Enhancing the Tool SDO with High Value Target

Francesco Chiarini, Founder & Chief Researcher | francesco@highvaluetarget.org

Reviewed by: Vasileios Mavroeidis, Professor of Cybersecurity | vasileim@ifi.uio.no

Problem statement

Abuse use-cases for legitimate software (tools) are not addressed in the STIX 2.1 specification. This prevents defenders from exchanging meaningful information about software abuse, accurately tracking threat actor target selection patterns, and mapping attack flows with data about legitimate software as an adversarial target. Threat-informed leadership and cyber risk personnel are equally unable to consume targeted legitimate software to quantify cyber risk and consequently fail to build precise defensive strategies.

About High Value Target

High Value Targets (HVTs) are applications, their underlying information systems, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to an organization's ability to perform its mission or conduct business. High Value Target is an open concept for the community to use. More information about the High Value Target concept is available at https://highvaluetarget.org/

Proposed solution

Add High Value Target to the STIX Common Objects Repository and consider the concept for inclusion in a future STIX specification release. In particular, the additions include:

- Updated definition of the Tool SDO (4.18)
- Enrichment of an open-vocab (10.16)
- Update definition of the "uses" relationship (4.18.2)

The proposed solution will enable defenders to exchange more precise and meaningful information on software abuse use-cases by leveraging the High Value Target concept. Adoption from the community will be encouraged and promoted by High Value Target via their large private sector network of contacts in various industries.

Solution details

4.18 Tool

Type Name: `tool`

Current definition

Tool types describe the categories of tools that can be used to perform attacks.
The Tool SDO characterizes the properties of these software tools and can be used as a basis for making an assertion about how a Threat Actor uses them during an attack.

Proposed definition

Tool types describe the categories of tools and critical software that can be utilized to conduct attacks by leveraging or abusing functionalities to impair the defender and ultimately cause an impact on an organization's ability to carry out its mission.

10.26 Tool Type Vocabulary

Vocabulary Name: `tool-type-ov`

Current version and comparison with High Value Target attributes

STIX Vocabulary Value	STIX Description	High Value Target Attributes	High Value Target Description
`denial-of-service`	Tools used to perform denial of service attacks or DDoS attacks, such as Low Orbit Ion Cannon (LOIC) and DHCPig.		
`exploitation`	Tools used to exploit software and systems, such as sqlmap and Metasploit.	`tamper-prone`	Tools' functionalities prone to be weaponized by an adversary to support malicious actions.
`information-gathering`	Tools used to enumerate system and network information, e.g., NMAP.	`internal-prospecting`	Tool used to manage systems or networks which can provide an adversary visibility into the management control plane.
`network-capture`	Tools used to capture network traffic, such as Wireshark and Kismet.		
`credential-exploitation`	Tools used to crack password databases or otherwise exploit/discover credentials, either locally or remotely, such as John the Ripper and NCrack.	`stores-secrets`	Tools that can provide an adversary access to stored secrets that can be stolen or abused.

https://highvaluetarget.org/stix

remote-access	Tools used to access machines remotely, such as VNC and Remote Desktop.		
vulnerability-scanning	Tools used to scan systems and networks for vulnerabilities, e.g., Nessus.		
unknown	There is not enough information available to determine the type of tool.		
		stealthiness	Tools used provide an adversary with the ability to bypass detection mechanisms and safeguards such as endpoint security or intrusion detection systems.
		External-exposure	Tools exposed to accessible network zones which provide access for initial compromise, allows pivoting from non-trusted to trusted networks.
		infiltrate-comms	Tools used to allow defenders to communicate (in-band or out-of-band) and can provide the adversary with visibility of defensive tactics.
		blindside-defense	Tools that provide the ability to directly target and impair CSIRT investigative and detective capabilities such as SIEM or SOAR.
		inhibit-restoration	Tools that can permanently damage backup and restore capabilities.
		stores-data	Tools that can provide an adversary access to highly valuable or large amount of data such as databases or storage.
		widespread-presence	Tools that are pervasively implemented in the victim's environment and equip the attacker with means to maximize their presence such as patching or software distribution.

Commented [VM1]: for some that are not straightforward, provide examples

Proposed additions

Vocabulary Value	Description
`Hypervisors-virtualization`	Tools used to virtualize execution of commands or operating systems with direct access and control to underlying hardware, such as VDI or containers.
`Identity-access-management`	Tools used to store secrets that can be stolen or abused, such as corporate directories, PKI etc.
`Security-monitoring`	Tools used to provide the defender the ability to monitor for malicious behaviors, such as SIEM or SOAR tools.
`Backup-storage`	Tools used to create copies and transfer data stored on endpoints or other devices, such as NAS, recovery managers, remote or local storage.
`Endpoint-management`	Tools used for remote endpoint administration, update and configuration such as patches management or asset inventory.
`Endpoint-security`	Tools used to protect the endpoints, contribute to the secure operation of the endpoint or collect information such as anti-malware or EDR.
`Network-management`	Tools used to manage systems or networks which can provide an adversary visibility into the management control plane, such as DNS, network configuration or traffic monitoring systems.
`Network-security`	Tools used to prevent malicious network traffic from entering or leaving a segment or boundary, such as NAC, firewall or NIPS.
`Office-productivity`	Tools used to collaborate, communicate or share unstructured data such as email, file sharing and meeting platforms.
`Crisis-management`	Tools used to allow defenders to communicate (in-band or out-of-band) and can provide adversary with visibility of defensive tactics.
`Business-Data-repository`	Tools used to enable the business to deliver the organization's mission and/or store highly valuable or large amount of data, such as critical business applications or databases.

4.18.2 Relationships

These are the relationships explicitly defined between the Tool object and other STIX Objects.

Current status

Threat actor or malware "uses" tools to achieve adversarial objectives.

Proposed addition

"Abuses" should be added to allow threat actor relationship with tools be more accurate to cover for software abuse uses cases as described in High Value Target. Updated text: "Threat actor or malware "uses" malicious tools or "abuses" legitimate tools to achieve adversarial objectives.

The "uses" relationship is still to be leveraged for these cases. The proposal just aims to update the definition.

Commented [VM2]: Since we already have the "uses" relationship in place, it can be reused.