circl.lu
Computer Incident Response Center
LUXEMBOURG

MISP - Malware Information Sharing Platform & Threat Sharing for the financial sector

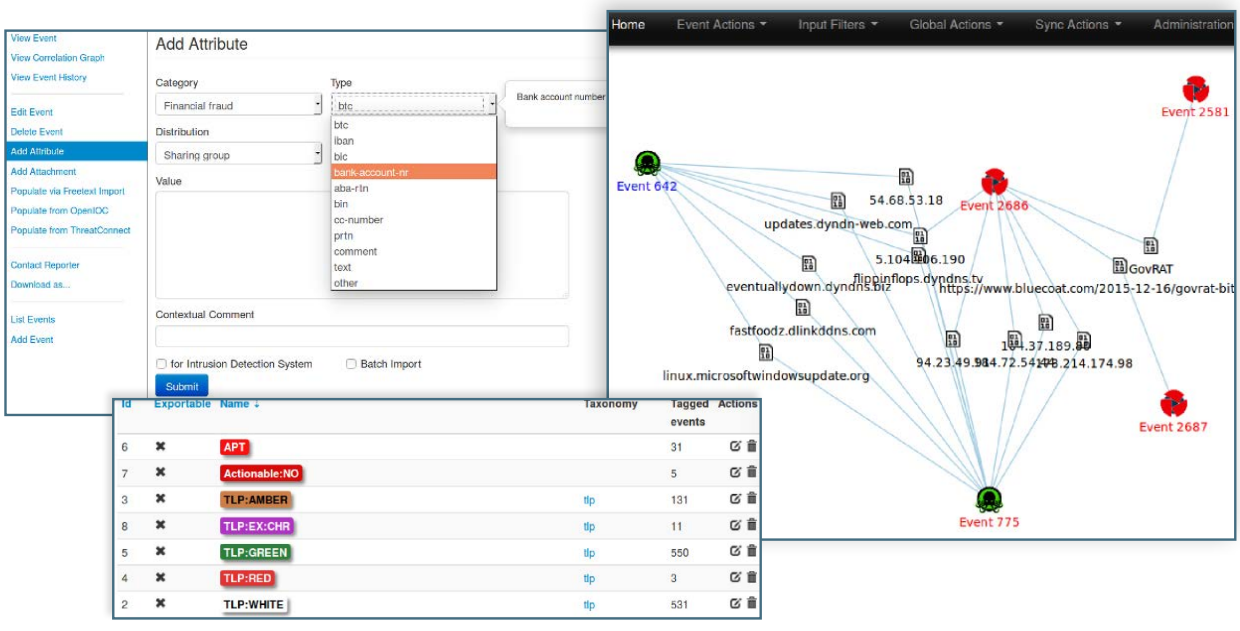
INFORMATION SHARING WITHIN THE FINANCIAL SECTOR

Information security and fraud detection are often transversal activities within banking or financial operators. One financial organization alone cannot perform all upcoming threat analysis and requires additional information shared by others. In that scope, CIRCL co-developed MISP, a threat sharing platform, to support information sharing in the context of cyber security as well as within the context of fraud. Financial services, like any other type of organization with an increased attack surface, need simple ways to share information while being able to ensure **an adequate balance between privacy, confidentiality and the need of sharing to protect customers and users of financial services.**

SUPPORTED FINANCIAL ATTRIBUTES

Attributes can be any indicators, observables or information used to monitor and detect potential frauds. MISP was initially designed for sharing cyber security attributes. Over time, it evolved to support as well financial attributes and especially indicators used by attackers to "cash out". The following financial attributes are supported by default in MISP:

- **BTC** - Bitcoin Address
- **IBAN** - International Bank Account Number
- **BIC** - Business or Bank Identifier Codes
- **Bank-account-nr** - Bank account number without any routing number
- **ABA-RTN** - ABA routing transit number
- **BIN** - Bank Identification Number
- **cc-number** - Credit-Card Number
- **PRTN** - Premium-Rate Telephone Number
- other values including text or specific comment



A user of MISP can combine multiple attributes in events. This allows to share mixed information (including cyber security indicators) about a specific attack or campaign against a specific financial service or operator. MISP verifies the correctness of the information and notifies the user if indicators are not valid.

MISP is built upon a strong and lively community of a variety of specialists. Their feedback constantly leads to improvements of the software and the data model. Hence a responsive adjustment of attribute types can be expected if required.

DELEGATION OF PUBLICATION

Reputation and trust are critical elements in the financial sector. A functionality called *delegation of publication* was introduced in MISP to support these aspects. A MISP user in the financial sector can delegate the publication of an event without revealing the name of their organization. The main intention is to allow users **to still benefit from information sharing without linking their name to specific indicators.** This pseudo-anonymity is achieved by requesting the delegation of publication to one of *your* trusted partners on a MISP platform.

SHARING GROUPS

Starting from MISP 2.4, a flexible scheme of sharing groups has been introduced, which allows financial organizations to create sharing groups among selected organizations. These *adhoc sharing groups* can also be created to support specific sharing on a case-by-case basis (e.g. an attack targeting a specific set of banks). The sharing groups can even be shared among MISP instances dynamically, ensuring a coherent view on all the sharing groups.

JOINING THE MISP COMMUNITY AT CIRCL

If you want to join the MISP community at CIRCL, don't hesitate to contact us:

CIRCL - Computer Incident Response Center Luxembourg
by SECURITYMADEIN.LU
41, avenue de la gare
L-1611 Luxembourg
Grand-Duchy of Luxembourg

(+352) 247 88444
info@circl.lu

www.circl.lu

CIRCL MISP Threat Sharing