Incident Response threat summary for Q1 2020

A RECAP OF THE TOP THREATS OBSERVED BETWEEN AUGUST AND OCTOBER

THE TAKEAWAY

Many attacks Cisco Talos Incident Response (CTIR) observed in Q1 2020 used the Trickbot commodity trojan and Ryuk ransomware alongside one another. This represents a partial continuation from the trends of the previous quarter, though we did see a decline in Emotet infections.

TOP THREATS

- **Commodity trojans:** Malware such as Trickbot that are openly available for purchase online, leading to their popularity.
- **Ryuk:** Most commonly observed ransomware.
- **Phishing:** Remains the top infection vector.

OTHER LESSONS

- There was an uptick in web application exploitation, including the exploitation of newer vulnerabilities such as in the Palo Alto GlobalProtect SSL VPN.
- Verticals targeted include media and entertainment, manufacturing, transportation, business services, government, health care, pharmaceuticals, biotech, telecommunications, insurance, financial services and education.
- Other observed threats include information stealers such as Lokibot and Avemaria, ASP web shells and the Frenchy toolkit.

HOW ARE OUR CUSTOMERS PROTECTED?

- 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.