CISCO TALOS

# Incident Response threat summary for Jan. – March 2024

## BEC spikes, makes up nearly half of all Talos IR engagements in Q1

### *The takeaway*

For the first time in several quarters, business email compromise (BEC) was the most common threat in Cisco Talos Incident Response (Talos IR) engagements during the first quarter of 2024. BEC made up 46 percent of all engagements in Q1, a significant spike from Q4 2023. Ransomware, which was the top-observed threat in the last quarter of 2023, decreased by 11 percent. BEC is a tactic adversaries use to disguise themselves as legitimate members of a business and send phishing emails to other employees or third parties, often pointing to a malicious payload or engineering a scheme to steal money.

### *Top threats*

- Talos IR also observed a variety of threats in engagements, including data theft extortion, brute-force activity targeting VPNs, and the previously seen commodity loader Gootloader.
- Talos IR responded to new variants of Phobos and Akira ransomware for the first time this quarter as well as the previously seen LockBit and Black Basta ransomware operations.
    - A recent Talos IR engagement suggests that Akira has returned to using encryption as an additional extortion method, now deploying a multipronged attack strategy to target Windows and Linux machines.
- Security researchers discovered an MFA bypassing phishing kit called “Tycoon 2FA” that has since become one of the most widespread phishing kits. However, this has yet to appear in any Talos IR engagements.

### *Other lessons*

- Manufacturing was the most targeted vertical, accounting for 21 percent of the total number of incident response engagements, closely followed by education.
- The most observed means of gaining initial access was the use of compromised credentials on valid accounts, which accounted for 29 percent of engagements, a 75 percent increase from the previous quarter.
- The use of email hiding inbox rules was the top observed defense evasion technique, accounting for 21 percent of engagements this quarter, which was likely due to an increase in BEC and phishing within engagements.

### *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 Akira.