CISCO TALOS

# Incident Response threat summary for April - June 2024

## MFA implementation continues to be top hurdle for targets of attacks

### *The takeaway*

Vulnerable or misconfigured systems, and the lack of proper multi-factor authentication, were the main security weaknesses in Cisco Talos Incident Response (Talos IR) engagements this quarter. Together, these two factors were observed in nearly 100 percent of all engagements. Eighty percent of targets in Talos IR ransomware engagements this quarter lacked proper MFA implementation on critical systems, such as VPNs. The lack or improper implementation of MFA continues to be a talking point in 2024 as attackers seek ways to bypass this login method or are looking for networks that do not have MFA at all.

### *Top threats*

- Business email compromise (BEC) and ransomware were tied for the top observed threats this quarter, together accounting for 60 percent of engagements.
  - Although there was a decrease in BEC engagements from the last quarter, it was still a major threat for the second quarter in a row.
- There was a slight increase in network device targeting this quarter, accounting for 24 percent of engagements.
- For the third quarter in a row, the most observed means of gaining initial access was the use of compromised credentials on valid accounts.

### *Other lessons*

- Technology was the most targeted vertical this quarter, accounting for 24 percent of engagements, which is almost a 30 percent increase from the previous quarter.
- The international law enforcement effort to disrupt several major botnets known as “Operation Endgame” seemed to have, at least temporarily, halted botnet and loader malware. Talos will continue to monitor some of the botnets said to have been disrupted, such as IcedID and Pikabot.
- PowerShell was the top observed execution technique observed this quarter, accounting for 41 percent of engagements this quarter, a 33 percent increase from the previous quarter.

### *How are our customers protected?*

- The lack of MFA remains one of the biggest impediments for enterprise security. All organizations should implement some form of MFA, such as Cisco Duo.
  - The implementation of MFA and a single sign-on system can ensure only trusted parties are accessing corporate email accounts to prevent the spread of BEC.
- Endpoint detection and response solutions like Cisco Secure Endpoint can detect malicious activity on organizations’ networks and machines.
  - Attackers frequently tried to bypass MFA on EDR solutions to disable their alerting mechanisms.
- Snort and ClamAV signatures can block many well-known ransomware families distributed this quarter, such as Black Basta and BlackSuit.