Malware Information Sharing Platform (MISP)

The Malware Information Sharing Platform (MISP) is an open source software solution created by a community of volunteers for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. MISP is designed by and for incident analysts, security and ICT professionals or malware reversers to support their day-to-day operations to share structured information efficiently.

The objective of MISP is to foster the sharing of structured information within the security and threat intelligence communities. MISP provides functionalities to support the sharing and consumption of information from tools such as Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS), and log analysis tools such as SIEMs.

It's important to mention that other similar platforms do exist, however we will be using MISP due to the functionality and availability as a result of it being a free and open-sourced project.

WHAT DOES MISP DO?

- Facilitate the storage of technical and non-technical information about seen malware and attacks
- Create automatically relations between malware and their attributes
- Store data in a structured format (allowing automated use of the database to feed detection systems or forensic tools)
- Generate rules for Network Intrusion Detection System (NIDS) that can be imported on IDS systems (e.g. IP addresses, domain names, hashes of malicious files, pattern in memory)
- Share malware and threat attributes with other parties and trust-groups
- Improve malware detection and reversing to promote information exchange among organizations (e.g. avoiding duplicate works)
- Create a platform of trust – trusted information from trusted partners
- Store locally all information from other instances (ensuring confidentiality on queries)

WHAT DOES MISP WORK?

Malware Information Sharing Platform is accessible from different interfaces like a web interface (for analysts or incident handlers) or via a ReST API (for systems pushing and pulling IOCs). The inherent goal of MISP is to be a robust platform that ensures a smooth operation from revealing, maturing and exploiting the threat information.

There are 4 options regarding distributing events and their respective attributes:

- Your organization only (private)
- This community only
- Connected communities
- All communities (public)

There is also a set of sharing groups accessible to various members per sector (such as the Financial sector).

MISP, Malware Information Sharing Platform and Threat Sharing, core functionalities are:

- An efficient IOC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.
- Automatic correlation finding relationships between attributes and indicators from malware, attack campaigns or analysis. The correlation engine includes a correlation between attributes and more advanced correlations like Fuzzy hashing correlation (e.g. ssdeep) or CIDR block matching. Correlation can also be enabled or event disabled per attribute.
- Built-in sharing functionality to ease data sharing using different models of distributions. MISP can automatically synchronize events and attributes among different MISP instances. Advanced filtering functionalities can be used to meet each organization's sharing policy including a flexible sharing group capacity and an attribute level distribution mechanisms.
- An intuitive user-interface for end-users to create, update and collaborate on events and attributes/indicators. A graphical interface to navigate seamlessly between events and their correlations. An event graph functionality to create and view relationships between objects and attributes. Advanced filtering functionalities and warning lists to help the analysts to contribute events and attributes and limit the risk of false-positives.
- Storing data in a structured format (allowing automated use of the database for various purposes) with the extensive support of cybersecurity indicators along with fraud indicators as in the financial sector.
- Export: generating IDS, OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools), Cache format (used for forensic tools), STIX (XML and JSON) 1 and 2, NIDS export (Suricata, Snort and Bro/Zeek) or RPZ zone. Many other formats can be easily added via the misp-modules.
- Import: bulk-import, batch-import, import from OpenIOC, GFI sandbox, ThreatConnect CSV, MISP standard format or STIX 1.1/2.0. Many other formats easily added via the misp-modules.
- Flexible free text import tool to ease the integration of unstructured reports into MISP.
- STIX support: import and export data in the STIX version 1 and version 2 format.

CONCLUSION

In the next lesson, we're going to teach you how to set up MISP yourself, so you can play around with the features, and get used to deploying MISP for internal threat intelligence purposes. As you now know, this open-source platform is great for any organization. It can help with tactical threat intelligence tasks, as well as cyber defense by feeding automated defenses with indicators of compromise such as intrusion detection and prevention systems, firewalls, and custom tools.

Previous Topic
Mark Complete
Next Topic
Back to Lesson