CISCO TALOS

Incident Response Trends: Q2 2024

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

550B security events per day

~2000 malware samples per minute

~9M emails blocked per hour

~2000 domains blocked per second

Founded in Fighting the Good fight

500+ dedicated responders and intelligence researches globally

43 languages

60+ government and law enforcement partnerships

Information Sharing

- Threat research and vulnerability publishing
- Industry partnerships

Customer Intelligence

- Enhanced context
- Emergency bulletins and notifications
- Proactive IR services

Product Protections

- Reputation
- Categorization
- Detection Content

Raising the Bar for Defensive Technology

2.7M networks protected

100M mailboxes protected

120M endpoints protected

CISCO TALOS

Reporting Scope

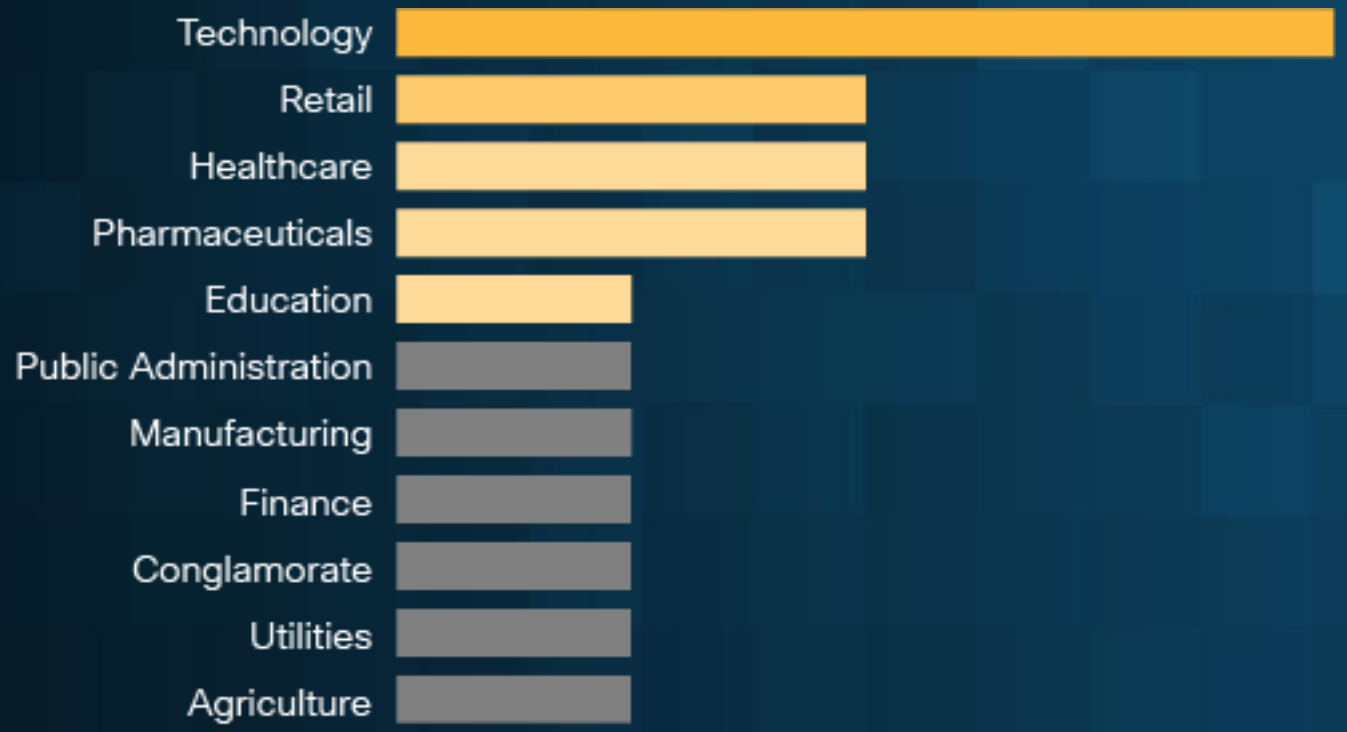
This presentation covers the incident response engagements closed out in Q2 2024 (April - June).

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.

CISCO TALOS

Technology was the most targeted vertical this quarter.



CISCO TALOS

Observed Trends

Top observed threats were business email compromise (BEC) and ransomware

Top initial access vector was the use of compromised credentials on valid accounts

Top weaknesses were vulnerable or misconfigured systems and a lack of MFA

CISCO TALOS

BEC and ransomware were the top threats this quarter

CISCO TALOS

There was a slight increase in network device targeting.

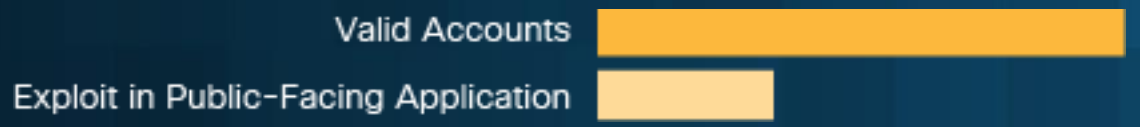
Password spraying

Active scanning

Exploitation of vulnerabilities

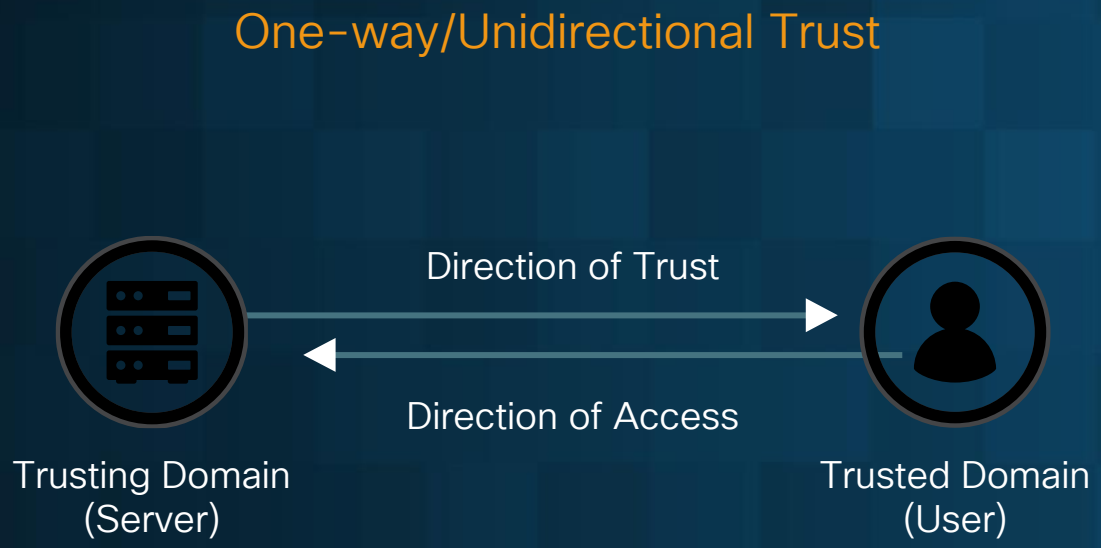
CISCO TALOS

The use of compromised credentials on valid accounts was the top infection vector in Q2



CISCO TALOS

Looking forward: Talos IR has observed an increase in compromises of trusted partners



CISCO TALOS

Looking forward: Talos IR has observed a decrease in botnet and loader activity which may be related to Operation Endgame

Actions after Compromise

Lateral Movement

Attackers abused remote services, such as RDP, SSH, and SMB, to move laterally in 60 percent of engagements.

CISCO TALOS

Establishing persistence

The creation of new accounts was the top persistence technique leveraged by adversaries this quarter.

Command and Control (C2)

The use of remote access software, like AnyDesk, was the top C2 technique this quarter.

CISCO TALOS

Defense Evasion

The abuse of the Windows utility Rundll32 was one of the top defense evasion techniques.

Top Security Weaknesses

CISCO TALOS

Recommendations

Implement MFA and educate users about MFA exhaustion attacks and QR code phishing attacks.

Follow industry best practices for password policies and consider using a password manager

Centralize logs and implement endpoint protection

Patch vulnerable systems

CISCO TALOS

Q&A

 blog.talosintelligence.com

 @talossecurity

TALOSINTELLIGENCE.COM