Talos IR Trends Q2 2023

Aug 2023

Agenda

1. Introduction
2. Top Threats
3. Targeted Industries
4. Attack Vectors
5. Industry Verticals

Speaker Background

Mike Trewartha

Senior Consultant, Cisco Talos Incident Response

- Certified Information Systems Security Professional (CISSP)
- ISO27001 Lead Auditor
- Google Cloud Professional Cloud Architect
- Red Hat Certified Engineer

An experienced veteran with over 20 years of combined Information Technology and Security experience.

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

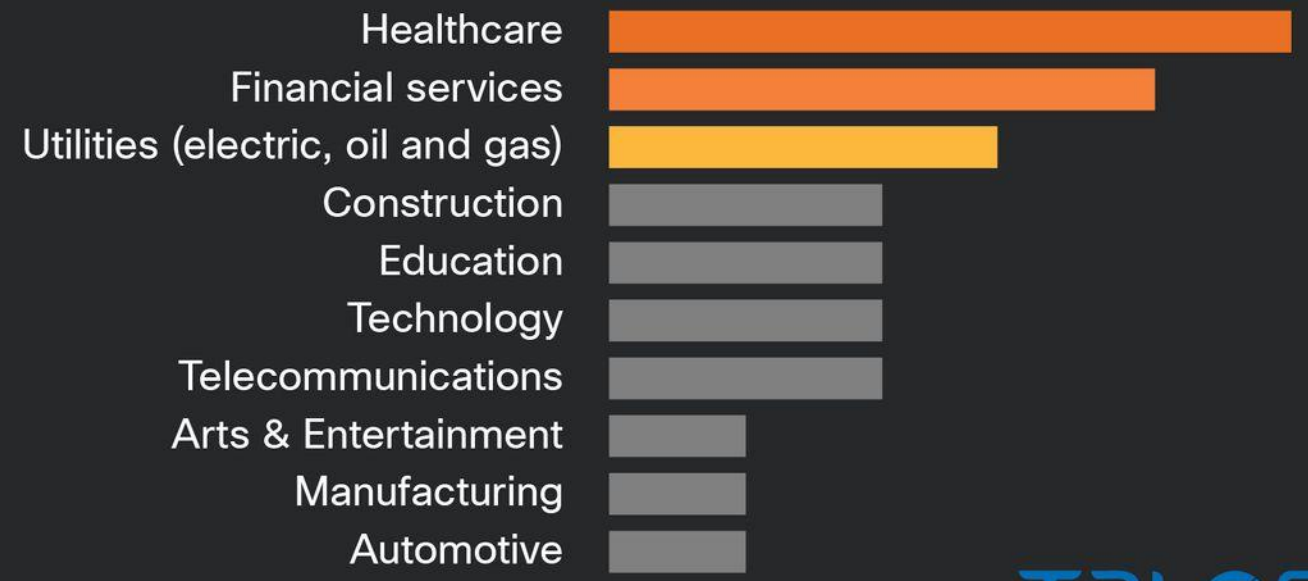
50M mailboxes protected

87M endpoints protected

Data theft extortion was the top threat in Q2

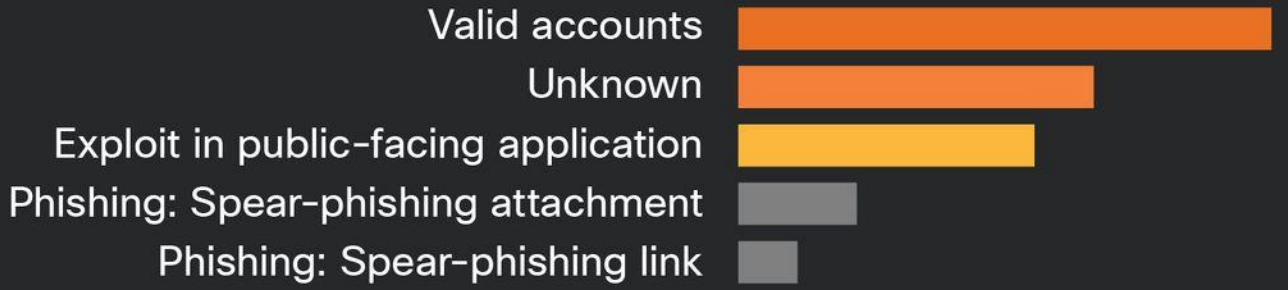
TALOS

Attackers targeted healthcare companies the most in the second quarter of 2023



TALOS

Valid accounts was the top infection vector in Q2



TALOS

https://attack.mitre.org/

Top-observed MITRE ATT&CK techniques

TACTIC	TECHNIQUE	EXAMPLE
Initial Access (TA0001)	T1078 Valid Accounts	Adversary leveraged stolen or compromised credentials.
Execution (TA0002)	T1059.001 Command and Scripting Interpreter: PowerShell	Executes PowerShell code to retrieve information about the client's Active Directory environment.
Persistence (TA0003)	T1053.005 Scheduled Task/Job: Scheduled Task	Scheduled tasks were created on a compromised server to execute malware during startup.
Defense Evasion (TA0005)	T1562.001 Impair Defenses: Disable or Modify Tools	Uninstall security tools to evade detection.
Credential Access (TA0006)	T1003.006 OS Credential Dumping: DCSync	Use DCSync attack to gather credentials for privilege escalation routines.
Lateral Movement (TA0008)	T1563.002 Remote Services Session: RDP Hijacking	Adversary compromised an existing user's Remote Desktop Protocol session.
Impact (TA0040)	T1486 Data Encrypted for Impact	Deploy ransomware and encrypt critical systems.
Software/Tool	S0359 Nltest	Enumerate remote domain controllers with Nltest.

Finance & Insurance

Key threats Talos is tracking

Killnet Ransomware

Pro-Russian group launching denial-of-service attacks.

LockBit Ransomware

Criminal ransomware. Exfiltrates data for double extortion, threatening disclosure and no decryption unless paid.

RA Group Ransomware

Ransomware group targeting wealth management and insurance providers.

Retail

Key threats Talos is tracking

Data Leak Misconfiguration

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

MajikPoS Infostealer

Stealing credit card information from point of sale environment.

BlackCat Ransomware

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

Transportation

Key threats Talos is tracking

Killnet Ransomware

State sponsored threat actor targeting engineers to steal secrets.

LockBit Ransomware

Criminal ransomware. Exfiltrates data for double extortion, threatening disclosure and no decryption unless paid.

Hacktivist Activity

Patriotic or ideologically motivated groups disrupting transport infrastructure.

Education

Key threats Talos is tracking

Targeted industry!

Vice Society Ransomware

- Criminal affiliate network targets to infiltrate and hit with ransomware, compromising administrator and IT user accounts.

Firebrick Ostrich Business Email Compromise

- Business email compromise group utilizing phishing campaigns to steal information and credentials

Transparent Tribe Infostealer

- Pakistani based APT actor targeting educational institutions.

Adversaries continue to target this industry due to providers' often underfunded cybersecurity budgets.

Half-Year in Review: Recapping the top threats and security trends so far in 2023

Threat trends

Many of the threats we've written about this year have involved extortion as part of the attackers' plans. We've seen threat actors utilize every chance they get to steal sensitive data, to be used in future attacks and/or to manipulate victims into paying up before their data ends up on the dark web. Another growing trend is the mercenary landscape – "hackers for hire" growing their wares and increasingly commercializing tools, such as spyware.

The mercenary space is a topic we'll talk more about in the "2023 Year in Review" which Cisco Talos researchers, detection specialists, linguists, threat hunters, incident responders, and analysts are now actively working on, and will be published later this year.

Last year's inaugural report represented an unprecedented effort within Cisco to tell a comprehensive story of our work, relying on a wide variety of data and expertise. This year, we are bringing all these elements together again, to report on how the threat landscape has changed from 2022 and delve deep into some of the most notorious and impactful threats of 2023.

Thank you!

TALOS INCIDENT RESPONSE

blog.talosintelligence.com

@talossecurity