CISCO TALOS

Incident Response threat summary for July–September 2023

Attacks targeting web applications rose, while telecommunications and education remain top-targeted verticals

THE TAKEAWAY

There was a notable increase in threats to web applications in Cisco Talos Incident Response (Talos IR) engagements this quarter, accounting for 30 percent of all incidents in Q3, compared to 8 percent the previous quarter. Exploitation of public-facing applications was the top observed means of gaining initial access, accounting for 30 percent of engagements, likely due to the higher number of web application attacks observed. The threats facing web applications are a continuation of a trend from Talos IR in Q1 2023 where web shells were the most-observed threat.

TOP THREATS

- Commodity loaders were observed in 10 percent of engagements this quarter, consistently distributed via drive-by compromise, including the previously seen Gootloader commodity loader.
- Telecommunications and education were the most targeted verticals, each accounting for 20 percent of the total number of incident response engagements, closely followed by public administration and manufacturing.
    - We observed a previously unidentified advanced persistent threat (APT) group, ShroudedSnooper targeting telecommunications firms in the Middle East , deploying two novel implants dubbed HTTPSnoop and PipeSnoop.

OTHER LESSONS

- In 25 percent of engagements, attackers abused remote services, such as Remote Desktop Protocol (RDP), to move laterally.
- Attackers are still trying to find ways to bypass multi-factor authentication (MFA), including with MFA exhaustion attacks in which the adversaries send many push notifications at once, hoping the targeted user will eventually accept one of the login attempts.
- Despite an effort from multiple international law enforcement agencies to take down the Qakbot commodity loader in August, Talos suspects the actors behind this threat may still be active.

HOW ARE OUR CUSTOMERS PROTECTED?

- 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 Qakbot and Gootloader.