Reinforce threat intelligence with the MITRE ATT&CK framework.

A key element of threat intelligence is the ability to share threat information and compromise indicators (IOCs). In order to do this effectively, a common structured format, such as STIX, is important. Starting from version 2, the STIX format implements a standard for setting and referencing destruction chains.

This blog covers a way to use this functionality with the MITRE ATT&CK framework, a knowledge base of tactics and techniques based on real-world malicious activities. An example of using STIX indicators developed by Nozomi Networks Labs is also presented to demonstrate how a standardized format can facilitate the sharing of threat information.

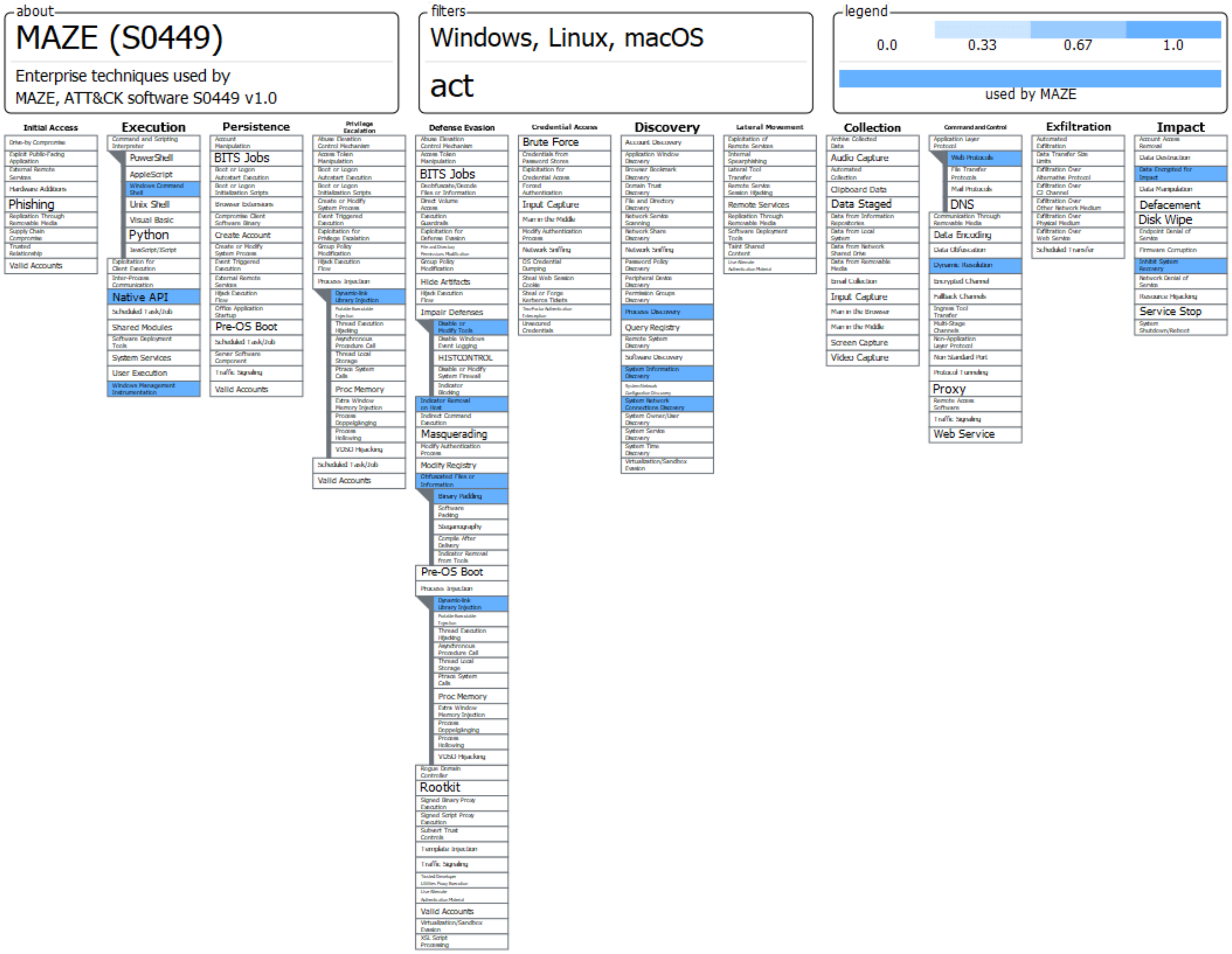


FIG: Enhancing Threat Hunting with MITRE ATT&CK - Check Point Software

Real-World Threat Intelligence is Provided through the ATT&CK Framework:

MITRE ATT&CK is a term that is frequently used to define and categorize how hostile actors execute reconnaissance, initial access, persistence, lateral movement, exfiltration, and a variety of other strategies. One or more distinct strategies are used to characterize malicious events, which are then organized into high-level tactics. ATT&CK methods and approaches are currently separated into three categories: enterprise, mobile, and industrial control systems (You can learn more about using MITRE ATT&CK in this blog). All of the techniques are organized into strategies and can be distinguished by their IDs.

Both blue and red teams benefit from MITRE ATT&CK strategies and approaches. From an offensive standpoint, the framework produces a detailed model of a specific attacker's behavior that may be emulated. Analysts can use MITRE ATT&CK to structure and disseminate threat information from a defensive standpoint. It's also possible to construct analytics to identify patterns in harmful actors' attack methods.

New data source objects reflect diverse information that can be collected by sensors and logs in ATT&CK version 10, which was just released. Each data component describes a data source's distinctive qualities, allowing for the detection of a specific Technique. As usual, this version provides updates and improvements to Enterprise Techniques, Groups, and Software.

The Value of Standardized Formats:

Sharing information allows everyone's cyber threat intelligence to grow. The more information we exchange, the more insights we can get and the faster and more efficiently we can anticipate and respond to assaults. To make contributing and digesting data easier, one crucial prerequisite for exchanging threat intelligence is to use standard formats.

The Structured Threat Information eXpression (STIXTM) language and serialization format are used to represent and exchange cyber threat information in a consistent and efficient manner. As this white paper points out, STIX also allows you to communicate a variety of data, including:

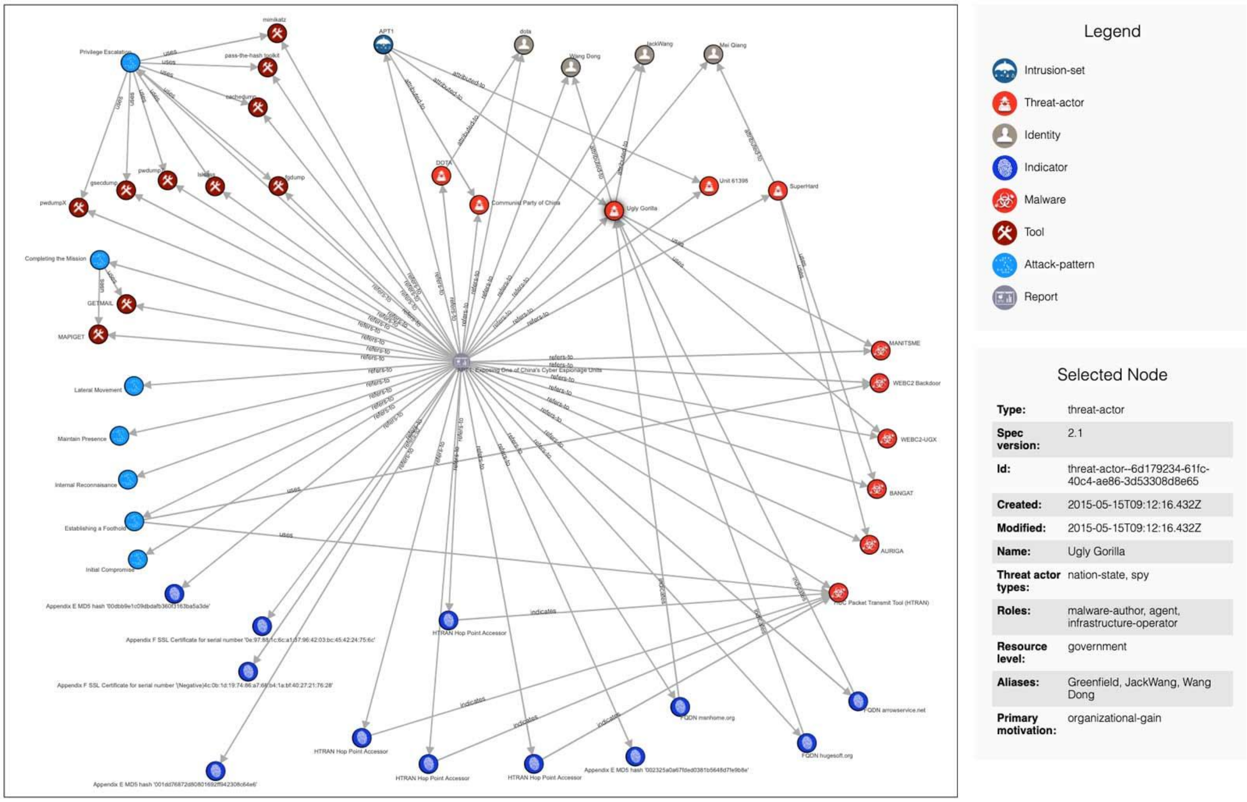
- Observables in cyberspace (e.g., a Registry key is created, network traffic occurs to specific IP addresses, email from a specific address is observed, etc.)
- Indicators
- Incidents
- TTPs (tactics, methods, and procedures) used by adversaries (including attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting, etc.)
- Targets to exploit (e.g., vulnerabilities and weaknesses)
- Action plans (for example, incident response or vulnerability/weakness remediation)
- Campaigns of cyber-attack
- Threat actors in cyberspace

The distinctions between STIX 1 and STIX 2:

The first version of STIX used XML syntax to describe indicators. The switch from the XML to the JSON format, which allows for a more lightweight syntax that is easier to interpret and so favored for development, is one of the most significant differences between version 1 and version 2.

Version 2 includes two validator tools: the STIX validator tests for conformance to the specification, and the Pattern validator checks for acceptable pattern syntax.

Another intriguing new feature is the STIX visualization: while a huge JSON file may be difficult to read, the visualization tool visualizes the JSON file as a graph, with nodes and edges representing STIX Domain Objects and STIX Relationship Objects, respectively.



Selected Node

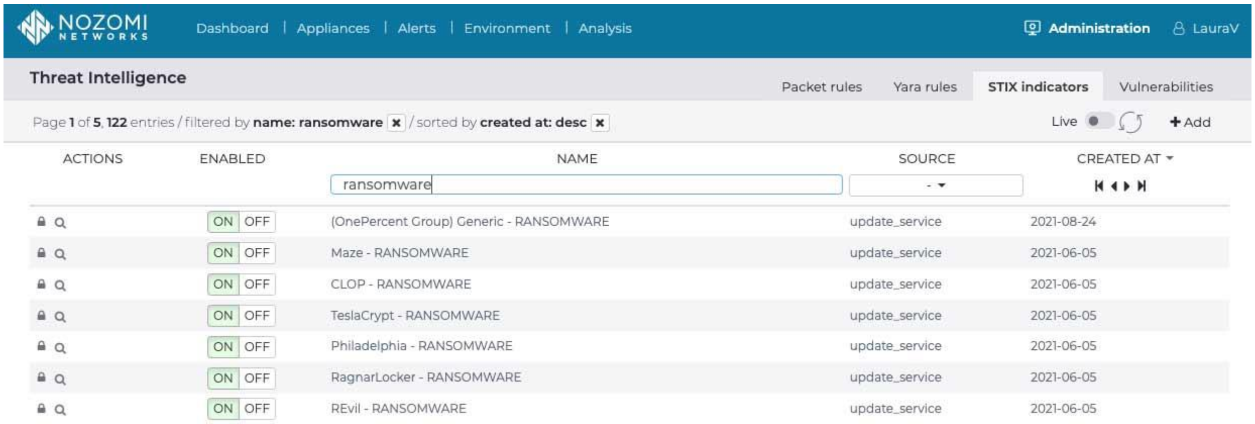
Type:	threat-actor
Spec version:	2.1
Id:	threat-actor--6d179234-61fc-40c4-ae86-3d53308d8e65
Created:	2015-05-15T09:12:16.432Z
Modified:	2015-05-15T09:12:16.432Z
Name:	Ugly Gorilla
Threat actor types:	nation-state, spy
Roles:	malware-author, agent, infrastructure-operator
Resource level:	government
Aliases:	Greenfield, JackWang, Wang Dong
Primary motivation:	organizational-gain

FIG: 2 The STIX Domain Objects and Relationship Objects for APT1 are shown in this STIX graph.

Threat Intelligence from Nozomi Networks includes MITRE ATT&CK:

Let's have a look at how Nozomi Networks supports STIX indicators before presenting an example of how to utilize them to respond to a ransomware assault.

The STIX 1 and STIX 2 formats are now supported by Nozomi Networks Guardian. Additionally, the appropriate MITRE ATT&CK Tactics and Techniques from both the Enterprise and ICS matrices can be added to STIX 2 indicators.

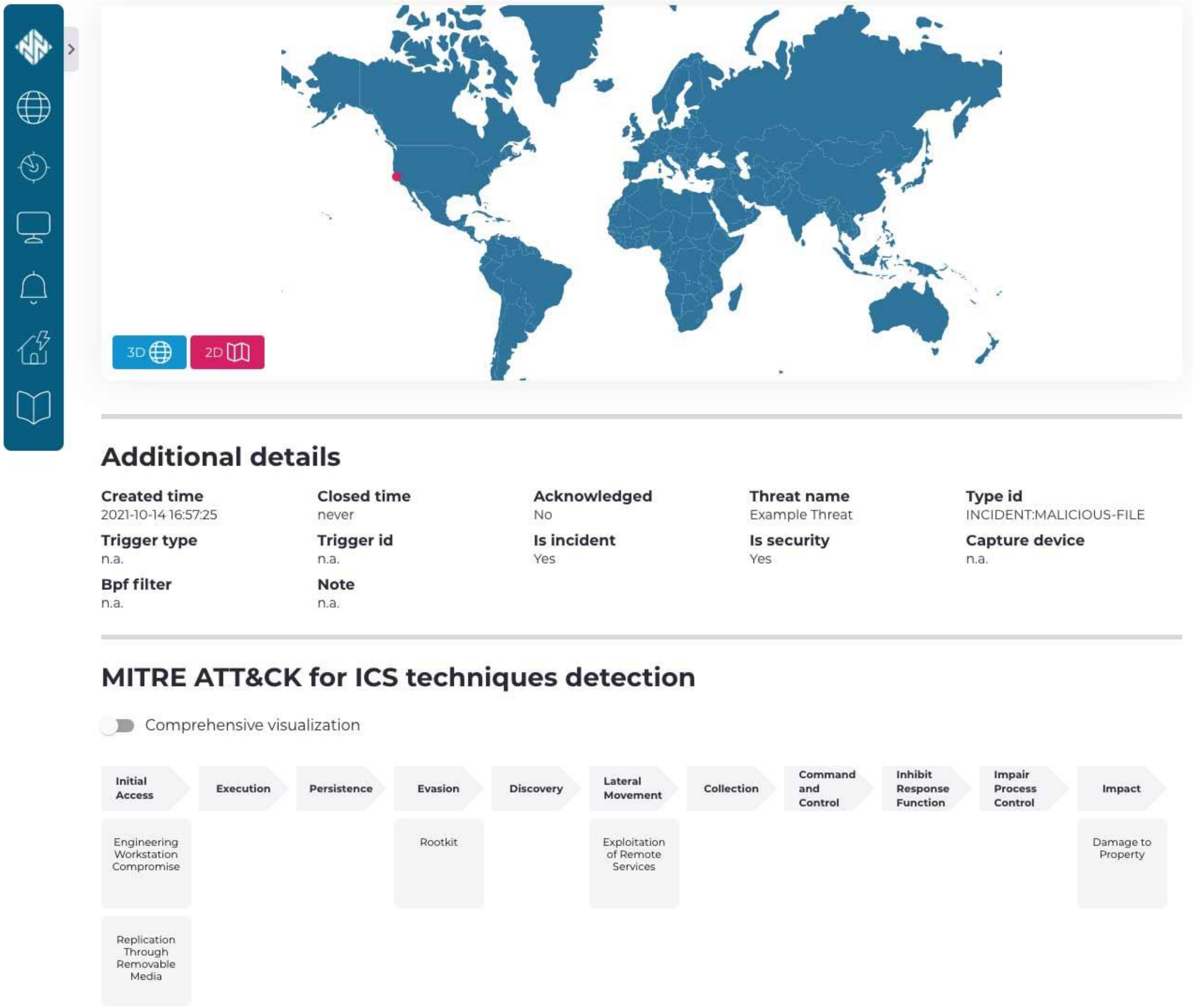


Page 1 of 5, 122 entries / filtered by **name: ransomware** ✖ / sorted by **created at: desc** ✖

ACTIONS	ENABLED	NAME	SOURCE	CREATED AT
		ransomware	-	
🔒 🔍	ON OFF	(OnePercent Group) Generic - RANSOMWARE	update_service	2021-08-24
🔒 🔍	ON OFF	Maze - RANSOMWARE	update_service	2021-06-05
🔒 🔍	ON OFF	CLOP - RANSOMWARE	update_service	2021-06-05
🔒 🔍	ON OFF	TeslaCrypt - RANSOMWARE	update_service	2021-06-05
🔒 🔍	ON OFF	Philadelphia - RANSOMWARE	update_service	2021-06-05
🔒 🔍	ON OFF	RagnarLocker - RANSOMWARE	update_service	2021-06-05
🔒 🔍	ON OFF	REvil - RANSOMWARE	update_service	2021-06-05

FIG: 3 Inside Guardian, STIX indicators

The MITRE ATT&CK methods detection view in Nozomi Networks Vantage is shown in the screenshot below. This illustration depicts a lab-created simulation of a real-world attack on industrial control systems. This virus acquires initial access by replicating through removable media and then exploiting remote services to undertake lateral movement with the goal of reaching the engineering workstation, as shown in the section dedicated to MITRE ATT&CK tactics for ICS (EWS). Once on the EWS, its ultimate goal is to alter the logic of the PLC, causing damage to the monitored equipment.



Additional details

Created time 2021-10-14 16:57:25	**Closed time** never	**Acknowledged** No	**Threat name** Example Threat	**Type id** INCIDENT:MALICIOUS-FILE
Trigger type n.a.	**Trigger id** n.a.	**Is incident** Yes	**Is security** Yes	**Capture device** n.a.
Bpf filter n.a.	**Note** n.a.			

MITRE ATT&CK for ICS techniques detection

Comprehensive visualization

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Engineering Workstation Compromise			Rootkit		Exploitation of Remote Services					Damage to Property
Replication Through Removable Media										

Figure 3: Nozomi Networks Vantage perspective of MITRE ATT&CK Techniques

STIX creation from IOCs:

Nozomi Networks Labs provides detailed usage instructions on how to construct STIX from indicators in the publicly accessible stix-tools repository. We'll show a quick example of how to use the tooling in the context of a recent malicious threat.

NEW Cooperative Inc., situated in Iowa, was a victim of the ransomware organization BlackMatter in September 2021. (read more details in this blog). It was critical for Nozomi Networks to investigate the matter very away and ensure that their clients were safe from the threat.

Takeaways: MITRE ATT&CK Makes Threat Intelligence Sharing Easier :

The need of sharing threat intelligence is one of the main ideas in this blog post. To do so, standardized formats must be used to transmit information in an efficient, consistent, and compatible manner. The threat intelligence community widely employs STIX for these purposes.

The MITRE ATT&CK paradigm has become a standard in the security field for quickly and effectively determining the context of a threat. ATT&CK can also be utilized to enhance threat detection and response by enriching the data supplied with STIX.