Incident Response threat summary

A RECAP OF THE TOP THREATS OBSERVED BETWEEN NOVEMBER 2020 AND FEBRUARY 2021

THE TAKEAWAY

For the seventh quarter in a row, ransomware was the most common type of cyber attack Cisco Talos Incident Response (CTIR) observed in engagements. The use of commodity trojans spiked in this quarter – they were involved in nearly 70 percent of all ransomware attacks. This is surprising given their relative absence the previous few quarters. CTIR also worked on several incident response engagements involving the SolarWinds supply chain compromise. Only one of these engagements involved post-compromise activity. It is expected the SolarWinds incident will continue to have ripple effects into the rest of 2021. Looking ahead, CTIR has been engaged in several IRs involving the recent Microsoft Exchange zero-day vulnerabilities.

TOP THREATS

- Ransomware comprised 50 percent of all attacks, trending up from 40 percent last quarter. Commodity trojans comprised the second most observed threat with 42 percent of all threats, a big rise for this category of malware.
- The top ransomware variants observed were Vatet and Ryuk, which is interesting considering there were no engagements involving Ryuk that closed out last quarter.
- Phishing remains the top infection vector for the seventh quarter in a row. For another quarter in a row, CTIR also observed actors exploiting a vulnerability in Telerik UI (CVE-2019-18935).
- CTIR observed successful attempts to exploit the F5 vulnerability tracked as CVE-2020-5902.

OTHER LESSONS

- Verticals targeted include business management, construction, education, energy and utilities, entertainment, financial, government, healthcare, industrial distribution, legal, manufacturing and technology.
- Health care was the most targeted industry, which CTIR predicted based off trends seen in the previous quarter and the strain on these systems given the COVID-19 pandemic.
- Adversaries are continuing to use open-source and commercially available tools as well, especially in ransomware attacks. For example, Cobalt Strike was used in half of all ransomware attacks this quarter, just as we saw last quarter.
- The threat landscape could shift in the coming months after international law enforcement agencies announced the takedown of Emotet. So far, CTIR has seen a drop-off in Emotet-based attacks, but this news is likely to change the threat landscape in other ways going forward.

HOW ARE OUR CUSTOMERS PROTECTED?

- Specific **SNORT®** rules and **ClamAV®** signatures protect against specific malware families like Vatet and Ryuk. 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 networks.
- 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 Secure Network Analytics** detects 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