LMNTRIX
BE THE HUNTER I NOT THE PREY

HOW MITRE ATT&CK CAN BE MAPPED TO FINISHED CYBER THREAT INTELLIGENCE

«Threat intelligence in its finished format is an actionable knowledge & insight on adversary and their malicious activities. Actionable intelligence enables the defenders to create the defence mechanism to save their respective organisation.»

Breaking Down ATT&CK

Tactics: The adversary's technical growth

Using the knowledge of adversary behaviours to inform defenders

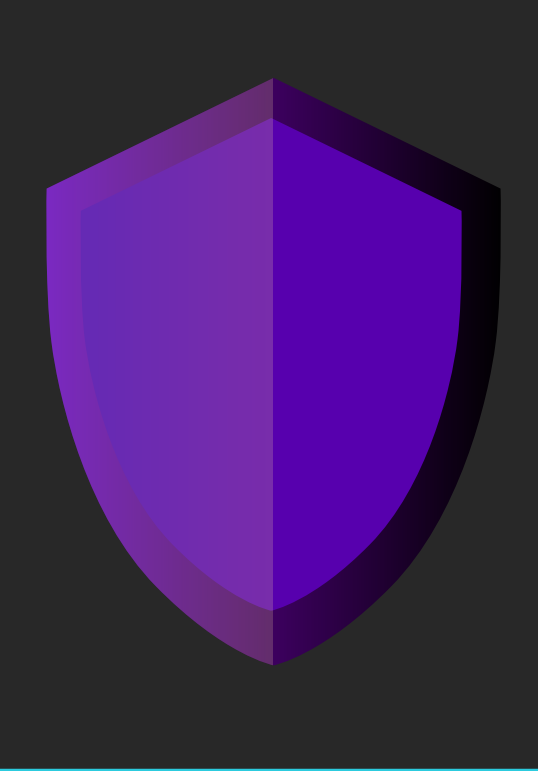
Structuring threat intelligence with ATT&CK allows us to :
- Compare behaviours of different threat actor groups
- Grouping the common techniques of adversary together
- Grouping based on time occurrences
- Grouping for defenders to create specific defences

Able to communicate the adversary behaviour in a common language.

To accomplish the process of taking the raw data of any threat incident and converting it to finished intelligence, we must follow the below cycle:

Understand ATT&CK

Map raw data to ATT&CK



Create defensive strategy on ATT&CK mapped data

Store and Analyse ATT&CK mapped data

Process of Mapping an Incident to ATT&CK

Finding the correct behaviour of Adversary from «Initial access to data Exfiltration»

Research the behaviour using open source platform

Translate the researched behaviour into a known «Tactic»

Map the behaviour to a «Technique» that can be best defined under a «Tactic»

Planning of ATT&CK data conversion into Cyber Threat Intelligence

Who's Consuming the data?

Human

Human readable document

Machine

How the context around the incident will be provided?

How detailed the context will be? (Just a Technique or a Procedure)

How the linkage to other intelligence will be?
- Incident, Group, Campaign, Indicator

How the import & export of data performed?
- Format

Actionable Intelligence

To make cyber threat intelligence data actionable one has to identify all of the tasks that the adversary is performing. For our example, consider the "REMCOS RAT" malware campaign which we detected at a client environment. The malware campaign is initially captured into a raw incident format and then mapped with ATT&CK techniques.
Raw Investigation Data:

Raw Investigation for Remcos RAT
During our routine endpoint monitoring process, a malicious Excel file was detected. The malicious file was opened from Outlook. The malicious executable has been classified as Remcos RAT Dropper. This is an active Malware Distribution (RAT infection) campaign targeting US organizations via spearphishing email attachments.

The observed file locations are as follows –
C:\Users\Adam\AppData\Local\Packages\oice_16_974fa576_32c1d314_19db\AC\Temp\8B6A4C5F.xlsm
C:\Users\Adam\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\QFKOUSJO\Remittance Advice (002).xlsm
C:\Users\Adam\Documents\Temp\Reed\Remittance Advice.xlsm
C:\Users\Adam\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\QFKOUSJO\Remittance Advice.xlsm

During analysis, we observed that the malicious Excel file contained VB Macro code which is executed on file open. The macro code performs the following actions –

Drops a VBS script and executes it with wscript.exe
The VBS script executes PowerShell via WMI
The PowerShell was executed with heavily obfuscated commands
Connects to IP 79[.]124[.]8[.]122 and access a JPG file which contains malicious code in hex format
Privilege Escalation is attempted by modifying registry values of Event Viewer for UAC Bypass
With high privileges, notepad is started, and 2nd stage malware is injected to Notepad
The actual RAT now resides in memory within the Notepad process running in the background without any window visible to the user
RAT connects to Command and Control IP 80[.]209[.]240[.]101 and downloads scripts containing further instructions
Performs checks to validate the user is Administrator and the system is not inside a Virtual Environment, otherwise, RAT instruction scripts are removed

The Raw investigation data is mapped with ATT&CK Techniques data.

Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Execution
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Component Object Model and Distributed COM
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Source
Space after Filename
Third-party Software
Trap
Trusted Developer Utilities
User Execution
Windows Management Instrumentation
Windows Remote Management
XSL Script Processing

Persistence
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
Emond
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Kernel Modules and Extensions
Launch Agent
Launch Daemon
Launchctl
LC_LOAD_DYLIB Addition
Local Job Scheduling
Login Item
Logon Scripts
LSASS Driver
Modify Existing Service
Netsh Helper DLL
New Service
Office Application Startup
Path Interception
Plist Modification
Port Knocking
Port Monitors
PowerShell Profile
Rc.common
Re-opened Applications
Redundant Access
Registry Run Keys / Startup Folder
Scheduled Task
Screensaver
Security Support Provider
Server Software Component
Service Registry Permissions Weakness
Setuid and Setgid
Shortcut Modification
SIP and Trust Provider Hijacking
Startup Items
System Firmware
Systemd Service
Time Providers
Trap
Valid Accounts
Web Shell
Windows Management Instrumentation Event Subscription
Winlogon Helper DLL

Privilege Escalation
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Elevated Execution with Prompt
Emond
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Parent PID Spoofing
Path Interception
Plist Modification
Port Monitors
PowerShell Profile
Process Injection
Scheduled Task
Service Registry Permissions Weakness
Setuid and Setgid
SID-History Injection
Startup Items
Sudo
Sudo Caching
Valid Accounts
Web Shell

Defense Evasion
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
Clear Command History
CMSTP
Code Signing
Compile After Delivery
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Connection Proxy
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Execution Guardrails
Exploitation for Defense Evasion
Extra Window Memory Injection
File and Directory Permissions Modification
File Deletion
File System Logical Offsets
Gatekeeper Bypass
Group Policy Modification
Hidden Files and Directories
Hidden Users
Hidden Window
HISTCONTROL
Image File Execution Options Injection
Indicator Blocking
Indicator Removal from Tools
Indicator Removal on Host
Indirect Command Execution
Install Root Certificate
InstallUtil
Launchctl
LC_MAIN Hijacking
Masquerading
Modify Registry
Mshta
Network Share Connection Removal
NTFS File Attributes
Obfuscated Files or Information
Parent PID Spoofing
Plist Modification
Port Knocking
Process Doppelgänging
Process Hollowing
Process Injection
Redundant Access
Regsvcs/Regasm
Regsvr32
Rootkit
Rundll32
Scripting
Signed Binary Proxy Execution
Signed Script Proxy Execution
SIP and Trust Provider Hijacking
Software Packing
Space after Filename
Template Injection
Timestomp
Trusted Developer Utilities
Valid Accounts
Virtualization/Sandbox Evasion
Web Service
XSL Script Processing

Credential Access
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials from Web Browsers
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning and Relay
Network Sniffing
Password Filter DLL
Private Keys
Securityd Memory
Steal Web Session Cookie
Two-Factor Authentication Interception

Discovery
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion

Lateral Movement
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management

Collection
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture

Command And Control
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service

Exfiltration
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer

Impact
ccount Access Removal
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
System Shutdown/Reboot
Transmitted Data Manipulation

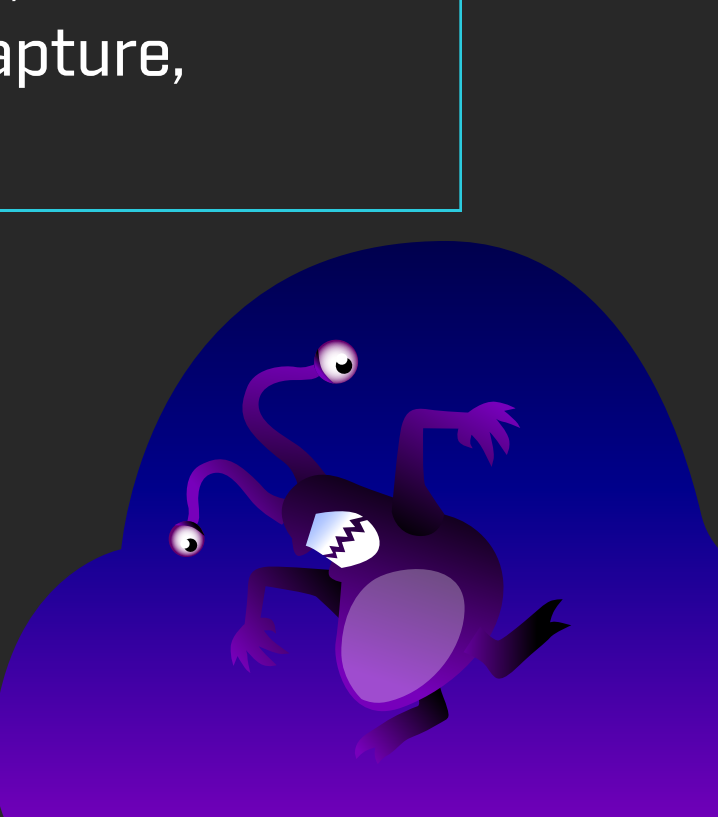
Final Actionable Intelligence

Gorgon Group is a threat group consisting of members who are suspected to be Pakistan-based or have other connections to Pakistan. The group has performed a mix of criminal and targeted attacks, including campaigns against government organizations in the United Kingdom, Spain, Russia, and the United States.

Campaign Name: Remcos RAT

Techniques used: Spearphishing attachment, Audio Capture, Bypass User Account Control, Clipboard Data, Command-Line Interface, Connection Proxy, File and Directory Discovery, Input Capture, Modify Registry, Obfuscated Files or Information, Process Injection, Registry Run Keys / Startup Folder, Remote File Copy, Screen Capture, Scripting, Video Capture, Virtualization/Sandbox Evasion.

Network Connections: 79.124.8.122; 80.209.240.101



LMNTRIX
BE THE HUNTER I NOT THE PREY