Incident Response threat summary for April – June, 2023

Data theft rises while healthcare remains most-targeted industry

THE TAKEAWAY

Data theft extortion was the top observed threat this quarter, accounting for 30 percent of Cisco Talos Incident Response (Talos IR) engagements this quarter, overtaking web shells and still ranking above ransomware. Talos IR saw a 25 percent increase in data theft extortion incidents compared to the last quarter. The rise in data theft extortion incidents compared to previous quarters is consistent with public reporting on a growing number of ransomware groups stealing data and extorting victims without encrypting files and deploying ransomware. Ransomware was the second most-observed threat this quarter, accounting for 17 percent of engagements, while web shells, which was a fast-rising threat in Q1, declined.

TOP THREATS

- In a novel increase compared to previous quarters, Talos IR responded to a growing number of data theft extortion incidents that did not encrypt files or deploy ransomware.
    - Carrying out ransomware attacks is likely becoming more challenging due to global law enforcement and industry disruption efforts, so ransomware actors are having to find new ways to generate revenue.
- Continuing a trend from last quarter, healthcare was the most-targeted vertical this quarter, accounting for 22 percent of the total number of incident response engagements, closely followed by financial services.
- Compromised credentials or valid accounts were the top observed means of gaining initial access this quarter, accounting for nearly 40 percent of total engagements.
    - However, it can be difficult to identify how the credentials were compromised given that it can occur outside a company's visibility, such as saved credentials on an employee's personal device that was compromised.

OTHER LESSONS

- Forty percent of engagements either did not have multi-factor authentication (MFA) enabled or only had it enabled on a select handful of accounts and critical services, an increase of 10 percent from last quarter.
- The Clop ransomware group exploited a major vulnerability in the MOVEit file transfer software. This has led to many follow-on instances of data theft, with more than 200 companies affected as of early July.
    - Talos IR has yet to respond to any incidents involving the MOVEit vulnerability, but in one case, Talos IR observed Clop exploiting a different vulnerability in the GoAnywhere file transfer software.
- Observed in over 50 percent of engagements this quarter, PowerShell is a dynamic command line utility that continues to be a popular utility of choice for adversaries.
- Exploitation of vulnerabilities in public-facing applications was seen in 22 percent of engagements this quarter, a significant decrease from 45 percent last quarter.

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.