Cybersecurity Automation and Threat Intelligence Sharing Best Practices

Feb. 2021

JOHNS HOPKINS APPLIED PHYSICS LABORATORY

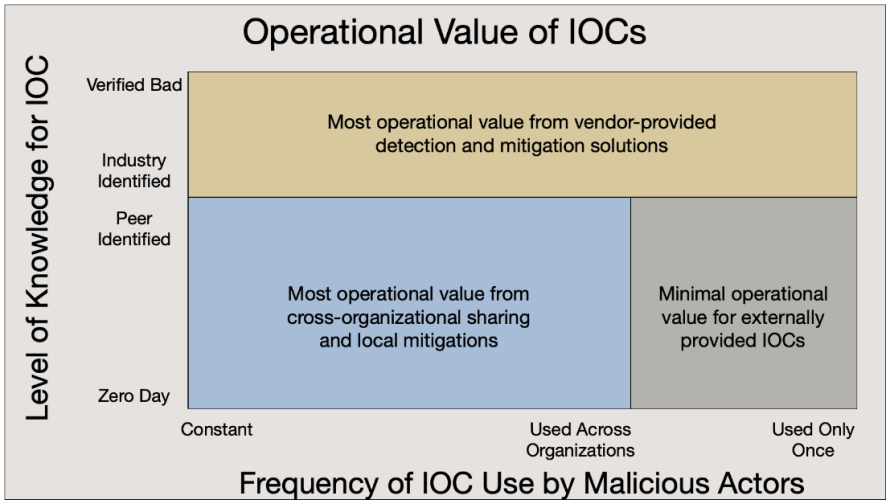
DEPLOYING INDICATORS OF COMPROMISE (IOCs) FOR NETWORK DEFENSE

Operational Value of IOCs

Kimberly K. Watson

Many organizations subscribe to IOC feeds. While one of the main purposes is to support network defense, many Security Operations Centers (SOCs) do not routinely use these feeds in their operations. Why? It has been our experience, having performed IOC automation pilots over the last four years, that it is because these feeds are too voluminous and too noisy, requiring significant resources to ingest these feeds into the SOC environment, enrich, investigate, determine the appropriate response, and then respond. There are just too many IOCs being shared with little to no context surrounding them, and the technical resources required to analyze their relevance or ability to be acted upon are already at capacity dealing with internal threat information (i.e., alerts).

Most organizations prioritize processing internal information over processing and acting on external IOC feeds. There is a significant debate in the cybersecurity community as to what operational value some IOCs provide to organizations, since threat actors can and do change IOCs routinely as a way to avoid detection. During our pilots, JHU/APL has discovered that the right question is not *if* IOCs are operationally valuable, but *when*. A SOC gains the most operational value from expending resources to ingest and use IOC feeds when the IOCs are being reused for attacks against multiple organizations and they are shared before industry considers them malicious.



Unfortunately, quickly sharing IOCs that have not been verified may just flood the SOC, making any operational use impractical. Therefore, there is a strong business case for investing resources in developing automated processes to ingest, triage, and respond to IOCs that peers have identified in operations and share before external services and providers determine their maliciousness. This is particularly true for IOCs that are associated with earlier stages of the malware lifecycle (e.g., exploitation or phishing infrastructure).

Malware Lifecycle

There is a lifecycle to malware, and only certain types of IOCs can be detected at different operational stages (e.g., exploitation, command and control) by different types of technologies. If one wants to share IOCs to most limit or prevent the compromise of members from malware infections identified by other members, then one needs to share IOCs that are associated with earlier stages. Unfortunately, the most common IOCs detected and shared by organizations are actually associated with the later stages. This is because it is easier to determine if the IOC is associated with malicious activity at this point. Working backwards from a detected incident to the initiating event is not easy and many organizations do not collect or maintain the information necessary to do this type of investigation. Late stage IOCs (i.e., command and control) are the easiest for the adversary to modify, making the window of "value" of sharing these IOCs small.

Sharing IOCs associated with earlier stages (i.e., exploitation) have the most potential to prevent or limit malware infection of others. Sharing IOCs associated with later stages assists in detection of compromised assets and possibly mitigating the impact of a compromise. In general, the later stage IOCs, which are often associated with Command and Control (C2) infrastructures, are changed frequently and as a matter of course for most attacks or campaigns.

One important thing to note is that unlike C2 IOCs, the exploitation IOCs may never be identified by reputation services as being associated with malicious activity. This is because most organizations are not able to determine how or when an asset was compromised, only that malware is present.

IOC Sources

When subscribing to an IOC feed for use in network defense operations, it is important to understand the sources used by the feed provider. If they are sources that identify IOCs later in the malware lifecycle or publish the information after the threat has been mitigated by industry, there is little value for SOC personnel to spend time investigating and responding. Examples of these types of sources include but are not limited to: other commercially available feeds, those derived from incident response or forensic reporting, or IOCs based on in-depth threat analysis. IOCs from these sources are valuable for more strategic threat analysis and investment decisions, threat hunting and alert validation, and compromise detection. In general, they are less valuable for SOCs to use for investigation and response.

Industry's Role

It is important to note that once external parties are aware of an IOC and have associated it with malware or malicious activity, then industry will often mitigate the threat on an organization's behalf. Once an IOC is marked as known bad in reputation services, in black lists for commercial products and services, or shared broadly by CTI providers, there is little value in the SOC implementing blocks or queries to identify compromised assets. Other tools in the organization now know to look for these IOCs and take appropriate action, and often the threat actor takes down or stops using the infrastructure that has been detected.

Some security vendors do not provide timely IOC updates as part of their default services, and can charge a premium for this service. In these cases, it may be operationally valuable for the SOC to continue to act on IOCs after industry labels the indicators as known bad but before they are included in vendor provided security services.

Maximizing Operational Value

Let industry do its job, and only use limited SOC resources to deal with the IOCs that have not yet been identified by products and services in your environment. Subscribe to IOC feeds derived from detection systems that are shared quickly with some sort of reasonableness filter applied. Then use automation to triage, prioritize, and respond to that subset of IOCs. Consider aging off IOC blocks or mitigations put in place by the SOC, allowing industry to more appropriately apply mitigations at scale. The goal is to use IOC feeds to protect the organization while the threat is active and before existing products and services implement mitigations.

Acknowledgement

This material is based upon work supported by the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency under Grant Award Number DHS-19-CISA-128-SLT-001 (State, Local, Tribal, and Territorial Indicators of Compromise Automation Pilot).

Disclaimer

The views and conclusions contained in this document are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency.

✉ Kimberly Watson
Kimberly.Watson@jhuapl.edu