Incident Response threat summary for January – March 2022

Telecommunications overtakes health care as most-targeted industry

THE TAKEAWAY

Ransomware was once again the top threat this quarter that Cisco Talos Incident Response (CTIR) saw in their engagements in Q1 2022, though there was a greater range of malware threats used by threat actors. CTIR did not see any ransomware family used more than once, indicative of a greater democratization of the threat landscape, a trend we first started seeing last year. A recent wave of leaks from the Conti ransomware group will also likely continue this shift.

TOP THREATS

- Continuing a year-long trend, ransomware was the top threat this quarter, although compared to previous quarters, it made up a slightly smaller percentage and comprised only 25 percent of all threats observed this quarter compared to 27 percent last quarter.
- The telecommunications industry was targeted the most often in CTIR engagements, breaking a several quarters-long streak in which attackers targeted health care more than any other industry.
- This quarter also saw the first appearances of three ransomware families, including Cerber (aka CerberImposter), Entropy and Cuba.
- Attackers frequently exploited the high-profile Log4j vulnerability, first disclosed in December 2021.
- Wave Browser, a supposed web browser, was observed in several engagements. This is a potentially unwanted program (PUP) associated with adware and browser hijacking that CTIR linked to subsequent malicious activity.

OTHER LESSONS

- The Conti ransomware-as-a-service (RaaS) gang experienced several waves of leaks over the past quarter, disclosing the malware's source code and other key pieces of information regarding the group. CTIR expects that these leaks may make threat actor attribution more difficult in cases involving typical Conti TTPs .
- Q1 2022 saw an increase in APT-type activity, specifically attacks from the Iranian state-sponsored MuddyWater group and the China-based Mustang Panda actor deploying the PlugX remote access trojan.
- Adversaries exploited the Log4j vulnerability to target VMware Horizon servers, which CTIR saw in engagements this quarter, with attackers leveraging the vulnerability to install malicious cryptocurrency miners.
- Although Log4j has been in the wild for several months, CTIR expects attackers will consistently include it in their tactics going forward.

HOW ARE OUR CUSTOMERS PROTECTED?

- Cisco Talos has released myriad coverage for the Log4j vulnerability discovered in December 2021, which continues to be a top infection vector. Users can download the latest SNORT® rules from Snort.org and read the Talos blog for a complete list of Cisco Secure product coverage.
- Cisco Secure Firewall and SNORT® rules protect against many of the ransomware families included in this report, including Conti and Cerber.
- 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 Email and Cisco Secure Malware Analytics protect users from targeted phishing emails and business email compromise, which adversaries commonly used this quarter.