

Module 3

MITRE ATT&CK

Sandeep K. Shukla
IIT Kanpur



Acknowledgement

- This material is based on the ATT&CK material created by Katie Nickels and Adam Pennington (MITRE Corporation)



Outline

- What is ATT&CK?
- Mapping to ATT&CK from Finished Cyber Incident Reports
- Mapping to ATT&CK from Raw Data from Cyber Incident
- ATT&CK Navigator
- From ATT&CK Mapping to Defence Recommendation



Why should Defenders know about Attacker's Tactics, Techniques and Procedures?

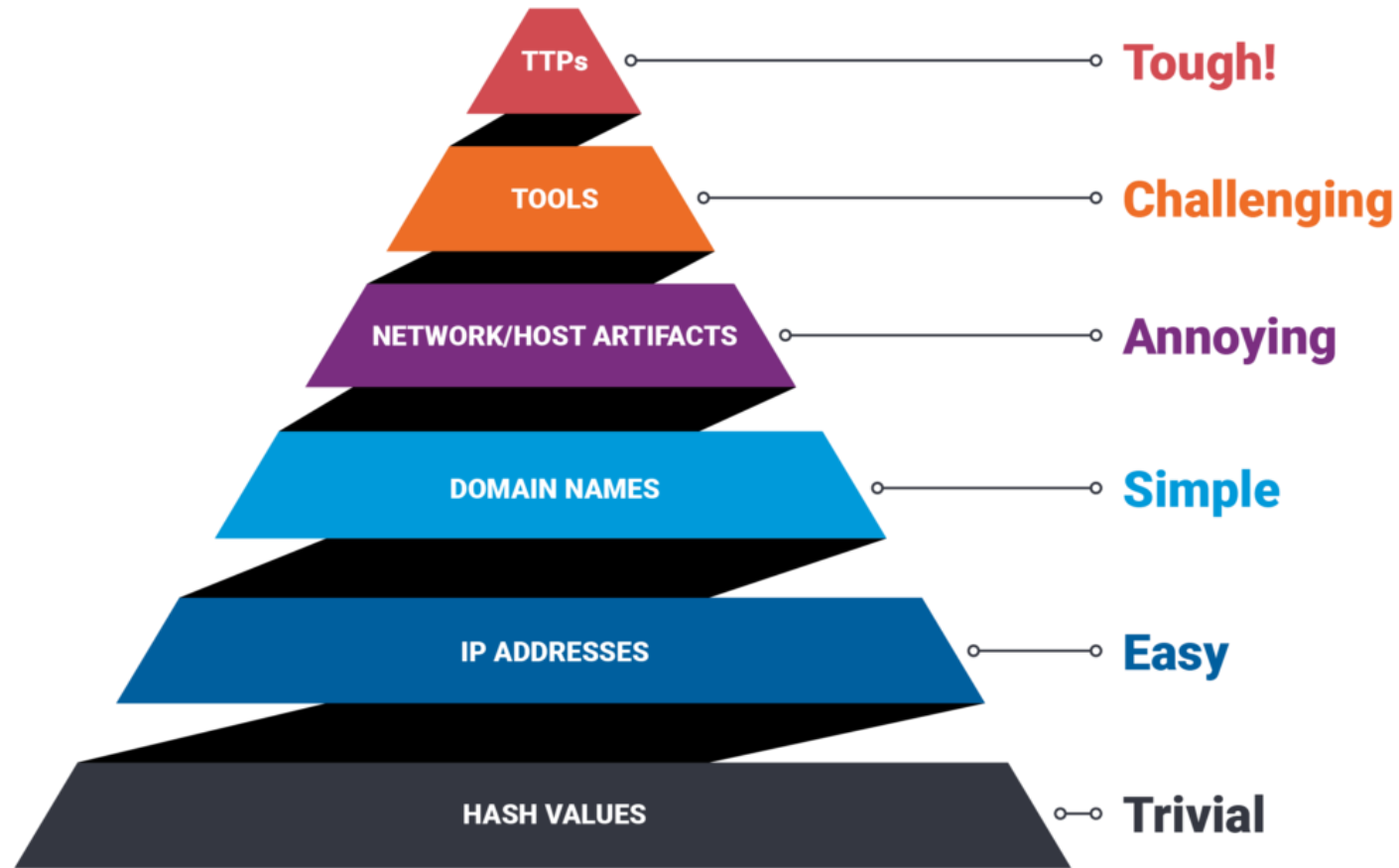


- As a defender of my organization, I need to know:
 - How effective are my protection and controls against advanced attackers?
 - Is my defensive posture enough to stop APT group attacks?
 - How about APT 3 or APT 29?
 - Can my detection technology and process detect an APT attack?
 - Is the data I collect during network and host monitoring useful in protection, detection or response?
 - Do the tools I have installed for defence – have overlapping functionalities?
 - Will the newest tool from a cyber security vendor help my cyber defence?

What is ATT & CK?

- A knowledge-base of adversary behaviour
 - Based on real-world incident analysis based on a large number of attacks
 - Organized into tactics, techniques and procedures
 - Developed by the MITRE Corporation, USA
 - Available for anyone to use in developing threat intelligence, post incidence analysis, and developing defence tactics, techniques and procedures
- An attacker uses a series of tactics
 - Each tactic can be realized by some technique from a set of techniques
 - Each technique can be implemented with procedures from a set of possible procedures
- The Knowledge-base is community driven and continuously improved

David Bianco's Pyramid of Pain



ATT & CK Matrix

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

Technique: Spearphishing Link

[Home](#) > [Techniques](#) > [Enterprise](#) > [Phishing](#) > [Spearphishing Link](#)

Phishing: Spearphishing Link

Other sub-techniques of Phishing (3) ^	
ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service

Adversaries may send spearphishing emails with a malicious link in an attempt to elicit sensitive information and/or gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](#). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons). Links may also direct users to malicious applications designed to [Steal Application Access Tokens](#), like OAuth tokens, in order to gain access to protected applications and information.^[1]

ID: T1566.002

Sub-technique of: [T1566](#)

Tactic: Initial Access

Platforms: Linux, Office 365, SaaS, Windows, macOS

Data Sources: DNS records, Detonation chamber, Email gateway, Mail server, Packet capture, SSL/TLS inspection, Web proxy

CAPEC ID: [CAPEC-163](#)

Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Mark Wee; Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC); Shailesh Tiwary (Indian Army)

Version: 1.0

Created: 02 March 2020

Last Modified: 02 March 2020

[Version Permalink](#)

Procedure Examples

Phishing for Information: Spearphishing Link

Other sub-techniques of Phishing for Information (3)

Adversaries may send spearphishing messages with a malicious link to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](#) or [Compromise Accounts](#)) and/or sending multiple, seemingly urgent messages.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, the malicious emails contain links generally accompanied by social engineering text to coax the user to actively click or copy and paste a URL into a browser.^{[1][2]} The given website may closely resemble a legitimate site in appearance and have a URL containing elements from the real site. From the fake website, information is gathered in web forms and sent to the attacker. Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](#) or [Search Victim-Owned Websites](#)) to craft persuasive and believable lures.

ID: T1598.003

Sub-technique of: [T1598](#)

- ① **Tactic:** Reconnaissance
- ① **Platforms:** PRE
- ① **Data Sources:** [Application Log](#): Application Log Content, [Network Traffic](#): Network Traffic Content, [Network Traffic](#): Network Traffic Flow

Contributors: Philip Winther; Robert Simmons, @MalwareUtkonos; Sebastian Salla, McAfee

Version: 1.1

Created: 02 October 2020

Last Modified: 15 April 2021

[Version Permalink](#)

Procedure Examples

ID	Name	Description
G0050	APT32	APT32 has used malicious links to direct users to web pages designed to harvest credentials. ^[3]
G0094	Kimsuky	Kimsuky has used links in e-mail to steal account information. ^[4]
G0034	Sandworm Team	Sandworm Team has crafted spearphishing emails with hyperlinks designed to trick unwitting recipients into revealing their account credentials. ^[5]
G0121	Sidewinder	Sidewinder has sent e-mails with malicious links to credential harvesting websites. ^[6]
G0122	Silent Librarian	Silent Librarian has used links in e-mails to direct victims to credential harvesting websites designed to appear like the targeted organization's login page. ^{[7][8][9][10][11][12]}

Tactics: Techniques: Procedures

ID: TA0001

Created: 17 October 2018

Last Modified: 19 July 2019

ID: T1566.002

Sub-technique of: T1566

- ① Tactic: Initial Access
 - ① Platforms: Google Workspace, Linux, Office 365, SaaS, Windows, macOS
- Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Kobi Haimovich, CardinalOps; Mark Wee; Menachem Goldstein; Philip Winther; Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC); Shailesh Tiwary (Indian Army)

Version: 2.5

Created: 02 March 2020

Last Modified: 06 September 2023

S0677 AADInternals

S0584 AppleJeuS

G0006 APT1

G0007 APT28

G0016 APT29

G0022 APT3

G0050 APT32

G0064 APT33

APT Groups



GROUPS

APT28

APT29

APT3

APT30

APT32

APT33

APT37

APT38

APT39

APT41

Aquatic Panda

Axiom

[Home](#) > [Groups](#) > [APT28](#)

APT28

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.^{[1][2]} This group has been active since at least 2004.^{[3][4][5][6][7][8][9][10][11][12][13]}

APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election.^[5] In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.^[14] Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as [Sandworm Team](#).

ID: G0007

① Associated Groups: IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

Contributors: Sébastien Ruel, CGI; Drew Church, Splunk; Emily Ratliff, IBM; Richard Gold, Digital Shadows

Version: 4.0

Created: 31 May 2017

Last Modified: 26 March 2023

Mitigations and Detection

Mitigations

ID	Mitigation	Description
M1047	Audit	Audit applications and their permissions to ensure access to data and resources are limited based upon necessity and principle of least privilege.
M1021	Restrict Web-Based Content	Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
M1054	Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation. ^{[117][118]} .



Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	<p>Monitor for third-party application logging, messaging, and/or other artifacts that may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.^{[117][118]} URL inspection within email (including expanding shortened links and identifying obfuscated URLs) can help detect links leading to known malicious sites.^[2]</p> <p>Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.</p>

Use Cases of ATT&CK

- Detection

processes = **search** Process:Create

reg = **filter** processes **where** (exe == "reg.exe" **and** parent_exe == "cmd.exe")

cmd = **filter** processes **where** (exe == "cmd.exe" **and** parent_exe != "explorer.exe")

reg_and_cmd = **join** (reg, cmd) **where** (reg.ppid == cmd.pid **and** reg.hostname == cmd.hostname)

output reg_and_cmd

Comparing two threat groups

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/3)	Account Discovery (1/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (2/4)	Automated Exfiltration (0/1)
Gather Victim Host Information (0/4)	Acquire Infrastructure (2/8)	Drive-by Compromise	Command and Scripting Interpreter (4/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits
Gather Victim Identity Information (1/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (1/14)	Boot or Logon Autostart Execution (T1547) (0/5)	Boot or Logon Autostart Execution (T1547) (0/5)	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (1/3)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/6)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution (1/14)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (1/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)
Phishing for Information (1/4)	Establish Accounts (1/3)	Phishing (2/4)	Inter-Process Communication (0/3)	Compromise Client Software Binary	Boot or Logon Initialization Scripts (0/5)	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)
Search Closed Sources (0/2)	Obtain Capabilities (1/6)	Replication Through Removable Media	Native API	Create Account (0/3)	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access	Input Capture (1/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (2/6)	Supply Chain Compromise	Scheduled Task/Job (1/5)	Create or Modify System Process (1/4)	Create or Modify System Process (1/4)	Domain Policy Modification (0/2)	Modify Authentication Process (0/8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Scheduled Transfer
Search Open Websites/Domains (0/3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (0/16)	Domain Policy Modification (0/2)	Execution Guardrails (0/1)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (2/4)	Data from Information Repositories (0/3)	Ingress Tool Transfer	
Search Victim-Owned Websites		Valid Accounts (1/4)	Shared Modules	External	Escape to Host	Exploitation for Defense Evasion	Multi-Factor Authentication Request	Device Driver Discovery		Data from Local System	Multi-Stage Channels	
			Software Deployment Tools			File and Directory Permissions Modification (1/2)		Domain Trust Discovery			Non-Application Layer Protocol	
						Hide Artifacts (3/11)		File and Directory Discovery				
						Hijack Execution Flow (1/12)		Group Policy Discovery				

Gap Analysis and Engineering Defence

FINES (000017) X										Selection controls										Type controls										Technique controls																																																																																																			
Reconnaissance 10 techniques										Resource Development 8 techniques										Initial Access 9 techniques										Execution 14 techniques										Persistence 19 techniques										Privilege Escalation 11 techniques										Defense Evasion 42 techniques										Credential Access 17 techniques																																																											
Active Scanning (10)										Acquire Access (8)										Drive-by Compromise (9)										Cloud Administration Command (14)										Account Manipulation (19)										Abuse Elevation Control Mechanism (11)										Abuse Elevation Control Mechanism (42)										Adversary in-the-Middle (17)																																																											
Gather Victim Host Information (10)										Acquire Infrastructure (8)										Exploit Public-Facing Application (9)										AppleScript (14)										BITS Jobs (19)										Access Token Manipulation (11)										Access Token Manipulation (42)																																																																					
Gather Victim Identity Information (10)										Compromise Accounts (8)										External Remote Services (9)										Cloud API (14)										Active Setup (19)										Authentication Package (11)										BITS Jobs (42)										Credential Stuffing (17)																																																											
Gather Victim Network Information (10)										Compromise Infrastructure (8)										Hardware Additions (9)										JavaScript (14)										Kernel Modules and Extensions (19)										Active Setup (11)										Build Image on Host (42)										Account																																																											
Gather Victim Org Information (10)										Develop Capabilities (8)										Phishing (9)										Network Device CLI (14)										Login Items (19)										Debugger Evasion (11)										Application Discovery (17)																																																																					
Phishing for Information (10)										Establish Accounts (8)										Spearphishing Attachment (9)										PowerShell (14)										LSASS Driver (19)										Deobfuscate/Decode Files or Information (11)										Browser Discovery (17)																																																																					
Search Cloud Sources (10)										Code Signing Certificates (8)										Spearphishing Link (9)										Python (14)										Port Monitors (19)										Deploy Container (11)										Credentials from Web Browsers (17)																																																																					
Search Open Technical Databases (10)										Digital Certificates (8)										Spearphishing via Service (9)										Unix Shell (14)										Print Processors (19)										Direct Volume Access (11)										Keychain (17)																																																																					
Search Open Websites/Domain (10)										Exploits (8)																				Visual Basic (14)										Re-opened Applications (19)										Domain Policy Modification (11)										Cloud in Discovery (17)																																																																					
Search Victim-Owned Websites (10)										Malware (8)																				Windows Command Shell (14)										Registry Run Keys / Startup Folder (19)										Execution Guardrails (11)										Cloud Service Dashboard (17)																																																																					
										Tool (8)																														Security Support Provider (19)										Exploitation for Credential Access (11)										Container Resource (17)																																																																					
										Vulnerabilities (8)																														Shortcut Modification (19)										Exploitation for Defense Evasion (11)										Container Resource (17)																																																																					
										Trusted Relationship (8)																														Time Providers (19)										File and Directory Permissions (11)										Debugger (17)																																																																					
										Valid (8)																														Winlogon Helper DLL (19)																																																																																									

Adversary Emulation

Local Job Scheduling		Access Token Manipulation		Credential Access
Trap		Bypass User Account Control		Forced Authentication
Launchctl		Process Injection		Hooking
Signed Binary Proxy Execution User Execution Exploitation for Client Execution	Image File Execution Options Injection		Password Filter DLL	
	Plist Modification		LLMNR/NBT-NS	
	Valid Accounts		Poisoning	
	DLL Search Order Hijacking		Private Keys	
CMSTP	AppCert DLLs	Signed Script Proxy Execution	Keychain	
Dynamic Data Exchange	Hooking	DCShadow	Input Prompt	
Mshta	Startup Items	Port Knocking	Bash History	
AppleScript	Launch Daemon	Indirect Command Execution	Two-Factor Authentication Interception	
Source	Dylib Hijacking	BITS Jobs Control Panel Items CMSTP Process Doppelgänger	Replication Through Removable Media	
Space after Filename	Application Shimming		Input Capture	
Execution through Module Load	Applnit DLLs		Network Sniffing	
Regsvcs/Regasm	Web Shell			
	Service Registry Permissions Weakness			
	New Service			

Cyber Threat Intelligence (CTI)



- To defend an organizational cyber infrastructure, you need to know
 - Who might be attacking you and their motivations
 - Frequency and volume of the attacks
 - The various attack surfaces they tend to exploit
 - The tactics used by different groups of attackers
 - The techniques they use to implement their tactics
 - The procedures they use to make the technique work
 - What kind of malware they use
 - Their Command-and-Control Infrastructure
 - Indicators of compromise
 - Artifacts – e.g. IP addresses, URLs, Malware, credentials, files. Certificates etc.



ATT&CK and CTI

- Knowledge of Adversary behaviour is helpful in planning defence
- Structuring CTI with ATT&CT TTPs help us:
 - Compare behaviours
 - Between threat groups
 - Same group over time
 - Groups to defences
 - Communicate in a common language for sharing CTI across organizations



Communicating to defenders

- APT 18 used legitimate credentials to log into external remote services
- APT 29 used compromised identities to access networks via VPNs and Citrix
- APT 41 compromised an online billing/payment service using VPN access between a 3rd party service provider and the targeted payment service
- All are using T1133 (External Remote Services) technique