CISCO TALOS

Incident Response Trends: Q4 2023

Speaker Background

Mike Trewartha

Senior Consultant, Cisco Talos Incident Response

- GIAC Cloud Forensics Responder (GCFR)
- Certified Information Systems Security Professional (CISSP)
- ISO27001 Lead Auditor
- Google Cloud Professional Cloud Architect
- Red Hat Certified Engineer (RHCE)

An experienced veteran with over 25 years of combined Information Technology and Security experience.

- Unix SysAdmin
- Cloud Solution Architect
- Head of Security
- Senior Cyber Risk Consultant
- Incident Response Consultant

Areas of Expertise:

- Unix Analysis
- Digital Forensics
- Incident Response
- Security Operations
- Consulting
- Cloud Security

Located in Adelaide, South Australia

Cisco Talos

The threat intelligence group at Cisco

Leading Threat Intelligence

625B web requests per day

200+ vulnerabilities discovered per year

1.4M+ new malware samples per day

30B endpoint events per day

Founded in Fighting the Good fight

Global Threat Hunting Team

43 languages

60+ government and law enforcement partnerships

30K critical infrastructure endpoints monitored in Ukraine

Global Capabilities

400+ dedicated responders and intelligence researchers

Leading security technology with the ability to reach across the entire Cisco enterprise

Raising the Bar for Defensive Technology

1.7M networks protected

50M mailboxes protected

87M endpoints protected

CISCO TALOS

Reporting Scope

This presentation covers the incident response engagements closed out in Q4 2023 (October – December).

It documents the top threats we observed, TTPs, impact, and security weaknesses that facilitated adversary actions.

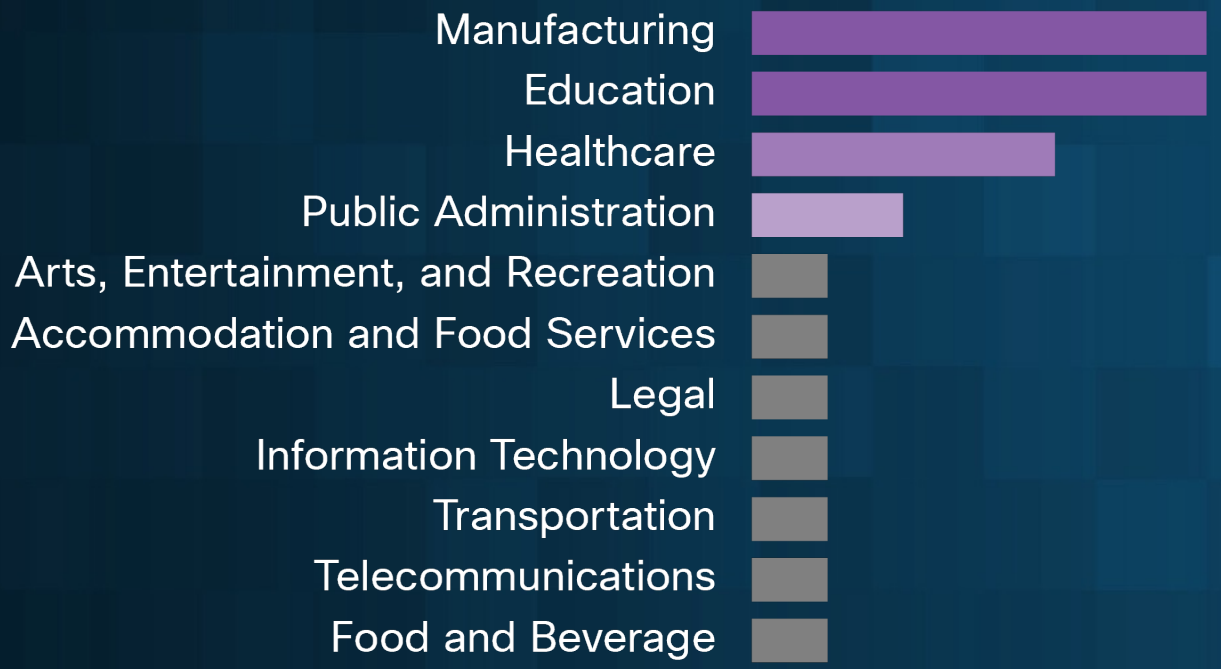
Covers engagements in organizations in a wide variety of industries and geographies.

CISCO TALOS

Ransomware was the top threat in Q4

CISCO TALOS

Attackers targeted manufacturing and education companies the most in the fourth quarter of 2023.



CISCO TALOS

Exploit in public-facing application and mis-use of valid accounts were the top infection vectors in Q4

CISCO TALOS

Observed Trends

Top observed threat was ransomware

Top initial access vector was exploit in public-facing applications

Top weakness was lack of MFA

CISCO TALOS

Ransomware increase from previous quarter

Talos IR responded to Play, Cactus, BlackSuit, and NoEscape ransomware groups for the first time in Q4

Play

- Anydesk persistence
- Disabled security tools
- MFA bypass

Cactus

- VPN account with no MFA
- Lateral movement with RDP
- Persistence with scheduled tasks and WMIC

BlackSuit

- Mimikatz
- ScreenConnect used for persistence
- Targeting Education

NoEscape

- CitrixBleed
- Itarian for persistence
- Cobalt Strike and Sliver

CISCO TALOS

Looking Forward

- December 19, 2023 – FBI Announced disruption of ALPHAV ransomware infrastructure.
- LockBit ransomware group offers to recruit ALPHAV developers.

Looking Forward

- Growing trend of QR Code Phishing -> MFA exhaustion attacks

CISCO TALOS

Looking Forward

CISCO TALOS

Actions after Compromise

Traversing the Network

Attackers abused remote services, such as RDP, SSH, and SMB, to move laterally in 24 percent of engagements.

Evasion

Indicator removal, such as file deletion was the top observed defense evasion this quarter

Disabling security tools, including EDR solutions

CISCO TALOS

Other Actions

Use of remote access software: AnyDesk, ScreenConnect, TeamViewer, SplashTop, etc.

Abuse of service accounts for privilege escalation

CISCO TALOS

Top ATT&CK Techniques

- T1078 Valid Accounts
- T1190 Exploit in Public-Facing Application
- T1003 OS Credential Dumping
- T1021 Remote Services
- T1219 Remote Access Software
- T1070.004 Indicator Removal: File Deletion
- T1218.011 System Binary Proxy Execution: Rundll32
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1018 Remote System Discovery
- T1105 Ingress Tool Transfer

Recommendations

Implement MFA

Educate users about MFA exhaustion attacks and QR code phishing attacks.

Centralize logs

Patch vulnerable systems

CISCO TALOS

Key threats Talos is tracking:
Aviation

APT29
Infostealer

Russian state-sponsored threat actor seeking to gather intelligence and data from entities in the public sector.

Lazarus
Infostealer

State-sponsored threat actor stealing information and credentials for the benefit of North Korea.

APT41

Nation state espionage group focusing on high-tech strategic industries.

CISCO TALOS

Key threats Talos is tracking:
Retail

Data Leak Misconfiguration

Leaking of customer data from poorly secured cloud storage, or theft of credentials.

Business Email Compromise

Criminals conducting financial fraud with the assistance of generative AI.

BlackCat Ransomware

Criminal ransomware group operating as ransomware-as-a-service (RaaS).

CISCO TALOS

Key threats Talos is tracking:
Telecommunications

LockBit
Ransomware

Criminal ransomware gang that exfiltrates data for double extortion, threatening disclosure and no decryption unless paid.

Lazarus Group

State-sponsored group targeting employees within high tech industries to gain access to systems.

Greatness
Phishing-as-a-service

Phishing-as-a-service (PaaS) targeting the tech sector.

CISCO TALOS

Q&A

blog.talosintelligence.com @talossecurity

TALOSINTELLIGENCE.COM

thank you!

blog.talosintelligence.com

@talossecurity

TALOSINTELLIGENCE.COM

TALOSINTELLIGENCE.COM