



ISMAEL VALENZUELA - @ABOUTSECURITY

MODELADO PRÁCTICO DE AMENAZAS Y DEFENSAS BLUE TEAM CON MITRE ATT&CK



Fundador de
G2 Security en 2000

Ingeniero Principal
Senior en McAfee

Autor e Instructor del
Instituto SANS



@aboutsecurity





MITRE qué??



PIENSA EN ROJO, ACTUA EN AZUL

- Un ataque (**red team**) que no resulta en la mejora del programa de seguridad no sirve para nada.
- La defensa (**blue team**) que no está priorizada por las amenazas y el impacto, no es efectiva.
- Es todo gestión de riesgos...
- **MITRE ATT&CK** te permite priorizar de manera práctica en qué enfocar tu defensa, mediante el conocimiento del enemigo.



¿Dónde comenzamos?

CASO DE USO: HACME CATS

Negocio: venta de comida para gatos online

Amenaza: FIN-Dogs (súper APT)

Herramientas:

- Página de MITRE ATT&CK
 - <https://attack.mitre.org/>
- ATT&CK Navigator
 - <https://mitre-attack.github.io/attack-navigator/>

The screenshot shows the MITRE ATT&CK website's search interface. A yellow box highlights the word 'retail' in the search bar, which is preceded by a magnifying glass icon. The search bar is located above a navigation menu with items: Matrices, Tactics ▾, Techniques ▾, Mitigations ▾, Groups, Software, Resources ▾, Blog ↗, and Contribute.

FIN6, ITG08, Group G0037

... as stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors.^{[1][2]} ID: G0037 Associated Groups: ITG08 Contributors: Drew Church, Splunk Version: 2.0 Created: 31 May 2017 Last Modified: 15 October 2019 Associated Group Descriptions Name Descr...

FIN7, Group G0046

FIN7 FIN7 is a financially-motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. FIN7 is sometimes referred...

FIN8, Group G0061

FIN8 FIN8 is a financially motivated threat group known to launch tailored spearphishing campaigns targeting the retail, restaurant, and hospitality industries. [1] [2] ID: G0061 Version: 1.0 Created: 18 April 2018 Last Modified: 01 October 2019 Techniques Used Domain ID Name Use Enterprise T1059 Command-Lin...

[Get Started »](#)

[Contribute »](#)

[Check out our Blog ↗](#)

[Embed](#)

[View on Twitter](#)

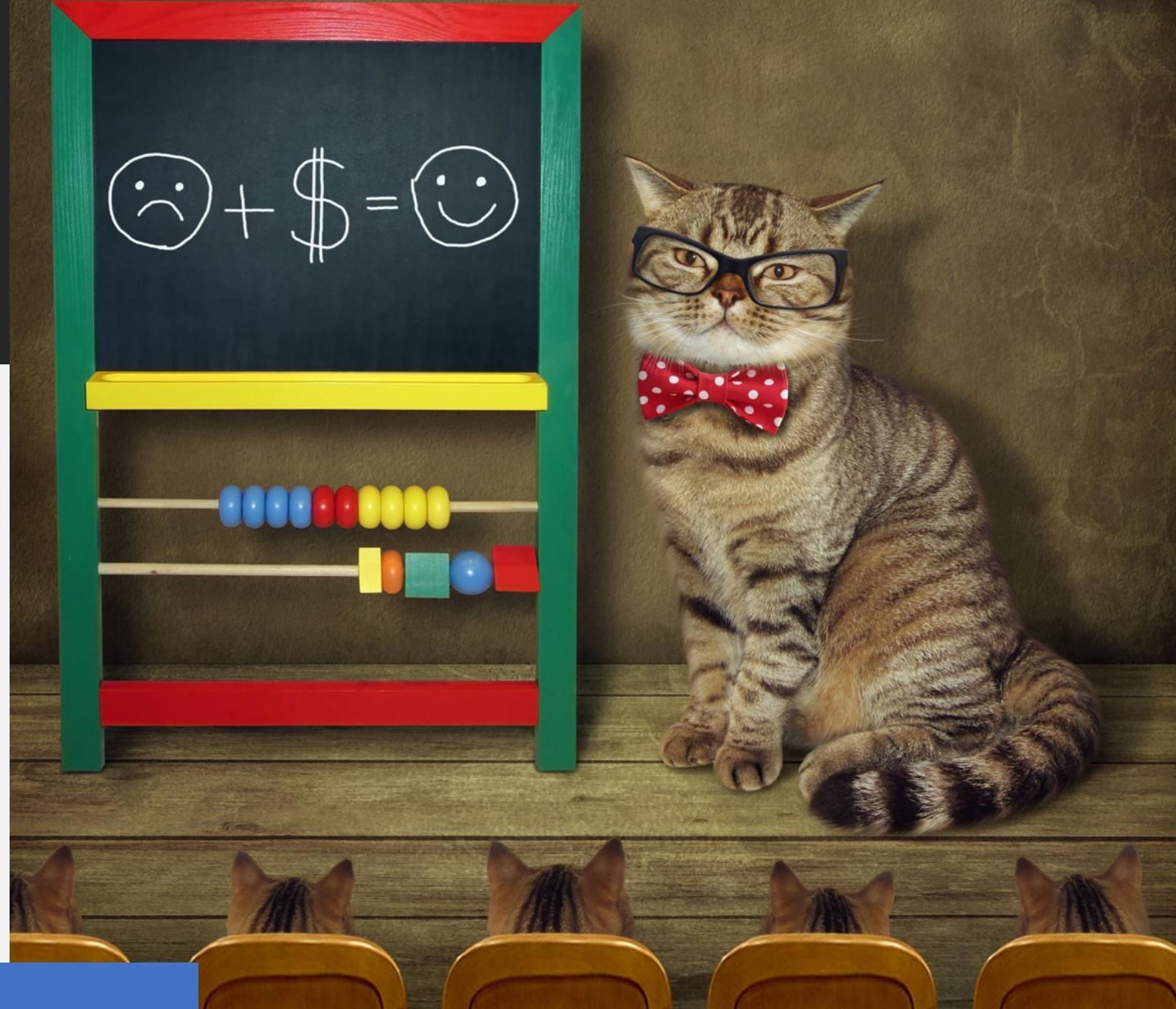
<https://attack.mitre.org/>

layer by operation

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Data from Information Repositories	Data from Local System	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Applnit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Exploitation of Remote Services	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Content Wipe
Spearphishing Attachment	Application Shimming	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Internal Spearphishing	Data from Network Shared Drive	Data from Removable Media	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Dynamic Data Exchange	BITS Jobs	Bypass User Account Control	Code Signing	Credentials in Registry	Network Share Discovery	Logon Scripts	Data Encoding	Domain Fronting	Data Obfuscation	Firmware Corruption
Spearphishing via Service	Execution through API	Bootkit	BITS Jobs	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Hash	Data from Removable Media	Data Staged	Exfiltration Over Other Network Medium	Inhibit System Recovery
Supply Chain Compromise	Execution through Module Load	Browser Extensions	DLL Search Order Hijacking	Compiled HTML File	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Physical Medium	Network Denial of Service
Trusted Relationship	Execution through Module Load	Change Default File Association	Dylib Hijacking	Component Firmware	Component Firmware	Permission Groups Discovery	Remote Desktop Protocol	Email Collection	Fallback Channels	Exfiltration Over Physical Medium	Resource Hijacking
Valid Accounts	Exploitation for Client Execution	Component Object Model Hijacking	Elevated Execution with Prompt	Emond	Component Object Model Hijacking	Remote System Discovery	Remote File Copy	Input Capture	Multi-hop Proxy	Multi-stage Channels	Runtime Data Manipulation
	Graphical User Interface	InstallUtil	Create Account	Component Firmware	Connection Proxy	Remote System Discovery	Remote File Copy	Man in the Browser	Screen Capture	Multiband Communication	Service Stop
	Launchctl	DLL Search Order Hijacking	Extra Window Memory Injection	DCShadow	Control Panel Items	Remote System Discovery	Replication Through Removable Media	Replication Through Removable Media	Video Capture	Multi-layer Encryption	Stored Data Manipulation
	Local Job Scheduling	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Input Capture	Security Software Discovery	Screen Capture	Shared Webroot	SSH Hijacking	Port Knocking	System Shutdown/Reboot
	LSASS Driver	Dylib Hijacking	Disabling Security Tools	Disabling Security Tools	Input Prompt	Software Discovery	Screen Capture	Taint Shared Content	Third-party Software	Remote Access Tools	Transmitted Data Manipulation
	Mshta	Emond	File System Permissions Weakness	DLL Search Order Hijacking	File System Permissions Weakness	System Information Discovery	Video Capture	Windows Admin Shares	Windows Admin Shares	Remote File Copy	
	PowerShell	External Remote Services	DLL Side-Loading	DLL Side-Loading	Hooking	System Network Configuration Discovery	Standard Application Layer Protocol	Windows Remote	Windows Remote	Standard	
	Regsvcs/Regasm	Image File Execution Options Injection	Execution Guardrails	Execution Guardrails	Image File Execution Options Injection	System Network Connections Discovery					
	Regsvr32	File System Permissions Weakness	Exploitation for Defense Evasion	Exploitation for Defense Evasion	Launch Daemon	System Owner/User Discovery					
	Rundll32		Extra Window Memory Injection	Extra Window Memory Injection	Steal Web Session Cookie						

Juguemos con algunas analíticas

- ATT&CK scripts:
<https://github.com/mitre-attack/attack-scripts>
- Jupyter notebook:
<https://mybinder.org/v2/gh/mitre-attack/attack-scripts/master>
- ATT&CK Python client:
<https://github.com/hunters-forge/ATTACK-Python-Client>





Data Source Investigation

Let's use the [ATT&CK Python Client](#) to manually examine the techniques, list the data sources, and build a heatmap out of our selected sources.

If you're looking for less development or a more in-depth and finely-grained dive, check out:

- [DeTTACK](#)
- [AttackDatamap](#)

Consider: What have you used to track data sources? What has worked well, and what has not worked so well?

```
In [ ]: # Import the packages we'll need

# Some basic python and jupyter stuff
from collections import defaultdict
import json
from IPython.display import FileLink, FileLinks

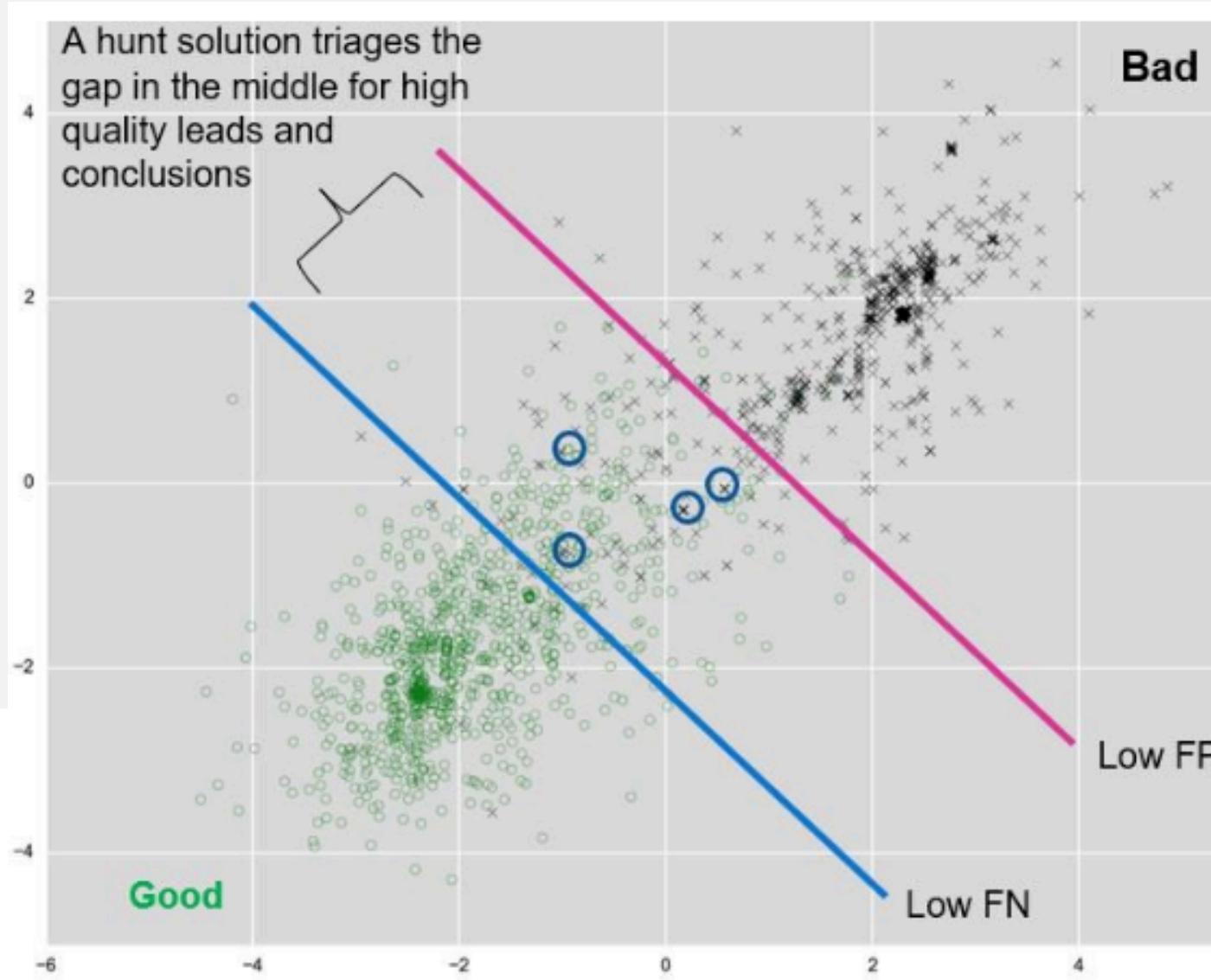
# Visualization and data libraries
import altair as alt
import pandas as pd

# ATT&CK Python Client, by @HuntersForge (https://github.com/hunters-forge/ATTACK-Python-Client)
from attackcti import attack_client

# Because this is in Jupyter notebooks we need to enable that renderer for the altair charts to work
alt.renderers.enable('notebook')
```

Get the ATT&CK Enterprise techniques using the client library

```
In [ ]: client = attack_client()
all_techniques = client.get_enterprise()['techniques'] # Note - this takes a few seconds to download and parse
```



Visibilidad vs Detección

La mayoría de productos de detección no son adecuados para threat hunting.

- Prevención y Detección -- Pocos FPs
- Visibilidad y Hunting – Pocos FNs

<https://deltarisk.com/blog/why-most-real-time-defensive-solutions-are-poor-threat-hunting-solutions/>

DeTT&CT

- Framework para administrar, evaluar y comparar la calidad de:
 - Data sources
 - Visibilidad
 - Detección
 - Threat actors

<https://github.com/rabobank-cdc/DeTTECT>

Data Sources

- <https://github.com/rabobank-cdc/DeTECT/wiki/Data-sources>
- Casi 60 fuentes de datos aplicables a distintas plataformas

Home > Techniques > Enterprise > Standard Application Layer Protocol

Standard Application Layer Protocol

Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic.

Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are RPC, SSH, or RDP.

<https://attack.mitre.org/techniques/T1071/>

ID: T1071

Tactic: Command And Control

Platform: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

Requires Network: Yes

Version: 1.0





HOME

DATA SOURCES

TECHNIQUES

GROUPS

Data Sources

New file

Select YAML file

File details

Filename: data-sources-new.yaml
File type: data-source-administration
Version: 1.0
Name: example
Platform: all Windows Linux macOS AWS GCP Azure Azure AD Office 365 SaaS

Save YAML file

Add data source

filter

Name	Date	Products	
DNS records	2020-04-11	Zeek sensor, DNS Logs from Windows Server	
Netflow/Enclave netflow	2020-04-11	Zeek sensor	
Network intrusion detection system	2020-04-11	Zeek sensor	



FIN6 x FIN7 x FIN8 x

Data sources example x

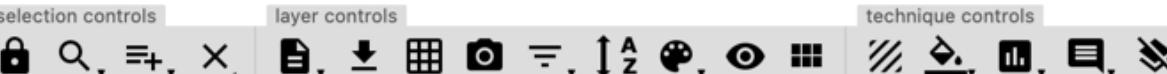
Visibility example x

Detections example x

FIN6+FIN7+FIN8 - Attack - Windows x

+

technique controls



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Transfer Size Limits	Defacement
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Application Shimming	CMSTP	CMSTP	Credentials in Files	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Endpoint Denial of Service	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Compile After Delivery	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Inhibit System Recovery	Network Denial of Service
Spearphishing via Service	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Component Object Model Hijacking	Network Sniffing	Pass the Ticket	Domain Fronting	Domain Generation Algorithms	Resource Hijacking	
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Change Default File Association	Extra Window Memory Injection	Component Object Model Hijacking	Forced Authentication	Peripheral Device Discovery	Data Staged	Domain Over Other Network Medium	Exfiltration Over Physical Medium	
Trusted Relationship	Graphical User Interface	Component Firmware	Graphical User Interface	Control Panel Items	Connection Proxy	Forced Authentication	Remote Desktop Protocol	Domain Staging	Domain Generation Algorithms	Exfiltration Over Other Network Medium	Network Denial of Service
Valid Accounts	InstallUtil	Component Object Model Hijacking	InstallUtil	Extra Window Memory Injection	Component Object Model Hijacking	Hooking	Remote File Copy	Email Collection	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	LSASS Driver	Create Account	LSASS Driver	Control Panel Items	Connection Proxy	Forced Authentication	Remote Services	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	Mshta	Hooking	Mshta	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	PowerShell	Disabling Security Tools	PowerShell	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	DLL Search Order Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	Regsvcs/Regasm	DLL Side-Loading	Regsvcs/Regasm	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	Regsvr32	New Service	Regsvr32	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	Rundll32	Execution Guardrails	Rundll32	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	Scheduled Task	Parent PID Spoofing	Scheduled Task	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	Scripting	Exploitation for Defense Evasion	Scripting	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	Service Execution	Steal Web Session Cookie	Service Execution	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	Hidden Files and Directories	System Network Configuration Discovery	Hidden Files and Directories	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
	Hooking	System Network Configuration Discovery	Hooking	Control Panel Items	Connection Proxy	Forced Authentication	Input Capture	Domain Staging	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking



DeTT&CT
Editor

HOME

DATA SOURCES

Ajustar visibilidad y detección

T1046	Network Service Scanning	
T1047	Windows Management Instrumentation	
T1048	Exfiltration Over Alternative Protocol	
T1065	Uncommonly Used Port	
T1071	Standard Application Layer Protocol	
T1076	Remote Desktop Protocol	
T1090	Connection Proxy	
T1094	Custom Command and Control Protocol	
T1095	Standard Non-Application Layer Protocol	
T1100	Web Shell	
T1102	Web Service	
T1104	Multi-Stage Channels	
T1105	Remote File Copy	
T1171	LLMNR/NBT-NS Poisoning and Relay	
T1188	Multi-hop Proxy	
T1189	Drive-by Compromise	
T1192	Spearphishing Link	
T1193	Spearphishing Attachment	
T1219	Remote Access Tools	
T1221	Template Injection	
T1483	Domain Generation Algorithms	

Score date: 2020-04-12

-1 1 2 3 4 5

Score logbook

Custom key value pairs

Add detection

Visibility

all

Visibility is applicable to

all

applicable to



Ac

Comment

...

Score date: 2020-04-10

0 1 2 3 4

Score logbook

Custom key value pairs

Visibilidad

- <https://github.com/rabobank-cdc/DeTECT/wiki/Visibility-coverage>
- Genera un fichero JSON con la cobertura de visibilidad en base a la plantilla de administración de técnicas: `python dettect.py v -ft sample-data/techniques-administration-endpoints.yaml -fd sample-data/data-sources-endpoints.yaml -l`
- La leyenda indica el tipo de visibilidad en base al input proporcionado.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Clipboard Data	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Data from Information Repositories	Data from Local System	Data Transfer Size Limits	Defacement	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Exploitation of Remote Services	Custom Command and Control Protocol	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Compile After Delivery	Credentials in Registry	Network Service Scanning	Internal Spearphishing	Data from Network Shared Drive	Data Encoding	Endpoint Denial of Service	Firmware Corruption
	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Share Discovery	Logon Scripts	Pass the Hash	Data from Removable Media	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearnphishing Attachment	Execution through Module Load	Bootkit	Component Firmware	Component Object Model Hijacking	Component Firmware	Network Sniffing	Pass the Ticket	Pass the Ticket	Data Obfuscation	Domain Fronting	legend
Spearnphishing Link	Execution through Module Load	Browser Extensions	Exploitation for Privilege Escalation	Forced Authentication	Connection Proxy	Password Policy Discovery	Remote Desktop Protocol	Remote Desktop Protocol	Data Staged	Domain Generation Algorithms	#BBDEFB Visibility score 1: Minimal
Spearnphishing via Service	Exploitation for Client Execution	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	#64B5F6 Visibility score 2: Medium	#1976D2 Visibility score 3: Good
Supply Chain Compromise	Graphical User Interface	Component Firmware	File System Permissions Weakness	DCShadow	Input Capture	Permission Groups Discovery	Remote Services	Input Capture	Fallback Channels	Multihop Paths	#0D47A1 Multiband
Trusted Relationship	InstallUtil	Component Object Model Hijacking	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Paths	Multi-Stage Channels	#BBDEFB Visibility score 4: Excellent
Valid Accounts	LSASS Driver	Mshta	Create Account	Hooking	Disabling Security Tools	Kerberoasting	Query Registry	Screen Capture	Shared Webroot	Video Capture	Visibility score 1: Minimal
	PowerShell	DLL Search Order	Image File	DLL Search Order	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Shared Webroot	Video Capture	Multiband	Visibility score 2: Medium	Visibility score 3: Good

Detección

- <https://github.com/rabobank-cdc/DeTECT/wiki/Detection-coverage>
- Genera un fichero JSON con la cobertura de detecciones en base a la plantilla de administración de técnicas: `python dettect.py d -ft sample-data/techniques-administration-endpoints.yaml -l`
- La leyenda indica la calidad de las detecciones en base al input proporcionado.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Clipboard Data	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	Applnit DLLs	Applnit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Data from Information Repositories	Data from Local System	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Exploitation of Remote Services	File and Directory Discovery	Exfiltration Over Alternative	Disk Content Wipe	Disk Structure Wipe
Spearnphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Compile After Delivery	Credentials in Registry	File and Directory Discovery	Internal Spearphishing	File and Directory Discovery	Custom Cryptograph Protocol	Custom Cryptograph Protocol	legends
Spearnphishing Attachment	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Compile After Delivery	Network Service Scanning	Logon Scripts	File and Directory Discovery	Data Encoding	#64B5F6	Detection score 0: Forensics
Spearnphishing Attachment	Execution through Module Load	Bootkit	Component Firmware	Component Firmware	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	File and Directory Discovery	Data Obfuscation	#DCEDC8	Detection score 1: Basic
Spearnphishing Link	Execution through Module Load	Browser Extensions	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Network Sniffing	Pass the Ticket	File and Directory Discovery	Domain Fronting	#AED581	Detection score 2: Fair
Spearnphishing via Service	Exploitation for Client Execution	Change Default File Association	Extra Window Memory Injection	Connection Proxy	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	File and Directory Discovery	Email Collection	#8BC34A	Detection score 3: Good
Supply Chain Compromise	Graphical User Interface	Component Firmware	File System Permissions Weakness	Control Panel Items	Hooking	Peripheral Device Discovery	Remote Desktop Protocol	File and Directory Discovery	Input Collection	Fallback Channel	Man in the Middle
Trusted Relationship	InstallUtil	Component Object Model Hijacking	File System Permissions Weakness	DCShadow	Input Capture	Permission Groups Discovery	Remote Services	File and Directory Discovery	Input Collection	Multi-hop Path	#689F38
Valid Accounts	LSASS Driver	Create Account	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Input Prompt	Process Discovery	Replication Through Removable Media	File and Directory Discovery	Man in the Browser	Multi-Stage Channels	#33691E
	Mshta	Create Account	Hooking	Disabling Security Tools	Kerberoasting	Query Registry	Screen Capture	File and Directory Discovery	Multi-Stage Channels	Shared Webroot	#33691E
					LLMNR/NBT-NS Poisoning and Impersonation	Shared Webroot					

Threat Actors

- <https://github.com/rabobank-cdc/DeTECT/wiki/Threat-actor-group-mapping>
- Genera un fichero JSON con el heatmap de solo los grupos en los que estamos interesados (FIN6, FIN7, FIN8): python detetect.py g -g 'fin7,fin8,fin6'
- El resultado está ordenado por técnicas más communes (rojo oscuro)

MITRE ATT&CK® Navigator

The screenshot shows the MITRE ATT&CK Navigator interface with several tabs at the top: FIN6, FIN7, FIN8, Data sources example, Visibility example, Detections example, and FIN6+FIN7+FIN8 - Attack - Windows. Below the tabs is a toolbar with various icons for selection controls, layer controls, and technique controls. The main area is a heatmap grid where rows represent threat actor groups and columns represent attack techniques. The color of each cell indicates the frequency of that technique within that specific group.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Spearphishing Attachment	PowerShell	Scheduled Task	Scheduled Task	Scripting	Credential Dumping	Remote System Discovery	Remote Desktop Protocol	Data Staged	Commonly Used Port	Data Compressed	Account Access Removal
Valid Accounts	Scheduled Task	Registry Run Keys / Startup Folder	Exploitation for Privilege Escalation	Code Signing	Account Manipulation	Account Discovery	Remote File Copy	Automated Collection	Remote File Copy	Data Encrypted	Data Destruction
Spearphishing Link	Scripting	Valid Accounts	Masquerading		Brute Force	Network Service Scanning	Windows Admin Shares	Screen Capture	Standard Application Layer Protocol	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Spearphishing via Service	Command-Line Interface	Application Shimming	Obfuscated Files or Information		Credentials from Web Browsers	Permission Groups Discovery	Application Deployment Software	Video Capture	Standard Cryptographic Protocol	Defacement	
Drive-by Compromise	User Execution	New Service	Valid Accounts		Credentials in Files	Security Software Discovery	Clipboard Data	Clipboard Data	Automated Exfiltration	Disk Content Wipe	
Exploit Public-Facing Application	Windows Management Instrumentation	Shortcut Modification	New Service	Web Service	File Deletion	Component Object Model and Distributed COM	Data from Information Repositories	Web Service	Web Service	Disk Structure Wipe	
	Dynamic Data Exchange	Accessibility Features	Access Token Manipulation	Indicator Removal on Host	File Deletion	Virtualization/Sandbox Evasion	Data from Information Repositories	Communication Through Removable Media	Communication Through Removable Media	Data Transfer Size Limits	
External Remote Services	Mshta	Account Manipulation	Accessibility Features	Modify Registry	Indicator Removal on Host	Application Window Discovery	Exploitation of Remote Services	Data from Local System	Exploitation Over Command and Control Channel	Endpoint Denial of Service	
Hardware Additions	Service Execution	AppCert DLLs	AppCert DLLs	Mshta	Modify Registry	Exploitation for Credential Access	Exploitation of Remote Services	Data from Local System	Connection Proxy	Firmware Corruption	
Replication Through Removable Media	CMSTP	Apnlt DLLs	Apnlt DLLs	Virtualization/Sandbox Evasion	Mshta	Forced Authentication	Browser Bookmark Discovery	Internal Spearphishing	Custom Command and Control Protocol	Inhibit System Recovery	
	Compiled HTML File	Bypass User Account Control	Bypass User Account Control	Virtualization/Sandbox Evasion	Apnlt DLLs	Hooking	Domain Trust Discovery	Logon Scripts	Data from Network Shared Drive	Exfiltration Over Other Network Medium	
	Component Object Model	Authentication Package	Access Token Manipulation	DLL Search	Access Token Manipulation	Input Capture	File and Directory Discovery	Pass the Hash	Data from Removable Media	Custom Cryptographic Protocol	Resource Hijacking
	Model Load							Pass the Ticket	Custom Cryptographic Protocol	Exfiltration Over Physical	Runtimes Data

Data sources example x

Visibility example x

Detections example x

Attack - Windows x

Attack - Windows, Linux, macOS x

Attack - Windows, Linu

selection controls layer controls technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Imp
11 items	34 items	62 items	42 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	Windows Management Instrumentation	Accessibility Features	Accessibility Features	Connection Proxy	LLMNR/NBT-NS Poisoning and Relay	Network Service Scanning	Internal Spearphishing	Audio Capture	Standard Application Layer Protocol	Exfiltration Over Alternative Protocol	End-Service
Spearphishing Attachment	Windows Remote Management	Registry Run Keys	Process Injection	Obfuscated Files or Information	Network Sniffing	Network Sniffing	Remote Desktop Protocol	Automated Collection	Standard Non-Application Layer Protocol	Data Transfer Size Limits	Netw
Spearphishing Link	Command-Line Interface	.bash_profile and .bashrc	Access Token Manipulation	Template Injection	Account Manipulation	Account Discovery	Clipboard Data	Clipboard Data	Multi-hop Proxy	Scheduled Transfer	Acc
Exploit Public Facing Application	PowerShell	Account Manipulation	AppCert DLLs	Web Service	Bash History	Application Window Discovery	Remote File Copy	Data from Information Repositories	Commonly Used Port	Automated Exfiltration	Data Imp
External Remote Services	Scripting	AppCert DLLs	AppInit DLLs	Disabling Security Tools	Masquerading	Bash History	Windows Remote Management	Data from Local System	Connection Proxy	Data Compressed	Defa
Hardware Additions	AppleScript	AppInit DLLs	Application Shimming	Process Injection	Brute Force	Browser Bookmark Discovery	AppleScript	Data from Network Shared Drive	Custom Command and Control Protocol	Data Encrypted	Disk
Replication Through Removable Media	CMSTP	Compiled HTML File	Bypass User Account Control	Scripting	Credential Dumping	Domain Trust Discovery	Application Deployment Software	Data from Removable Media	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firm
Supply Chain Compromise	Component Object Model and Distributed COM	Authentication Package	DLL Search Order Hijacking	Bypass User Account Control	Credentials from Web Browsers	File and Directory Discovery	Component Object Model and Distributed COM	Data from Peripheral Device Discovery	Domain Generation Algorithms	Inhib Rec	Res
Trusted Relation	BITS Jobs	Dylib Hijacking	Binary Padding	Access Token Manipulation	Credentials in Files	Network Share Discovery	Logon Scripts	Data Staged	Email Collection	Exfiltration Over Other Network Medium	Run Man
Valid Ac	Supply Chain Compromis	Code Signing	BITS Jobs	Authentication Package	_credentials in Registry	Password Policy Discovery	Pass the Hash	Input Capture	Fallback Channels	Multi-Stage Channels	Exfiltration Over Physical Medium
	Trusted Relation	Compile After Delivery	Dylib Hijacking	DLL Search Order Hijacking	Bypass User Account Control	Peripheral Device Discovery	Man in the Browser	Man in the Browser	Screen Capture	Multiband Communication	Stor Man
	Valid Ac	Input Capture	Binary Padding	Component Object Model Hijacking	CMSTP	Process Discovery	Multi-Stage Channels	Multi-Stage Channels	Video Capture	Remote Access Tools	System Shu
		Input Prompt	Component Firmware	Code Signing	Forced Authentication	Query Registry	Screen Capture	Screen Capture	Video Capture	Remote File Copy	Trans Man
		Kerberoasting	Compiled HTML File	Component Object Model Hijacking	Hooking	Remote System Discovery	Replication Through Removable Media	Replication Through Removable Media	Standard Cryptograph	Standard Cryptograph	legen
		Keychain	Create Account	File System Permissions Weakness	Input Capture	Security Software Discovery	Shared Webroot	Shared Webroot	Protocol	Protocol	
		SSH Hijacking	Graphical User Interface	DLL Search Order Hijacking	Input Prompt	Software Discovery	Taint Shared	Taint Shared			
		System Information Discovery	InstallUtil	File System Permissions Weakness	Kerberoasting	System Information Discovery					
		Control Panel Items		Component Object Model Hijacking	Keychain	Control Panel Items					
				Control Panel Items	Pass the Hash						
					Pass the Ticket						
					Man in the Browser						
					Multi-Stage Channels						
					Screen Capture						
					Video Capture						
					Standard Cryptograph						

Gap Análisis de Visibilidad (Purple Teaming)

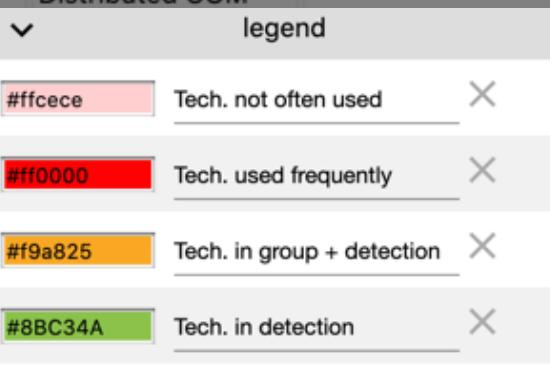


legend

- #ffcece Tech. not often used
- #ff0000 Tech. used frequently
- #f9a825 Tech. in group + visibility
- #1976D2 Tech. in visibility

Gap Análisis de Detección (Purple Teaming)

Potential Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command Control	
Items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	
Spearphishing Attachment	Command Line Interface	Accessibility Features	Accessibility Features	Connection Proxy	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Domain Generation Algorithms	
Drive-by Impersonation	PowerShell Scripting	Registry Run Keys / Startup Folder	Process Injection	Disabling Security Tools	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Clipboard Data	
Exploit Public-facing Application	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Masquerading	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Data from Information Repositories	Common Port	
Internal Remote Services	MSFSP	Account Manipulation	AppCert DLLs	Process Injection	Credential Dumping	Domain Trust Discovery	Data from Local System	Exploitation of Remote Services	Connect	
Hardware Conditions	Compiled HTML File	AppCert DLLs	Applnit DLLs	Scripting	Access Token Manipulation	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Network Shared Drive	
Application through Removable Media	Component Object Model and Distributed COM	Applnit DLLs	Application Shimming	Binary Padding	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Removable Media	Custom and Con.	
Spearphishing Link	#ffcece	Tech. not often used	Bypass User Account Control	BITS Jobs	Credentials in Registry	Network Share Discovery	Pass the Hash	Data Staged	Custom Cryptog.	
Spearphishing Service	#ffff00	Tech. used frequently	DLL Search Order Hijacking	Bypass User Account Control	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Data Enc.	
Supply Chain Impromise	#f9a825	Tech. in group + detection	CMSTP	Clear Command History	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Email Collection	Custom Cryptog.	
Established Relationship	#8BC34A	Tech. in detection	Dylib Hijacking	Dylib Hijacking	Code Signing	Permission Groups Discovery	Remote File Copy	Input Capture	Data Ob.	
Exploration for Client Execution	Change Default File Association	Elevated Execution with Prompt	Elevated Execution with Prompt	Compile After Delivery	Hooking	Process Discovery	Remote Services	Man in the Browser	Domain Fallback	
Graphical User Interface	Graphical User Interface	Emond	Emond	Compiled HTML File	Input Capture	Query Registry	Replication Through			
Exploitation for Persistence	Change Default File Association	Exploitation for Persistence	Exploitation for Persistence	Component Firmware	Input Prompt					



Recursos adicionales

@aboutsecurity

- Thinking Red, Acting Blue -
<https://www.sans.org/webcasts/defensible-security-architecture-engineering-2-thinking-red-acting-blue-mindset-actions-109710>
- Guión de esta charla -
<https://github.com/aboutsecurity/Talks-and-Presentations/blob/master/c0r0n4con.md>
- The Githubification of InfoSec by John Lambert -
<https://medium.com/@johnlatwc/the-githubification-of-infosec-afbdbfaad1d1>
- DETT&CT - <https://github.com/rabobank-cdc/DeTECT>
- MITRE's Red Teaming dataset -
<https://github.com/mitre/brawl-public-game-001>