MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

ATT&CK®

Jamie Williams

ATT&CK for Enterprise Lead

Principal Adversary Emulation Engineer

Key Takeaways

ATT&CK®

Can help you

See the threats

Track and understand their behaviors

Orient your defensive recommendations towards behaviors

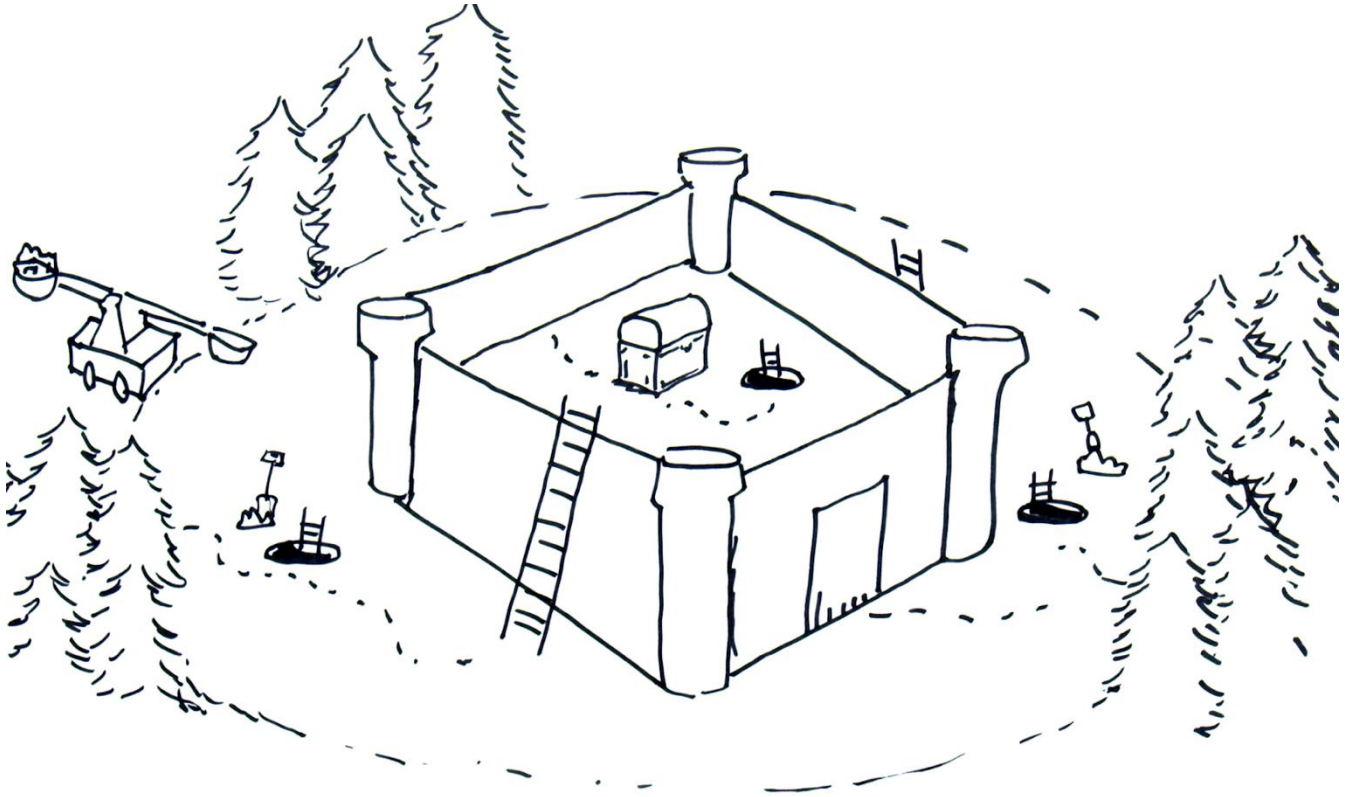
See The Threats

How Do We Measure Security?

- How effective are my defenses?
- Do I have a chance at detecting **{insert threat}**?
- Is the data I'm collecting useful?
- What risks does **{insert decision}** expose?

Threat-Informed Defense

Knowledge of my adversary can help me…

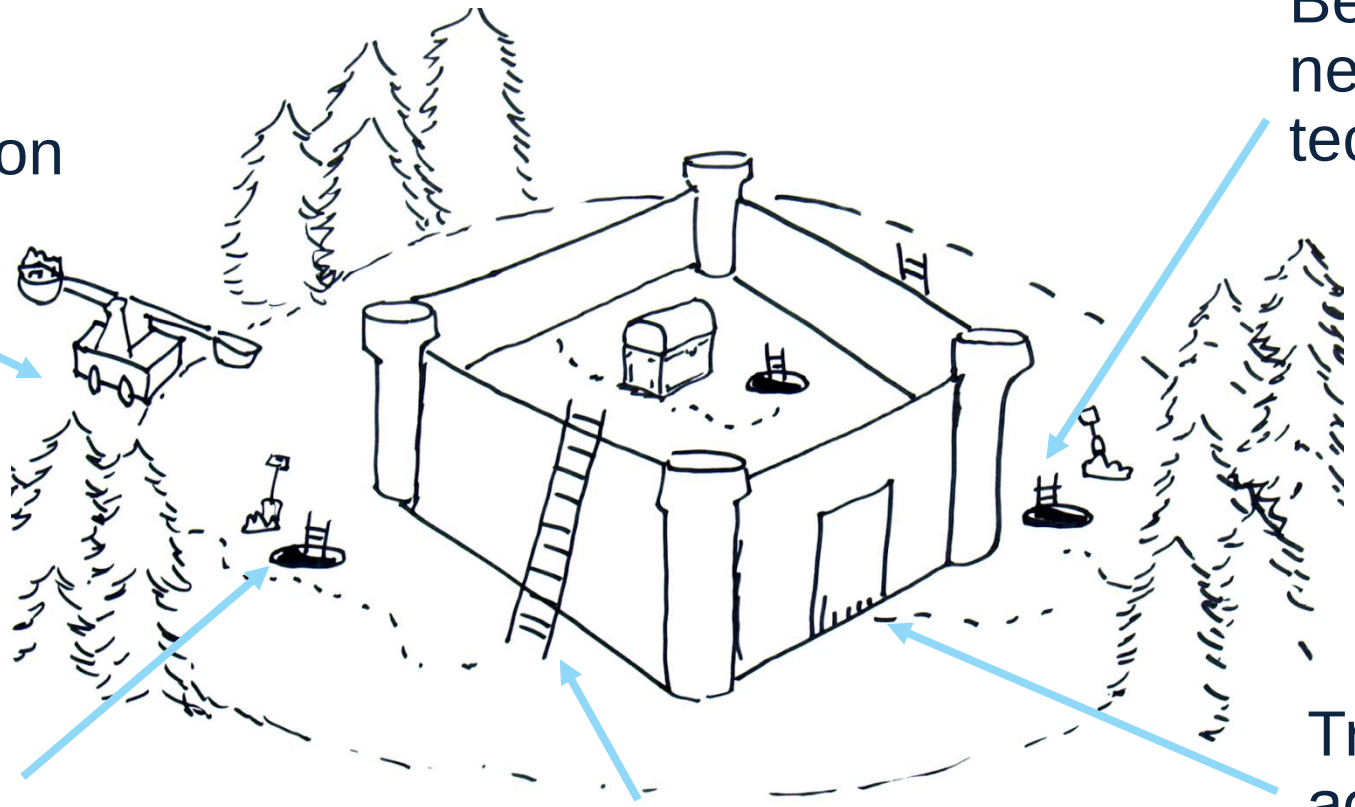


Threat-Informed Defense

Knowledge of my adversary can help me…

Prioritize detection/mitigation of heavily used techniques

Better evaluate new security technologies



See defenses from an adversary's perspective

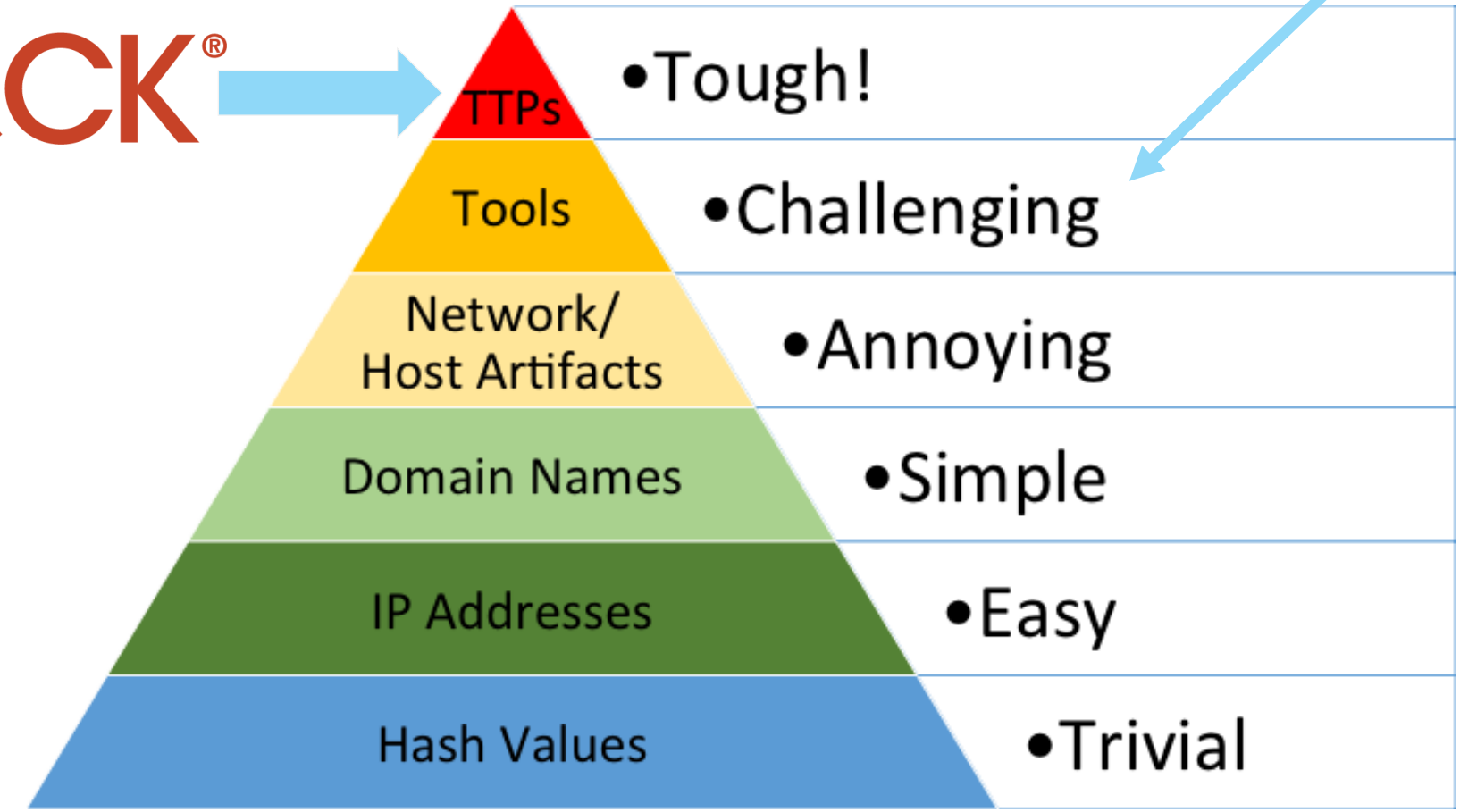
Perform gap analysis of current defenses

Track a specific adversary's set of techniques

How Do We Describe Adversaries?

Difficulty/cost for the adversary to modify their activity

ATT&CK®



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

ATT&CK®

ATT&CK is a **globally-accessible** knowledge base of adversary tactics and techniques, developed by MITRE **based on real-world observations** of adversaries' operations.

ATT&CK is increasingly being used by the community as a **common language** to describe adversary behavior.

attack.mitre.org

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Container and Resource Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deploy Container	Forge Web Credentials	File and Directory Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Direct Volume Access	Input Capture	Group Policy Discovery	Software Deployment Tools	Data from Configuration Repository	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Domain Policy Modification	Modify Authentication Process	Network Service Scanning	Taint Shared Content	Data from Information Repositories	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Execution Guardrails	Network Sniffing	Network Share Discovery	Use Alternate Authentication Material	Data from Local System	Multi-Stage Channels		Inhibit System Recovery
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow	Exploitation for Defense Evasion	OS Credential Dumping	Network Sniffing		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service
			User Execution	Hijack Execution Flow	Process Injection	File and Directory Permissions Modification	Steal or Forge Kerberos Tickets	Password Policy Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	Hide Artifacts	Steal Web Session Cookie	Peripheral Device Discovery		Data Staged	Protocol Tunneling		Service Stop
				Modify Authentication Process	Valid Accounts	Hijack Execution Flow	Two-Factor Authentication Interception	Permission Groups Discovery		Email Collection	Proxy		System Shutdown/Reboot
				Office Application Startup		Impair Defenses	Unsecured Credentials	Process Discovery		Input Capture	Remote Access Software		
				Pre-OS Boot		Indicator Removal on Host		Query Registry		Screen Capture	Traffic Signaling		
				Scheduled Task/Job		Indirect Command Execution		Remote System Discovery		Video Capture	Web Service		
				Server Software Component		Masquerading		Software Discovery					
				Traffic Signaling		Modify Authentication Process		System Information Discovery					
				Valid Accounts		Modify Registry		System Location Discovery					
						Modify System Image		System Network Configuration Discovery					
						Network Boundary Bridging		System Network Connections Discovery					
						Obfuscated Files or Information		System Owner/User Discovery					
						Pre-OS Boot		System Service Discovery					
						Process Injection		System Time Discovery					
						Reflective Code Loading		Virtualization/Sandbox Evasion					
						Rogue Domain Controller							
						Rootkit							
						Signed Binary Proxy Execution							
						Signed Script Proxy Execution							
						Subvert Trust Controls							
						Template Injection							
						Traffic Signaling							
						Trusted Developer Utilities Proxy Execution							
						Use Alternate Authentication Material							
						Valid Accounts							
						Virtualization/Sandbox Evasion							
						Weaken Encryption							
						XSL Script Processing							

Tactic: Adversary's technical goal

Technique: How the adversary achieves the goal

Procedure: What the adversary did

User Execution: Malicious File

Other sub-techniques of User Execution (3)

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Attachment. Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl.

Adversaries may employ various forms of Masquerading and Obfuscated Files or Information to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.[1]

While Malicious File frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after Internal Spearphishing.

ID: T1204.002
Sub-technique of: T1204
Tactic: Execution
Platforms: Linux, Windows, macOS
Contributors: TruKno
Version: 1.2
Created: 11 March 2020
Last Modified: 20 May 2022

Version Permalink

What is the behavior?

Real-world examples

LOWBALL Malware Analysis

The spear phishing emails contained three attachments in total, each of which exploited an older vulnerability in Microsoft Office (CVE-2012-0158):

MD5	Filename
b9208a5b0504cb2283b1144fc455eaaa	使命公民運動 我們的異象.doc
ec19ed7cddf92984906325da59f75351	新聞稿及公佈.doc
6495b384748188188d09e9d5a0c401a4	(代發)[采訪通知]港大校友關注組遞信行動.doc

Procedure Examples

ID	Name	Description
G0018	admin@338	admin@338 has attempted to get victims to launch malicious Microsoft Word attachments delivered via spearphishing emails.[2]
S0331	Agent Tesla	Agent Tesla has been executed through malicious e-mail attachments [3]
G0130	Ajax Security Team	Ajax Security Team has lured victims into executing malicious files.[4]
G0138	Andariel	Andariel has attempted to lure victims into enabling malicious macros within email attachments.[5]
S0584	AppleJeus	AppleJeus has required user execution of a malicious MSI installer.[6]

Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria). Note: cloud-delivered protection must be enabled for certain rules. [225]
M1038	Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
M1017	User Training	Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.

Detection

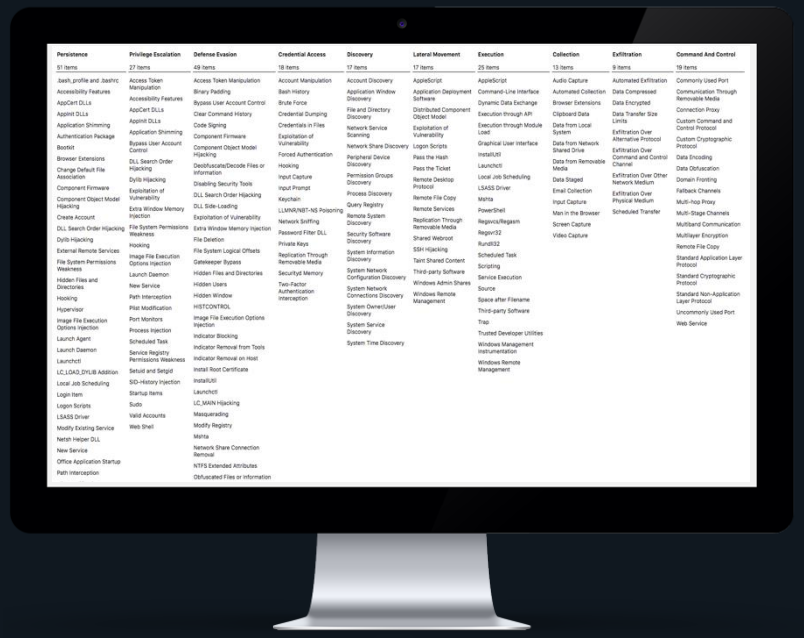
ID	Data Source	Data Component	Detects
DS0022	File	File Creation	Monitor for newly constructed files that are downloaded and executed on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning powershell.exe).
DS0009	Process	Process Creation	Monitor for newly constructed processes and/or command-lines for applications that may be used by an adversary to gain initial access that require user interaction. This includes compression applications, such as those for zip files, that can be used to Deobfuscate/Decode Files or Information in payloads.

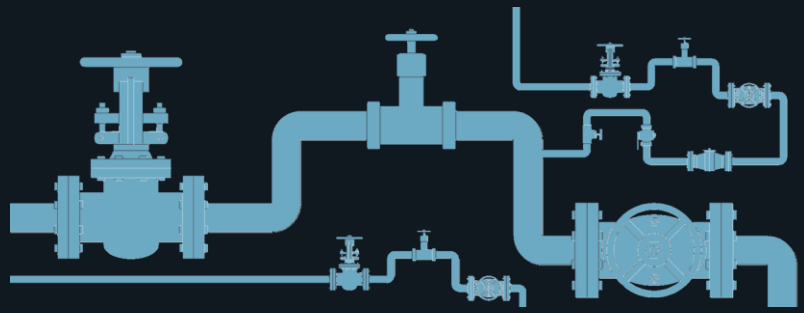
How we can defend

As of April 2022:

- 150+ Techniques
- 350+ Sub-Techniques
- 100+ Groups
- 600+ Software

ATT&CK Spans Multiple Technology Domains





Enterprise:
Windows, Linux, macOS, Cloud, Network, Containers, PRE

Mobile:
Android, iOS

ATT&CK for ICS

Track And Understand Their Behaviors

ATT&CK Provides

1. Context to understand TTPs

2. A common language for describing and sharing TTPs

1. Context to Understand TTPs

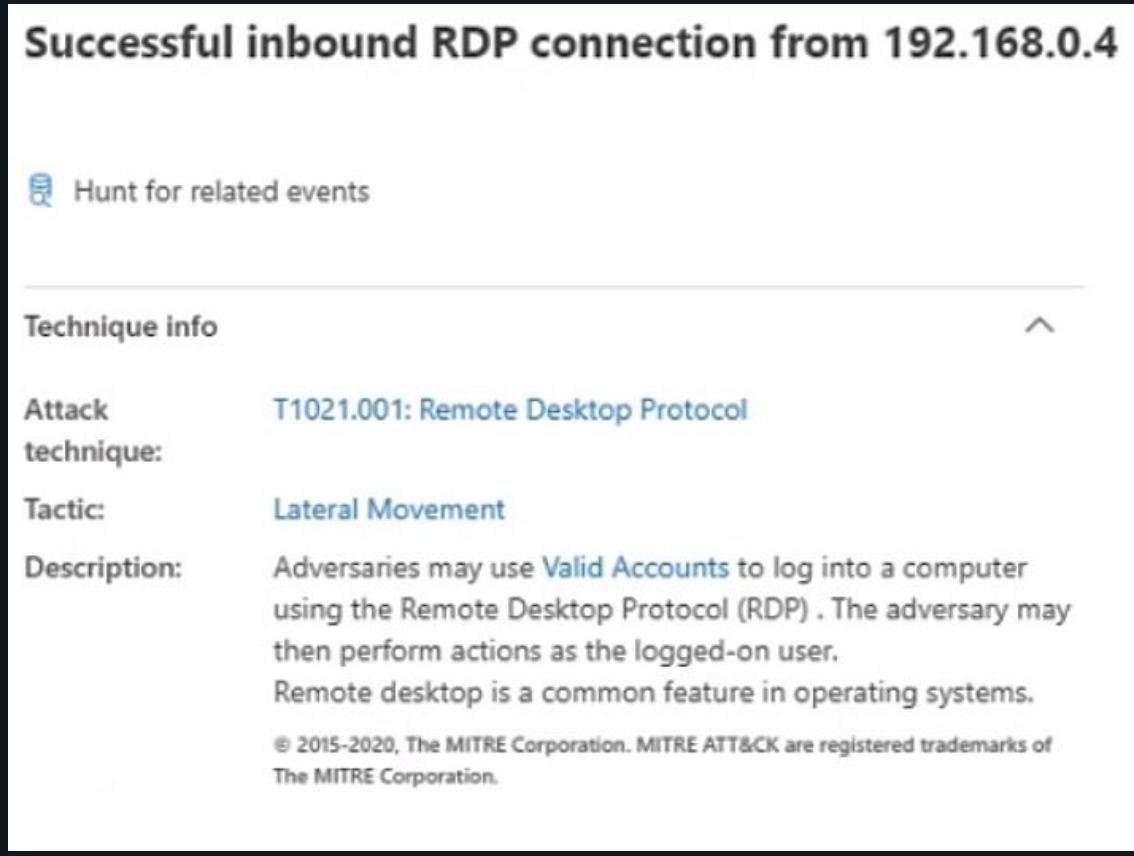
T1059 .003

T1027

```
cmd.exe /c mofcomp.exe C:\Windows\SERVIC~1\MSSQL$~1\AppData\Local\Temp\xitmf
```

T1546 .003

Source: The DFIR Report https://thedfirreport.com



Source: ATT&CK Evaluations https://attackevals.mitre-engenuity.org

2. A Common Language for Describing and Sharing TTPs

JOINT
CYBERSECURITY ADVISORY

CISA | FBI | NSA | USSS

TLP:WHITE

To secure systems against Conti ransomware, CISA, FBI, and the National Security Agency (NSA) recommend implementing the mitigation measures described in this Advisory, which include requiring multifactor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date.

Click here for indicators of compromise (IOCs) in STIX format.

Note: *This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.*

TECHNICAL DETAILS

While Conti is considered a ransomware-as-a-service (RaaS) model ransomware variant, there is variation in its structure that differentiates it from a typical affiliate model. It is likely that Conti developers pay the deployers of the ransomware a wage rather than a percentage of the proceeds from a successful attack.

Conti actors often gain initial access [TA0001] to networks through:

- Spearphishing campaigns using tailored emails that contain malicious attachments [T1566.001] or malicious links [T1566.002];
  - Malicious Word attachments often contain embedded scripts that can be used to download or drop other malware—such as TrickBot and IcedID, and/or Cobalt Strike—to assist with lateral movement and later stages of the attack life cycle with the eventual goal of deploying Conti ransomware.[1],[2],[3]
- Stolen or weak Remote Desktop Protocol (RDP) credentials [T1078];[4]

Conti ransomware uses the ATT&CK techniques listed in table 1.

Table 1: Conti ATT&CK techniques for enterprise

Initial Access		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	Conti actors have been observed gaining unauthorized access to victim networks through stolen Remote Desktop Protocol (RDP) credentials.
Phishing: Spearphishing Attachment	T1566.001	Conti ransomware can be delivered using TrickBot malware, which is known to use an email with an Excel sheet containing a malicious macro to deploy the malware.
Phishing: Spearphishing Link	T1566.002	Conti ransomware can be delivered using TrickBot, which has been delivered via malicious links in phishing emails.
Execution		
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Conti ransomware can utilize command line options to allow an attacker control over how it scans and encrypts files.

Source: Joint Cybersecurity Advisory https://media.defense.gov/2021/Sep/22/2002859507/-1/-1/0/CSA_Conti_Ransomware_20220309.PDF

Orient Your Defensive Recommendations Towards Behaviors

ATT&CK Provides

1. A medium to measure yourself

2. Means to identify gaps and prioritize operations

A Medium to Measure Yourself

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application	Command and Scripting Interpreter	Server Software Component	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Unsecured Credentials	Network Service Scanning	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Exfiltration Over Alternative Protocol	Data Manipulation
Valid Accounts	Software Deployment Tools	Valid Accounts	Valid Accounts	Valid Accounts	Adversary-in-the-Middle	Network Sniffing	Software Deployment Tools	Data from Information Repositories	Remote Access Software	Exfiltration Over Physical Medium	Firmware Corruption
Drive-by Compromise	Inter-Process Communication	Create or Modify System Process	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Exploitation for Credential Access	Domain Trust Discovery	Remote Service Session Hijacking	Automated Collection	Proxy	Exfiltration Over C2 Channel	Service Stop
External Remote Services	Windows Management Instrumentation	Hijack Execution Flow	Create or Modify System Process	Indicator Removal on Host	OS Credential Dumping	Password Policy Discovery	Remote Services	Data from Removable Media	Encrypted Channel	Exfiltration Over Web Service	Inhibit System Recovery
Phishing	Exploitation for Client Execution	Pre-OS Boot	Escape to Host	Hijack Execution Flow	Steal or Forge Kerberos Tickets	Account Discovery	Lateral Tool Transfer	Browser Session Hijacking	Non-Application Layer Protocol	Data Transfer Size Limits	Data Encrypted for Impact
Replication Through Removable Media	Scheduled Task/Job	External Remote Services	Hijack Execution Flow	Pre-OS Boot	Modify Authentication Process	Network Share Discovery	Replication Through Removable Media	Email Collection	Protocol Tunneling	Scheduled Transfer	Data Destruction
Supply Chain Compromise	System Services	Modify Authentication Process	Scheduled Task/Job	Subvert Trust Controls	Brute Force	Application Window Discovery	Taint Shared Content	Data from Local System	Traffic Signaling	Exfiltration Over Other Network Medium	Defacement
Trusted Relationship	User Execution	Browser Extensions	Domain Policy Modification	Signed Binary Proxy Execution	Network Sniffing	Browser Bookmark Discovery	Use Alternate Authentication Material	Archive Collected Data	Communication Through Removable Media	Automated Exfiltration	Disk Wipe
Hardware Additions	Native API	Create Account	Process Injection	Impair Defenses	Forced Authentication	File and Directory Discovery	Internal Spearphishing	Audio Capture	Dynamic Resolution		Endpoint Denial of Service
	Shared Modules	Scheduled Task/Job	Boot or Logon Initialization Scripts	Modify Authentication Process	Steal Web Session Cookie	Group Policy Discovery		Clipboard Data	Fallback Channels		Network Denial of Service
		BITS Jobs	Access Token Manipulation	BITS Jobs	Forge Web Credentials	Peripheral Device Discovery		Data from Network Shared Drive	Ingress Tool Transfer		Account Access Removal
		Office Application Startup	Event Triggered Execution	Template Injection	Two-Factor Authentication Interception	Permission Groups Discovery		Data Staged	Multi-Stage Channels		Resource Hijacking
		Account Manipulation	Boot or Logon Autostart Execution	Domain Policy Modification	Credentials from Password Stores	Process Discovery		Input Capture	Non-Standard Port		System Shutdown/Reboot
		Boot or Logon Initialization Scripts		Masquerading	Input Capture	Query Registry		Screen Capture	Web Service		
		Compromise Client Software Binary		Process Injection		Remote System Discovery		Video Capture	Data Encoding		
		Traffic Signaling		File and Directory Permissions Modification		Software Discovery			Data Obfuscation		
		Event Triggered Execution		Traffic Signaling		System Information Discovery					
		Boot or Logon Autostart Execution		Trusted Developer Utilities Proxy Execution		System Location Discovery					
				Access Token Manipulation		System Network Configuration Discovery					
				Use Alternate Authentication Material		System Network Connections Discovery					
				Obfuscated Files or Information		System Owner/User Discovery					
				Signed Script Proxy Execution		System Service Discovery					
				XSL Script Processing		System Time Discovery					
				Modify Registry		Virtualization/Sandbox Evasion					
				Deobfuscate/Decode Files or Information							
				Direct Volume Access							
				Execution Guardrails							
				Hide Artifacts							
				Indirect Command Execution							
				Reflective Code Loading							
				Rogue Domain Controller							
				Rootkit							
				Virtualization/Sandbox Evasion							

Source: NIST 800-53 Controls to ATT&CK Mappings https://ctid.mitre-engenuity.org/our-work/nist-800-53-control-mappings

MITRE

A Medium to Measure Yourself

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application	Command and Scripting Interpreter	Server Software						Adversary-in-the-Middle	Application Layer Protocol	Exfiltration Over Alternative Protocol	Data Manipulation
Valid Accounts	Software Deployment Tools	Valid Acc						Data from Information Repositories	Remote Access Software	Exfiltration Over Physical Medium	Firmware Corruption
Drive-by Compromise	Inter-Process Communication	Create or Mod Proces						Automated Collection	Proxy	Exfiltration Over C2 Channel	Service Stop
External Remote Services	Windows Management Instrumentation	Hijack Execut						ata from Removable Media	Encrypted Channel	Exfiltration Over Web Service	Inhibit System Recovery
Phishing	Exploitation for Client Execution	Pre-OS B						Browser Session Hijacking	Non-Application Layer Protocol	Data Transfer Size Limits	Data Encrypted for Impact
Replication Through Removable Media	Scheduled Task/Job	External Remot						Email Collection	Protocol Tunneling	Scheduled Transfer	Data Destruction
								Data from Local System	Traffic Signaling	Exfiltration Over Other Network Medium	Defacement
								Archive Collected Data	Communication Through Removable Media	Automated Exfiltration	Disk Wipe
								Audio Capture	Dynamic Resolution		Endpoint Denial of Service
								Clipboard Data	Fallback Channels		Network Denial of Service
								Data from Network Shared Drive	Ingress Tool Transfer		Account Access Removal
								Data Staged	Multi-Stage Channels		Resource Hijacking
								Input Capture	Non-Standard Port		System Shutdown/Reboot
								Screen Capture	Web Service		
								Video Capture	Data Encoding		
									Data Obfuscation		

Supply Chain Compromise (T1195)

CA-2	Control Assessments
CA-7	Continuous Monitoring
CM-11	User-installed Software
CM-7	Least Functionality
RA-10	Threat Hunting
RA-5	Vulnerability Monitoring and Scanning
SA-22	Unsupported System Components
SI-2	Flaw Remediation

Boot or Logon Execution

Proxy Execution
Access Token Manipulation
Use Alternate Authentication Material
Obfuscated Files or Information
Signed Script Proxy Execution
XSL Script Processing
Modify Registry
Deobfuscate/Decode Files or Information
Direct Volume Access
Execution Guardrails
Hide Artifacts
Indirect Command Execution
Reflective Code Loading
Rogue Domain Controller
Rootkit
Virtualization/Sandbox Evasion

System Location Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion

Source: NIST 800-53 Controls to ATT&CK Mappings https://ctid.mitre-engenuity.org/our-work/nist-800-53-control-mappings

MITRE

Means to Identify Gaps and Prioritize Operations

Tactic	Common Techniques	Log and Event Sources	Indicators
Initial Access	Phishing [T1566], Drive-by Compromise [T1189], Exploit Public Facing Application [T1190], External Remote Services [T1133]	Email, web proxy, server application logs, IDS/IPS	Phishing, redirect, and payload servers (domains and IP addresses), delivery mechanisms (lures, macros, downloaders, droppers, etc.), compromised credentials, web shells
Execution	Command and Script Interpreters [T1059], Exploitation for Client Execution [T1203]	Host event logs, Windows event logs, Sysmon, anti-malware, EDR, PowerShell logs	Invocation of command or scripting interpreter, exploitation, API calls, tools, malware, payloads
Persistence	Account Manipulation [T1098], Scheduled Task/Job [T1053], Valid Accounts [T1078]	Host event logs, Authentication logs, Registry	Scheduled Tasks, registry keys, autoruns, etc.
Lateral Movement	Exploitation of Remote Services [T1210], Remote Session Hijacking [T1563], Software Deployment Tools [T1072]	Internal network logs, host event logs, Application Logs	Mismatch of users and applications/credentials, workstation to workstation communication, beaconing from hosts not intended to be internet accessible, etc.
Credential Access	Brute Force [T1110], Modify Authentication Process [T1556], Man-in-the-Middle [T1557]	Authentication Logs, Domain Controller Logs, network traffic monitoring	LSASS reads, command or scripting interpreters accessing LSASS, etc.
C2	Application Layer Protocol [T1071], Protocol Tunneling [T1572]	Firewall, Web Proxy, DNS, Network Traffic, Cloud activity logs, IDS/IPS	C2 domains, IP addresses
Exfiltration	Exfiltration Over C2 Channel [T1041], Exfiltration Over Alternative Protocol [T1048]	Firewall, Web Proxy, DNS, Network Traffic, Cloud activity logs, IDS/IPS	Domains, URLs, IP addresses, IDS/IPS signatures

Source: Cybersecurity Incident & Vulnerability Response Playbooks https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Key Takeaways

ATT&CK®

Can help you

See the threats

Track and understand their behaviors

Orient your defensive recommendations towards behaviors

ATT&CK®

attack@mitre.org

@MITREattack

mitre-att&ck

jcwilliams@mitre.org