Talos
Cisco Security Research

Incident Response threat summary for Q3 2020

A RECAP OF THE TOP THREATS OBSERVED BETWEEN JANUARY AND APRIL

THE TAKEAWAY

Many attacks Cisco Talos Incident Response (CTIR) observed in Q3 2020 used ransomware. However, we surprisingly did not see many attacks utilizing COVID-19 themes, which have been popular since the pandemic took hold in America. However, there remain several challenges for defenders as more individuals work from home and need to access files remotely.

TOP THREATS

- Commodity trojans: CTIR responded to more incidents in Q3 than in Q2, with the majority involving ransomware or trojans like Emotet and Trickbot.
- Ryuk: Most commonly observed ransomware.
- Phishing: Remains the top infection vector.

OTHER LESSONS

- Ransomware and commodity trojans remained the top threat, with Ryuk leading the way.
- The top targeted verticals in Q3 2020 were energy and utilities, a change from last quarter when the top targeted vertical was the public sector and government organizations.
- Actors frequently targeted VPN and remote desktop services.
- Ryuk is adapting to use more living-off-the-land tools rather than its traditional reliance on commodity trojans.

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