Information Sharing and Cyber Security - The Benefits of the Malware Information Sharing Platform (MISP)

CIRCL Computer Incident Response Center Luxembourg

It has been emphasized in various international reports[1] that information sharing on cyber security threats has become highly critical, reinforcing the need for more cooperation across borders, individuals and organizations. Information sharing is a key factor to improve security, but a consistent approach is required. MISP is being used and constantly improved to support such a methodical way.

Objectives

All information sharing initiatives have the common goal to improve cyber incident/attack prevention, detection, prediction, response and recovering. Sharing of data can be performed to reach different goals, including:

- Better ICT innovations and incident handling methodologies between sharing partners.
- Improving the security of network and system monitoring tools.

An important element is that cyber defense encompasses not only technology but more specifically focuses on people and processes.

Following this global and urgent need, CIRCL has developed MISP[2] in order to facilitate the exchange of Indicators of Compromise (IOC[3]) about targeted malware and attacks within a community of trusted members.

Benefits of Sharing

During MISP enrollment, involvement in information sharing is gradually increasing depending on the maturity of the individual organization. Each of these phases, with their respective benefits, as we identified them, are described below:

Reviewing of Indicators and Threats

- Facilitate the storage of technical and non-technical information about seen malware and attacks.
- Learn from others and the security issues they are facing or detecting.
- Start a specific research regarding current and past events.
- Reflect about current activities and threats (e.g. what are the risks of the current threats against my organization?).
- Improve your own internal processes and tools by evaluating the currently shared threats.
- Use the indicators from the system to protect your infrastructure.
- Collect the information to support your intelligence team.
- Learn the common language and taxonomies used among incident response teams.

[1] e.g. ENISA - Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches https://www.enisa.europa.eu/activities/cert/support/information-sharing/cybersecurity-information-sharing/at_download/fullReport

[2] https://www.circl.lu/services/misp-malware-information-sharing-platform/

[3] IOCs are artifact and/or relevant traces which indicate a computer intrusion or an ongoing cyber security threat.

Inspecting and Contributing Improvements

- The active use of information-sharing helps to find out if someone else or an organisation is already working on the same incident or an incident that follows a similar schema or uses similar tools.
- The contribution and correlation of threats leads to an increased quality of the indicators (i.e. by verification of other people's analyses).
- Automatically create relations between malware and their attributes.
- Contribute to improve malware detection and reverse engineering to promote information exchange among organizations (i.e. avoiding duplicate work).

Sharing your Research Results

- Your information security team is actively engaged in the analysis of security threats.
- Showing your capabilities among the sharing community (i.e. increasing your visibility to attract additional researches on the same topics).
- Ensuring that your indicators can be peer reviewed in the information security community.

Caveats

Information sharing plays a significant role in ICT security. Nevertheless it is not a magical solution but can be seen as a catalyzer for a security team to improve their operational and analysis capabilities. One of the developement goals of MISP is to support analysis roles. Ensuring a smooth and safe sharing platform without encumbering day-to-day services is a clear focus. Another objective is to secure a favorable set of MISP functionalities to share among trusted groups or even delegate the sharing to trusted partners.

Contact

CIRCL is the CERT (Computer Emergency Response Team/Computer Security Incident Response Team) for the private sector, communes and non-governmental entities in Luxembourg. For more information about CIRCL: https://www.circl.lu/

Trusted partners, in Luxembourg and abroad, can contact CIRCL in order to join the MISP information sharing community operated by CIRCL.

CIRCL MISP Threat Sharing

Classification

TLP:WHITE Information may be distributed without restriction, subject to copyright controls - First publication February, 16 2016.