Incident Response threat summary for Q1 2021

A RECAP OF THE TOP THREATS OBSERVED BETWEEN AUGUST AND NOVEMBER 2020

THE TAKEAWAY

For the sixth quarter in a row, ransomware was the most common type of cyber attack Cisco Talos Incident Response (CTIR) observed in engagements. However, the use of Ryuk, specifically, dropped, which was somewhat of a surprise given previous quarters' trends. The use of commodity trojans in these attacks remained low. We expect to see a rise in the frequency of attacks against health care organizations as they continue to address the COVID-19 pandemic, making them more likely to pay any requested extortion payment. Relatedly, we have observed a rise in the use of the Vatet loader, which typically targets the health care sector.

TOP THREATS

- Ransomware comprised 43 percent of all attacks, trending up from 33 percent last quarter, and more closely aligning to Q3 2020, in which ransomware comprised 42 percent. The next most observed threat was Business Email Compromise (BEC), comprising 15 percent of all threats.
- Maze was one of the most frequently observed variants this quarter. However, it is worth highlighting that the Maze ransomware group announced they have officially closed their ransomware operation and claimed they will no longer be leaking new company data on their site.
- Phishing remains the top infection vector for the sixth quarter in a row. CTIR also observed exploitation of some web applications, such as Oracle WebLogic.

OTHER LESSONS

- Verticals targeted agriculture, food and beverage, health care, education, energy and utilities, industrial distribution, law enforcement, local government, manufacturing and technology.
- Manufacturing was the most-targeted vertical, a continuation of last quarter, though there was a sharp uptick in health care targeting toward the end of the quarter.
- The usage of Cobalt Strike decreased by half this quarter. However, we do note there are many open engagements that rely on Cobalt Strike for post-exploitation, and we continue to observe leveraging of native tools, LoLbins, and other offensive security tools.
- Commodity trojans, such as Trickbot and Emotet, were barely present this quarter, with Emotet and Qakbot present in one engagement, and Trickbot completely absent.

HOW ARE OUR CUSTOMERS PROTECTED?

- Specific **SNORT®** rules and **ClamAV®** signatures protect against specific malware families like Sodinokibi and Maze. 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 Firewalls** 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