Incident Response threat summary for October - December 2023

Ransomware attacks rose for the first time all year

The takeaway

Ransomware, including pre-ransomware activity, was the top-observed threat in the fourth quarter of 2023, accounting for 28 percent of all Cisco Talos Incident Response engagements. That is a 17 percent increase from Q3. Talos IR observed multiple ransomware operators in the wild last quarter, involving Play, Cactus, BlackSuit and NoEscape. In one case, Talos IR responded to a Play ransomware attack for the first time ever.

Top threats

- Substantial threats this quarter included an insider threat attack and phishing campaigns.
  - Talos IR responded to many incidents with miscellaneous post-compromise activity, though these attacks were limited in scale and contained by security efforts early in the attack chain.
- Education and manufacturing were tied for the most targeted verticals, accounting for nearly 50 percent of the total number of incident response engagements.
- The top observed means of gaining initial access was tied between using compromised credentials on valid accounts and exploiting public-facing applications, each accounting for 28 percent of engagements.

Other lessons

- A lack of multi-factor authentication (MFA) implementation was the top security weakness, accounting for 36 percent of engagements, continuing a trend we observed throughout 2023.
- There was a significant increase in QR code phishing in 2023, according to public reporting. Talos IR responded to a QR code phishing campaign for the first time in an engagement in Q4.
- Although the infamous zero-day vulnerability dubbed "Log4Shell" was patched in December 2021, attackers continue to exploit vulnerable systems two years later.
- In nearly 60 percent of all engagements this quarter, adversaries gained initial access by using compromised credentials on valid accounts and exploiting public-facing applications.

How are our customers protected?

- The lack of MFA remains one of the biggest impediments for enterprise security. All organizations should implement some form of MFA, such as Cisco Duo.
- Endpoint detection and response solutions like Cisco Secure Endpoint can detect malicious activity on organizations' networks and machines.
  - Attackers frequently tried to bypass MFA on EDR solutions to disable their alerting mechanisms.
- Snort and ClamAV signatures can block many well-known pre-ransomware tools attackers deployed this quarter, such as Play and NoEscape.