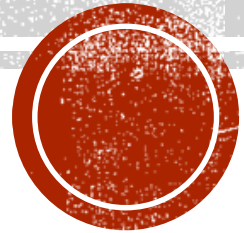
INTRODUCTION TO MITRE'S ATT&CK FRAMEWORK

CySecK Webinar Series

On 24-Jun-2020

By Kirtar Oza



SETTING EXPECTATIONS

- Introduction and Overview MITRE's ATT&CK
- Anatomy of MITRE ATT&CK – Components of ATT&CK
- For people who want to get started with ATT&CK
- Will not get in to too much of technical weeds
- Deliberately kept simple and at high level
- Can have workshop in-depth for some technical actions

BACKGROUND

- MITRE – Non-profit Organization established in 1958
- Felt the need to document common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against Windows enterprise
- Started in 2013 as a part of FMX Project
- Investigate use of endpoint telemetry data and analytics to improve post-compromise detection of adversaries operating

AGENDA

- What is ATTA&CK ?
- Why ATT&CK was needed? Why ATT&CK received the wide acceptance?
- Anatomy of ATT&CK
- Demo: A Sample Technique and its detection
- ATT&CK Navigator
- ATT&CK Navigator in Cyber Threat Intelligence (CTI)
- Approach to actionize ATT&CK

WHAT IS ATT&CK ?

- Repository of the Attackers' Behaviour
- MITRE ATT&CK™ is a globally-accessible knowledge base of adversary **tactics** and **techniques based** on **real-world observations**.
- Common Language
- Community Driven

ATT&CK™

Adversarial Tactics, Techniques, and Common Knowledge

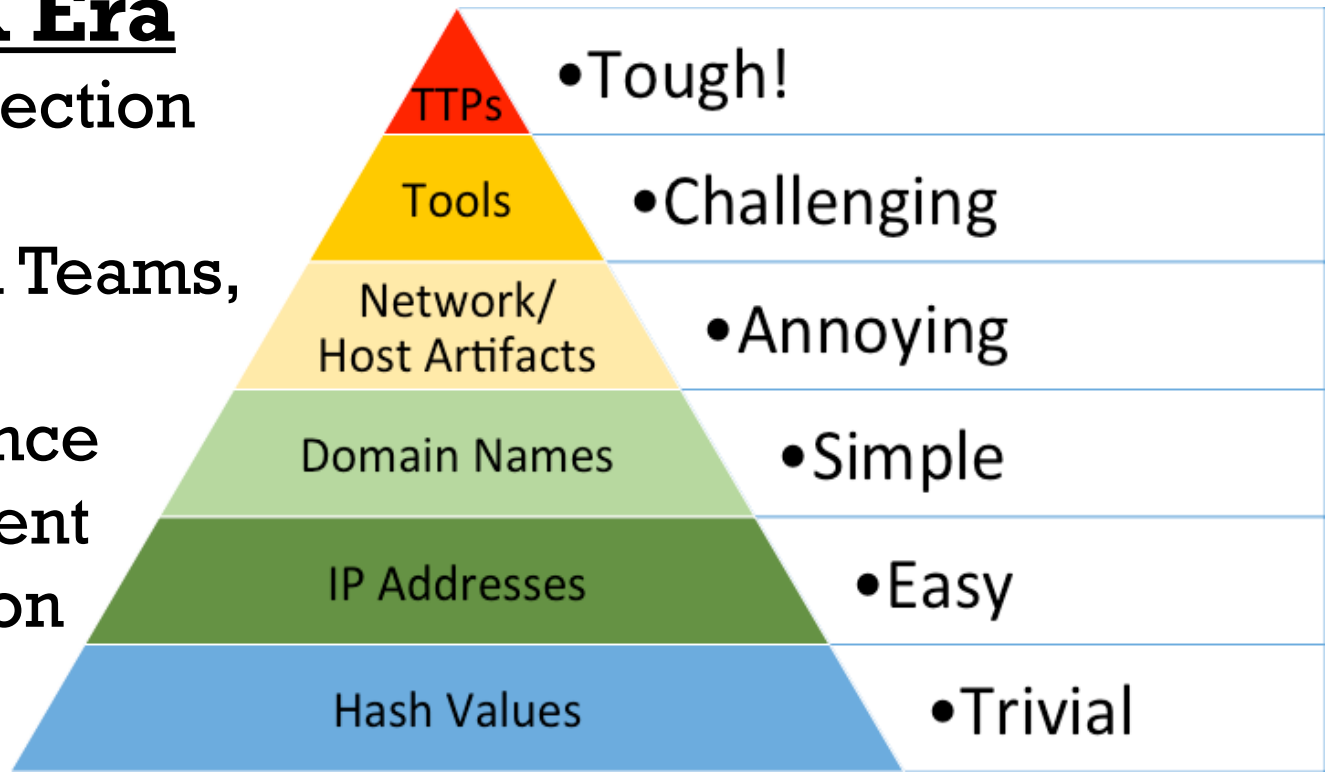
- Pre-ATT&CK
- Enterprise ATT&CK
- Mobile
- ICS (Industrial Control Systems)

WHY ATT&CK WAS NEEDED ?

Challenges in Pre-ATT&CK Era

- Lack of resources for building detection capabilities
- Scattered resources (Reports, Red Teams, SANS, Legacy Usecases)
- Unreliable Cyber Threat Intelligence
- Lack of Benchmark for measurement
- Lack of guidance for data collection

Pyramid of pain



David J Bianco's Pyramid of Pain

Source: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

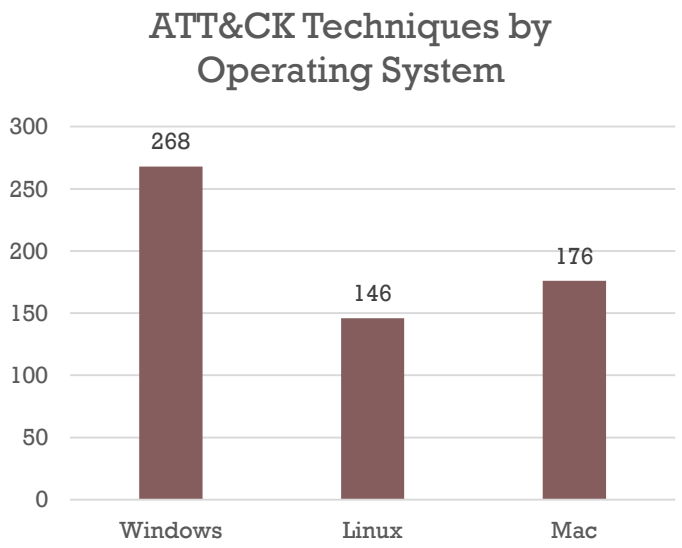
ANATOMY OF ATT&CK

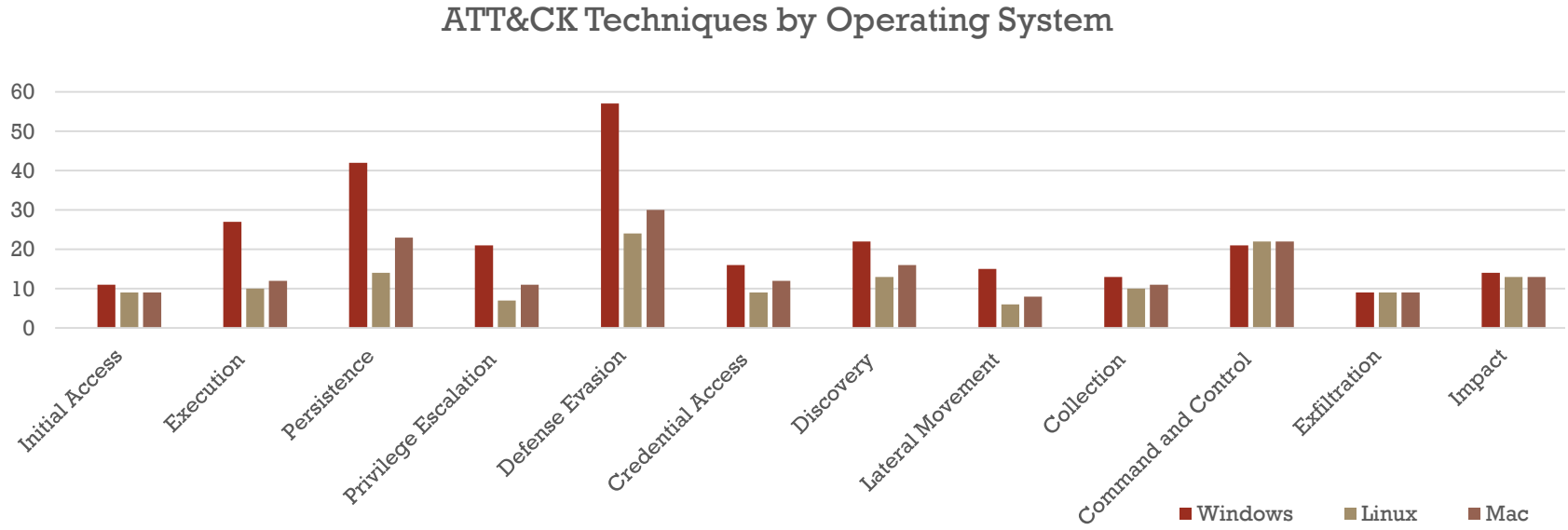
Tactics(12) – Technical Goals of the Adversary

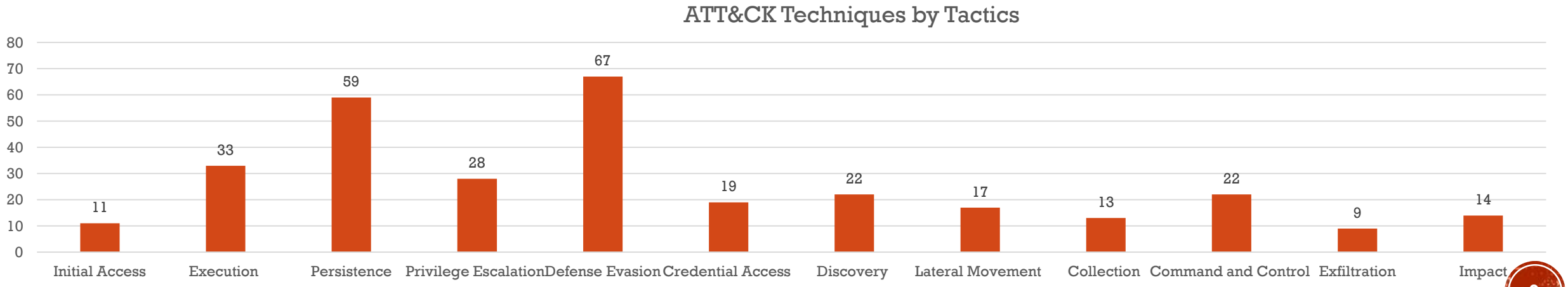
Techniques – How the Goals are achieved

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
						System Network					

ANATOMY OF ATT&CK







TECHNIQUES

Home > Techniques > Enterprise > PowerShell

PowerShell

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. [1] Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer.

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

Administrator permissions are required to use PowerShell to connect to remote systems.

A number of PowerShell-based offensive testing tools are available, including Empire, PowerSploit, [2] and PSAttack. [3]

PowerShell commands/scripts can also be executed without directly invoking the powershell.exe binary through interfaces to PowerShell's underlying System.Management.Automation assembly exposed through the .NET framework and Windows Common Language Interface (CLI). [4][5] [6]

PROCEDURES

Procedure Examples

Name	Description
APT19	APT19 used PowerShell commands to execute payloads.[66]
APT28	APT28 downloads and executes PowerShell scripts.[71]
APT29	APT29 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke. APT29 also used PowerShell scripts to evade defenses.[16][54][55]
APT3	APT3 has used PowerShell on victim systems to download and run payloads after exploitation.[67]
APT32	APT32 has used PowerShell-based tools, PowerShell one-liners, and shellcode loaders for execution.[49][50][51]
APT33	APT33 has utilized PowerShell to download files from the C2 server and run various scripts.[99]
APT41	APT41 leveraged PowerShell to deploy malware families in victims' environments.[109]
AutoIt backdoor	AutoIt backdoor downloads a PowerShell script that decodes to a typical shellcode loader.[13]
BONDUPDATER	BONDUPDATER is written in PowerShell.[14][35]

REFERENCES

References

1. Microsoft. (n.d.). Windows PowerShell Scripting. Retrieved April 28, 2016.
2. PowerSploit. (n.d.). Retrieved December 4, 2014.
3. Haight, J. (2016, April 21). PS>Attack. Retrieved June 1, 2016.
4. Warner, J.. (2015, January 6). Inexorable PowerShell – A Red Teamer's Tale of Overcoming Simple AppLocker Policies. Retrieved December 8, 2018.
5. Christensen, L.. (2015, December 28). The Evolution of Offensive PowerShell Invocation. Retrieved December 8, 2018.
6. Babinec, K. (2014, April 28). Executing PowerShell scripts from C#. Retrieved April 22, 2019.
7. Strategic Cyber LLC. (2017, March 14). Cobalt Strike Manual. Retrieved May 24, 2017.
8. Nicolas Verdier. (n.d.). Retrieved January 29, 2018.
9. PowerShellMafia. (2012, May 26). PowerSploit - A PowerShell Post-Exploitation Framework. Retrieved February 6, 2018.
10. PowerSploit. (n.d.). PowerSploit. Retrieved February 6, 2018.
11. Schroeder, W., Warner, J., Nelson, M. (n.d.). Github PowerShellEmpire. Retrieved April 28, 2016.
12. The Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NZ NCSC), CERT New Zealand, the UK National Cyber Security Centre (UK NCSC) and the US National Cybersecurity and Communications Integration Center (NCCIC). (2018, October 11). Joint report on publicly available hacking tools. Retrieved March 11, 2019.
13. Settle, A., et al. (2016, August 8). MONSOON - Analysis Of An APT Campaign.
57. Gorelik, M.. (2017, June 9). FIN7 Takes Another Bite at the Restaurant Industry. Retrieved July 13, 2017.
58. Kaspersky Lab's Global Research and Analysis Team. (2016, February 9). Poseidon Group: a Targeted Attack Boutique specializing in global cyber-espionage. Retrieved March 16, 2016.
59. FireEye Threat Intelligence. (2016, April). Follow the Money: Dissecting the Operations of the Cyber Crime Group FIN6. Retrieved June 1, 2016.
60. McKeague, B. et al. (2019, April 5). Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware. Retrieved April 17, 2019.
61. Villadsen, O.. (2019, August 29). More_eggs, Anyone? Threat Actor ITG08 Strikes Again. Retrieved September 16, 2019.
62. Counter Threat Unit Research Team. (2017, June 27). BRONZE UNION Cyberespionage Persists Despite Disclosures. Retrieved July 13, 2017.
63. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.
64. FireEye. (2018, March 16). Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries. Retrieved April 11, 2018.
65. ClearSky Cyber Security and Trend Micro. (2017, July). Operation Wilted Tulip: Exposing a cyber espionage apparatus. Retrieved August 21, 2017.
66. Ahl, I. (2017, June 06). Privileges and Credentials: Phished at the Request of Counsel. Retrieved May 17, 2018.
67. Moran, N., et al. (2014, November 21). Operation Double Tap. Retrieved

METADATA

ID: T1086

Tactic: Execution

Platform: Windows

Permissions Required: User, Administrator

Data Sources: PowerShell logs, Loaded DLLs, DLL monitoring, Windows Registry, File monitoring, Process monitoring, Process command-line parameters

Supports Remote: Yes

Contributors: Praetorian

Version: 1.1

Created: 31 May 2017

Last Modified: 18 July 2019

MITIGATIONS & DETECTION

Mitigations

Mitigation	Description
Code Signing	Set PowerShell execution policy to execute only signed scripts.
Disable or Remove Feature or Program	It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.
Privileged Account Management	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.

Detection

If proper execution policy is set, adversaries will likely be able to define their own execution policy if they obtain administrator or system access, either through the Registry or at the command line. This change in policy on a system may be a way to detect malicious use of PowerShell. If PowerShell is not used in an environment, then simply looking for PowerShell execution may detect malicious activity.

Monitor for loading and/or execution of artifacts associated with PowerShell specific assemblies, such as System.Management.Automation.dll (especially to unusual process names/locations). [4][5]

It is also beneficial to turn on PowerShell logging to gain increased fidelity in what occurs during execution (which is applied to .NET invocations). [110] PowerShell 5.0 introduced enhanced logging capabilities, and some of those features have since been added to PowerShell 4.0. Earlier versions of PowerShell do not have many logging

GROUPS

APT3

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. [1] [2] This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. [1] [3] As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong. [4]

MITRE has also developed an APT3 Adversary Emulation Plan.[5]

ID: G0022

Associated Groups: Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110

Version: 1.2

Created: 31 May 2017

Last Modified: 11 October 2019

version permalink

Associated Group Descriptions

Name	Description
Gothic Panda	[11] [2] [4]
Pirpi	[11]
UPS Team	[1] [2] [4]
Buckeye	[4]
Threat Group-0110	[2] [4]

GROUPS: TECHNIQUES & SOFTWARE USED

Techniques Used

ATT&CK® Navigator Layers

Software

ID	Name	References	Techniques
S0349	LaZagne	[4]	Credential Dumping, Credentials from Web Browsers, Credentials in Files
S0165	OSInfo	[4]	Account Discovery, Network Share Discovery, Permission Groups Discovery, Query Registry, Remote System Discovery, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery
S0013	PlugX	[10]	Command-Line Interface, Commonly Used Port, Custom Command and Control Protocol, Deobfuscate/Decode Files or Information, DLL Side-Loading, Execution through API, File and Directory Discovery, Input Capture, Masquerading, Modify Existing Service, Modify Registry, Multiband Communication, Network Share Discovery, New Service, Process Discovery, Query Registry, Registry Run Keys / Startup Folder, Remote File Copy, Screen Capture, Standard Application Layer Protocol, Standard Non-Application Layer Protocol, System Network Connections Discovery, Trusted Developer Utilities, Virtualization/Sandbox Evasion, Web Service

USECASES OF ATT&CK

- Detection and Analytics
- Cyber Threat Intelligence (CTI)
- Assessment and Engineering
- Adversary Emulation & Red Teaming

TECHNIQUES IN ACTION (DETECTION)

DEMO

ATT&CK NAVIGATOR INTRODUCTION

- Introduction & Demo

- https://mitre-attack.github.io/attack-navigator/enterprise/#

ATT&CK NAVIGATOR USE IN CTI

- India Vs China
  - Gothic Panda
  - Stone Panda

APPROACH TO ACTIONIZE

- Ways to Prioritize the techniques

- Data Sources - what data sources we have already
- Threat Intelligence - what our adversaries are doing ?
- Tools - what your current tools can cover
- Red Team - what can you see red teamer doing ?

Thank You