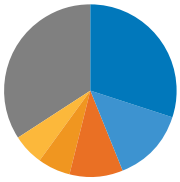
Incident Response threat summary for Q4 2020

A RECAP OF THE TOP THREATS OBSERVED BETWEEN MAY AND JULY

THE TAKEAWAY

Most of the attacks Cisco Talos Incident Response (CTIR) observed in Q4 2020 were ransomware infections, mainly involving the Maze and Ryuk families. The use of commodity trojans in these attacks remained low. This represents a partial continuation of the trends from the previous quarter, as ransomware actors appear to rely more on living-off-the-land tools and the Cobalt Strike framework.

TOP THREATS



- Ransomware | 30%
- Commodity Trojans | 14%
- Remote Access Trojan | 10%
- Web Shells | 6%
- Business Email Compromise | 6%
- Other | 34%

OTHER LESSONS

- Verticals targeted include manufacturing, education, construction, facility services, food and beverage, energy and utilities, financial services, healthcare, industrial distribution, real estate, technology, and telecommunications. Manufacturing was the most targeted.
- Despite a decline from earlier in the year, commodity trojans, such as Trickbot and Qakbot, were the second most popular threat used by adversaries this quarter.
- The Maze ransomware cartel continues to threaten enterprises by publishing sensitive information during ransomware attacks.

HOW ARE OUR CUSTOMERS PROTECTED?

- Specific **SNORT®** rules and **ClamAV®** signatures protect against specific malware families like Ryuk 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