

DeTT&CT

Mapping your blue team to ATT&CK™

23-10-2019

ATT&CK™



Rabobank

Ruben Bouman

- Freelance Cyber Defense Expert
- Co-owner Sirius Security
- Roots in development
- Nine years of experience in Info Security
- Co-developer of the DeTT&CT framework

 @RubenB_2



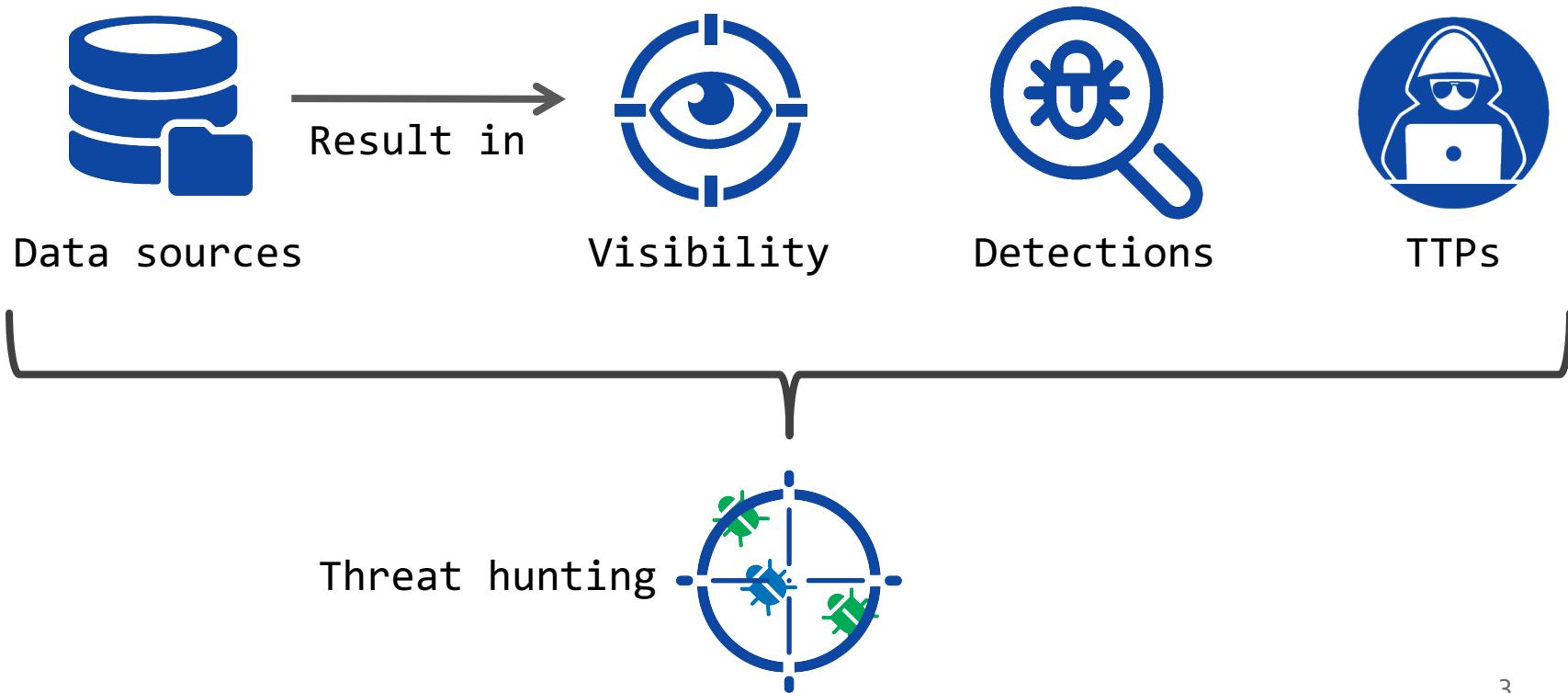
Marcus Bakker

- Freelance Cyber Defense Expert
- Nine years of experience in Info Security
- Co-developer of the DeTT&CT framework
- Co-author of the TaHiTI Threat Hunting Methodology

 @Bakk3rM

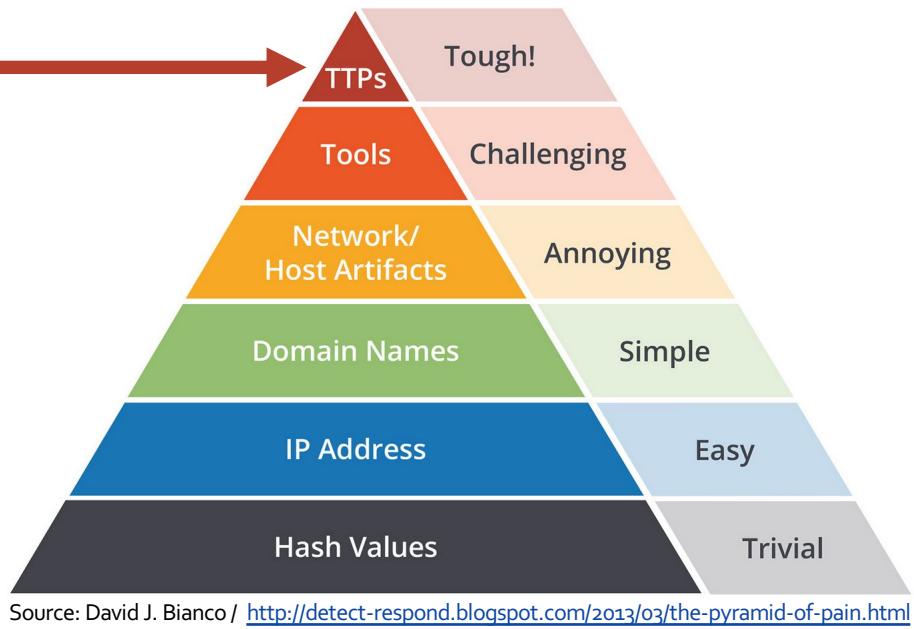


- Intelligence-driven approach with a focus on TTPs





“Wikipedia on cyber attacks”

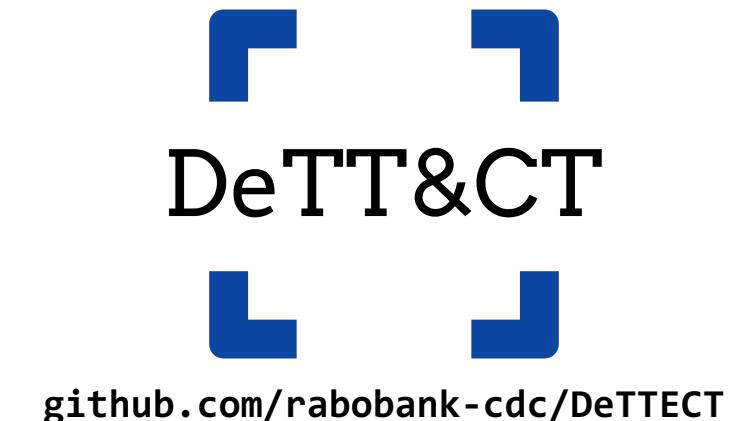


Cyber Kill Chain

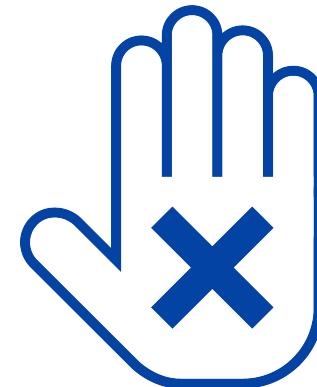


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding	Network Sniffing	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction	
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Encrypted for Impact	
External Remote Services	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Transfer Size Limits	Defacement
Hardware Additions	LSASS Driver		Extra Window Memory Injection		Brute Force		Data from Information Repositories	Data from Local System	Custom Command and Control Protocol	Disk Content Wipe	Disk Structure Wipe
Replication Through Removable Media	Trap		Process Injection		Credential Dumping	Browser Bookmark Discovery	Data from Network Shared Drive	Data from Removable Media	Exfiltration Over Other Network Medium	Endpoint Denial of Service	
Spearphishing Attachment	AppleScript	DLL Search Order Hijacking		Credentials in Files	Domain Trust Discovery	Custom Cryptographic Protocol	Data from Local System	Data Staged	Exfiltration Over Command and Control Channel	Firmware Corruption	Inhibit System Recovery
Spearphishing Link	CMSTP	Image File Execution Options Injection		Credentials in Registry	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service	
Spearphishing via Service	Compiled HTML File	Plist Modification		Exploitation for Credential Access	Network Service Scanning	Pass the Hash	Data from Removable Media	Data Obfuscation	Resource Hijacking	Rumtime Data Manipulation	
Supply Chain Compromise	Control Panel Items	Valid Accounts		Forced Authentication	Network Share Discovery	Pass the Ticket	Domain Fronting	Email Collection	Exfiltration Over Physical Medium	Service Stop	
Trusted Relationship	Dynamic Data Exchange	AppCert DLLs	BITS Jobs	Hooking	Password Policy Discovery	Remote Desktop Protocol	Domain Generation Algorithms	File Staged	File Obfuscation	Scheduled Transfer	Stored Data Manipulation
Valid Accounts	Execution through API	Applnit DLLs	Clear Command History	Input Capture	Peripheral Device Discovery	Remote File Copy	Man in the Browser	Screen Capture	Fallback Channels		
	Execution through Module Load	Application Shimming	CMSTP	Input Prompt	Permission Groups Discovery	Remote Services		Video Capture	Multiband Communication		
	Application Shimming	Dylib Hijacking	Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media			Multi-hop Proxy		
	File System Permissions Weakness	Component Firmware	Keychain	Query Registry	Remote System Discovery	Shared Webroot			Multilayer Encryption		
Graphical User Interface	Hooking	Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay		Security Software Discovery	SSH Hijacking			Multi-Stage Channels		
InstallUtil	Launch Daemon	New Service	Control Panel Items	Input Filter DLL	System Information Discovery	Taint Shared Content			Port Knocking		
Mshta	Path Interception	Deobfuscate/Decode Files or Information	DCShadow	Private Keys	Third-party Software	Windows Admin Shares			Remote Access Tools		
PowerShell	Port Monitors	Setuid and Setgid	Disabling Security Tools	Securityd Memory	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
Regsvcs\Regasm	Service Registry Permissions Weakness	StartupScript Items	DLL Side-Loading			System Network Connections Discovery			Standard Application Layer Protocol		
Regsvr32	Rundll32	Startup Items	Execution Guardrails			System Owner/User Discovery			Standard Cryptographic Protocol		
Scripting	Web Shell					System Service Discovery			Standard Non-Application Layer Protocol		
Service Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Exploitation for Defense Evasion			System Time Discovery			Uncommonly Used Port		
Signed Binary Proxy Execution	Account Manipulation	Authentication Package	SID-History Injection	File Deletion		Virtualization/Sandbox Evasion			Web Service		
Signed Script Proxy Execution	BITS Jobs	Sudo	Sudo Caching	File Permissions Modification							
Source	Browser Extensions			File System Logical Offsets							
Space after Filename	Change Default File Association			Gatekeeper Bypass							
Third-party Software	Component Firmware			Group Policy Modification							
Trusted Developer Utilities	Hidden Files and Directories			Hidden Files and Directories							
User Execution	Component Object Model Hijacking			Hidden Users							
Windows Management Instrumentation	Create Account			Hidden Window							
Windows Remote Management	External Remote Services			HISTCONTROL							
XSL Script Processing	Hidden Files and Directories			Indicator Blocking							
	Kernel Modules			Indicator Removal from Tools							
				Indicator Removal on Host							

- Framework to administrate, score and compare:
 - Data source quality
 - Visibility
 - Detections
 - Threat actor behaviours
- Result: where do you focus on
 - Which techniques?
 - Where to improve visibility?
- Scoring tables to guide you
- Administration = YAML files



All shown data and visualisation regarding data quality, visibility, detection and threat actor groups are based on sample data.





Identify data sources

Process injection

ID: T1055

Tactic: Defense Evasion, Privilege Escalation

Platform: Linux, macOS, Windows

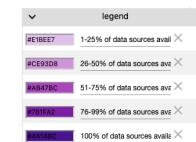
Permissions Required: User, Administrator, SYSTEM, root

Effective Permissions: User, Administrator, SYSTEM, root

Data Sources: API monitoring, Windows Registry, File monitoring, DLL monitoring, Process monitoring, Named Pipes

- Score data quality (DQ)
- Visualise in the ATT&CK Navigator
- Export to Excel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Account Manipulation	Account Discovery	Application Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction	
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Manipulation	Binary Padding	Brute Force	Application Window Discovery	Communication Through Removable Media	Data Compressed	Communication Through Data Impact	Data Encrypted for Impact	
External Remote Services	Compiled HTML File	AppCert DLLs	Accessibility Features	BITS jobs	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Transfer Size Limit	Defacement
Hardware Addition	Control Panel Item	AppInit DLLs	AppCert DLLs	Bypass User Account Control	Credentials In Metadata	Available: Domain Trust Discovery	Data from Information Repositories	Custom Command and Control	Custom Command and Control	Disk Content Wipe	Disk Structure Wipe
Replication Through Removable Media	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials In	Exploitation for Powershell logs	Exploitation of Remote Services	data from Local System	Custom Cryptographic Protocol	Encryption Over Alternative Protocol	End-to-End Denial of Service
Replication Through Removable Media	Execution through Module Load	Bypass User Account Control	Code Signing	Forced Author	Exploitation for monitoring, logging, and scanning	Forced Author	File Monitoring, Log Monitoring, Process Monitoring, Process Scanning	Logon Scripts	Exfiltration Over Command and Control Channel	Firmware Corruption	
Spearphishing Attachment	Execution through Module Load	BITS Jobs	Compile After Delivery	Forced Author	Forced Author	Forced Author	Forced Author	Pass the Hash	Data Encoding	Data Obfuscation	Initial System Recovery
Spearphishing Attachment	Exploration for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Hooking	Input Capture	Input Capture log	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Network Denial of Service
Spearphishing Link	Execution	Browser Extensions	Component Object Model	Hijacking	Input Prompt	Input Peripheral Device Discovery	Input Peripheral Device Discovery	Man in the Browser	Multi-hop Proxy	Network Manipulation	Runtime Data Manipulation
Spearphishing via Device Driver	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Kerberoasting	Input Query Registry	Input Remote Desktop	Input Shared Content	Shared Webroot	Screen Capture	Multi-Stage Channels	Resource Hijacking
Supply Chain Compromise	InstallUI	Component Firmware	Extra Window Memory Injection	LLMNR/NBT-NS Poisoning and Relay	Input Replication Through Removable Media	Input Remote Desktop	Input Remote Services	Input Screen Capture	Video Capture	Multiband Communication	Runtime Data Manipulation
Trusted Relationship	LSASS Driver	Component Object Model	File System Permissions	Network Sniffing	Input Security Software Discovery	Input Shared Content	Input Shared Content	Input Shared Content	Video Capture	Multilayer Encryption	Stored Data Manipulation
Valid Accounts	Malta	Component Object Model Hijacking	Weakness	Obfuscate/Decode Files or Information	Input System Information Discovery	Input System Network Connections Discovery	Input System Owner/User Discovery	Input System Time Discovery	Windows Admin Shares	Remote Access Tools	Transmitted Data Manipulation
	PowerShell	Create Account	Information	Pass the Hash	Input System Monitoring	Input System Network Connections Discovery	Input System Service Discovery	Input System Time Discovery	Windows Remote Management	Remote File Copy	
	Regvics/Regasm	DLL Search Order Hijacking	Hijacking	Hooks	Input Template Injection	Input Virtualization/Sandbox Evasion	Input Virtualization/Sandbox Evasion	Input Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	
	Rgbsrv32	External Remote Services	Image File Execution Options	Image File Execution Options	Input Web Shell	Indicator Blocking	Indicator Removal from Tools	Indicator Removal on Host	Indicator Removal on Network	Standard Application Layer Protocol	
	Scheduled Task	File System Permissions	Image File Execution Options	Image File Execution Options	Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	Standard Cryptographic Protocol	
	Scripting	Hidden Files and Directories	Path Interception	Path Interception	Install Root Certificate	InstallUtil	InstallUtil	InstallUtil	InstallUtil	Standard Non-Application Layer Protocol	
	Service Execution	Port Monitors	Process Execution	File Deletion	Masquerading	Modify Registry	Modify Registry	Modify Registry	Modify Registry	Uncommonly Used Port	
	Signed Binary Proxy Execution	Scheduled Task	Signed Script Proxy Execution	File Permissions Modification	MShta	MShta	MShta	MShta	MShta	Web Service	
	Signed Script Proxy Execution	Service Registry Permissions	Service Registry Permissions	File System Logical Offsets	Network Share Connection Removal	Network Share Connection Removal	Network Share Connection Removal	Network Share Connection Removal	Network Share Connection Removal		
	Third-party Software	Weakness	Weakness	Group Policy Modification	NTFS File Attributes	Obfuscated Files or Information	Obfuscated Files or Information	Obfuscated Files or Information	Obfuscated Files or Information		
	Trusty Developer Utilities	Logon Scripts	SID-History Injection	Hidden Files and Directories	Process Doppelganging	Process Doppelganging	Process Doppelganging	Process Doppelganging	Process Doppelganging		
	Trusty Developer Utilities	LSASS Driver	Valid Accounts	Image File Execution Options	Process Hollowing	Process Hollowing	Process Hollowing	Process Hollowing	Process Hollowing		
	Trusty Developer Utilities	Modify Existing Service	Web Shell	Injection	Process Injection	Process Injection	Process Injection	Process Injection	Process Injection		
	Windows Management Instrumentation	Ntsh Helper DLL	Path Interception	Redundant Access	Redundant Access	Redundant Access	Redundant Access	Redundant Access	Redundant Access		
	Windows Remote Management	New Service	Port Monitors	Rootkit	Rootkit	Rootkit	Rootkit	Rootkit	Rootkit		
	XSL Script Processing	Office Application Startup	Redundant Access	Rundll32	Rundll32	Rundll32	Rundll32	Rundll32	Rundll32		
		Registry Run Keys / Startups	Scheduled Task	Scripting	Signed Binary Proxy Execution	Signed Binary Proxy Execution	Signed Binary Proxy Execution	Signed Binary Proxy Execution	Signed Binary Proxy Execution		
			Screen Saver	Signed Script Proxy Execution	Signed Script Proxy Execution	Signed Script Proxy Execution					
			Security Support Provider	SIP and Trust Provider Hijacking	SIP and Trust Provider Hijacking	SIP and Trust Provider Hijacking					
			Service Registry Permissions Weakness	System Firmware	System Firmware	System Firmware	System Firmware	System Firmware	System Firmware		
			Shortcut Modification	Time Providers	Time Providers	Time Providers	Time Providers	Time Providers	Time Providers		
			SIP and Trust Provider Hijacking	Windows Management Instrumentation Event Subscription	Windows Management Instrumentation Event Subscription	Windows Management Instrumentation Event Subscription					
				Winlogon Helper DLL	Winlogon Helper DLL	Winlogon Helper DLL	Winlogon Helper DLL	Winlogon Helper DLL	Winlogon Helper DLL		





- Manual score visibility
 - Allows you to be exact
 - One source is more important than the other
 - Minimal set of data sources to have useful visibility
- Administrate in YAML file
- Visualise in the ATT&CK Navigator
- Export to Excel

Visibility scores

Score	Score name	Description
0	None	No visibility at all.
1	Minimal	Sufficient data sources with sufficient quality available to be able to see one aspect of the technique's procedures.
2	Medium	Sufficient data sources with sufficient quality available to be able to see more aspects of the technique's procedures compared to "1/Minimal".
3	Good	Sufficient data sources with sufficient quality available to be able to see almost all known aspects of the technique's procedures.
4	Excellent	All data sources and required data quality necessary to be able to see all known aspects of the technique's procedures are available.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Account Manipulation	Application Deployment Software	Audio Capture	Community Used Port	Data Encrypted for Impact	Data Exfiltration	Data Encryption	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Access Token Manipulation	Binary Padding	Brute Force	Application Window Discovery	Automated Collection	Communication Through Metadatas	Custom Command	Data Encrypted for Impact	Data Exfiltration
External Remote Services	Compiled HTML File	AppCraft DLLs	Accessories Features	Bypass JBS Jobs	Credential Dumping	Browser Bookmarks Discovery	Clipboard Data	Custom Command	Data from Information Model	Data Monitoring	Data Protection
Hardware Aborts	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	AppCraft DLLs	Credentials in Files	Domain Trust Discovery	Distributed Object Model	Disk Content Wipe	Disk Structure Wipe	Disk Wipe	Disk Wipe
Replication Through API	Execution through API	Authentication Packags	Code Signing	Comprehensive Exploitation	Comprehensive Privilege Escalation	File and Directory Discovery	File from Local System	File from Network	File Staged	File Transfer	File Transfer
Removable Media	Execution Through Module Spoofering Attack	BITS Jobs	Control	Compile After Delivery	Custom Cryptographic Protocol	Custom Service Scanning	Customized Command	Data from Local System	Data Obfuscation	Data Obfuscation	Data Obfuscation
Remote User Authentication	Execution for Client	BITS Jobs	Control	Customization of Application	Data from Network	Data from Removable Media	Data Monitoring	Data Staged	Data Transfer	Data Transfer	Data Transfer
Screenerphishing Link	Execution	Browser Extensions	Change Default File Extension	Compromised Executable	Decompression	Device Communication	Device Monitoring	Device Removal	Device Staged	Device Transfer	Device Transfer
Screenerphising via Service	Graphical User Interface	Component Firmware	DLL Search Order Hijacking	Disk Shadowing	DiskShadow	Disk Sniffing	Disk Write	DiskWrite	DiskWrite	DiskWrite	DiskWrite
Supply Chain Compromise	Installation	Component Object Model Hijacking	Extra Window Memory Interception	Fake System Permissions	File Copy	File from Network	File Monitoring	File Staged	File Transfer	File Transfer	File Transfer
Trusted Relationship	LSASS Driver	Component Object Model Hijacking	Fake System Permissions	Fake System Weakness	File Interception	File Monitoring	File Staged	File Transfer	File Transfer	File Transfer	File Transfer
Valid Accounts	PowerShell	CredSSP Account	Hijacking	Hijacking	Hijacking	Hijacking Security Tools	Hijacking Filter DLL	Hijacking Shared Websocket	Hijacking Shared Websocket	Hijacking Shared Websocket	Hijacking Shared Websocket
Reqwest/Reqwest	Regsvr32	DLL Side-Order Hijacking	Hijacking File Execution Options	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception
Rundll32	External Remote Services	Rundll32	Hijacking File and Directories	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception	Hijacking File Interception
Scheduled Task	File System Permissions Walkthrough	New Service	Path Interception	Exploitation for Defense Evasion	Two-Factor Authentication	Image File Discovery	Image File Discovery	Image File Discovery	Image File Discovery	Image File Discovery	Image File Discovery
Scripting	Hyper-V	Hyper-V	Port Monitor	Extra Window Memory Injection	Indicator Blocking	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools
Service Execution	Signed Binary Proxy	Hijacking	Process Injection	File Deletion	File Deletion	File Deletion	File Deletion	File Deletion	File Deletion	File Deletion	File Deletion
Signed Binary Proxy	Execution	Hyper-V	Hyper-V	File Permissions Modification	File Permissions Modification	File System Offsets	File System Offsets	File System Offsets	File System Offsets	File System Offsets	File System Offsets
Third-party Software	Image File Execution Options	Image File Interception	Image File Interception	File Permissions Modification	File System Offsets	File System Offsets	File System Offsets	File System Offsets	File System Offsets	File System Offsets	File System Offsets
Trusted Developer Utilities	LSASS Driver	SID-History Injection	Hidden Files and Directories	Hidden Files and Directories	Hidden Files and Directories	Image File Execution Options	Image File Execution Options	Image File Execution Options	Image File Execution Options	Image File Execution Options	Image File Execution Options
User Execution	Modify Existing Service	Valid Accounts	Image File Interception	Image File Interception	Image File Interception	Indicator Blocking	Indicator Blocking	Indicator Blocking	Indicator Blocking	Indicator Blocking	Indicator Blocking
Windows Management	Notch Helper DLL	Web Shell	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools
Windows Remote Management	New Service	Web Shell	Indirect Command Execution	Install Root Certificate	Indirect Command Execution	Install Root Certificate	Install Root Certificate	Install Root Certificate	Install Root Certificate	Install Root Certificate	Install Root Certificate
XSL Script Processing	Office Application	Windows Remote Management	Port Monitors	InstallUtil	InstallUtil	Masquerading	Masquerading	Masquerading	Masquerading	Masquerading	Masquerading
File Interception	Port Monitors	Reduced Access	Registry Run Keys / Startup Folder	Modifying Registry	Modifying Registry	Modifying Registry	Modifying Registry	Modifying Registry	Modifying Registry	Modifying Registry	Modifying Registry



- Manual score detection
- Administrated in the same YAML file as visibility
- Visualise in the ATT&CK Navigator
- Export to Excel

Detection scores

Score	Score name	Description	Initial Access	Execution	Persistence	Pivilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
-1	None	No detection.	7 items	37 items	42 items	57 items	57 items	58 items	72 items	73 items	73 items	74 items	74 items	74 items
0	Forensics / context	No detection, but the technique is being logged for forensic purposes and can be used to provide context.	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item
1	Basic	Detection is in place using a basic signature to detect a specific part(s) of the technique's procedures. Therefore, only a very small number of aspects of the technique are covered. Hence number of false negatives is high and possible (but not necessarily) a high false positive rate. Detection is possibly not real time.	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item
2	Fair	The detection no longer only relies on a basic signature but makes use of a (correlation) rule to cover more aspects of the technique's procedures. Therefore, the number of false negatives is lower compared to "1/Poor" but may still be significant. False positives may still be present. Detection is possibly not real time.	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item
3	Good	Effective in detecting malicious use of the technique by making use of more complex analytics. Many known aspects of the technique's procedures are covered. Bypassing detection by means of evasion and obfuscation could be possible. False negatives are present. False positives may still be present but are easy to recognize and can possibly be filtered out. Detection is real time.	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item
4	Very good	Very effective in detecting malicious use of the technique in real time by covering almost all known aspects of the technique's procedures. Bypassing detection by means of evasion and obfuscation methods is harder compared to level "3/good". The number of false negatives is low but could be present. False positives may still be present but are easy to recognize and can possibly be filtered out.	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item
5	Excellent	Same level of detection as level "4/very good" with one exception: all known aspects of the technique's procedures are covered. Therefore, the number of false negatives is lower compared to level "4/very good".	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item	1 item





- Generate heat maps
 - Threat actor group data from ATT&CK
 - Own intel stored in a group YAML file
 - Threat actor data from third parties *₁
- Compare threat actors

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Spearing Phishing Attachment	Scripting	Registry Run Keys / Startup Folder	Valid Accounts	Scripting	Credential Dumping	Process Discovery	Remote File Copy	Data from Local System	Remote File Copy	Data Compressed	Disk Structure Wipe
Valid Accounts	PowerShell	Scheduled Task	Obfuscated File or Information	Input Capture	System Information Discovery	Remote Desktop Protocol	T1105 - Staged Persistence	Standard Application Layer Protocol	Data Encrypted	Data Destruction	
Spearing Phishing Link	Command-Line Interface	Scheduled Task	Process Injection	Valid Accounts	Brute Force	System Network Configuration Discovery	Windows Admin Shares	Metadata	Exfiltration Over Command and Control Channel	Data Encrypted for Impact	
Drive-by Compromise	External Remote Services	New Service	File Deletion	Credentials in Files	File and Directory Discovery	System Owner/User Discovery	Remote Services	Commonly Used Port	Web Services	Stored Data Manipulation	
External Remote Services	Exploitation for Client Execution	Web Shell	Masquerading	Account Manipulation	Network Sniffing	Remote System Discovery	Pass the Hash	Standard Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	
Exploit Public-Facing Application	Windows Management Instrumentation	Shortcut Modification	Deobfuscate/Decode Files or Information	Forced Authentication	Software Packing	Credentials in Registry	Account Discovery	Connection Proxy	Automated Exfiltration	Resource Hijacking	
Replication Through Removable Media	Dynamic Data Exchange	Accessibility Features	Exploitation for Privilege Escalation	Windows Service	Hooking	System Network Connections Discovery	Exploitation of Services	Uncommonly Used Port	Data Transfer Size Limits	Runtime Data Manipulation	
Spearing via Rundll32 Service	Rundll32	Create Account	Code Signing	Input Prompt	Network Service Scanning	Logon Scripts	Data Encoding	Data Encoding	Exfiltration Over Other Network Medium	Service Stop	
Trusted Relationship	Regsvr32	Hidden Files and Directories	Access Token Manipulation	Modify Registry	Exploitation for Credential Access	Security Software Discovery	Replication Through Repositories	Custom Command and Control Protocol	Transmitted Data Manipulation		
Supply Chain Compromise	Service Execution	DLL Search Order Hijacking	Process Injection	Bypass User Account Control	Kerberoasting	Query Registry	Data from Information Repositories	Remote Access Tools	Exfiltration Over Physical Medium		
Hardware Additions	Compiled HTML File	Accumulation	AppCert DLLs	Disabling Security Tools	LLMNR/NBT-NS Poisoning and Relay	Application Deployment	Clipboard Data	Custom Cryptographic Protocol			
Masta	Execution through API	Modify Existing Service	Application Shimming	DLL Side-Loading	Password Filter DLL	Deployment Software	Man in the Browser	Standard Non-Application Layer Protocol			
WMI Management	Execution	Instrumentation Event	Options Injection	Indicator Removal from Tools	Private Keys	Network Service Discovery	Taint Shared Content	Data Obfuscation			
Signed Binary Proxy Execution	Signed Binary Proxy	BITS Jobs	Port Monitors	Indicator Removal on Host	Two-Factor Authentication Interception	Distributed Component Object Model	Third-party Software	Fallback Channels			
CMSIPT	Execution	Bootkit	AppInit DLLs	Indicator Removal from Tools	Network Share Discovery	Component Object Model	Network Sniffing	Multi-hop Proxy			
Graphical User Interface	Signed Script Proxy Execution	DLL Search Order Hijacking	Redundant Access	Indicator Removal on Host	Peripheral Device Discovery	Application Window Discovery	Virtualization/Sandbox Evasion	Multi-Stage Channels			
Logon Scripts	Execution	Extra Window Memory Injection	Path Interception	Timestamp	Shared Webroot	Shared Webroot	Shared Webroot	Communication Through Removable Media			
Windows Remote Management	Windows Remote Management	Office Application Startup	Binary Padding	Access Token Manipulation	System Time Discovery	Third-party Software	Third-party Software	Domain Fronting			
XSL Script Processing	Winlogon Helper DLL	Weakness	File System Permissions	Permissions	Network Sniffing	Network Share Discovery	Windows Remote Management	Multi-hop Fronting			
Control Panel Items	AppCert DLLs	Weakness	Hidden Files and Directories	Weakness	Virtualization/Sandbox Evasion	Browser Bookmark Discovery	Domain Trust Discovery	Multi-layer Communication			
Execution Through Module Load	Application Shimming	SID-History Injection	Template Injection	Weakness	Compile After Delivery	Component Object Model	Domain Generation Algorithms	Domain Generation Algorithms			
InstallUtil	Browser Extensions	Component Firmware	Process Hollowing	Weakness	Component Firmware	Exploit for Defense Evasion	Multi-layer Encryption	Multi-layer Encryption			
LSASS Driver	Component Object Model Hijacking	Component Firmware	Signed Binary Proxy Execution	BITS Jobs	Rootkit	File Permissions Modification					
Trusted Developer Utilities	Hooking	Image File Execution Options Injection	Execution Guardrails	CMSTP							
	Port Monitors	Port Monitors	Rootkit								
	ApInit DLLs	ApInit DLLs	Virtualization/Sandbox Evasion								
	Authentication Package	Authentication Package	Compile After Delivery								
	Change Default File Association	Change Default File Association	Component Firmware								
	File System Permissions Weakness	File System Permissions Weakness	Component Object Model Hijacking								
	Hypervisor	Hypervisor	Exploit for Defense Evasion								
	LSASS Driver	LSASS Driver	File Permissions Modification								

*₁ <https://github.com/rabobank-cdc/DeTTECT/tree/master/threat-actor-data>



- Generate heat maps
 - Threat actor group data from ATT&CK
 - Own intel stored in a group YAML file
 - Threat actor data from third parties *₁
- Compare threat actors

```
%YAML 1.2
---
version: 1.0
file_type: group-administration
groups:
  - group_name: Red team
    campaign: Scenario 1
    technique_id: [T1086, T1053, T1193, T1204, T1003, T1055, T1027, T1085, T1099, T1082, T1016, T1033, T1087, T1075, T1057, T1039, T1041, T1071, T1043, T1001, T1114, T1002]
    software_id: [S0002] # Mimikatz
    enabled: True
```



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Spearphishing Attachment	PowerShell	Scheduled Task	Process Injection	Obfuscated Files or Information	Credential Access	Account Discovery	Pass the Hash	Data from Network Shared Drive	Commonly Used Port	Data Compressed	Data Destruction
Drive-by Compromise	Rundll32	Accessibility Features	Scheduled Task	Process Injection	Process Discovery	System Information Discovery	Deployment Software	Email Collection	Standard Application Layer Protocol	Data Obfuscation	Data Encrypted for Impact
Exploit Public-Facing Application	Scheduled Task	Account Manipulation	User Execution	Timestamp	Brute Force	System Network Configuration Discovery	Distributed Component Object Model	Audio Capture	Exfiltration Over Command and Control Channel	Defacement	Disk Content Wipe
External Remote Services	CMSTP	AppCert DLLs	CMSTP	Access Token Manipulation	Credentials in Files	System Owner/User Discovery	Automated Collection	Communication Through Removable Media	Automated Exfiltration	Data Encrypted	Disk Structure Wipe
Hardware Additions	AppInit DLLs	Accessibility Features	AppInit DLLs	Access Token Manipulation	Credentials in Registry	Application Window Discovery	Clipboard Data	Connection Proxy	Data Transfer	Custom Command and Control Protocol	Endpoint Denial of Service
Replication Through Removable Media	Compiled HTML File	Application Shimming	Control Panel Items	Binary Padding	Exploitation for Credential Access	Browser Bookmark Discovery	Logon Scripts	Data from Information Repositories	Custom Size Limits	Custom Command and Control Protocol	Firmware Corruption
					Bypass User Account Control	Pass the Ticket	Remote Desktop Protocol	Data from Local System	Exfiltration Over Alternative		
					Forced Authentication	Domain Trust Discovery					
					Code Signing						

*₁ <https://github.com/rabobank-cdc/DeTECT/tree/master/threat-actor-data>



- Generate heat maps
 - Threat actor group data from ATT&CK
 - Own intel stored in a group YAML file
 - Threat actor data from third parties *1
- Compare threat actors

```
groups:
  - group_name: Red team
    campaign: Scenario 1
    technique_id: [T1086, T1053, T1193, T1204, T1003, T1055, T1027, T1085, T1099, T1082, T1016, T1033, T1087, T1075, T1057, T1039, T1041, T1071, T1043, T1001, T1114, T1002]
    software_id: [S0002]
    enabled: True

  - group_name: APT3 (MITRE ATT&CK evaluation)
    campaign: First Scenario
    technique_id: [T1204, T1064, T1085, T1060, T1043, T1071, T1132, T1016, T1059, T1033, T1057, T1106, T1007, T1082, T1069, T1087, T1012, T1088, T1134, T1055, T1018, T1049, T1003, T1026, T1076, T1136, T1061, T1105, T1053, T1083, T1056, T1010, T1113, T1039, T1041, T1078]
    software_id: [S0154]
    enabled: True
```



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Spearphishing Attachment	Rundll32	Scheduled Task	Process Injection	Process Injection	Credential Dumping	Account Discovery	Pass the Hash	Data from Network Shared Drive	Commonly Used Port	Exfiltration Over Command and Control Channel	Data Destruction
Valid Accounts	Scheduled Task	Create Account	T1055 Score: 2	Metadata: Token -Groups: APT3 (MITRE ATT&CK evaluation), Red team as User Account	Input Capture	Process Discovery	Remote Desktop Protocol	Email Collection	Standard Application Layer Protocol	Data Encrypted for Impact	Defacement
Drive-by Compromise	User Execution	Registry Run Keys / Startup Folder	Access Token Manipulation	Control	Account Manipulation	System Information Discovery	Remote File Copy	Input Capture	Data Encoding	Data Compressed	Data Content
Command-Line Interface	Valid Accounts		Bypass User Account Control	Obfuscated Files or Information	Brute Force	System Network Configuration Discovery	Screen Capture	Data Obfuscation	Automated Exfiltration	Disk Structure Wipe	Firmware Corruption
Exploit Public-Facing Application	Execution through API	Accessibility Features	Timestamp	Credentials in Registry	Credentials in Files	Application Window Discovery	Multi-band Communication	File and Directory Discovery	File Transfer Through Object Model	Endpoint Denial of Service	Inhibit System Recovery
External Remote Services	Graphical User Interface	Account Manipulation	Valid Accounts	Scripting	Exploitation for Credential Access	Distributed Component Object Model	Automated Collection	Clipboard Data	Communication Through Removable Media	Denial of Service	Runtime Data Manipulation
Hardware Additions	PowerShell	AppCert DLLs	Accessibility Features	Valid Accounts	Forced Authentication	Exploitation of Remote Services	File Transfer Size Limits	Logon Scripts	Custom Alternative Protocol	Exfiltration Over Other Network Medium	Resource Hijacking
Replication Through Removable Media	Scripting	Appnit DLLs	AppCert DLLs	Binary Padding	Object Model	Query Registry	Custom Connection Proxy	Remote System Discovery	Custom Command and Control Protocol	Network Denial of Service	Runtime Data Manipulation
Spearphishing Link	CMSTP	Application Shimming	Appnit DLLs	BITS Jobs	Forced Authentication	Remote System Discovery	Custom Remote Services	Pass the Ticket	Custom Domain Fronting	Exfiltration Over Physical Medium	Resource Hijacking
Spearphishing via Service	Compiled HTML File	Authentication Package	Application Shimming	CMSTP	Hooking	System Network Connections Discovery	Custom Replication Through Removable Media	Remote Services	Domain Staged	Exfiltration Over Network Medium	Runtime Data Manipulation
Supply Chain Compromise	Control Panel Items	BITS Jobs	Code Signing	Input Prompt	Kerberos	System Service Discovery	Custom Service	Local System	Domain Man in the Middle	Exfiltration Over Physical Medium	Resource Hijacking
	Dynamic Data Exchange	DLL Search Hijacking	Compile After Delivery	Compiled HTML File	LLMNR/NBT-NS Poisoning and Relay						
*1 https://github.com/rabobank-cdc/DeTECT/tree/master/threat-actor-data	Execution through Module Load	Browser Extensions	Exploitation for Privilege Escalation	Component Firmware Escalation	Component Object						



- Intelligence-driven approach with a focus on TTPs

Legend

The technique only present in the group
We have some level of detection
We have detection and used by the group

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	Control Panel Items	Security Support Provider	Access Token Manipulation	Access Token Manipulation	Input Capture	Password Policy Discovery	Logon Scripts	Input Capture	Domain Fronting	Data Compressed	Endpoint Denial of Service
Supply Chain Compromise	Service Execution	AppCert DLLs	Extra Window Memory Injection	Control Panel Items	Credential Dumping	Remote System Discovery	Pass the Hash	Data from Network Shared Drive	Uncommonly Used Port	Data Encrypted	Network Denial of Service
Spearphishing Attachment	PowerShell	Regsvr32	Logon Scripts	Extra Window Memory Injection	Credentials in Registry	System Information Discovery	Application Deployment Software	Email Collection	Remote Access Tools	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
Exploit Public-Facing Application	Rundll32	Image File Execution Options	Process Injection	Masquerading	LLMNR/NBT-NS Poisoning and Relay	System Owner/User Discovery	Distributed Component Object Model	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
External Remote Services	Scripting	Injection	AppCert DLLs	Process Injection	Process Injection	Account Discovery	Automated Collection	Clipboard Data	Data Obfuscation	Data Transfer	Defacement
Hardware Additions	Scheduled Task	Application Shimming	Image File Execution Options	Regsvr32	Account Manipulation	Process Discovery	Exploitation of Remote Services	Standard Application Layer Protocol	Size Limits	Exfiltration Over Wipe	Disk Content
Replication Through Removable Media	User Execution	Scheduled Task	Injection	Rundll32	Brute Force	System Network Configuration Discovery	Pass the Ticket	Data from Information Repositories	Communication Through Removable Media	Alternative Protocol	Disk Structure Wipe
Spearphishing Link	CMSTP	Accessibility Features	Scripting	Brute Force	Pass the Ticket	Application Window Discovery	Remote Desktop Protocol	Data from Local System	Connection Proxy	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Services	Command-Line Interface	Account Manipulation	Image File Execution Options	Credentials in Files	Exploitation for Credential Access	Browser Bookmark Discovery	Remote File Copy	Data from Removable Media	Custom Command and Control Protocol	Exfiltration Over Physical Medium	Inhibit System Recovery
	Compiled HTML File	Compiled HTML File	Scheduled Task	Timestamp	Forced Authentication	Domain Trust Discovery	Remote Services	Replication Through	Data Staged		Resource
	Dynamic Data Exchange	AppInit DLLs	Accessibility Features	Obfuscated Files or Information	Hooking	File and Directory					
	Execution through API	Authentication Package	AppInit DLLs	Binary Padding							

- Use EQL to filter your YAML data in DeTT&CT



- Example use case: how did our detection coverage look like X time ago?

```
python dettect.py d -ft sample-data/techniques-admin.yaml --layer  
--search-detection "techniques where detection.score_logbook.date  
< '2017-11-01'" --all-scores
```

Detection coverage over time

```
[unknown:DeTECT mb$ python dettect.py d -ft sample-data/techniques-administration-endpoints.yaml --layer
--search-detection "techniques where detection.score_logbook.date < '2017-11-01'" --all-scores]
The detection query executed successfully and provided 13 results.
File written:    output/detection_example.json
```

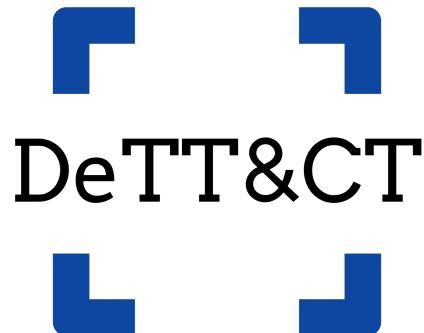
Detection coverage before 2017-11-01

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Supply Chain Compromise	CMSTP Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	LLMNR/NBT-NS Poisoning and Relay	Password Policy Discovery	Application Deployment Software	Audio Capture	Remote Access Tools	Data Compressed	Endpoint Denial of Service
Drive-by Compromise	Compiled HTML	Account Manipulation	Accessibility Features	Binary Padding	Account Manipulation	Remote System Discovery	Distributed Component Discovery	Automated Collection	Commonly Used Port	Data Encrypted	Network Denial of Service
Exploit Public-Facing Application	File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	System Information Object Model	Clipboard Data	Communication Through Removable Media	Exfiltration Over Command and Control Channel	Data Encrypted for Impact	
External Remote Services	Control Panel Items	AppInit DLLs	AppInit DLLs	Credential Dumping	System Owner/User Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Connection Proxy	Data Destruction	
Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Account Discovery	Logon Scripts	Data from Local System	Custom Exfiltration	Automated Exfiltration	Defacement	
Hardware Additions	Execution through API	Authentication Package	Bypass User Account Control	Compile After Delivery	Credentials in Registry	Application Window Discovery	Pass the Hash	Data from Network	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Component Firmware	Browser Bookmark Discovery	Pass the Ticket	Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Execution for Client Execution	Bootkit	Component Object Model Hijacking	Component Object Model Hijacking	Exploitation for Credential Access	Domain Trust Discovery	Remote Desktop Protocol	Data from Removable Media	Data Encoding	Data Obfuscation	Exfiltration Over Other	Firmware Corruption
Exploitation for Client Execution	Browser Extensions	Change Default File Association	Control Panel Items	Forced Authentication	File and Directory Discovery	Remote File Copy	Data Staged	Domain Generation Algorithm	Domain Generation Algorithm		
Graphical User Interface	Extra Window	DCShadow	Deobfuscate/Decode Files or Information	Hooking	Network Service Scanning	Remote Services	Email Collection	Domain Generation Algorithm	Domain Generation Algorithm		
InstallUtil	Component Firmware	Memory Injection	Input Capture	Input Prompt	Network Share Discovery	Replication Through Removable Media	Input Capture	Domain Generation Algorithm	Domain Generation Algorithm		
LSASS Driver	Component Object Model Hijacking	File System Permissions Weakness	Disabling Security Tools	Network Sniffing	Man in the Browser	Input Capture	Domain Generation Algorithm	Domain Generation Algorithm	Domain Generation Algorithm		
Mshta	Object Model Hijacking	Weakness	Hijacking	Kerberoasting	Peripheral Device Discovery	Network Sniffing	Man in the Browser	Domain Generation Algorithm	Domain Generation Algorithm		
PowerShell	PowerShell	Weakness	DLL Search Order Hijacking	Network Sniffing	Screen Capture	Network Sniffing	Man in the Browser	Domain Generation Algorithm	Domain Generation Algorithm		
Regsvcs/Regasm	Create Account	Hooking	DLL Side-Loading	Network Sniffing	Video Capture	Network Sniffing	Man in the Browser	Domain Generation Algorithm	Domain Generation Algorithm		
Regsvr32	DLL Search Order Hijacking	Image File Execution Options	Execution Guardrails	Password Filter DLL	Shared Webroot	Network Sniffing	Man in the Browser	Domain Generation Algorithm	Domain Generation Algorithm		
Rundll32	External Remote Services	Injection	Exploitation for Defense Evasion	Private Keys	Taint Shared Content	Network Sniffing	Man in the Browser	Domain Generation Algorithm	Domain Generation Algorithm		
Scheduled Task	New Service	Extra Window Memory Injection	Two-Factor Authentication Interception	Process Discovery	Third-party Software	Network Sniffing	Man in the Browser	Domain Generation Algorithm	Domain Generation Algorithm		
Scripting	File System Permissions Weakness	Path Interception	Security Software Discovery	Query Registry	Windows Admin Shares	Network Sniffing	Man in the Browser	Domain Generation Algorithm	Domain Generation Algorithm		
Service Execution	Hidden Files and Port Monitors	File Deletion	File Deletion	System Network	File Deletion	Network Sniffing	Man in the Browser	Domain Generation Algorithm	Domain Generation Algorithm		
Signed Binary Proxy Execution											

```
unknown:DeTTECT mb$ python detect.py d -ft sample-data/techniques-administration-endpoints.yaml --layer
File written:    output/detection_example.json
```

Current detection coverage

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	Control Panel Items	Security Support Provider	Access Token Manipulation	Access Token Manipulation	Input Capture	Password Policy Discovery	Logon Scripts	Input Capture	Domain Fronting	Data Compressed	Endpoint Denial of Service
Supply Chain Compromise	Service Execution	AppCert DLLs	Extra Window	Control Panel Items	Credential Dumping	Remote System Discovery	Application Deployment Software	Audio Capture	Uncommonly Used Port	Data Encrypted	Network Denial of Service
Exploit Public-Facing Application	Regsvr32	Logon Scripts	Memory Injection	Extra Window Memory Injection	Credentials in Registry	System Information Discovery	Distributed Component Object Model	Automated Collection	Remote Access Tools	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
External Remote Services	Rundll32	Image File Execution Options	Process Injection	Masquerading	LLMNR/NBT-NS Poisoning and Relay	System Owner/User Discovery	Clipboard Data	Clipboard Data	Commonly Used Port	Command and Control Channel	Data Destruction
Hardware Additions	Scripting	AppCert DLLs	Injection	AppCert DLLs	Process Injection	Exploitation of Remote Repositories	Exploitation of Remote Services	Communication Through Removable Media	Communication Through Removable Media	Automated Exfiltration	Defacement
Replication Through Removable Media	CMSTP	Application Shimming	Regsvr32	Image File Execution Options	Account Manipulation	Account Discovery	Data from Local System	Pass the Hash	Pass the Hash	Data Transfer Size Limits	Disk Content Wipe
Spearphishing Attachment	Command-Line Interface	Accessibility Features	Rundll32	Scripting	Brute Force	Application Window Discovery	Pass the Ticket	Data from Network Shared Drive	Connection Proxy	Custom Command and Control Protocol	Disk Structure Wipe
Spearphishing Link	Compiled HTML File	Account Manipulation	Scripting	Application Shimming	Credentials in Files	Browser Bookmark Discovery	Remote Desktop Protocol	Remote File Copy	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing via Service	Dynamic Data Exchange	AppInit DLLs	Image File Execution Options Injection	Timestamp	Exploitation for Credential Access	Domain Trust Discovery	Data from Removable Media	Data Staged	Custom Cryptographic Protocol	Exfiltration Over Other	Data
Spearphishing Attachment	Execution through API	Authentication Package	AppInit DLLs	Accessibility Features	Binary Padding	File and Directory Discovery	Remote File Copy	Email Collection	Data	#64B5F6 Detection score 0: Forensics	Data
Spearphishing Link	Execution through Module Load	BITS Jobs	AppInit DLLs	BITS Jobs	Forced Authentication	Network Service Scanning	Remote Services	Man in the Browser	Dom Gene Algor	#DCEDC8 Detection score 1: Basic	Dom Gene Algor
Spearphishing via Service	Exploitation for Client Execution	Bootkit	BITS Jobs	Bypass User Account Control	Hooking	Network Share Discovery	Replication Through Removable Media	Screen Capture	Fallbz Multi-Chan	#AED581 Detection score 2: Fair	Fallbz Multi-Chan
Trusted Relationship	Graphical User Interface	Browser Extensions	BITS Jobs	CMSTP	Input Prompt	Network Sniffing	Man in the Browser	Video Capture	Multi-Chan	#BBC34A Detection score 3: Good	Multi-Chan
Valid Accounts	Change Default File Association	Change Default File Association	BITS Jobs	CMSTP	Network Sniffing	Peripheral Device Discovery	Shared Webroot	Windows Admin Shares	Multi-Chan	#689F38 Detection score 4: Very good	Multi-Chan
	InstallUtil	Component Firmware	BITS Jobs	CMSTP	Compile After Delivery	Network Sniffing	Permission Groups Discovery	Windows Admin Shares	Multi-Encry	#33691E Detection score 5: Excellent	Multi-Encry
	LSASS Driver	Component Firmware	BITS Jobs	CMSTP	Privilege Escalation	Component Firmware	Permission Groups Discovery	Windows Admin Shares			
	Mshta	Component Object Model	BITS Jobs	CMSTP	File System Permissions Weakness	Component Object Model Hijacking	Private Keys	Process Discovery			
	Regsvcs/Regasm	Hijacking	BITS Jobs	CMSTP	Exploitation for Compile After Delivery	Component Object Model Hijacking	Two-Factor Authentication Interception	Taint Shared Content			
	Scheduled Task	Create Account	BITS Jobs	CMSTP	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Query Registry	Third-party Software			
	Signed Binary Proxy Execution	DLL Search Order Hijacking	BITS Jobs	CMSTP	Hooking	Deobfuscate/Decode Files or Information	Security Software Discovery	Windows Admin Shares			



github.com/rabobank-cdc/DeTTECT

Questions?



@Bakk3rM
@RubenB_2