



# 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**



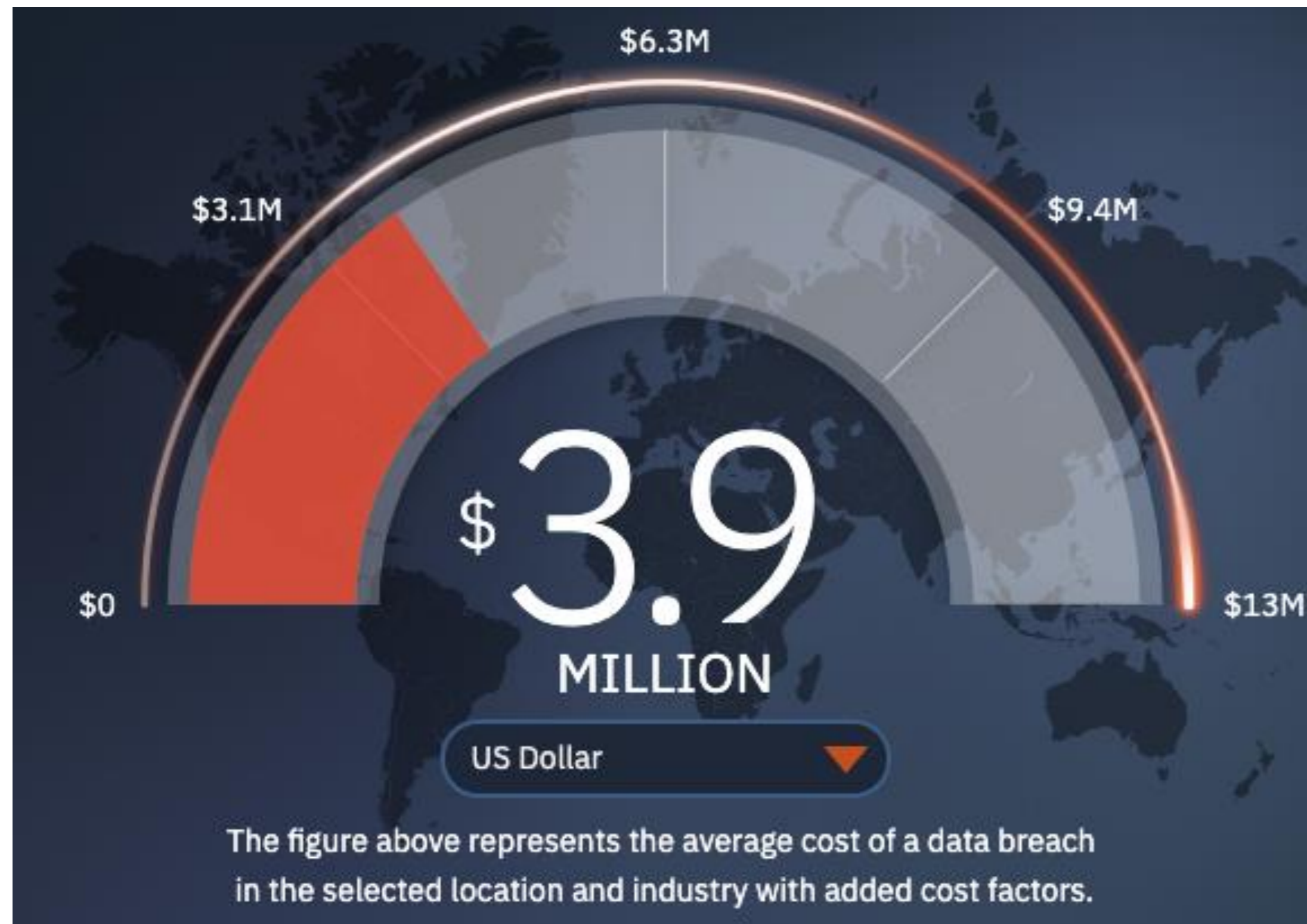
proprietary & confidential



# 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.







# MITRE ATT&CK™ INTRODUCTION

Adversarial Tactics, Techniques, and Common Knowledge

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

Pre-ATT&CK™ covers activity left of initial access

Mobile ATT&CK™ covers adversarial behavior on mobile devices

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



proprietary & confidential



# MITRE ATT&CK™ 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)



proprietary & confidential



# MITRE ATT&CK™ 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  | Execution           | Persistence  | Privilege Escalation |
| Defense Evasion | Credential Access   | Discovery    | Lateral Movement     |
| Collection      | Command and Control | Exfiltration | Impact               |



proprietary & confidential



# MITRE ATT&CK™ 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: [CAPEC-163](#)

### 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: [CAPEC-550](#)

### 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

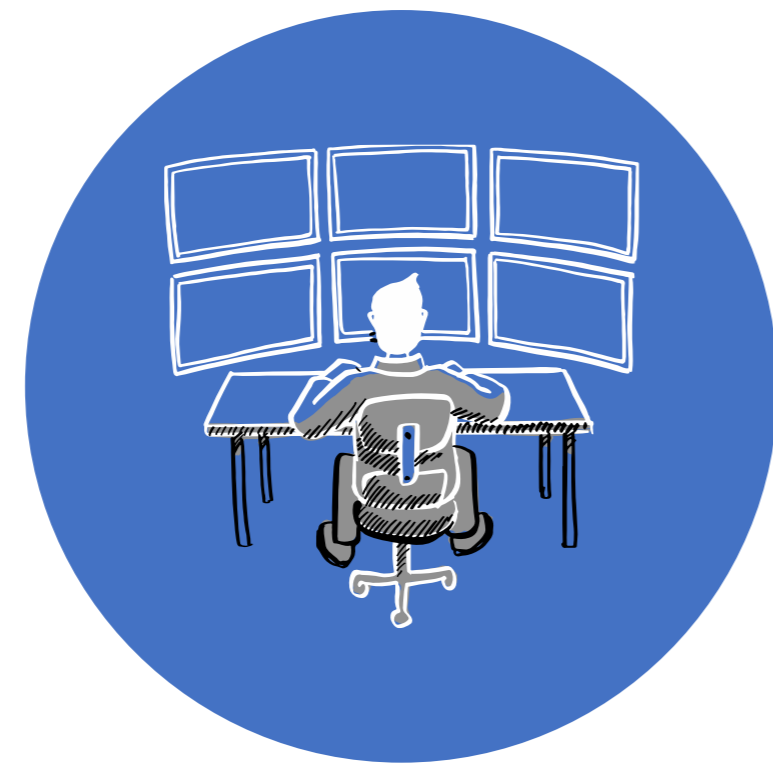


proprietary & confidential



# 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                    |
|                                     | Launchctl                          | Component Firmware                     | Hooking                                | DCShadow                                | Kerberoasting                          | Query Registry                         | Shared Webroot                      | Screen Capture                     |                                               | 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                      |                                               | Multilayer Encryption                   |
|                                     | LSASS Driver                       | Create Account                         | Launch Daemon                          | Disabling Security Tools                | LLMNR/NBT-NS Poisoning                 | Security Software Discovery            | Taint Shared Content                |                                    |                                               | Port Knocking                           |
|                                     | Mshsa                              | 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             |                                        |                                        |                                     |                                    |                                               | 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            |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | Signed Script Proxy Execution      | Launch Agent                           | Startup Items                          | Hidden Users                            |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | Source                             | Launch Daemon                          | Sudo                                   | Hidden Window                           |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | Space after Filename               | Launchctl                              | Sudo Caching                           | HISTCONTROL                             |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | Third-party Software               | LC_LOAD_DYLIB Addition                 | Valid Accounts                         | Image File Execution Options Injection  |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | Trap                               | Local Job Scheduling                   | Web Shell                              | Indicator Blocking                      |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | Trusted Developer Utilities        | Login Item                             |                                        | Indicator Removal from Tools            |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | User Execution                     | Logon Scripts                          |                                        | Indicator Removal on Host               |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | Windows Management Instrumentation | LSASS Driver                           |                                        | Indirect Command Execution              |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | Windows Remote Management          | Modify Existing Service                |                                        | Install Root Certificate                |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     | XSL Script Processing              | Netsh Helper DLL                       |                                        | InstallUtil                             |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     |                                    | New Service                            |                                        | Launchctl                               |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     |                                    | Office Application Startup             |                                        | LC_MAIN Hijacking                       |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     |                                    | Path Interception                      |                                        | Masquerading                            |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     |                                    | Plist Modification                     |                                        | Modify Registry                         |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     |                                    | Port Knocking                          |                                        | Mshsa                                   |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     |                                    | Port Monitors                          |                                        | Network Share Connection Removal        |                                        |                                        |                                     |                                    |                                               |                                         |
|                                     |                                    | Rc.common                              |                                        | NTFS File Attributes                    |                                        |                                        |                                     |                                    |                                               |                                         |

**Legend**

Low Priority

High Priority

## Finding Gaps in Defense



```

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

```

```

;
yes(); i; i >>= 1 )

```

```

Name = 0;

```

```

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

```

```

_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.

## Keylogger and Information Stealer

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.

## USB Infector

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: [CAPEC-163](#)

### 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: [CAPEC-550](#)

### 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



proprietary & confidential



# 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 Discovery             | Exploitation of Remote Services     | Data from Information Repositories | Exfiltration Over Physical Medium             | Remote Access Tools   |
| Trusted Relationship                | LSASS Driver                      |             | Extra Window Memory Injection          |                 | Exploitation for Credential Access     | Network Share Discovery                | Distributed Component Discovery     | Video Capture                      | Exfiltration Over Command and Control Channel | Port Knocking         |
| Supply Chain Compromise             | Local Job Scheduling              |             | Access Token Manipulation              |                 |                                        |                                        |                                     |                                    |                                               | Forced Authentication |
| Spearphishing Attachment            | Trap                              |             | Bypass User Account Control            |                 | Hooking                                | Peripheral Device Discovery            | Remote File Copy                    | Automated Collection               | Multi-hop Proxy                               |                       |
| Exploit Public-Facing Application   | Launchctl                         |             | Process Injection                      |                 | Password Filter DLL                    | File and Directory Discovery           | Replication Through Removable Media | Email Collection                   | Automated Exfiltration                        |                       |
| Replication Through Removable Media | Signed Binary Proxy Execution     |             | Image File Execution Options Injection |                 | LLMNR/NBT-NS Poisoning                 | Permission Groups Discovery            | Windows Admin Shares                | Screen Capture                     | Exfiltration Over Other Network Medium        |                       |
| Spearphishing via Service           | User Execution                    |             | Plist Modification                     |                 | Private Keys                           | Process Discovery                      | Pass the Hash                       | Data Staged                        | Exfiltration Over Alternative Protocol        |                       |
| Spearphishing Link                  | Exploitation for Client Execution |             | Valid Accounts                         |                 | Keychain                               | System Network Connections Discovery   | Third-party Software                | Input Capture                      | Data Transfer Size Limits                     |                       |
| Drive-by Compromise                 | CMSTP                             |             | DLL Search Order Hijacking             |                 | Input Prompt                           | System Owner/User Discovery            | Windows Remote Management           | Data from Network Shared Drive     | Scheduled Transfer                            |                       |
| Valid Accounts                      | Dynamic Data Exchange             |             | Appert DLLs                            |                 | Bash History                           | System Network Configuration Discovery | Application Deployment Software     | Man in the Browser                 | Commonly Used Port                            |                       |
|                                     | Mshta                             |             | Hooking                                |                 | Two-Factor Authentication Interception | Application Window Discovery           | SSH Hijacking                       | Data from Removable Media          | Standard Application Layer Protocol           |                       |
|                                     | AppleScript                       |             | Startup Items                          |                 | Indirect Command Execution             | Password Policy Discovery              | AppleScript                         |                                    | Custom Cryptographic Protocol                 |                       |
|                                     | Source                            |             | Launch Daemon                          |                 | Port Knocking                          | System Time Discovery                  | Tail Shared Content                 |                                    | Data Obfuscation                              |                       |
|                                     | Space after Filename              |             | AppInit DLLs                           |                 | BITS Jobs                              | Account Discovery                      | Remote Desktop Protocol             |                                    | Custom Command and Control Protocol           |                       |
|                                     | Execution through Module Load     |             | Web Shell                              |                 | Control Panel Items                    | System Information                     | Remote Services                     |                                    | Communication                                 |                       |
|                                     | Regsvcs/Regasm                    |             | Service Registry Permissions Weakness  |                 | CMSTP                                  |                                        |                                     |                                    |                                               |                       |
|                                     | InstallUtil                       |             | New Service                            |                 | Process Doppelgänger                   |                                        |                                     |                                    |                                               |                       |
|                                     | Regsvr32                          |             | File System Permissions Weakness       |                 | Mshata                                 |                                        |                                     |                                    |                                               |                       |
|                                     | Execution through API             |             | Path Interception                      |                 | Hidden Files and Directories           |                                        |                                     |                                    |                                               |                       |
|                                     | PowerShell                        |             | Accessibility Features                 |                 | Space after Filename                   |                                        |                                     |                                    |                                               |                       |
|                                     | Rundll32                          |             | Port Monitors                          |                 | Space after Filename                   |                                        |                                     |                                    |                                               |                       |
|                                     | Kernel Modules                    |             | Sudo Caching                           |                 | Account Manipulation                   |                                        |                                     |                                    |                                               |                       |

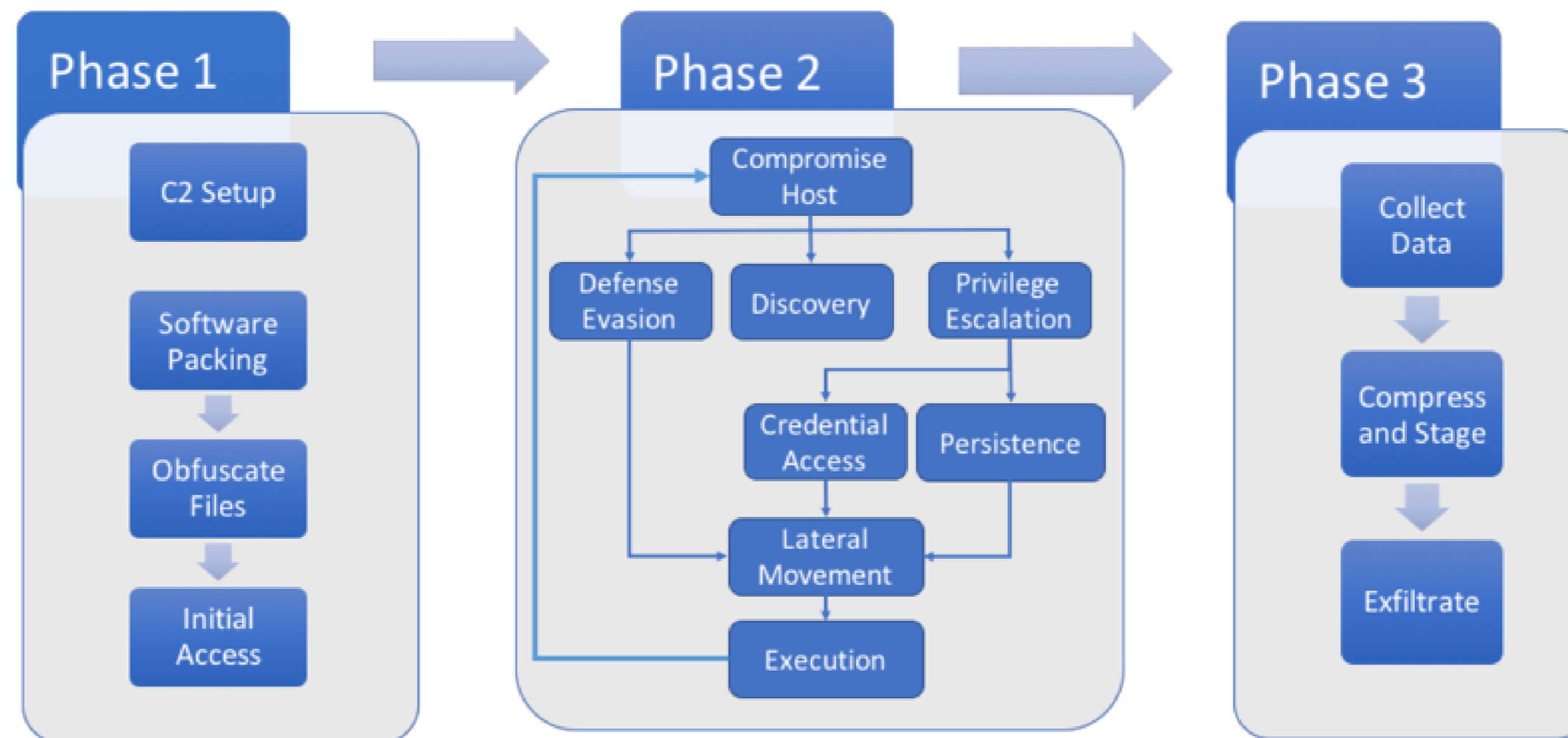


# TESTABLE DETECTION

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

MITRE

# 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

Initial Cohort

|                                                                                                                           |                                                                                                                                                                                                  |                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>CarbonBlack</p> <p><b>Carbon Black.</b></p> <p>Carbon Black   Response</p>                                             | <p>CounterTack</p> <p><b>GoSECURE</b><br/>POWERED BY COUNTERTACK</p> <p>CounterTack   GoSecure</p>                                                                                               | <p>CrowdStrike</p>  <p>CrowdStrike   Falcon</p> <p>Endpoint Protection Standard Bundle</p> <p>CloudGuard   InSight   Dragoon</p> |
| <p>Endgame</p> <p><b>ENDGAME.</b></p> <p>Endgame</p>                                                                      | <p>Microsoft</p>  <p><b>Windows Defender ATP</b></p> <p>Microsoft   Defender</p> <p>Windows Defender ATP</p> | <p>RSA</p> <p><b>RSA</b></p> <p>RSA   NetWitness</p>                                                                                                                                                                |
| <p>SentinelOne</p>  <p>SentinelOne</p> |                                                                                                                                                                                                  |                                                                                                                                                                                                                     |

<https://attackedvals.mitre.org/>



CONTACT US



SidianSecurity

Paseo de la Reforma 296, Piso 42  
Colonia Juárez  
Delegación Cuahutemoc  
Ciudad de México, CDMX, México 06600  
+52 55 4624 0236  
hola@sidiansecurity.com