# Cyber Threat Intelligence (CTI) Submission Form: Malicious Traffic

## Attack Summary

Event Date: Click or tap to enter a date.

Source IP: Click or tap here to enter text.

Source Port: Click or tap here to enter text.

Source ISP: Click or tap here to enter text.

Source Location: Click or tap here to enter text.

Source Machine Type:

☐ Server ☐ Workstation ☐ Mobile Device ☐ Other: Click or tap here to enter text.

Source OS: Click or tap here to enter text.

Destination IP: Click or tap here to enter text.

Destination Port: Click or tap here to enter text.

Destination ISP: Click or tap here to enter text.

Destination Location: Click or tap here to enter text.

Destination Machine Type:

☐ Server ☐ Workstation ☐ Mobile Device ☐ Other: Click or tap here to enter text.

Destination OS: Click or tap here to enter text.

## Analysis

What attack was attempted with this traffic?

☐ SQL Injection (SQLi) ☐ Cross Site Scripting (XSS) ☐ Remote Code Execution (RCE)
☐ Port Scanning ☐ Denial of Service (DoS) ☐ Distributed Denial of Service (DDoS)
☐ Web Crawling ☐ Intrusion Attempt ☐ Botnet Activity
☐ Phishing Host ☐ Malware Activity ☐ Other: Click or tap here to enter text.

What led you or your organization to discover this activity? Click or tap here to enter text.

## Reporting

**Indicators of Compromise (IOC) or Indicators of Attack (IOA):**

*List all indicators and describe malicious behavior associated.*

Domain(s): Click or tap here to enter text.

IP(s): Click or tap here to enter text.

URL(s): Click or tap here to enter text.

Filename(s): Click or tap here to enter text.

Hash Value(s): Click or tap here to enter text.

Other: Click or tap here to enter text.

**Non-Malicious (Legitimate Application Malicious Execution [LAME]) Observables**

*List all indicators and describe malicious behavior associated.*

Domain(s): Click or tap here to enter text.

IP(s): Click or tap here to enter text.

URL(s): Click or tap here to enter text.

Filename(s): Click or tap here to enter text.

Hash Value(s): Click or tap here to enter text.

Other: Click or tap here to enter text.

## Attribution

The above information is ok to be share with:

☐ Members without attribution ☐ Members with attribution ☐ The public without attribution

☐ The public with attribution ☐ Do not share

The above information is being shared with the following TLP classification:

☐ RED ☐ AMBER+STRICT ☐ AMBER ☐ GREEN ☐ CLEAR

For more information about Traffic Light Protocol (TLP) definitions and usage: <https://www.cisa.gov/tlp>

## Questions/Comments/Additional Information

Click or tap here to enter text.

## Incident Reporting

In the case of a cybersecurity incident related to information found in this threat bulletin, Md. Code, Public Safety Article § 14-104.1 (c)(2) and Md. Code, State Finance & Procurement Article § 3.5- 406(b)(2)) mandate that you report this via the [Maryland Incident Reporting System](https://doitmaryland.service-now.com/cybersecurityincident/). It is also recommended that you submit any shareable cyber threat intelligence to the MD-ISAC via the MD-ISAC Threat Intelligence Platform (TIP).