Incident Response threat summary for April - June 2022

Commodity trojans outpace ransomware for first time in several months

THE TAKEAWAY

For the first time in more than a year, ransomware was not the top threat seen in Cisco Talos Incident Response (CTIR) engagements this quarter, as commodity trojans surpassed ransomware by a narrow margin. Compared to previous quarters, ransomware made up a significantly smaller percentage, comprising 15 percent of all threats observed this quarter compared to 25 percent last quarter. This can be attributed to several factors, such as recent law enforcement takedowns of ransomware groups and their continued internal fracturing.

TOP THREATS

- The telecommunications industry was again targeted the most often in CTIR engagements, continuing a trend from last quarter.
  - The education and health care sectors were the next most-targeted.
- High-profile ransomware-as-a-service (RaaS) groups like Conti and BlackCat targeted organizations seeking large payouts.
  - Conti announced it was ceasing operations earlier this year, though the potential effects on the ransomware landscape are still unknown.
  - A new RaaS variant called “Black Basta” is a suspected rebranding of Conti and is likely to be a threat in the coming quarters.
- LockBit ransomware released a new version that includes new cryptocurrency payment options for victims, additional extortion tactics and a new bug bounty program.

OTHER LESSONS

Commodity malware was the top threat seen this quarter, comprising 20 percent of the threats observed. This includes the Remcos RAT, Vidar information stealer, Redline Stealer, and Qakbot banking trojan.

- The next most commonly observed threats included phishing, business email compromise (BEC), and insider threats.

- In line with Q1 2022, we continue to observe email-based threats leveraging a variety of social engineering techniques to entice users to click or execute a given link or file.
- One notable CTIR engagement involved a previously unknown ransomware variant that had overlapping artifacts and components with at least three other ransomware families.
- The top targeted country continues to be the U.S., largely reflected in CTIR’s customer base. Other targeted organizations are seen globally across Europe, Asia, North America and the Middle East.

HOW ARE OUR CUSTOMERS PROTECTED?

- Cisco Secure Firewall and SNORT® rules protect against many of the commodity trojans and malware outlined in our full report, including Qakbot and Redline.
- Cisco Secure Email and Cisco Secure Malware Analytics protect users from targeted phishing emails and business email compromise, which adversaries commonly used this quarter.
- Talos’ top recommendation for this quarter asks organizations implement multi-factor authentication (MFA) on all critical services, such as Cisco Duo.
- Endpoint detection and response solutions like Cisco Secure Endpoint can detect malicious activity on organizations’ networks and machines.