Incident Response threat summary for Q4 2019

A RECAP OF THE TOP THREATS AND TRENDS CTIR OBSERVED BETWEEN MAY AND JULY

THE TAKEAWAY

The majority of the threats CTIR saw in Q4 were relatively unsophisticated, leveraging well-known malware and simple, commonly seen infection methods.

TOP THREATS

- **Ryuk:** The most common ransomware strain.
- **Emotet & Trickbot:** Adversaries’ most-used banking trojans.
- **Phishing:** Remains most popular infection vector.

OTHER LESSONS

- Post-infection, adversaries most often encrypted files, mined for cryptocurrencies, reached out to a C2 or traversed the network.
- Adversaries utilized open-source tools such as PowerShell Empire and Mimikatz.
- Verticals targeted include retail, media, tech, manufacturing, government services, health care and education.

HOW ARE OUR CUSTOMERS COVERED?

- Using two-factor authentication, such as **Cisco Duo**, will help prevent adversaries from accessing users’ accounts on the corporate network.
- **CTIR’s Cyber Range** can provide employees with the appropriate training to know how to detect and avoid phishing attempts.
- **Cisco Email Security Appliance** and **Threat Grid** protect users from targeted phishing emails and malicious documents, which adversaries commonly used this quarter.
- **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.
- Specific **SNORT®** rules and **ClamAV®** signatures protect against specific malware families, including Emotet, Ryuk and Trickbot. Refer to snort.org/advisories for more information.