Talos
Cisco Security Research

Incident Response threat summary for Q2 2020

A RECAP OF THE TOP THREATS OBSERVED BETWEEN NOVEMBER AND JANUARY

THE TAKEAWAY

Many attacks Cisco Talos Incident Response (CTIR) observed in Q2 2020 used ransomware. In several attacks actors threatened to publish victims' sensitive information if the ransom is not paid. This is a concerning new trend that may compel more victims to make an extortion payment, likely encouraging the bad actors to try again in the future.

TOP THREATS

- Commodity trojans: CTIR responded to more incidents in Q2 than in Q1, with the majority involving ransomware or trojans like Emotet and Trickbot.
- Ryuk: Most commonly observed ransomware.
- Phishing: Remains the top infection vector.

OTHER LESSONS

- Although ransomware and commodity trojans remained the top threat, there was an increased amount of incidents involving DDoS attacks and cryptomining attacks.
- The top targeted verticals in Q2 2020 were financial services and government, a change from last quarter when the top targeted vertical was manufacturing.
- We continue to observe open-source tools such as PowerShell Empire, Mimikatz and Meterpreter used in these attacks. We also observed the red-teaming tool CobaltStrike being leveraged.

HOW ARE OUR CUSTOMERS COVERED?

- Specific SNORT® rules and ClamAV® signatures protect against specific malware families like Ryuk and Emotet. Refer to snort.org/advisories and clamav.net for the latest updates.
- Using two-factor authentication, such as Cisco Duo, will help prevent adversaries from accessing users' accounts and spreading malware deeper into the corporate network.
- Constant updates to the Talos and Snort blogs keep users alert for when potential serious patches are released or new Snort rules are added.
- Should an infection occur, having a CTIR retainer gives customers peace of mind that they will have help as soon as possible from our experts.
- Cisco Next-Generation Firewall and Stealthwatch detect changes in your network and monitor outbound and inbound traffic patterns, helping to identify and stop the most advanced threats.

talos-external@cisco.com | talosintelligence.com