REPORTING CYBER INCIDENTS AND SHARING INDICATORS OF COMPROMISE

Issued: December 2023

Pub. No 3526-0124

U.S. Customs and Border Protection (CBP) is committed to partnering with trade entities with data connections to CBP to identify and disrupt future cyberattacks through the collection of cyberattack Indicators of Compromise. This guidance applies to companies that transmit data to CBP's cargo processing system, the Automated Commercial Environment (ACE) directly, or indirectly using a service provider. It also applies to accessing any web-based applications, such as ACE or CTPAT portals. This document provides a systematic and repeatable process for reporting the right information in the event of an active cyberattack on private industry.

Section 1: IOC Overview and Benefits

What is an IOC?

An Indicator of Compromise (IOC) is forensic evidence on a computer (host) or network that indicates the security of the network has been breached. IOCs act as flags that cybersecurity uses to detect unusual activity that is evidence of or can lead to a future attack. They also act as clues that may indicate actor intent and attribution and can help provide correlation of possible future attacks.

Benefits of reporting IOCs for Trade Industry

- ✓ IOCs can help with understanding how bad actors were able to gain access to a trade member's IT systems and they can provide insight on how to best address the identified weaknesses and fortify cybersecurity efforts.
- ✓ Consistent and comprehensive IOC reporting lets CBP aggregate and share critical cybersecurity best-practices which benefits every player at every step in our supply chains.

Benefits of reporting IOCs for CBP

- ✓ IOCs provide CBP with the data on the latest criminal cyber-intrusion methods and trends on what methods and/or targeted systems have the highest success rate.
- ✓ CBP can utilize IOC data to continuously bolster the identification of legitimate cyber-threats and notify the potentially impacted parties before an attack is successful.

Section 2: Common IOCs and Suspicious Activities

Unusual inbound or outbound network traffic	If inbound or outbound traffic patterns are unusual, this can be indicative of a potential attack.
Anomalies in privileged user account activity	If user account anomalies are identified, this could indicate a user trying to escalate privileges of a particular account or using the account to access others with more privileges.
Geographical irregularities	If network activity occurs outside of regular geographic locations, this can be evidence of a cyber threat actor in another country trying to penetrate the system.
Other login red flags	If an existing user - or an account that should not exist - has multiple login attempts, this may indicate an attempt to penetrate the system by a threat actor.
Increase in database read volume	If an attacker tries to extract your data, their efforts may result in a swell in read volume.
HTML response sizes (web/Internet)	If HTML data results are usually small, but you notice a far larger response size, it may indicate that data has been extracted.
Multiple requests for same file	If multiple requests to access the same file are detected, this may indicate threat actors are trying to steal files.
Mismatched port-application traffic	If an unusual port is being used, this can indicate an attacker attempting to penetrate the network through the application.

Investigative Resources

- System logs (including event logs)
- Operating System files
- Memory information
- Preliminary Reports (Authorized 3rd Party Observations)
- Desktop, laptop, mobile device (if requested)
- Network traffic captures

Common Suspicious Activities

- Erroneous sender email
- Suspicious external emails
- New unknown contacts
- Strange/Unknown weblinks
- Poor grammar or punctuation
- Follow-up with phone call on strange email requests
- Suspicious attachments
- Domain, CDIR information, IP range data

Section 3: Communication Best Practices

1) **Immediately notify** CBP's Office of Information Technology Security Operations Center (SOC) in the event of a cyberattack.
2) **Report** the most up-to-date IOCs and the relevant data of a successful cyberattack.
3) **Coordinate** with CBP and agency officials on preventing future attacks.
4) **Communicate** with CBP throughout the remediation of a cyberattack.

CBP Security Operations Center

703-921-6507

cbpsoc@cbp.dhs.gov