



# GRAPHICAL PRESENTATION OF MITRE'S ATT&CK CTI DATA

FOR CMD'S ZERODAYS BY *KIRTA*R OZA

29-JAN-2020

# DISCLAIMER

- This is an Informal Presentation with minimal Slides
- Lightning Presentation – Quick 15-20 mins

# WHAT IS STIXX AND TAXII

- STIXX – Schema/Structure/Format/Templates to represent the Threat Intelligence data in a standard way globally
- Information represented in STIXX Objects and Relationships
- Inputs to the STIXX
- TAXII – A way to transmit the threat intel data which is in STIXX format

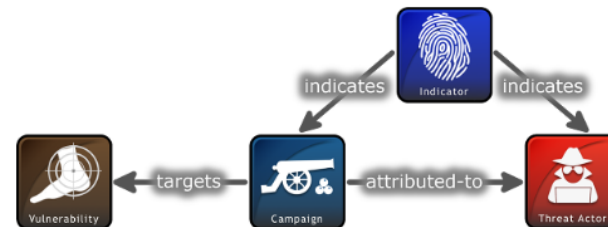


*A structured language for cyber threat intelligence*

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).

STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.

STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.



STIX Relationship Example

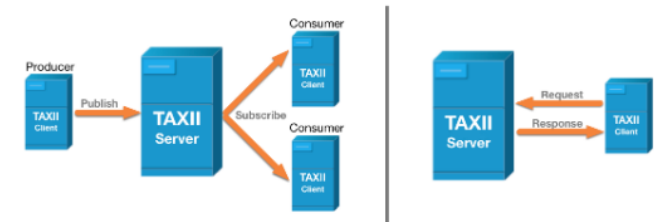


*A transport mechanism for sharing cyber threat intelligence*

Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner.

TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models.

TAXII is specifically designed to support the exchange of CTI represented in STIX.



TAXII Collections

# MITRE'S ATT&CK CTI DATA

- Groups
- Techniques Used
- Software
- <https://mitre-attack.github.io/attack-navigator/enterprise/>

| Privilege Escalation                   | Defense Evasion                         | Credential Access                  | Discovery                              | Lateral               |
|--|---|------------------------------------|--|-----------------------|
| 2 items                                | 69 items                                | 21 items                           | 23 items                               | 18 items              |
| Access Token Manipulation              | Access Token Manipulation               | Account Manipulation               | Account Discovery                      | AppleS                |
| Accessibility Features                 | Binary Padding                          | Bash History                       | Application Window Discovery           | Applica<br>Softwai    |
| AppCert DLLs                           | BITS Jobs                               | Brute Force                        | Browser Bookmark Discovery             | Compo<br>Model<br>COM |
| AppInit DLLs                           | Bypass User Account Control             | Credential Dumping                 | Domain Trust Discovery                 | Exploit:<br>Service   |
| Application Shimming                   | Clear Command History                   | Credentials from Web Browsers      | File and Directory Discovery           | Interna               |
| Bypass User Account Control            | CMSTP                                   | Credentials in Files               | Network Service Scanning               | Logon :               |
| DLL Search Order Hijacking             | Code Signing                            | Credentials in Registry            | Network Share Discovery                | Pass th               |
| Dynamic Library Hijacking              | Compile After Delivery                  | Exploitation for Credential Access | Network Sniffing                       | Pass th               |
| Elevated Execution with Prompt         | Compiled HTML File                      | Forced Authentication              | Password Policy Discovery              | Remote<br>Protoco     |
| Firmware                               | Component Firmware                      | Hooking                            | Peripheral Device Discovery            | Remote                |
| Exploitation for Privilege Escalation  | Component Object Model Hijacking        | Input Capture                      | Permission Groups Discovery            | Remote                |
| Extra Window Memory Injection          | Connection Proxy                        | Input Prompt                       | Process Discovery                      | Remote                |
| File System Permissions Weakness       | Control Panel Items                     | Kerberoasting                      | Query Registry                         | Replica<br>Remov:     |
| Hooking                                | DCShadow                                | Keychain                           | Remote System Discovery                | Shared                |
| Image File Execution Options Injection | Deobfuscate/Decode Files or Information | LLMNR/NBT-NS Poisoning and Relay   | Security Software Discovery            | SSH Hij               |
| Launch Daemon                          | Disabling Security Tools                | Network Sniffing                   | Software Discovery                     | Taint St              |
| New Service                            | DLL Search Order Hijacking              | Password Filter DLL                | System Information Discovery           | Third-p               |
| Parent PID Spoofing                    | DLL Side-Loading                        | Private Keys                       | System Network Configuration Discovery | Window                |
|  | Execution Guardrails                    | Securityd Memory                   | System Network Connections Discovery   | Window<br>Manag       |
|  | Exploitation for Defense Evasion        | Steal Web Session Cookie           | System Owner/User Discovery            |                       |
|  | Extra Window Memory Injection           |                                    | System Service Discovery               |                       |

# MAPPING BETWEEN STIX2 AND ATT&CK

- **A Group** (Intrusion-set/Threat Actor)

“uses” xyz

**Techniques** (attack-pattern)

and “uses” abc

**Software** (tools)

## Mapping Concepts

First, we must describe how ATT&CK objects and properties map to STIX 2.0 objects and properties.

### Objects

In ATT&CK, there are three main concepts (excluding Tactics for now): Techniques, Groups, and Software. Most techniques also have Mitigations. STIX 2.0 describes these as objects and uses different terminology to describe them. The following table is a mapping of ATT&CK concepts to STIX 2.0 objects:

| ATT&CK concept       | STIX Object type |
|----------------------|------------------|
| <del>Technique</del> | attack-pattern   |
| <del>Group</del>     | intrusion-set    |
| <del>Software</del>  | malware or tool  |
| Mitigation           | course-of-action |
| Tactic               | x-mitre-tactic   |
| Matrix               | x-mitre-matrix   |

The above STIX types are found as literal strings assigned to the `type` property of the STIX JSON object. As shown in the table, in STIX 2.0, there are objects called "Course(s) of Action" used to describe mitigations to ATT&CK techniques. Similarly, the STIX 2.0 object called "Attack Pattern" describes techniques, etc. It should also be noted that Tactics are not an explicit object type in STIX 2.0, and they are referenced implicitly as kill chain phases within the other object types, as described in the tables below.

## MOVING TO SCRIPTS

- Pull the “Groups” , “Software” , and “Techniques”
- Build the Relationships between them
- Visual Representation Required
- Neo4j – Graph Database for Visual Representation
- Python – Py2Neo Library for Creating Nodes and Relationships in the Graph Representation
- TAXII2 Client – to pull the STIXX2 ATT&CK CTI data



## APT39

APT39 is an Iranian cyber espionage group that has been active since at least 2014. They have targeted the telecommunication and travel industries to collect personal information that aligns with Iran's national priorities. <sup>[1][2]</sup>

ID: G0087

Associated Groups: (

Version: 2.0

Created: 19 February ;

Last Modified: 29 Apr

### Associated Group Descriptions

| Name   | Description   |
|--------|---|
| Chafer | Activities associated with APT39 largely align with a group publicly referred to as Chafer. <sup>[1][2]</sup> |

### Techniques Used

| Domain     | ID    | Name                     | Use  |
|------------|-------|--------------------------|--|
| Enterprise | T1090 | Connection Proxy         | APT39 used custom tools to create SOCK5 proxies between infected hosts. <sup>[1]</sup> |
| Enterprise | T1003 | Credential Dumping       | APT39 has used Mimikatz, Ncrack, Windows Credential Editor and ProcDump to dump cre    |
| Enterprise | T1002 | Data Compressed          | APT39 has used WinRAR and 7-Zip to compress an archive stolen data. <sup>[1]</sup>     |
| Enterprise | T1046 | Network Service Scanning | APT39 used a custom port scanner known as BLUETORCH <sup>[1]</sup>                     |

### Software

| ID    | Name                      | References        | Techniques  |
|-------|---------------------------|-------------------|---|
| S0073 | ASPKSpy                   | <sup>[1]</sup>    | Web Shell   |
| S0002 | Mimikatz                  | <sup>[1]</sup>    | Account Manipulation, Credential Dumping, Credentials in Files, DCShadow, Pass the Hash, Pass the Ticket, Private Keys, Security Support Provider, SID-History Injection  |
| S0029 | PsExec                    | <sup>[1]</sup>    | Service Execution, Windows Admin Shares   |
| S0375 | Remexi                    | <sup>[2][3]</sup> | Application Window Discovery, Clipboard Data, Command-Line Interface, Data Encrypted, Deobfuscate/Decode Files or Information, Exfiltration Over Command and Control Channel, File and Directory Discovery, Input Capture, Obfuscated Files or Information, Registry Run Keys / Startup Folder, Scheduled Task, Screen Capture, Scripting, Standard Application Layer Protocol, Windows Management Instrumentation, Winlogon Helper DLL |
| S0005 | Windows Credential Editor | <sup>[1]</sup>    | Credential Dumping  |

## PYTHON SCRIPTS

- Script 1 – Pulls the CTI data ( Groups, Techniques, Software) from ATT&CK TAXII2 Server and Creates Nodes
- Script 2 – Scrap the ATT&CK's Group Webpage and Push the data - and Build Relationships between them



DEMO TIME





THANKS