Incident Response threat summary for July - September 2022

Education sector becomes more frequently targeted during back-to-school season

THE TAKEAWAY

For the first time in three quarters, the education sector was the most targeted in Cisco Talos Incident Response (CTIR) engagements this quarter, surpassing telecommunications organizations, which were consistently targeted most often in the first part of the year. This is commonly a popular time of year for adversaries to target the education sector to disrupt core services such as financial aid and student loans, as schools and universities may be more susceptible to cyber attacks while students and teachers head back to school.

TOP THREATS

- Ransomware was the top threat this quarter, a slight change from last quarter where commodity trojans surpassed ransomware by a narrow margin.
    - CTIR saw an equal number of ransomware and pre-ransomware engagements (nearly 40 percent total) close out this quarter. Pre-ransomware engagements made up 18 percent of engagements this quarter, up significantly from less than 5 percent last quarter.
- Several high-profile ransomware groups appeared in CTIR engagements this quarter, including Hive and Vice Society.
    - The Black Basta group appeared for the first time since researchers first discovered their activities in April.
- CTIR observed adversaries leveraging a variety of publicly available tools and scripts hosted on GitHub repositories or from third-party websites to support operations across multiple stages of the attack lifecycle.
- The next most observed threats this quarter included commodity malware such as the Qakbot banking trojan and infostealers like Redline.

OTHER LESSONS

- Nearly 18 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.
- Adversaries' tools focused on accessing and collecting credentials, highlighting the role these tools play in potentially furthering an adversary's objectives.
- Talos has been monitoring the increased use of dual-use tools in these attacks, such as Anonymous Fox, Brute Ratel, Sliver and Manjusaka.
- We also continued to observe threats which are consistently seen across previous quarters, including phishing and business email compromise (BEC), attempts to take advantage of weaknesses or vulnerabilities in public-facing applications, distributed-denial-of-service (DDoS) attacks, and insider threats.

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.
- Snort and ClamAV signatures can block many well-known pre-ransomware tools attackers deployed this quarter, such as Mimikatz and Cobalt Strike.