

Using the MITRE ATT&CK Framework to Measure Security Effectiveness

Lessons learned from DARK TEQUILA

BACKGROUND

Global Information Security Spending to Exceed \$124B USD in 2019

Average Cost of a Data Breach is \$3.86M USD (Global)

~1,244 Breaches Reported in 2018

The Number of Breaches Decreased 23% in 2018, but PII Compromises Increased 123%.

INCREASE IN TARGETED ATTACKS



COST OF COMPROMISE

\$3.9M USD AVG COST (GLOBAL)

The US leads costs at over \$7M avg cost per compromise. The compromise of PII, Intellectual property, and reputational damage continues to push this figure higher.



TIME TO DETECT

The global average time for organizations to detect a compromise is **196 days**.

Once an organization has confirmed a compromise, the global average to contain the breach is 69 days.

Kaspersky Antivirus identified **DARK TEQUILA** malware went undetected for nearly **5 years**.

DARK TEQUILA focused on targets in Mexico with the intent to steal banking credentials.





4

HOW DO WE IMPROVE?

MEASURE SECURITY EFFECTIVENESS

Measuring Capabilities and Maturity

- Not knowing what you don't know
- Baseline threat profile and key risks
- Identify how well program and personnel perform today
- Action plan for addressing key gaps (roadmap)

Measuring Return on Investment (ROI)

- Metrics based on what should improve
- Demonstrate improvement over time

Measuring Readiness to Respond

- Red Teaming
- Compromise Assessment or Threat Hunt
- Wargaming

MITRE ATT&CKTM

ADVERSARIAL TACTICS, TECHNIQUES, AND COMMON KNOWLEDGE

March Colored Part Security Part Security Part Security Part Security Part Par	Initial Access	Execution	Penistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Estitration	Command and Control		
Treat department of the control of t													
September Sept	Trusted Relationship	1	(en)	Proce:	is Injection	Two-Fector Authentication	System Time Discovery		Screen Capture	Exfiltration Over	Uncommonly Used Port		
Descriptive ID Secrit Control Descriptive ID Desc	Supply Chain Compromise	LSAS	S Driver	Extra Window	Memory Injection	Interception	System Service Discovery	Third-party Software	Man in the Browser	Physical Medium	Standard Non-Application		
Second Procession Comment of the	Spearphishing via Service	Local Job	Scheduling	Bypass User	Account Control	Private Keys	System Owner/User	Taint Shared Content	Input Capture	Exfiltration Over Command	Layer Protocol		
Particular Phage Proceedings Procedure Program Procedure Program Procedure Program Procedure Program Procedure Pro			nchetl		n Manipulation		Discovery						
Process of Control Process of Control (Control Process)													
India Audit Transport Trist State Tris					-1								
## State of protection of the control of the contro		-			tion	-							
Streto Efforts (Companies) The set of Services (Companies) The			181nin		Mich Sendes								
Dies to Consonital South of Filteries Description of Secription of Secreption of Sec													
Socie Book Deep (Investment Workshort) Book Deep (Investment Workshort) Socie of Mark Street (Investment Street Medical Street Street) Socie of Mark Street (Investment Street) Socie of Mark Str									,				
Space Larger Frequency Fre													
Secret Cancer Receiver from the Committee Secret Secret		Signed Script	Port M	tonitors	Space after Filename	Credential Access	Password Policy Discovery	Exploitation of			Domain Fronting		
Supplied County Product Product Product Supplied Supplie		Proxy Execution	Path Into	erception	Software Packing	Credentials in Files	Network Share Discovery	Remote Services			Data Obfuscation		
Regard February Windows February February Windows February Febru		Service Execution	New 5	Service		Credential Dumping	Network Service Stanning	Application Deployment			Data Encoding		
Regard Recommendation Recommendati					Provider Hijacking	Bash History Account Manipulation Securityd Memory							
Pages Allegary Page								Remote Services Distributed Component Object Model					
Powerful and specified to showing specified to specify the specified to specified to specify the specified to specified to specify the specified to specify the specified to specified													
Public Production of Petrical Specific Production Specific Product				, .									
Freid Mill According February (September 1) Grayman of part of the Control of Control o													
Good State of Particles Content of Partic							·						
Content from the Content of Con													
Centre Personal Foundation Large PAT Comment Set Service PAT Comment Set Set Service PAT Comment Set Set Set Service PAT Comment Set Set Set Set Set Set Set Set Set Se				·									
Section of the standard of the				Sudo SID-History Injection Exploitation for									
Consider Milks B. Bloome Product Consider Product Product Consider Product Product Consider Product Produc		Execution through API			Part Knocking						Commonly Used Port		
Commodel (1984 File Hisport) Product Commodel (1984 File Hisport) Product Commodel (1984 File Hisport)		Dynamic Data Exchange	Event Subscription		Obfuscated Files								
Consend the interiors Script Support Product CASTER Applicities When Support Register Principle Profession August When Support Bland Brav Profession Control Profession Control Received Profession Received Profession Received Profession Received Profession Received Received Profession Received R					or Information								
Modify Register Application Progress Plan Wyl Forward Strangement													
Application Process													
Workset National February Company of Park Records (September 1997) (Septem						-							
Helpmenteline Based Bury Proc Scores Proc Models Said Berrind Brest Berrind Berrin													
From Excessive through Post Excessive through Modification Service Insertince through Modification Service Insertince through Modification Service Insertince through													
Proce Decoders Instructure through Instructure through Module Load Mean Febrer Del. Module Load Mean Febrer Module Load													
Modely Esting Service Lagan Se													
Indicate Remova from Teas Ingoline Protects Ingoline Protects Ingoline Protects Indicate Remova from Teas Indicate Remova		Execution through	Office Application Startup		Indirect Command Execution								
Ingen Scriece Ligation Agent (Ligation Agent) (Ligation A		Module Load	Netsh Helper DUL										
Service Medical Medical Services Servic			Modify Existing Service		Indicator Removal from Tools								
Service Merilla Merilla Historia Users Historia Branch Service Flat and Branch Service Flat and Branch Service Flat Article Branch Service Flat Article Branch Service Compare with Clajest Model Flat Branch Branch Flat Application Flat Application Flat Substant Branch Flat Su							NAITDE ATT9.€V™						
Service Medical Medical Services Servic							IVILLYE ALLAYAK						
Section Materials								, , ,, , ,					
Compared Cityles Model Februaries Febr				-		-			_				
Compared Cityles Model Februaries Febr							Enterprise Framework						
Compared Cityles Model Februaries Febr													
Exploitation for Detended Procedure Exploitation for Detended Procedure Excelling Security Tools			External Remote Services	1		1	C - L						
Misoting Defense Basisin			Creste Account		File Deletion								
Change The Fairth File Association Booksis Booksis BITS Jobs Authoritation Perkapy Account Managolation both profile and Joshine Time Provisers System Firmware Shorton Medification Redundent Access Hypervision Component Firmware Shorton Medification Redundent Access Hypervision Component Firmware Browser Extensions Distribution Model Redundent Access Hypervision Component Firmware Browser Extensions Mistribution Mi													
Bootch Bootch Bootch Bill State Autherbracker Prickage Account Nampulation Book provide and, booker Time Providers System Firmware Shorton Modification Reflandant Access Hypersion Component Firmware Browser Excessions Water Browser Stripting ATTS He Attributes Mare Indicater Removal on Host Others Attributes Mare Indicater Removal on Host Others Othe				-			attack withour						
Authentronion Package Account Manipulation Both_confrie and Josepho Time Provices System Firmware She tout Modification Redunder Access Higherisor Gemponent Pirmware Browser Extensions Control Panel Items Companied High Companied Companied Companied Companied High Companied													
BITS Jobs Authentrostion Package Account Manipulation Back_confile and Josepho Time Provices Time Provices System Firmware She tout Modification Redunder Access Hypervisor Compress Signal Stripe Stripe Signal Str				-			attack.n	nitre.ori					
Authentration Package Account Manipulation bash_profile and Josefin Time Providers Code Signing System Firmware Shortout Modification Redundent Access Hypersian Component Pistory Signed Signing From Leading From L				-					9				
Account Manipulation bath profile and bathe Time Provices Code Signing System Firmware Shortout Medification General Manipulation Redundant Access Hypervisor Component Firmware Firmware Browser Extensions Model Hijacking Code Command Fistory Gest Command Fistory Signed Script Procy Execution Scripting NFFF He Attributes Mistre Indicator Removal on Host Dit Side-Loading OCSIstatow													
Compiled HTML File			A										
Time Providers System Firmware CMSTP Chest Command History Redundant Access Hyperstor Component Firmware Browser Extensions MYES Hie Attributes Mistra Indicator Removal on Host DIL Side-Leading OCShedow OCShedow				-									
System Firmware Shortout Medification Gear Command History Redundant Access Hypervision Hypervision Component Firmware Browser Extensions Mits Indicator Removal on Host OIL Side-Leading OCShedrow OCShedrow				1									
Shortout Modification Redundant Access REStates Rependent Access Rependent Forey Execution Signed Strip Execution Scripting Browser Extensions Rependent Forey Execution Scripting NFFF In Attributes Matric Indicator Removal on Host DIL Side-Leading OCSheutow				1									
Hypervisor Component Firmware Browser Extensions Mistre Indicator Removal on Host DIL Side-Leading OCSharlow				1									
Component Firmware Browser Extensions NTFS FI e Attributes Minite Indicator Removal on Host DIL Side-Loading OCShedow			Redundant Access]									
Browser Extensions METER THE Attributes Methra Indicator Removal on Host D11. Side-Loading OCSheutow			Hypervisor		Signed Script Proxy Execution								
Mshta Indicator Removal on Host DLL Side-Loading DCShedow			Component Firmware		Scripting								
Indicator Removal on Host OLL Side-Leading OCShedow			Browser Extensions										
DLL Side-Loading DCShedow													
OCShedow .						-							
						-							
WILKE	AAITDE				DC3H400M								
	MIIKE												





MITRE ATT&CKTM INTRODUCTION

Adversarial Tactics, Techniques, and Common Knowledge

Curated knowledge base and model for cyber adversary behavior covering Windows, Linux, and Mac

Pre-ATT&CKTM covers activity left of initial access

Mobile ATT&CKTM covers adversarial behavior on mobile devices

Work began in 2010 with the first Windows model created in 2013



MITRE ATT&CKTM INTRODUCTION

TACTICS

Denote short-term, tactical adversary goals during an attack (the columns)

TECHNIQUES

Describe the means by which an adversary achieves tactical goals (the individual cells)

COMMON KNOWLEDGE

Documented adversary usage of techniques and other metadata (linked to techniques)



MITRE ATT&CKTM SCOPE

Developed by both adversary emulation teams and defender teams

Publicly released in 2015 with 96 techniques organized under 9 tactics

12 Enterprise Tactics

Initial Access

Defense Evasion

Collection

Execution
Credential Access
Command and Control

Persistence
Discovery
Exfiltration

Privilege Escalation
Lateral Movement
Impact



MITRE ATT&CKTM SCOPE

244 Enterprise Techniques

Initial Access

→ Spearphishing Link

ID: T1192

Tactic: Initial Access

Platform: Windows, macOS, Linux

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

CAPEC ID: <u>CAPEC-163</u>

Initial Access

→ Replication Through Removable Media

ID: T1091

Tactic: Lateral Movement, Initial Access

Platform: Windows

System Requirements: Removable media allowed,
Autorun enabled or vulnerability present that allows

for code execution

Permissions Required: User

Data Sources: File monitoring, Data loss prevention

Persistence

→ New Service

ID: T1050

Tactic: Persistence, Privilege Escalation

Platform: Windows

Permissions Required: Administrator, SYSTEM

Effective Permissions: SYSTEM

Data Sources: Windows Registry, Process monitoring, Process command-line parameters, Windows event

logs

CAPEC ID: <u>CAPEC-550</u>

Command and Control

→ Commonly Used Port

ID: T1043

Tactic: Command And Control

Platform: Linux, macOS, Windows

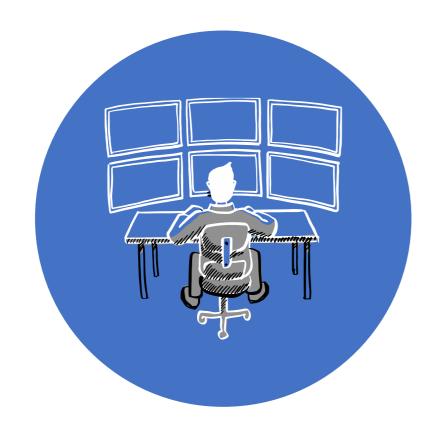
Data Sources: Packet capture, NetFlow/Enclave NetFlow, Process use of network, Process monitoring

Requires Network: Yes



ASSUME COMPROMISE

No one has perfect security. Assume an attacker can penetrate and focus on ability to detect.



FOCUS ON DETECTION

An ounce of detection is worth a pound of prevention. Focus efforts on documented adversary behavior. This can be **tested and measured**.



NO ONE IS IMMUNE

By assuming compromise, you can put your mind into that of an attacker. Understand your vulnerabilities and how well you can respond.

Continually test your weaknesses and risks.

ASSUME COMPROMISE

Prioritize your vulnerabilities and likely path attackers will take. Measure progress in detection.

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	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	Applnit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser]	Multi-Stage Channels
	Launchetl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture	1	Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture	1	Multilayer Encryption
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content		-	Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software]		Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares]		Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery		-		Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets	1		_			Web Service
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass]					
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories]					

Legend Low Priority
High Priority

Finding Gaps in Defense



Signed Script Proxy Execution

Space after Filename

Trusted Developer Utilities

Windows Remote Management

XSL Script Processing

Launch Agent

Launchctl

Login Item
Logon Scripts

LSASS Driver

Launch Daemon

Local Job Scheduling

Modify Existing Service

Office Application Startup

Netsh Helper DLL

Path Interception

Plist Modification

Port Knocking
Port Monitors

Startup Items

Sudo Caching

Hidden Users

Hidden Window

HISTCONTROL

Indicator Blocking

Image File Execution Options

Indicator Removal from Tools

Indicator Removal on Host

Indirect Command Execution

Install Root Certificate

LC_MAIN Hijacking

Masquerading

Modify Registry

NTFS File Attributes

Network Share Connection Removal

InstallUtil Launchct1

```
dcall *)(HANDLE))::CloseHandle;
threadex(0, 0, monitor_usb_devi
```

```
Name = 0;
4);
me, 8, v6, (char)disk_name);
RootPathName) == DRIVE_REMOVABL
```

ves(); i; i >>= 1 }

_BYTE) disk_name + 1;

DARK TEQUILA

Complex, multi-stage malware campaign targeting Mexican users and evaded detection for five years.

Defense Evasion

Look for running security applications, debuggers, or virtualization. If found, would cleanup and remove itself from host.



Specifically targeted several Mexican banking institutions since at least 2013. Additionally, would capture and record credentials for cloud services, e-mail providers, or flight reservation systems.



Look for USB drive insertion and infect, allowing the malware to move offline to new machines.



DARK TEQUILA

Tactics and Technique Detection

Initial Access

→ Spearphishing Link

ID: T1192

Tactic: Initial Access

Platform: Windows, macOS, Linux

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

CAPEC ID: <u>CAPEC-163</u>

Initial Access

→ Replication Through Removable Media

ID: T1091

Tactic: Lateral Movement, Initial Access

Platform: Windows

System Requirements: Removable media allowed,
Autorun enabled or vulnerability present that allows

for code execution

Permissions Required: User

Data Sources: File monitoring, Data loss prevention

Persistence

→ New Service

ID: T1050

Tactic: Persistence, Privilege Escalation

Platform: Windows

Permissions Required: Administrator, SYSTEM

Effective Permissions: SYSTEM

Data Sources: Windows Registry, Process monitoring, Process command-line parameters, Windows event

logs

CAPEC ID: <u>CAPEC-550</u>

Command and Control

→ Commonly Used Port

ID: T1043

Tactic: Command And Control

Platform: Linux, macOS, Windows

Data Sources: Packet capture, NetFlow/Enclave NetFlow, Process use of network, Process monitoring

Requires Network: Yes



TESTABLE DETECTION

Plan valid scenarios to stress and identify weak detection and protection. Improve and revisit.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Hardware Additions		Scheduled Task		Binary Padding	Credentials in Registry	Browser Bookmark	Exploitation of Remote	Data from Information	Exfiltration Over	Remote Access Tools
Trusted Relationship	LSASS [river Extra Window M		Memory Injection	Exploitation for	Discovery	Services	Repositories	Physical Medium	Port Knocking
Supply Chain	Local Job S	cheduling	Access Toker	Manipulation	Credential Access	Network Share	Distributed Component	Video Capture	Exfiltration Over	Multi-hop Proxy
Compromise		р	Bypass User A	ccount Control	Forced Authentication	Discovery	,	Audio Capture	Command and	Domain Fronting
Spearphishing	Laund	chcu	Process	Injection	Hooking	Peripheral Device	Remote File Copy	Automated Collection	Control Channel	Data Encoding
Attachment	5. Thed Binary	lmage	e File Execution Options Inj	ection	Password Filter DLL	Discovery	Replication Theough Removable Madia	Clipboard Data	Dat Encrypted	Remote File Copy
Exploit Public-Facing	Prox Execution		Plist Modification		LLMNR/NBT-NS	Discovery		Email Collection	Automated Enfiltration	Multi-Stage Channels
Application	User Execution		Valid Accounts		Poisoning Private Yovs			Screen Capture	Exfiltration Over Other	Web Service
Replication Through	Explored con 10f		DLL Search Order Hijacking	3			Windows Admin Shares	Data Staged	Network Medium	Standard
Removable Media	Client Execution	Approp	rt DLLs	Signed Script	Keychain	Discovery	Pass the Ha h	Input Capture	Exfiltration Over	Non-Application
Spearphishing via	CMSTP	Hoo	king	Prox, Execution	Input Prompt	rocess Discovery	Third-party Sof ware	Data from Network	Alternative Protocol	Layer Protocol
Service	Dynamic Data Exchange	Startu	rtems	DCShadow	Bash History	System Network	Shared Web oot	Shared Drive	Data Transfer	Connection roxy
Spearphishing Link	Mshta	Launch	Launch Daemon		Two-Factor	Connections Discovery	Logon Scripts	Data from Local System	Size Limits	Multilayor Encryption
Drive-by Compromise	AppleScript	Dylib H	Dylib Hijacking		Authentication	System Owner/ User	Windows R mote	Man in the Browser	Data Compressed	standard Application
Valid Accounts	Source	Application	Application Shimming		Interception	Discovery	Managernent	Data from Removable	Scheduled Transfer	Laver Protocol
	Space after Filename	Appln	it DLLs	BITS Jobs	Replication Through Removable Media	System Network Configuration Discovery	Application	Media		Commonly Used Port
	Execution through	Web	Shell	Control Panel Items			Deployme It Software			Standard Cryptographic
	Module Load	Module Load Service Registry Permissions Weakness Regsvcs/Regasm New Service InstallUtil File System Permissions Weakness Regsvr32 Path Interception Execution through API Accessibility Features PowerShell Port Monitors		CMSTP	Inpa Capture	Application Window	SSH Hijacking			Protocol
	Regsvcs/Regasm			Process Doppelgänging	Moture Criffing	Discovery	/ppleScript			Custom Cryptographic
	InstallUtil			Mshta	Credential Dumping	Password Policy	Tail t Shared Content			Protocol
	Regsvr32			Hidden Files	Kerperousting	Discovery	Remote Desktop Protocol			Data Obfuscation
	Execution through API			and Directories	Securityd Memory	System 1 me Discovery			Custom Command	
	PowerShell			Space after Filename	Brute Force	Account Discovery	Remote Services			and Control Protocol
	Rundll32	Kernel Modules	Sudo Caching		Account Manipulation	System-imormation				Communication
										ı

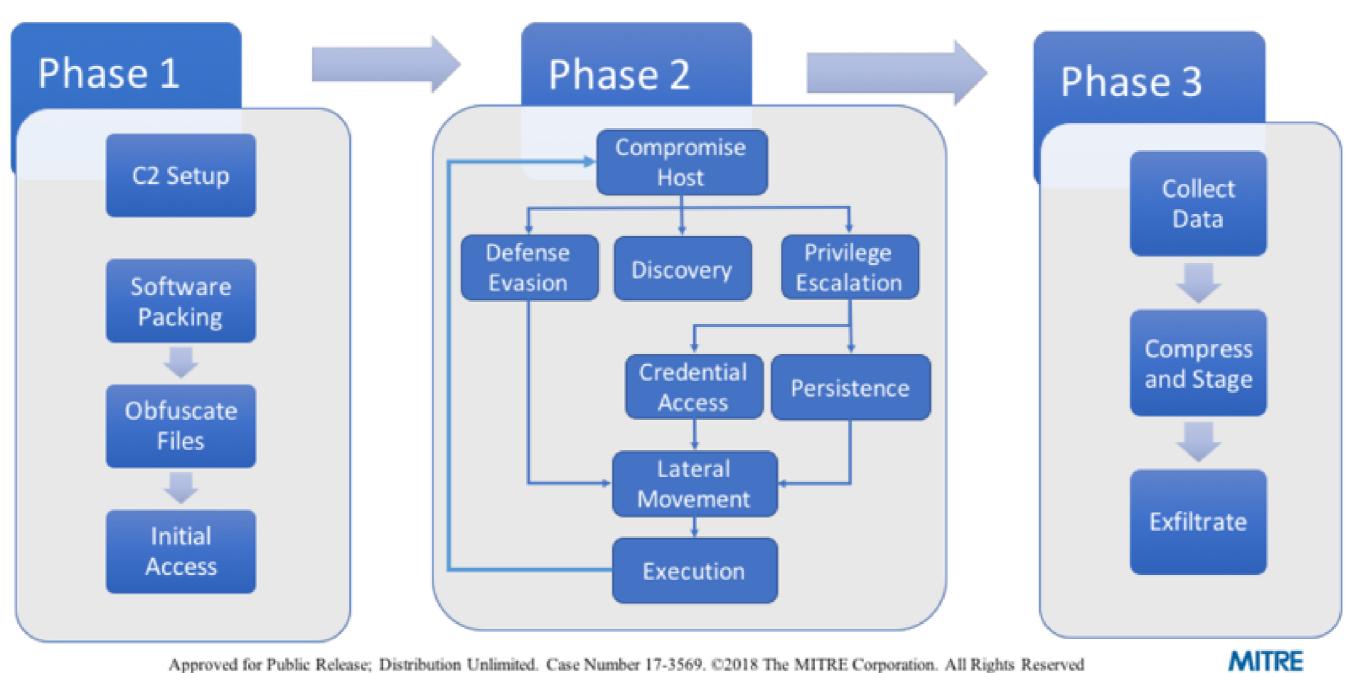


TESTABLE DETECTION

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

https://attack.mitre.org/groups/G0022/

APT 3 Emulation Plan



Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved



TESTABLE DETECTION

Red Team Automation

https://github.com/endgameinc/RTA

RTA provides a framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft, modeled after MITRE ATT&CK ™.

Atomic Red Team

https://github.com/redcanaryco/atomic-red-team

Atomic Red Team is a collection of small, highly portable detection tests mapped to MITRE ATT&CK™. This gives defenders a highly actionable way to immediately start testing their defenses against a broad spectrum of attacks.



SUMMARY

Focus on detection!

Develop key metrics to measure how effective your security program is

- Capabilities and Maturity
- Return on Investment
- Readiness to Respond

Plan Red Team engagements to stress test your vulnerabilities

Blue Teams should produce analytic progress measurement demonstrating improvement in detection and response

Collaborate, Communicate, and Engage with security communities

MITRE ATT&CK strength depends on community involvement





FURTHER READING

Current Evaluations



https://attackevals.mitre.org/



