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

FOR CMD'S ZERODAYS BY *KIRTAR OZA*

29-JAN-2020

# DISCLAIMER

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

# WHAT IS STIXX AND TAXII

- STIXX – Schema/Structure/Format/Template 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

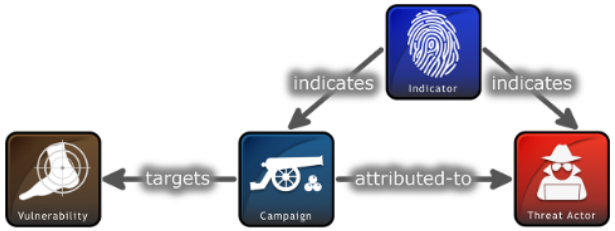
STIX™

*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**

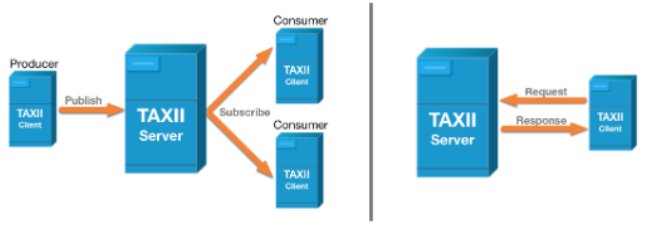
TAXII™

*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/

| rivilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral |
|---|---|---|---|---|
| 2 items | 69 items | 21 items | 23 items | 18 item |
| ccess Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleS |
| ccessibility Features | Binary Padding | Bash History | Application Window Discovery | Applica Softwa |
| ppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Compo Model COM |
| ppInit DLLs | Bypass User Account Control | Credential Dumping | Domain Trust Discovery | |
| pplication Shimming | Clear Command History | Credentials from Web Browsers | File and Directory Discovery | Exploit Service |
| ypass User Account ontrol | CMSTP | Credentials in Files | Network Service Scanning | Interna |
| LL Search Order ijacking | Code Signing | Credentials in Registry | Network Share Discovery | Logon |
| ylib Hijacking | Compile After Delivery | Exploitation for Credential Access | Network Sniffing | Pass th |
| levated Execution with rompt | Compiled HTML File | Forced Authentication | Password Policy Discovery | Pass th |
| mond | Component Firmware | Hooking | Peripheral Device Discovery | Remote Protoc |
| xploitation for Privilege scalation | Component Object Model Hijacking | Input Capture | Permission Groups Discovery | Remote |
| xtra Window Memory jection | Connection Proxy | Input Prompt | Process Discovery | Remote |
| ile System Permissions Weakness | Control Panel Items | Kerberoasting | Query Registry | Replica Remov |
| looking | DCShadow | Keychain | Remote System Discovery | Shared |
| nage File Execution ptions Injection | Deobfuscate/Decode Files or Information | LLMNR/NBT-NS Poisoning and Relay | Security Software Discovery | SSH Hij |
| aunch Daemon | Disabling Security Tools | Network Sniffing | Software Discovery | Taint Sh |
| lew Service | DLL Search Order Hijacking | Password Filter DLL | System Information Discovery | Third-p |
| arent PID Spoofing | DLL Side-Loading | Private Keys | System Network Configuration Discovery | Windo |
| | Execution Guardrails | Securityd Memory | System Network Connections Discovery | Windo 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

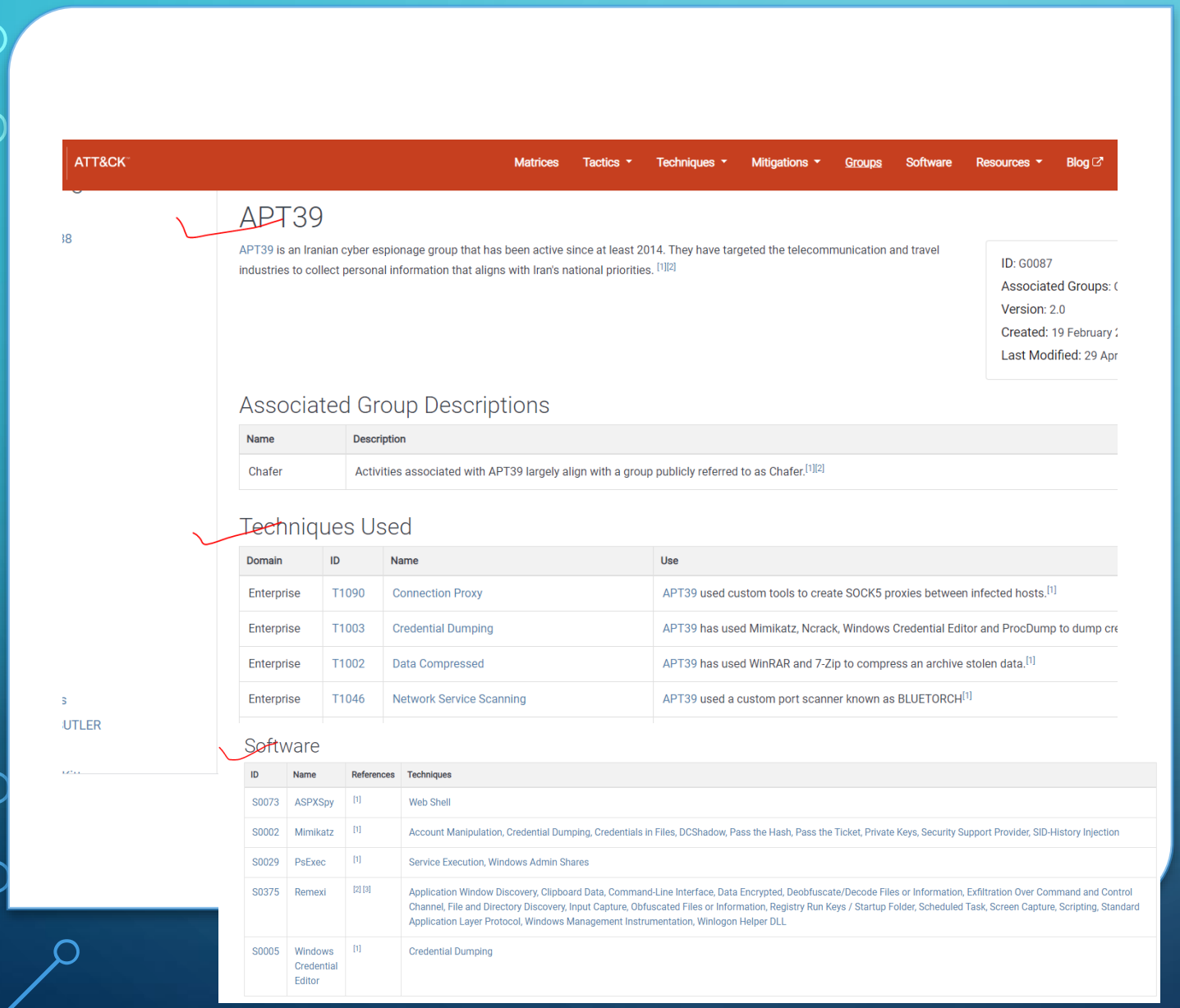
In ATT&CK, there are three main concepts (excluding Tactics for now): Techniques, Groups, and Software. Most techniques also have Mitigations. STIX 2.0 describes these as objects and uses different terminology to describe them. The following table is a mapping of ATT&CK concepts to STIX 2.0 objects:

| ATT&CK concept | STIX Object type |
|---|---|
| Technique | `attack-pattern` |
| Group | `intrusion-set` |
| Software | `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




# 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