Talos
Cisco Security Research

Incident Response threat summary for October – December 2021

Health care was once again the most-targeted industry, continuing a yearlong trend

THE TAKEAWAY

Ransomware was once again the top threat this quarter that Cisco Talos Incident Response (CTIR) saw in their engagements in Q4 2021, wrapping up a year that was dominated by major news stories around ransomware attacks. Health care was the top-targeted vertical throughout the majority of 2021, a trend that continued in the winter. The only exception was in Q3, in which the top targeted vertical was local government.

TOP THREATS

- Continuing a year-long trend, ransomware was the top threat this quarter, although compared to previous quarters, it made up a much smaller percentage and comprised only 27 percent of all threats observed this quarter compared to 38 percent last quarter.
- This quarter had fewer ransomware engagements than last, leading to a decrease in the number of groups observed this quarter.
- The Stop ransomware family, also known as Djvu, was a newly observed ransomware variant observed this quarter.
- While ransomware was the top threat, there were slightly more observations of commodity trojans this quarter. These types of malware are often purchased online as a one-stop solution for threat actors who want an out-of-the-box tool to infect users.

OTHER LESSONS

- Ransomware was the clear top threat throughout the year 2021, as highlighted by Q4.
- The most commonly observed initial vectors included exploitation of internet-facing applications and phishing attacks.
- CTIR dealt with four major security incidents this year, one of which, Log4j, started in Q4:
  - The SolarWinds supply chain attack.
  - Mass exploitation of Microsoft Exchange Server vulnerabilities.
  - REvil's attack against IT solutions provider Kaseya.
  - The discovery of the Log4j vulnerability.
- Of these four, the Microsoft Exchange vulnerabilities appear to be the most impactful for CTIR customers so far, as we have continued to see incidents leveraging Exchange this Winter.

HOW ARE OUR CUSTOMERS PROTECTED?

- Cisco Talos has released myriad coverage for the Log4j vulnerability discovered in December, which wound up being the top story of Q4 2021. Users can download the latest SNORT® rules from Snort.org and read the Talos blog for our latest insights.
- Cisco Secure Firewall and Secure Network Analytics detect changes in your network and monitor outbound and inbound traffic patterns, helping to identify and stop the most advanced threats.
- Using multi-factor authentication (MFA), such as Cisco Duo, will help prevent adversaries from accessing users' accounts and spreading malware deeper into networks. CTIR frequently observes all types of incidents that could have been prevented if MFA had been enabled on critical services.
- 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.