Analyze indicators of compromise with investigative tools

So far, you've learned about the different types of detection methods that can be used to detect security incidents. This reading explores how investigative tools can be used during investigations to analyze suspicious **indicators of compromise (IoCs)** and build context around alerts. Remember, an IoC is observable evidence that suggests signs of a potential security incident.

Adding context to investigations

You've learned about the Pyramid of Pain which describes the relationship between indicators of compromise and the level of difficulty that malicious actors experience when indicators of compromise are blocked by security teams. You also learned about different types of IoCs, but as you know, not all IoCs are equal. Malicious actors can manage to evade detection and continue compromising systems despite having their IoC-related activity blocked or limited.

For example, identifying and blocking a single IP address associated with malicious activity does not provide a broader insight on an attack, nor does it stop a malicious actor from continuing their activity. Focusing on a single piece of evidence is like fixating on a single section of a painting: You miss out on the bigger picture.

Une femme observe une section d'un grand tableau.

Security analysts need a way to expand the use of IoCs so that they can add context to alerts. **Threat intelligence** is evidence-based threat information that provides context about existing or emerging threats. By accessing additional information related to IoCs, security analysts can expand their viewpoint to observe the bigger picture and construct a narrative that helps inform their response actions.

Une femme regarde le grand tableau d'un éléphant dans son intégralité.

By adding context to an IoC—for instance, identifying other artifacts related to the suspicious IP address, such as suspicious network communications or unusual processes—security teams can start to develop a detailed picture of a security incident. This context can help security teams

detect security incidents faster and take a more informed approach in their response.

The power of crowdsourcing

Crowdsourcing is the practice of gathering information using public input and collaboration. Threat intelligence platforms use crowdsourcing to collect information from the global cybersecurity community. Traditionally, an organization's response to incidents was performed in isolation. A security team would receive and analyze an alert, and then work to remediate it without additional insights on how to approach it. Without crowdsourcing, attackers can perform the same attacks against multiple organizations.

> Un attaquant réussit à attaquer cinq entreprises différentes.

With crowdsourcing, organizations harness the knowledge of millions of other cybersecurity professionals, including cybersecurity product vendors, government agencies, cloud providers, and more. Crowdsourcing allows people and organizations from the global cybersecurity community to openly share and access a collection of threat intelligence data, which helps to continuously improve detection technologies and methodologies.

Examples of information-sharing organizations include Information Sharing and Analysis Centers (ISACs), which focus on collecting and sharing sector-specific threat intelligence to companies within specific industries like energy, healthcare, and others. **Open-source intelligence (OSINT)** is the collection and analysis of information from publicly available sources to generate usable intelligence. OSINT can also be used as a method to gather information related to threat actors, threats, vulnerabilities, and more.

This threat intelligence data is used to improve the detection methods and techniques of security products, like detection tools or anti-virus software. For example, attackers often perform the same attacks on multiple targets with the hope that one of them will be successful. Once an organization detects an attack, they can immediately publish the attack details, such as malicious files, IP addresses, or URLs, to tools like VirusTotal. This threat intelligence can then help other organizations defend against the same attack.

> Un attaquant est empêché d'attaquer des entreprises grâce aux renseignements crowdsourcé

VirusTotal

VirusTotal

is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content. VirusTotal also offers additional services and tools for enterprise use. This reading focuses on the VirusTotal website, which is available for free and non-commercial use.

It can be used to analyze suspicious files, IP addresses, domains, and URLs to detect cybersecurity threats such as malware. Users can submit and check artifacts, like file hashes or IP addresses, to get VirusTotal reports, which provide additional information on whether an IoC is considered malicious or not, how that IoC is connected or related to other IoCs in the dataset, and more.



Une capture d'écran de la page d'accueil du site VirusTotal.

Here is a breakdown of the reports summary:



Une capture d'écran d'un récapitulatif des rapports VirusTotal.

1. **Detection**: The Detection tab provides a list of third-party security vendors and their detection verdicts on an IoC. For example, vendors can list their detection verdict as malicious, suspicious, unsafe, and more.
2. **Details**: The Details tab provides additional information extracted from a static analysis of the IoC. Information such as different hashes, file types, file sizes, headers, creation time, and first and last submission information can all be found in this tab.
3. **Relations**: The Relations tab provides related IoCs that are somehow connected to an artifact, such as contacted URLs, domains, IP addresses, and dropped files if the artifact is an executable.
4. **Behavior**: The Behavior tab contains information related to the observed activity and behaviors of an artifact after executing it in a controlled or sandboxed environment. This information includes tactics and techniques detected, network communications, registry and file systems actions, processes, and more.
5. **Community:** The Community tab is where members of the VirusTotal community, such as security professionals or researchers, can leave comments and insights about the IoC.
6. **Vendors' ratio and community score**: The score displayed at the top of the report is the vendors' ratio. The vendors' ratio shows how many security vendors have flagged the IoC as malicious overall. Below this score, there is also the community score, based on the inputs of the VirusTotal community. The more detections a file has and the higher its community score is, the more likely that the file is malicious.

Note: Data uploaded to VirusTotal will be publicly shared with the entire VirusTotal community. Be careful of what you submit, and make sure you do not upload personal information.

Other tools

There are other investigative tools that can be used to analyze IoCs. These tools can also share the data that's uploaded to them to the security community.

Jotti malware scan

Jotti's malware scan

is a free service that lets you scan suspicious files with several antivirus programs. There are some limitations to the number of files that you can submit.

Urlscan.io

Urlscan.io

is a free service that scans and analyzes URLs and provides a detailed report summarizing the URL information.

CAPE Sandbox

CAPE Sandbox

is an open source service used to automate the analysis of suspicious files. Using an isolated environment, malicious files such as malware are analyzed and a comprehensive report outlines the malware behavior.

MalwareBazaar

MalwareBazaar

is a free repository for malware samples. Malware samples are a great source of threat intelligence that can be used for research purposes.

Key takeaways

As a security analyst, you'll analyze IoCs. It's important to understand how adding context to investigations can help improve detection capabilities and make informed and effective decisions.

Revision #1
Created 2023-09-22 11:22:35 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai