# Incident Response threat summary for April - June 2021

## RANSOMWARE RETURNS AS THE DOMINANT CYBER THREAT

## THE TAKEAWAY

Cisco Talos Incident Response (CTIR) saw more engagements involving ransomware than any other threat during the second quarter of 2021. Ransomware made up 46 percent of all CTIR engagements this quarter. There were very few observations of commodity trojan use this quarter, which is remarkable considering that, in the past, they had been associated with 70 percent of ransomware attacks CTIR dealt with.

## TOP THREATS

- Ransomware was the clear top threat this quarter, comprising nearly 46 percent of all threats and more than tripling the next most common threat which was exploitation of Microsoft Exchange servers.
- There were also some interesting "blasts from the past" including several attacks involving trojanized USB drives, including one that dropped the Sality malware.
- Although ransomware was the top threat, there were very few observations of commodity trojan use this quarter.
- Ransomware actors continued to use commercial tools such as Cobalt Strike, open-source tools such as Rubeus, and tools native on the victim's machine, like PowerShell.

## OTHER LESSONS

- Verticals targeted in Q2 2021 include transportation, utilities, health care, government, telecoms, technology, machinery, chemical distribution, manufacturing, education, real estate, and agriculture.
- Health care was targeted the most out of all verticals for the third quarter in a row, with government being the second most-targeted.
- While phishing as an infection vector remained low this quarter, we observed at least two business email compromise (BEC) engagements for the coming quarter.
- Targeted countries included Australia, Canada, China, Germany, United States, Japan and Philippines, with the top targeted country being the United States.

## HOW ARE OUR CUSTOMERS PROTECTED?

- Using multi-factor authentication, such as Cisco Duo, will help prevent adversaries from accessing users' accounts and spreading malware deeper into networks. CTIR frequently observes ransomware incidents that could have been prevented if MFA had been enabled on critical services.
- Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of any BEC campaigns. You can try Secure Email for free here.
- 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 Endpoint is ideally suited to prevent the execution of ransomware and other malware families. Try Secure Endpoint for free here.