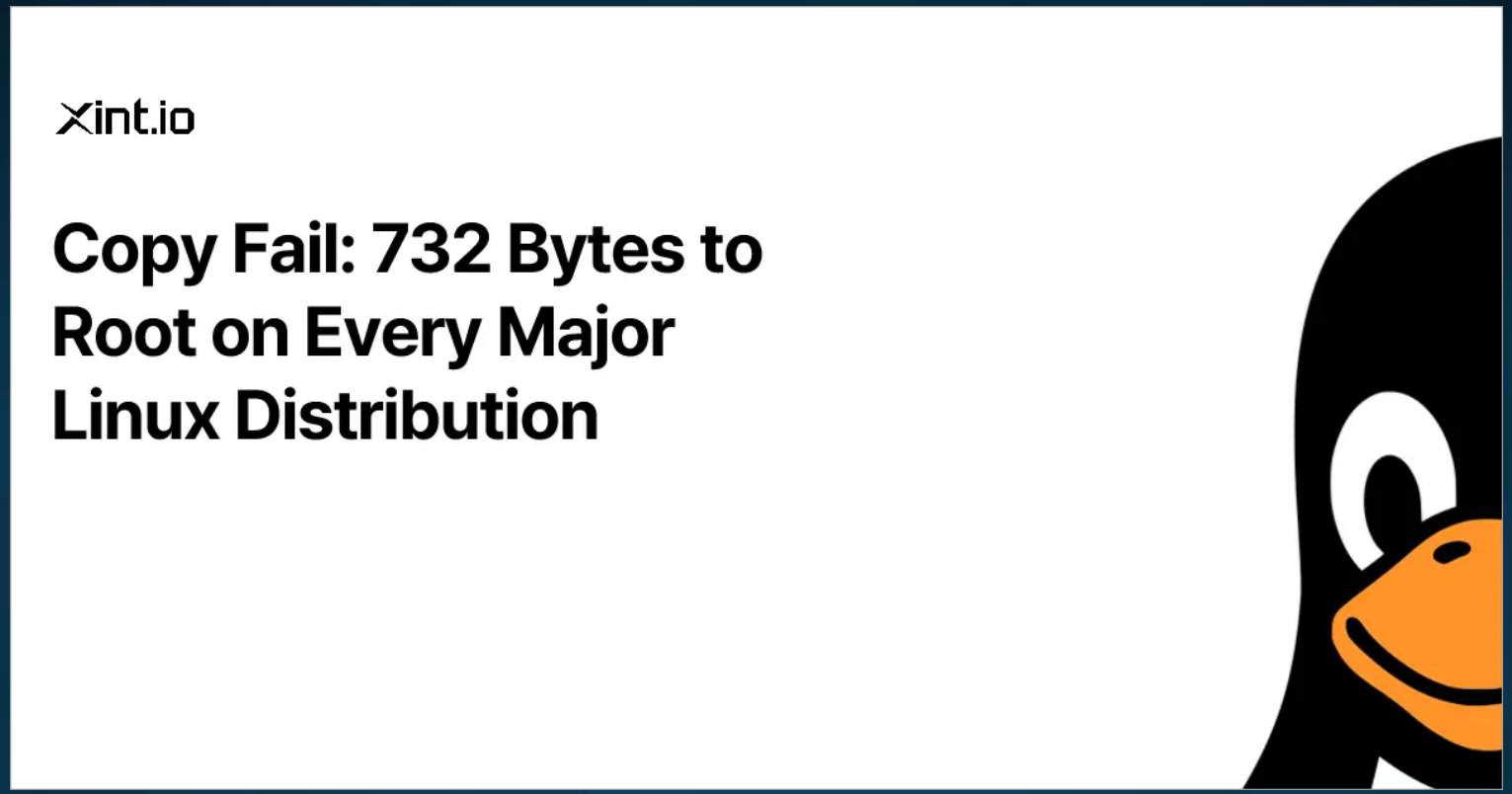
From Vulnerability to Exploitation

TTE (Time-to-Exploit) measures the gap between CVE disclosure and confirmed exploitation



Based on 3,531 CVE-exploit pairs from trusted sources (CISA KEV, VulnCheck KEV & XDB)

zerodayclock.com



"""
This finding was AI-assisted, but began with an insight from Theori researcher Taeyang Lee, who was studying how the Linux crypto subsystem interacts with page-cache-backed data. He used Xint Code to scale his research across the entire crypto subsystem, and Copy Fail was the most critical finding in the report.
"""

https://xint.io/blog/copy-fail-linux-distributions
https://www.ipa.go.jp/security/security-alert/2026/alert20260501.html

AI主導型脅威に対する構造的防衛戦略

「人間の応答速度」から、「マシンスピード」へのパラダイムシフト

現状の認識

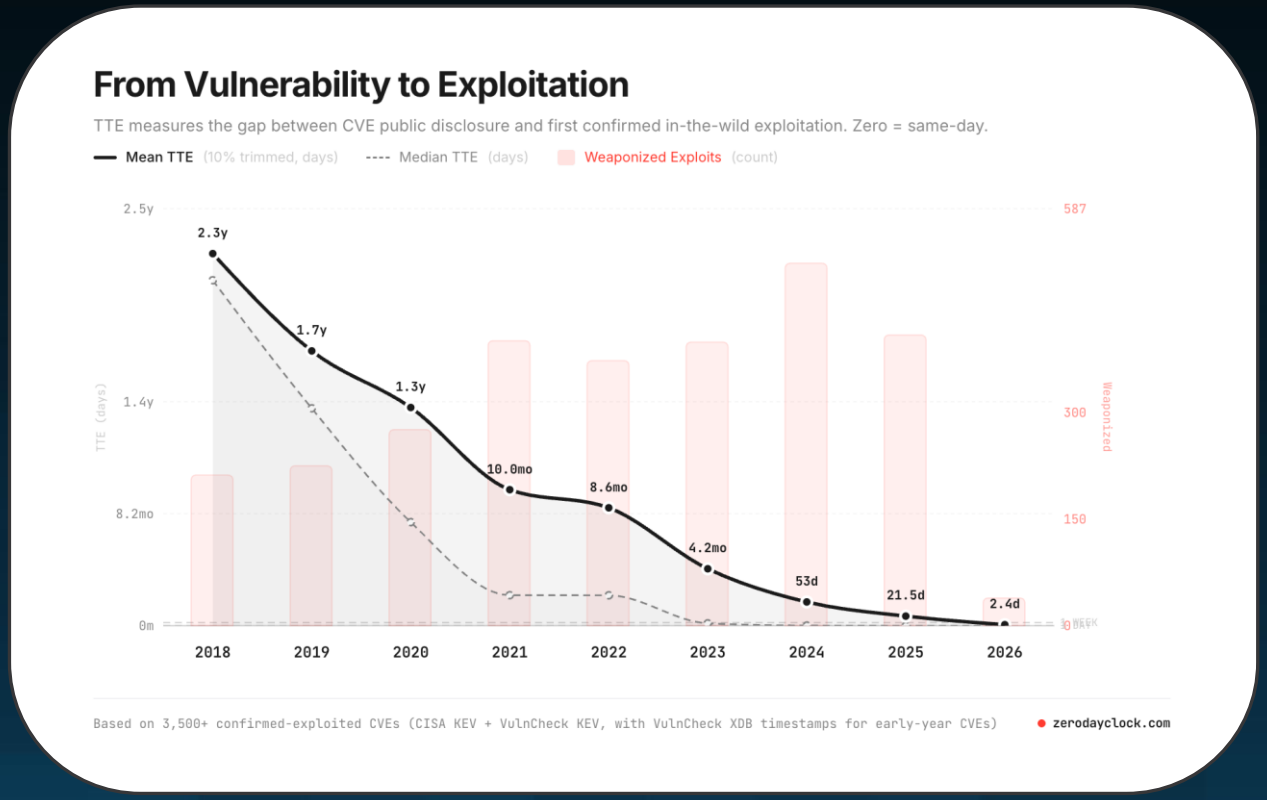
AIは単なるサイバー攻撃の「補助ツール」から、自律的に目標を達成する「エージェント」へと進化

Ciscoの視点

先行プレビューであるAnthoripicの「Mythos」モデルとの協業検証により、特定の悪用手法における「スキルの壁」が劇的に低下し、ゼロデイ脆弱性の発見が加速することを確認

戦略的要件

政府およびユーザ企業は、インフラの根本的な近代化と、ワークロードに直接組み込まれた「アクティブディフェンス」の導入を、急務としなければならない



脆弱性発見からエクスプロイトまでの猶予が実質ゼロになる時代において、手動対応を前提とした従来の防御モデルは、機能不全に陥る。

CISCO TALOS

ランサムウェア

ランサムウェア攻撃は、持続的かつ適応的

CISCO TALOS

Ransomware Summary

1. 製造業が最も標的とされた業界でした。
2. Qilinは攻撃件数において最多でした。
3. 1月の活動低下は、防御側にとって戦略的な対応の好機を提供します。
4. すべての攻撃段階において、有効なアカウントと認証済みツールが利用されていました。

ランサムウェアは2025年においても、世界中の企業に対する主要な脅威であり続けました。
その背景には、攻撃者が戦術・技術・手順（TTP）を継続的に進化させ、RaaS（Ransomware-as-a-Service）の能力を強化し、被害者への圧力を高めていることがあります。

40+

2025年におけるQilinのデータリークサイトに掲載された月間平均被害組織数。

RDP

ランサムウェア攻撃全体で最も一貫して使用されたツール。

#1
35

LockBit 3.0は、ランサムウェアグループの順位において大幅な低下を示しました。

CISCO TALOS

注目の脅威アクター：Qilin

Qilinは2025年において支配的な存在として台頭し、Talos IRのランサムウェア対応案件および、当社が追跡するすべてのグループの中でデータリークサイトへの投稿数において最大の割合を占めました。
本RaaS（Ransomware-as-a-Service）に関する分析からは、今年の成功要因として複数の点が明らかになっています。

アフィリエイトへの報酬分配

Qilinのアフィリエイトは、身代金収益の大部分（最大80〜85%）を受け取っており、一般的なRaaSの分配構造よりも高い割合となっています。

標的化能力

QilinのランサムウェアはGolangとRustの両方で開発されており、多様なオペレーティングシステムを標的とすることが可能で、潜在的な被害対象を拡大しています。

包括的サービス

Qilinはアフィリエイトに対して、法的支援、専属ジャーナリスト、自動交渉サービス、DDoS攻撃機能、スパムキャンペーン支援など、独自のサービスを提供しています。

勧誘戦略

同グループはRAMPやXSSといったハッキングフォーラムで積極的にアフィリエイトを募集しており、技術的優位性、カスタマイズ可能な攻撃、そして高い収益分配を訴求しています。

Qilinは二重恐喝（ダブルエクストーション）戦略を採用しています。

同グループのデータリークサイトによると、2025年には1月を除き毎月40件以上の被害者を標的としており、このランサムウェアグループが2026年も持続的な脅威であり続けることを示唆しています。

セキュリティチームへのガイダンス

1. ランサムウェア攻撃者は攻撃ライフサイクル全体を通じて有効な認証情報に依存するため、アイデンティティ保護を強化する。
2. ラテラルムーブメントに利用されるRDP、PowerShell、PsExecなどの組み込み管理ツールの使用を監視する。
3. 基本の徹底が重要である。バックアップ、セグメンテーション、および復旧能力を強化する。
4. ランサムウェア対応の準備状況を定期的に検証する。

多要素認証に対する攻撃

攻撃者はアイデンティティ検証を担うシステムを標的としている。

CISCO TALOS

Attacks on MFA Summary

2025年において、攻撃者はアイデンティティアクセス管理（IAM）への攻撃を一層強化するとともに、高価値な特権ユーザーアカウントへの攻撃も拡大しました。IAMアプリケーションに対するスプレー攻撃の増加は、脅威アクターがシングルサインオン（SSO）や条件付きアクセスで保護されたログインフローへの攻撃を強化していることを示しています。

1. 攻撃者は、ユーザーのリソースアクセスを制御するソフトウェアツールを重点的に標的としました。
2. 攻撃者は、長期的な特権アクセスの獲得をますます狙うようになっています。
3. 攻撃者は、業界に応じてMFA攻撃の手法を調整していました。
4. また、ログインフローに対する自動化攻撃キャンペーンも強化しました。

178%

不正なデバイス登録イベント数の増加率

30%

MFAスプレー攻撃のうち、IAMアプリケーションを標的とした割合

36%

MFAスプレー攻撃のうち、テクノロジー業界を標的とした割合。

CISCO TALOS

国家支援型アクター

State-sponsored actors summary

国家支援型アクターは、明確な戦略的意図と高い持続性（忍耐性）を引き続き示しています。新規性を追求するのではなく、情報収集、経済的利益の獲得、影響工作といった国家目標にサイバー作戦を一貫して整合させています。

1. 国家支援型グループは、即時的な影響よりも、持続性および長期的なアクセスの確保に重点を置いています。
2. ロシアのサイバー活動は、広範な情報機関および軍事的目標と戦略的に整合した状態を維持していました。
3. 中国に関連するサイバー犯罪活動の増加は、金銭的動機への重視を浮き彫りにしています。
4. 今年のイラン系APTの活動では、ShroudedSnooperのツールキットの更新が確認されています。

74%

2025年における中国関係調査案件の増加率

$1.5b

北朝鮮系アクターによってBybit取引所から窃取された金額

60%

2025年における主要なイラン系ハクティビストグループの活動増加率

CISCO TALOS

North Korea

注目すべき脅威アクター：
Famous Chollima

Contagious Interview at a glance

338以上の悪意ある
npmパッケージ

50,000件以上の
ダウンロード

180以上の
偽装ペルソナ

数十の
C2エンドポイント

数百の確認済み
被害組織

2025年を通じてTalosは、北朝鮮系脅威アクターFamous Chollimaが、偽の採用スキームを悪用する「Contagious Interview」キャンペーンの能力を強化していることを観測しました。

Iran

イスラエル・ハマス紛争の激化により、ハクティビスト活動が急増

イスラエル・ハマス紛争に伴うハクティビスト活動の急増とその特徴は、ロシア・ウクライナ戦争で観測された動向と非常によく似ている

軍事的・地政学的イベントが活動急増の触媒として機能する

DDoS攻撃が主要な役割を果たしており、特に政府、メディア、公共サービスが標的となっている

攻撃者グループは紛争当事地域を超えて、世界各地から参加者を引き寄せている

活動はソーシャルメディア上で拡散され、分断を助長し偏見を煽る扇動的な言葉が用いられている

重要サービスやインフラに影響を与える攻撃は稀であり、その多くは確証の低い攻撃である

CISCO TALOS

イランに関連づけられるグループによる活動は、2025年6月に前月比でほぼ3倍に増加し、軍事的衝突とハクティビスト活動の連動性を示しています。

本分析は、主要なイラン連携ハクティビストグループおよびそれらが管理するアカウントへの投稿の追跡に基づいています。

Threat actor spotlight: Z-Pentest

Z-Pentest（別名Z-Alliance）は、2024年後半に結成された親ロシア系ハクティビスト集団であり、2025年には親イラン的な立場を公に示しており、イデオロギー的な重なりの可能性を示唆している。

同グループは、重要インフラ組織を標的とした可視性の高いOT（オペレーショナルテクノロジー）侵入に関与しており、DDoSなど従来型のハクティビスト攻撃とは異なる顕著な傾向を示している。

今後を見据えると、本グループはその能力、他のハクティビスト集団との協働実績、そして親イラン的立場の公然化により、本脅威環境において注視すべき存在である。

Typical attack chain:

Reconnaissance	Resource Development	Initial Access	Impact
			
公開されているOTシステムのスキャン	一時的なVPSインフラの利用	脆弱またはデフォルトの認証情報の悪用	OTシステムの改ざんや操作を行い、その証拠を公開チャネルに投稿

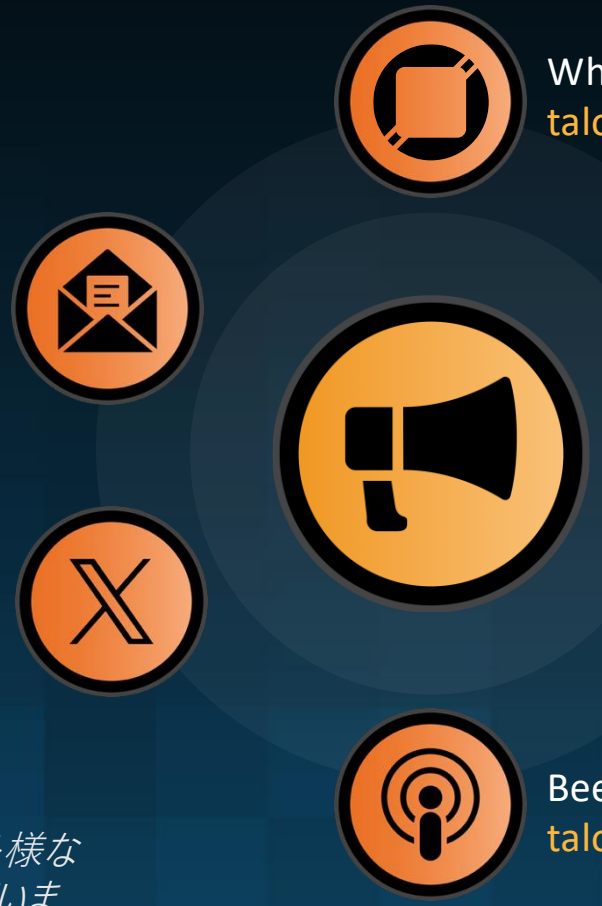
レポートはウェブからダウンロード可能です。

https://gblogs.cisco.com/jp/2026/04/2025-talos-year-in-review-speed-scale-and-staying-power/

CISCO TALOS

Stay connected and up to date

セキュリティに関するニュース、最新情報、
その他の情報を一般に広く発信



White papers, articles, and other information
talosintelligence.com

Threat Source Newsletter
cs.co/Threatsource

Talos blog
blog.talosintelligence.com

Social media posts
LinkedIn: Cisco Talos
X: @talossecurity
Bluesky: @talosintelligence.com

Videos
cs.co/talostube

Beers with Talos and Talos Takes
talosintelligence.com/podcasts

Talosは、インターネットをより安全にするため、多様なチャネルを通じてセキュリティ情報を広く公開しています。

CISCO TALOS

TALOSINTELLIGENCE.COM