IoC

In cybersecurity, IoC stands for Indicators of Compromise. These are pieces of forensic data that identify potentially malicious activity on a network or system. IoCs are used to detect, respond to, and remediate cyber attacks. Here are the main types of IoCs, along with examples for each:

1. Network IoCs

These indicators relate to network traffic, protocols, and communication patterns.

Example: A suspicious IP address (e.g., 185.143.223.122) that is known to be associated with a malicious command and control (C2) server.

2. Host IoCs

These indicators are related to system files, processes, and registry entries
Example: A malicious executable file (e.g., "malware.exe") that is detected in a system's temporary folder

3. Email IoCs

These indicators are related to email communications, such as sender addresses, subject lines, and attachments.

Example: A hishing email with a suspicious sender address (e.g., "support@microsoft-security.com") and a malicious attachment (e.g., "update.exe").

4. Endpoint IoCs

These indicators are related to endpoint devices, such as laptops, desktops, and mobile devices.

Example: A suspicious process (e.g., "svchost.exe") running on an endpoint device, which is known to be a common malware masquerade.

5. Behavioral IoCs

These indicators are related to the behavior of malware or attackers, such as command and control (C2) communication patterns.

Example: A system exhibiting suspicious DNS queries (e.g., frequent queries to a specific domain) that may indicate a malware infection.

6. Anomaly IoCs
These indicators are related to unusual system or network behavior that may indicate a potential security incident.

Example: A sudden spike in system CPU usage or network traffic that may indicate a crypto jacking attack.

7. YARA IoCs

YARA (Yet Another Recursive Acronym) is a rule-based language used to identify malware and other threats. YARA IoCs are used to detect specific patterns in files, such as malware signatures.

Example: A YARA rule that detects a specific malware family (e.g., "Trojan:Win32/Malware.A") based on its binary pattern.

These IoCs can be used by security teams to detect, respond to, and prevent cyber attacks. By monitoring these indicators, organizations can improve their incident response and threat hunting capabilities.

TTPs

In cybersecurity, TTPs stand for Tactics, Techniques, and Procedures. They refer to the methods and strategies used by attackers to compromise systems, networks, and organizations. TTPs are used to understand the behavior of attackers, anticipate their next moves, and develop effective defenses.

Here's a breakdown of each component:

Tactics:

1. The high-level goals and objectives of an attacker, such as data exfiltration, lateral movement, or disruption of services.
2. Examples: Data theft, ransomware, espionage, or sabotage.

Techniques:

1. The specific methods used to achieve the attacker's goals, such as exploiting vulnerabilities, using social engineering, or leveraging malware.
2. Examples: Phishing, SQL injection, cross-site scripting (XSS), or drive-by downloads.

Procedures:

1. The detailed, step-by-step actions taken by an attacker to execute their techniques, such as creating a malicious payload, setting up a command and control (C2) server, or using encryption to evade detection.
2. Examples: Creating a phishing email campaign, setting up a malware distribution network, or using a specific exploit kit.

By recognizing the TTPs used by attackers, organizations can better prepare themselves to defend against future attacks.

Cyberattack Indicator Sources

The following are RSS feeds that post cyber attack indicators:

1. **US-CERT National Cyber Awareness System**
2. **AlienVault Open Threat Exchange (OTX)**
3. **Talos Intelligence**
4. **Malware Traffic Analysis**
5. **SANS Internet Storm Center**
6. **Krebs on Security**
7. **Threatpost**
8. **The Hacker News**
9. **Bleeping Computer**
10. **ZDNet Zero Day**

The following sources are known for providing the most reliable cyber attack indicators. We will use these sources to acquire the indicators with which we will populate our knowledge graphs:

1. **US-CERT National Cyber Awareness System Access: https://www.cisa.gov/uscert/ncas/alerts.xml Details: Highly reliable, government-sourced information. Provides alerts about current security issues, vulnerabilities, and exploits. Updates are less frequent but highly vetted.**
2. **AlienVault Open Threat Exchange (OTX) Access: Requires free account creation at https://otx.alienvault.com/ Details: Community-driven threat intelligence platform. Offers a wide range of indicators including IP addresses, domains, and file hashes. Updates frequently with real-time threat data.**
3. **Talos Intelligence Access: https://blog.talosintelligence.com/feeds/posts/default Details: Cisco's threat intelligence team. Provides in-depth analysis of threats, vulnerabilities, and malware. Known for high-quality, well-researched content. Updates several times a week.**
4. **SANS Internet Storm Center Access: https://isc.sans.edu/rssfeed.xml Details: Offers daily summaries of significant cyber threats and analyses. Highly respected**

in the cybersecurity community. Provides a mix of technical details and broader threat landscape information.

5. **Malware Traffic Analysis Access: http://www.malware-traffic-analysis.net/blog-entries.rss Details: Focuses specifically on network traffic related to malware infections. Provides packet capture (PCAP) files and detailed analyses. Updates frequently with recent malware campaigns.**

These sources are known for their reliability and the quality of their indicators. They offer a mix of government, commercial, and community-sourced intelligence, which can provide a well-rounded view of current cyber threats.