Mitre ATT&CK

Mariano Ceccato

mariano.ceccato@univr.it

Lecture Outline

- MITRE PRE-ATT&CK and ATT&CK models
  - Tactics
  - Techniques and Sub-Techniques
  - Procedures
  - Groups

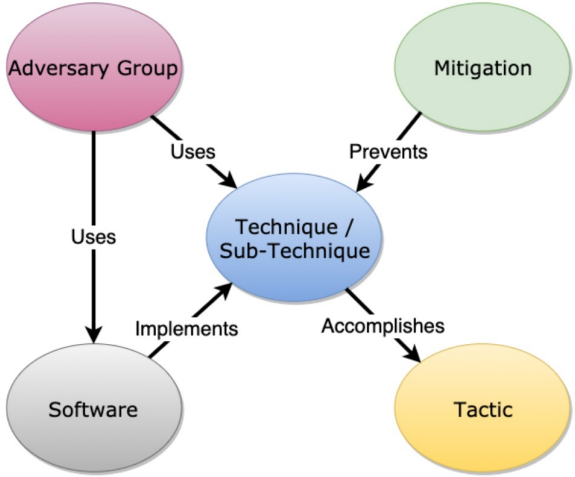
What is ATT&CK

- A globally accessible knowledge base of adversary tactics and techniques
  - On how adversaries compromise and operate within computer information networks
- Common taxonomy for both offense and defense
- Foundation for the development of specific threat models and methodologies
  - In the private sector
  - in government
  - in the cybersecurity product and service community

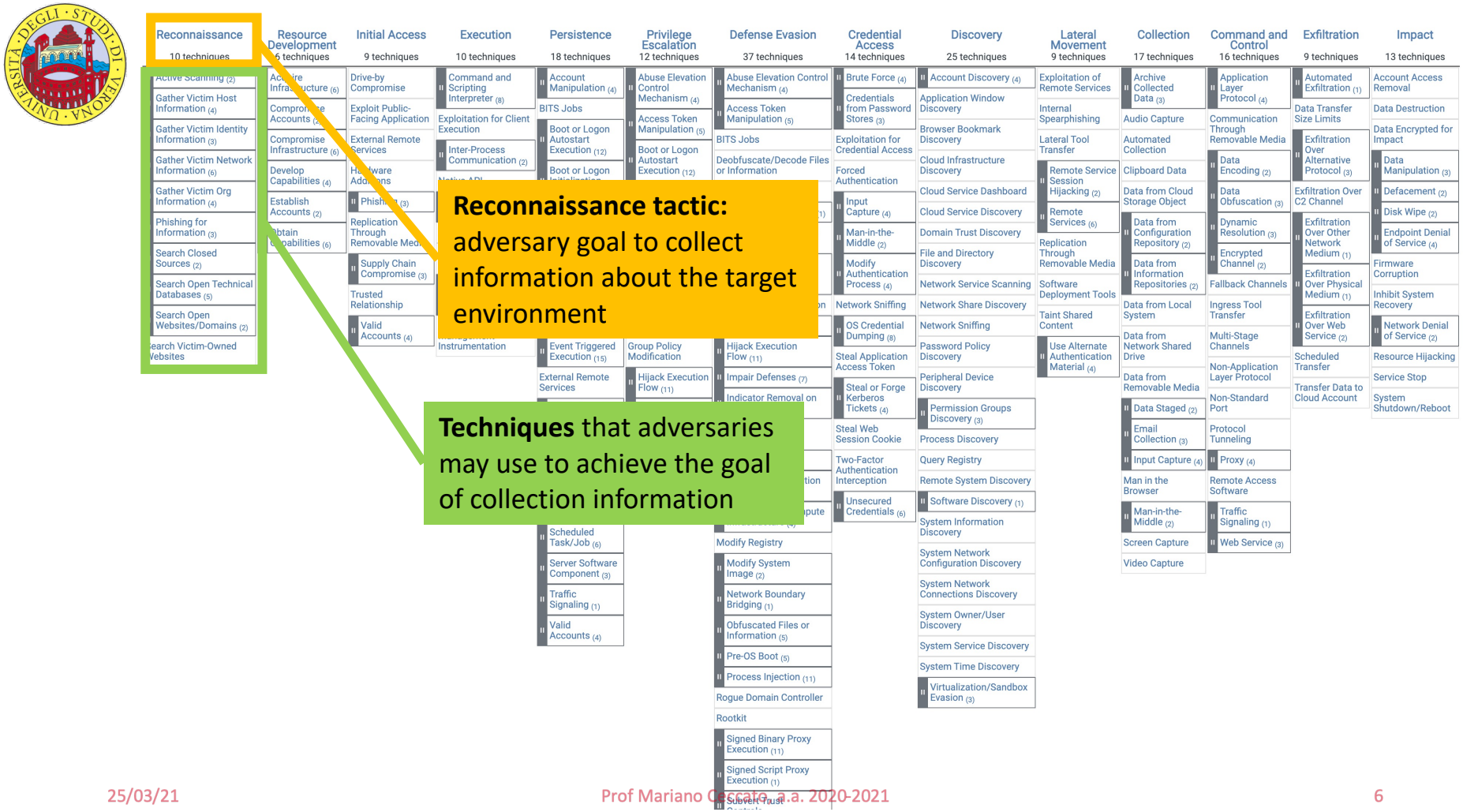
Data sources

- Community based contributions, based on real-world observations
- Publicly reported incidents on suspected APT group behavior
  - Threat intelligence analysts typically track incidents, threat groups
- Defenders see adversaries in action and are often in a position to see when new techniques are being used
  - Threat hunters
  - Malware analysts
  - Incident responders
- Techniques discovered and reported through offensive research into areas that adversaries and red teams are likely to leverage against enterprise networks
  - Red teams provide a useful source of information on how techniques are done

ATT&CK Matrix



- **Tactics**: short-term, tactical adversary goals during an attack;
- **Techniques:** means by which adversaries achieve tactical goals;
- **Groups:** known adversaries that are tracked and reported on in threat intelligences reports
- **Software**: commonly used during intrusions (instantiation of a technique or sub-technique)
- **Mitigations**: security concepts and technologies that can be used to prevent a technique or sub-technique from being successfully executed


Reconnaissance
10 techniques
Active Scanning (2)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (2)
Search Victim-Owned Websites
Resource Development
6 techniques
Compromise Infrastructure (6)
Develop Capabilities (4)
Establish Accounts (2)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
10 techniques
Command and Scripting Interpreter (8)
Exploitation for Client Execution
Inter-Process Communication (2)
Instrumentation
Persistence
18 techniques
Account Manipulation (4)
BITS Jobs
Boot or Logon Autostart Execution (12)
Event Triggered Execution (15)
External Remote Services
Scheduled Task/Job (6)
Server Software Component (3)
Traffic Signaling (1)
Valid Accounts (4)
Privilege Escalation
12 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (12)
Group Policy Modification
Hijack Execution Flow (11)
Defense Evasion
37 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Deobfuscate/Decode Files or Information
Hijack Execution Flow (11)
Impair Defenses (7)
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Obfuscated Files or Information (5)
Pre-OS Boot (5)
Process Injection (11)
Rogue Domain Controller
Rootkit
Signed Binary Proxy Execution (11)
Signed Script Proxy Execution (1)
Credential Access
14 techniques
Brute Force (4)
Credentials from Password Stores (3)
Exploitation for Credential Access
Forced Authentication
Input Capture (4)
Man-in-the-Middle (2)
Modify Authentication Process (4)
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (6)
Discovery
25 techniques
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service 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 (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Archive Collected Data (3)
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (2)
Data from Information Repositories (2)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Man in the Browser
Man-in-the-Middle (2)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (1)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot
Reconnaissance tactic: adversary goal to collect information about the target environment
Techniques that adversaries may use to achieve the goal of collection information

Tactic “Reconnaissance”

Reconnaissance

The adversary is trying to gather information they can use to plan future operations.

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

ID: TA0043
Created: 02 October 2020
Last Modified: 18 October 2020

Version Permalink

Techniques

Techniques: 10

ID	Name	Description
T1595	Active Scanning	Before compromising a victim, adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
.001	Scanning IP Blocks	Before compromising a victim, adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.
.002	Vulnerability Scanning	Before compromising a victim, adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.
T1592	Gather Victim Host Information	Before compromising a victim, adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.).
.001	Hardware	Before compromising a victim, adversaries may gather information about the victim's host hardware that can be used during targeting. Information about hardware infrastructure may include a variety of details such as types and versions on specific hosts, as well as the presence of additional components that might be indicative of added defensive protections (ex: card/biometric readers, dedicated encryption hardware, etc.).
.002	Software	Before compromising a victim, adversaries may gather information about the victim's host software that can be used during targeting. Information about installed software may include a variety of details such as types and versions on specific hosts, as well as the presence of additional components that might be indicative of added defensive protections (ex: antivirus, SIEMs, etc.).

Technique “Gather Victim Identity Information”

Gather Victim Identity Information

Sub-techniques (3)

Before compromising a victim, adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials.

Adversaries may gather this information in various ways, such as direct elicitation via Phishing for Information. Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: Social Media or Search Victim-Owned Websites).[1][2][3][4][5][6][7][8] Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Phishing for Information), establishing operational resources (ex: Compromise Accounts), and/or initial access (ex: Phishing or Valid Accounts).

ID: T1589
Sub-techniques: T1589.001, T1589.002, T1589.003
Tactic: Reconnaissance
Platforms: PRE
Version: 1.0
Created: 02 October 2020
Last Modified: 27 October 2020

Mitigations

Mitigation	Description
Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

Sub-technique: “Email Addresses”

Gather Victim Identity Information: Email Addresses

Other sub-techniques of Gather Victim Identity Information (3)

Before compromising a victim, adversaries may gather email addresses that can be used during targeting. Even if internal instances exist, organizations may have public-facing email infrastructure and addresses for employees.

Adversaries may easily gather email addresses, since they may be readily available and exposed via online or other accessible data sets (ex: Social Media or Search Victim-Owned Websites).[1][2] Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Phishing for Information), establishing operational resources (ex: Email Accounts), and/or initial access (ex: Phishing).

ID: T1589.002
Sub-technique of: T1589
Tactic: Reconnaissance
Platforms: PRE
Version: 1.0
Created: 02 October 2020
Last Modified: 24 October 2020

Mitigations

Mitigation	Description
Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

Technique: “Phishing”

Phishing

Sub-techniques (3)

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems or to gather credentials for use of Valid Accounts. Phishing may also be conducted via third-party services, like social media platforms.

ID: T1566

Sub-techniques: T1566.001, T1566.002, T1566.003

Tactic: Initial Access

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

Data Sources: Anti-virus, Detonation chamber, Email gateway, File monitoring, Mail server, Network intrusion detection system, Packet capture, SSL/TLS inspection, Web proxy

CAPEC ID: CAPEC-98

Version: 2.0

Created: 02 March 2020

Last Modified: 18 October 2020

Sub-technique: “Spearphishing Attachment”

Phishing: Spearphishing Attachment

Other sub-techniques of Phishing (3)

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

ID: T1566.001

Sub-technique of: T1566

Tactic: Initial Access

Platforms: Linux, Windows, macOS

Data Sources: Detonation chamber, Email gateway, File monitoring, Mail server, Network intrusion detection system, Packet capture

CAPEC ID: CAPEC-163

Version: 2.0

Created: 02 March 2020

Last Modified: 18 October 2020

Procedures

Procedure Examples

Name	Description
admin@338	admin@338 has sent emails with malicious Microsoft Office documents attached.[1]
APT-C-36	APT-C-36 has used spearphishing emails with password protected RAR attachment to avoid being detected by the email gateway.[2]
APT1	APT1 has sent spearphishing emails containing malicious attachments.[3]
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached.[4][5]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits.[6]
APT28	APT28 sent spearphishing emails containing malicious Microsoft Office attachments.[7][8][9][10][11][12]
APT29	APT29 has used spearphishing emails with an attachment to deliver files with exploits to initial victims.[13][14][15]
APT30	APT30 has used spearphishing emails with malicious DOC attachments.[16]
APT32	APT32 has sent spearphishing emails with a malicious executable disguised as a document or spreadsheet.[17][18][19][20][21]
APT33	APT33 has sent spearphishing e-mails with archive attachments.[22]
APT37	APT37 delivers malware using spearphishing emails with malicious HWP attachments.[23][24][25]
APT39	APT39 leveraged spearphishing emails with malicious attachments to initially compromise victims. [26][27]
APT41	APT41 sent spearphishing emails with attachments such as compiled HTML (.chm) files to initially compromise their victims.[28]

Mitigation and detection

Mitigations

Mitigation	Description
Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.
Restrict Web-Based Content	Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.
User Training	Users can be trained to identify social engineering techniques and spearphishing emails.

Detection

Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Detonation chambers may also be used to identify malicious attachments. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Anti-virus can potentially detect malicious documents and attachments as they're scanned to be stored on the email server or on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the attachment is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as Exploitation for Client Execution or usage of malicious scripts.

Group: Dragonfly 2.0

Dragonfly 2.0

Dragonfly 2.0 is a suspected Russian group that has targeted government entities and multiple U.S. critical infrastructure sectors since at least March 2016. [1] [2] There is debate over the extent of overlap between Dragonfly 2.0 and Dragonfly, but there is sufficient evidence to lead to these being tracked as two separate groups. [3][4]

ID: G0074

Associated Groups: IRON LIBERTY, DYMALLOY, Berserk Bear

Version: 1.3

Created: 17 October 2018

Last Modified: 15 October 2020

Group: Dragonfly 2.0

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087	.002	Account Discovery: Domain Account	Dragonfly 2.0 used batch scripts to enumerate users on a victim domain controller.[1]
Enterprise	T1098		Account Manipulation	Dragonfly 2.0 added newly created accounts to the administrators group to maintain elevated access.[1][7]
Enterprise	T1071		Application Layer Protocol	Dragonfly 2.0 used SMB for C2.[1]
Enterprise	T1560		Archive Collected Data	Dragonfly 2.0 compressed data into .zip files prior to exfiltrating it.[1]
Enterprise	T1547	.009	Boot or Logon Autostart Execution: Shortcut Modification	Dragonfly 2.0 manipulated .lnk files to gather user credentials in conjunction with Forced Authentication.[1]
		.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Dragonfly 2.0 added the registry value ntdll to the Registry Run key to establish persistence.[1]
Enterprise	T1110	.002	Brute Force: Password Cracking	Dragonfly 2.0 dropped and executed tools used for password cracking, including Hydra and CrackMapExec.[1][7][8]
Enterprise	T1059		Command and Scripting Interpreter	Dragonfly 2.0 used command line for execution.[1]
		.003	Windows Command Shell	Dragonfly 2.0 used various types of scripting to perform operations, including batch scripts.[1][7]
		.001	PowerShell	Dragonfly 2.0 used PowerShell scripts for execution.[1][2][7]
		.006	Python	Dragonfly 2.0 used various types of scripting to perform operations, including Python scripts. The group was observed installing Python 2.7 on a victim.[1][7]
Enterprise	T1136	.001	Create Account: Local Account	Dragonfly 2.0 created accounts on victims, including administrator accounts, some of which appeared to be tailored to each individual staging target.[1][7]
Enterprise	T1005		Data from Local System	Dragonfly 2.0 collected data from local victim systems.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	Dragonfly 2.0 created a directory named "out" in the user's %AppData% folder and copied files to it.[1]

Software

Software

ID	Name	References	Techniques
S0488	CrackMapExec	[1]	Account Discovery: Domain Account, Brute Force: Password Guessing, Brute Force, Brute Force: Password Spraying, Command and Scripting Interpreter: PowerShell, File and Directory Discovery, Modify Registry, Network Share Discovery, OS Credential Dumping: NTDS, OS Credential Dumping: LSA Secrets, OS Credential Dumping: Security Account Manager, Password Policy Discovery, Permission Groups Discovery: Domain Groups, Remote System Discovery, Scheduled Task/Job: At (Windows), System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, Use Alternate Authentication Material: Pass the Hash, Windows Management Instrumentation
S0357	Impacket	[1][7][9]	Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Network Sniffing, OS Credential Dumping: Security Account Manager, OS Credential Dumping: LSASS Memory, OS Credential Dumping: NTDS, OS Credential Dumping: LSA Secrets, Steal or Forge Kerberos Tickets: Kerberoasting, System Services: Service Execution, Windows Management Instrumentation
S0500	MCMD	[5]	Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, Hide Artifacts: Hidden Window, Indicator Removal on Host, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Obfuscated Files or Information, Scheduled Task/Job: Scheduled Task
S0039	Net	[1]	Account Discovery: Local Account, Account Discovery: Domain Account, Create Account: Local Account, Create Account: Domain Account, Indicator Removal on Host: Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery: Local Groups, Permission Groups Discovery: Domain Groups, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, System Time Discovery
S0108	netsh	[1]	Event Triggered Execution: Netsh Helper DLL, Impair Defenses: Disable or Modify System Firewall, Proxy, Software Discovery: Security Software Discovery
S0029	PsExec	[1][2]	Lateral Tool Transfer, Remote Services: SMB/Windows Admin Shares, System Services: Service Execution
S0075	Reg	[1]	Modify Registry, Query Registry, Unsecured Credentials: Credentials in Registry
S0094	Trojan.Karagany	[2][10]	Application Layer Protocol: Web Protocols, Application Window Discovery, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Credentials from Password Stores: Credentials from Web Browsers, Data Staged: Local Data Staging, Encrypted Channel: Asymmetric Cryptography, File and Directory Discovery, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Input Capture: Keylogging, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information, OS Credential Dumping, Process Discovery, Process Injection: Thread Execution Hijacking, Screen Capture, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Owner/User Discovery, Virtualization/Sandbox Evasion: System Checks

Resources

- MITRE ATT&CK Matrix https://attack.mitre.org/matrices/enterprise/
- MITRE ATT&CK: Design and Philosophy, MITRE Corporation
- MITRE, Getting started with ATT&CK