



DeTT&CT

Mapping your blue team to ATT&CK™

12-12-2019

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



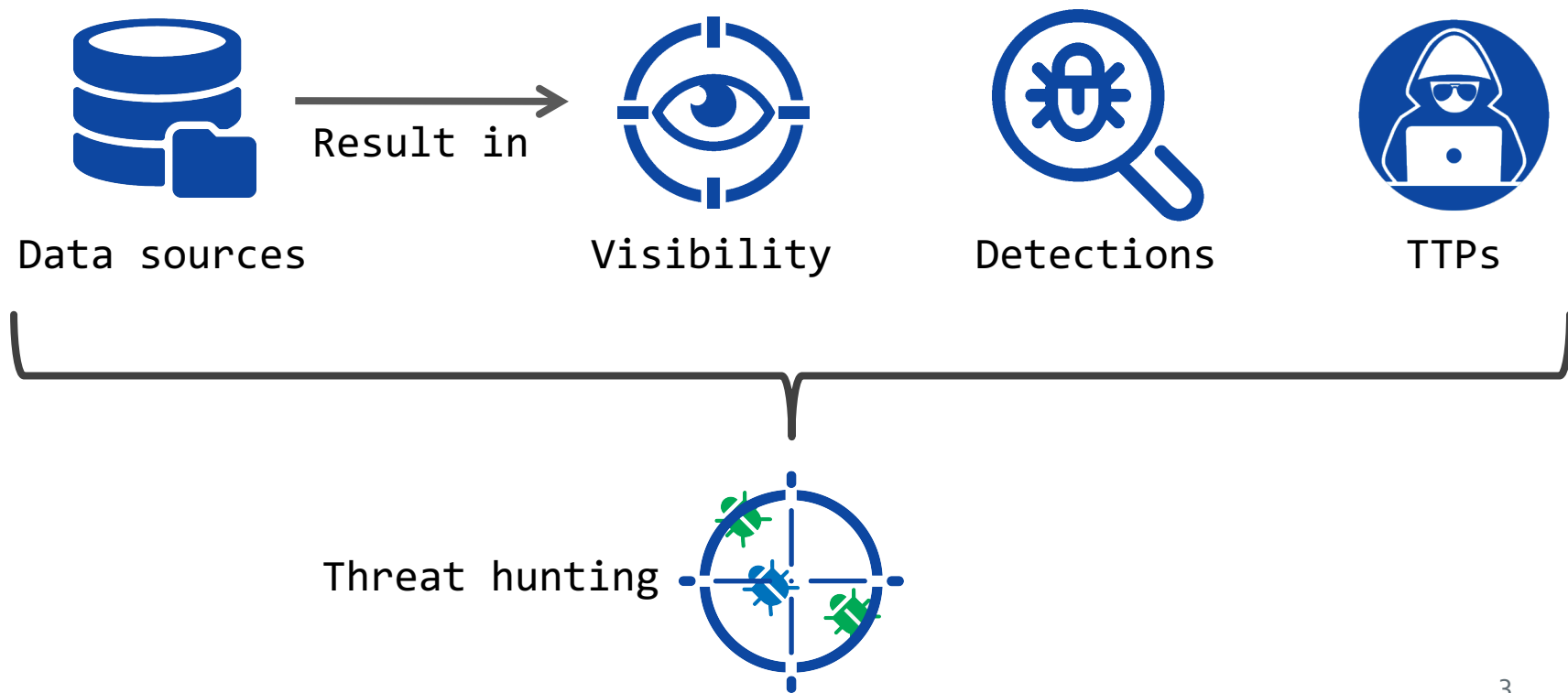
Marcus Bakker

- 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

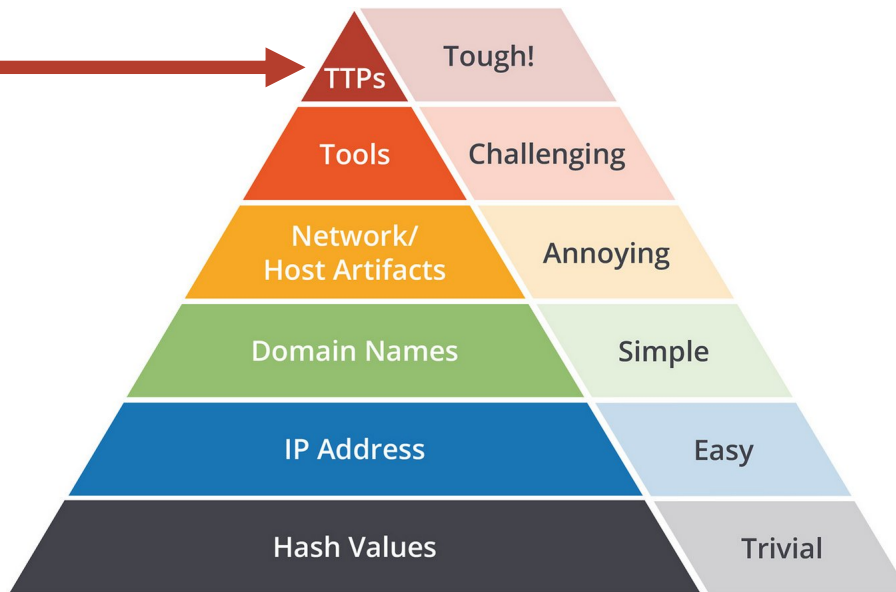


- Intelligence-driven approach with a focus on TTPs





“Wikipedia on cyber attacks”



Source: David J. Bianco / <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

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

Tactics: the adversary's technical goals:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Hardware Additions	Scheduled Task			Binary Padding	Credentials in Registry	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Exfiltration Over Physical Medium	Remote Access Tools
Trusted Relationship	LSASS Driver		Extra Window Manipulation	Access Token Manipulation	Exploitation for Credential Access	Network Share Discovery	Distributed Component Object Model	Video Capture	Exfiltration Over Command and Control Channel	Port Knocking
Supply Chain Compromise	Local Job Scheduling	Trap	Bypass User Account Control	Process Injection	Forced Authentication	Peripheral Device Discovery	Remote File Copy	Automated Collection	Remote File Copy	Multi-hop Proxy
Spearphishing Attachment	Launchctl		Image File Execution Options Injection	Hooking	Password Filter DLL	File and Directory Discovery	Replication Through Removable Media	Email Collection	Automated Exfiltration	Domain Fronting
Exploit Public-Facing Application	Signed Binary Proxy Execution		Plist Modification	Valid Accounts	DMNR/NBT-NS Poisoning	Permission Groups Discovery	Windows Admin Shares	Screen Capture	Exfiltration Over Other Network Medium	Data Encoding
Replication Through Removable Media	Exploitation for Client Execution		DLL Search Order Hijacking	Signed Script Proxy Execution	Private Key	System Network Connection Discovery	Pass the Hash	Data Staged	Exfiltration Over Alternative Protocol	Remote File Copy
Spearphishing via Service	CMSX		AppCert DLLs	DCshadow	Keychain	System Owner/User Discovery	Shared Webroot	Input Capture	Exfiltration Over Alternative Protocol	Multi-Stage Channels
Spearphishing Link	Dynamic Data Exchange		Hooking	Port Knocking	Input Prompt	Windows Remote Management	Shared Drive	Data from Network Shared Drive	Standard Application Layer Protocol	Web Service
Drive-by Compromise	Mshsta		Startup Items	Indirect Command Execution	Batch History	System Network Connection Discovery	Logon Scripts	Data from Local System	Data Transfer	Connection Proxy
Valid Accounts	AppleScript		Launch Daemon	Application Shimming	Two-Factor Authentication Interception	System Owner/User Discovery	Windows Remote Management	Man in the Browser	Size Limits	Multilayer Encryption
	Source		Application Shimming	BITS Jobs	Replication Through Removable Media	System Network Configuration Discovery	Application Deployment Software	Data from Removable Media	Scheduled Transfer	Standard Cryptographic Protocol
	Space after Filename		Applnit DLLs	Control Panel Items	Input Capture	Application Window Discovery	SSH Hacking			Custom Cryptographic Protocol
	Execution through Module Load		Service Registry Permissions Weakness	CMSTP	Network Sniffing	Discovery	AppleScript			Data Obfuscation
	Regsvcs/Regasm		New Service	Process Doppelganging	Credential Dumping	Password Policy Discovery	Taint Shared Content			Custom Command and Control Protocol
	InstallUtil		File System Permissions Weakness	Mshsta	Kerberoasting	Discovery	Remote Desktop Protocol			Communication Through Removable Media
	Regsvr32		Path Interception	Hidden Files and Directories	Custom Tool Execution	Discovery	Remote Desktop Protocol			Multiband Communication
	Execution through API		Accessibility Features	Port Manipulation	Custom Tool Execution	Discovery	Remote Desktop Protocol			Fallback Channels
	PowerShell		Port Manipulation	Kernel Modules and Extensions	Port Manipulation	Discovery	Remote Desktop Protocol			Uncommonly Used Port
	Rundll32		Port Manipulation	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Third-party Software		Port Manipulation	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Scripting		Port Manipulation	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Graphical User Interface		SIP and Trust Provider Hijacking	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Command-Line Interface		Screen Saver	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Service Execution		Browser Extensions	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Windows Remote Management		Re-opened Applications	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Signed Script Proxy Execution		Rc.common	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Control Panel Items		Login Item	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Trusted Developer Utilities		LC_LOAD_DYLIB Addition	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
	Windows Management Instrumentation		Hidden Files and Directories	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			
			Office Application Startup	Port Manipulation	Port Manipulation	Discovery	Remote Desktop Protocol			

Techniques: how the goals are achieved

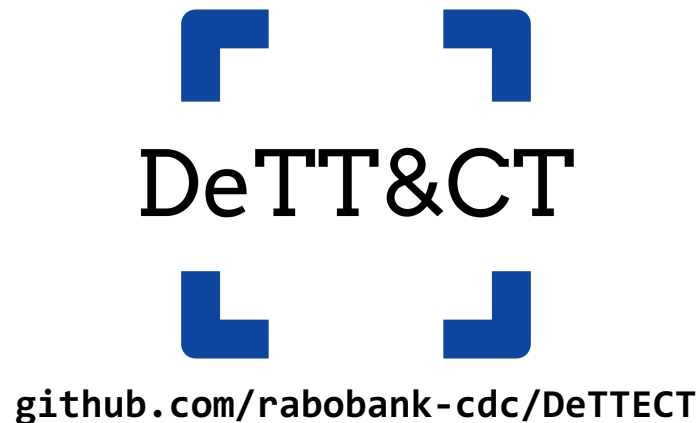
Procedures: Specific technique implementation

Examples

Name	Description
APT18	APT18 actors used the native at Windows task scheduler tool to use scheduled tasks for execution on a victim network. ^[2]
APT29	APT29 used named and hijacked scheduled tasks to establish persistence. ^[3]

Modify Registry

- 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	CMS/PT	Accessibility Features	Access Token Manipulation	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	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	Applet DLLs	Applet DLLs	Bypass User Account Control	Credentials in Files	Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	Code Signing	Exploitation of Credentials	Discovery	Exploitation of Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Execution through API	Authentication Package	Authentication Package	Code Signing	Exploitation of Credentials	Discovery	Exploitation of Remote Services	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Load	Bootkit	Bootkit	Compile After Delivery	Exploitation of Credentials	Discovery	Exploitation of Remote Services	Data from Removable Media	Data Encoding	Exfiltration Over Command and Control Channel	Forward Corruption
Spearphishing via Service	Browser Extensions	Browser Extensions	Browser Extensions	Component Firmware	Exploitation of Credentials	Discovery	Exploitation of Remote Services	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Inhibit System Recovery
Supply Chain Compromise	Change Default File Association	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Discovery	Exploitation of Remote Services	Domain Fronting	Domain Generation Algorithms	Exfiltration Over Network Medium	Network Denial of Service
Trusted Relationship	Graphical User Interface	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
Valid Accounts	InstanceID	Component Firmware	Component Firmware	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	LSASS Driver	Component Firmware	Component Firmware	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Mhta	Model Hijacking	Model Hijacking	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	PowerShell	Create Account	Create Account	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Regsvcs/Regasm	DLL Search Order	DLL Search Order	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Regsvr32	External Remote Services	External Remote Services	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Rundll32	File System Permissions Weakness	File System Permissions Weakness	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Scheduled Task	File System Permissions Weakness	File System Permissions Weakness	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Scripting	Hidden Files and Directories	Hidden Files and Directories	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Task Scheduler	Image File Execution Options Injection	Image File Execution Options Injection	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Signed Binary Proxy Execution	Image File Execution Options Injection	Image File Execution Options Injection	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Signed Script Proxy Execution	Image File Execution Options Injection	Image File Execution Options Injection	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Third-party Software	Image File Execution Options Injection	Image File Execution Options Injection	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Untrusted Developer Utilities	Image File Execution Options Injection	Image File Execution Options Injection	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	User Execution	Image File Execution Options Injection	Image File Execution Options Injection	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Windows Management Instrumentation	Image File Execution Options Injection	Image File Execution Options Injection	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	Windows Remote Management	Image File Execution Options Injection	Image File Execution Options Injection	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking
	XSL Script Processing	Image File Execution Options Injection	Image File Execution Options Injection	Control Panel Items	Input Prompt	Discovery	Exploitation of Remote Services	Domain Generation Algorithms	Domain Generation Algorithms	Exfiltration Over Network Medium	Resource Hijacking

legend
#E1BEE7 1-25% of data sources available
#E193D8 26-50% of data sources available
#A8745C 51-75% of data sources available
#F08080 76-99% of data sources available
#E16A5C 100% of data sources available



- 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	ExecScan	Persistence	Privilege Escalation	Defense Evasion	Discovery	Denial of Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
-1	None	No detection.	11 Items	27 Items	42 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items
0	Forensics / context	No detection, but the technique is being logged for forensic purposes and can be used to provide context.	11 Items	27 Items	42 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items
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.	11 Items	27 Items	42 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items
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.	11 Items	27 Items	42 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items
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.	11 Items	27 Items	42 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items
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.	11 Items	27 Items	42 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items
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".	11 Items	27 Items	42 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items	18 Items



- 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	
Spearphishing 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	User Execution	Valid Accounts	Scheduled Task	Obfuscated Files or Information	Input Capture	System Information Discovery	Remote Desktop Protocol	1105 Core-20 Metadata	Standard Application Layer Protocol	Data Encrypted	Data Destruction	
Spearphishing Link	PowerShell	Valid Accounts	Process Injection	Valid Accounts	Brute Force	System Network Configuration Discovery	Windows Admin Shares	Group: Threat Group-3390, APT3, Cobalt Group, Soft Cell, Magic Hound, FRO, LeetTeam, HidenWood, APT38, Gorgon	Commonly Used Port	Command and Control Channel	Data Encrypted for Impact	
Drive-by Compromise	Command-Line Interface	Scheduled Task	New Service	File Deletion	Credentials in Files	File and Directory Discovery	Removable Media	Group: Threat Group-3390, APT3, Cobalt Group, Soft Cell, Magic Hound, FRO, LeetTeam, HidenWood, APT38, Gorgon	Web Service	Stored Data Manipulation	Command and Control Channel	
External Remote Services	Scheduled Task	External Remote Services	New Service	Web Shell	Masquerading	System Owner/User Discovery	Removable Media	Group: Threat Group-3390, APT3, Cobalt Group, Soft Cell, Magic Hound, FRO, LeetTeam, HidenWood, APT38, Gorgon	Web Service	Stored Data Manipulation	Command and Control Channel	
Exploit Public-Facing Application	Exploitation for Client Execution	Web Shell	Bypass User Account Control	Deobfuscation/Decode Files or Information	Network Sniffing	Remote System Discovery	Pass the Hash	Group: Threat Group-3390, APT3, Cobalt Group, Soft Cell, Magic Hound, FRO, LeetTeam, HidenWood, APT38, Gorgon	Standard Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	
Replication Through Removable Media	Windows Management Instrumentation	Redundant Access	Exploitation for Privilege Escalation	Software Packing	Faceted Authentication	Account Discovery	Pass the Ticket	MuddyWater, APT18, Generation Group, TA505, Turis, FINL, Rancor, APT37, Glig, FINN, RIGOR, BUTLER, Paschwerk, APT32, APT11, APT33, APT28, APT35, APT36, APT37, APT38, APT39, APT40, APT41, APT42, APT43, APT44, APT45, APT46, APT47, APT48, APT49, APT50, APT51, APT52, APT53, APT54, APT55, APT56, APT57, APT58, APT59, APT60, APT61, APT62, APT63, APT64, APT65, APT66, APT67, APT68, APT69, APT70, APT71, APT72, APT73, APT74, APT75, APT76, APT77, APT78, APT79, APT80, APT81, APT82, APT83, APT84, APT85, APT86, APT87, APT88, APT89, APT90, APT91, APT92, APT93, APT94, APT95, APT96, APT97, APT98, APT99, APT100	Uncommonly Used Port	Data Transfer Size Limits	Runtime Data Manipulation	Resource Hijacking
Spearphishing via Service	Dynamic Data Exchange	Accessibility Features	Accessibility Features	Code Signing	Hooking	System Network Connections Discovery	Exploitation of Services	Logon Scripts	Data Encoding	Exfiltration Over Other Network Medium	Service Stop	
Trusted Relationship	Rundll32	Create Account	Access Token Manipulation	Modify Registry	Input Prompt	Network Service Scanning	Exploitation of Services	Replication Through Removable Media	Custom Command and Control Protocol	Exfiltration Over Physical Medium	Service Stop	
Supply Chain Compromise	Regsvr32	Hidden Files and Directories	DLL Search Order Hijacking	Process Injection	Exploitation for Credential Access	Security Software Discovery	Query Registry	Application Deployment Software	Remote Access Tools	Exfiltration Over Network Medium	Service Stop	
Hardware Additions	Service Execution	Account Manipulation	AppCert DLLs	Disabling Security Tools	LLMNR/NBNS Poisoning and Relay	System Service Discovery	Network Service Discovery	Video Capture	Custom Cryptographic Protocol	Exfiltration Over Network Medium	Service Stop	
MShta	Compiled HTML File	Modify Existing Service	Application Shimming	DLL Side-Loading	PLMN/NBNS Poisoning and Relay	System Service Discovery	Peripheral Device Discovery	Clipboard Data	Standard Non-Application Layer Protocol	Exfiltration Over Network Medium	Service Stop	
Signed Binary Proxy Execution	Execution through API	Hooking	Rundll32	Private Keys	Password Filter DLL	System Time Discovery	System Time Discovery	Man in the Browser	Data Obfuscation	Exfiltration Over Network Medium	Service Stop	
CMSTP	BITS Jobs	Port Monitors	Port Monitors	Indicator Removal from Host	Two-Factor Authentication Interception	Network Sniffing	Virtualization/Sandbox Evasion	Shared Webroot	Multi-hop Proxy	Exfiltration Over Network Medium	Service Stop	
Graphical User Interface	Image File Execution Options Injection	Indicator Removal from Host	Indicator Removal from Host	Redundant Access	Virtualization/Sandbox Evasion	Application Window Discovery	Application Window Discovery	Shared Webroot	Multi-Stage Channels	Exfiltration Over Network Medium	Service Stop	
Signed Script Proxy Execution	Port Monitors	Appinit DLLs	Appinit DLLs	Virtualization/Sandbox Evasion	Application Window Discovery	Password Policy Discovery	Browser Bookmark Discovery	Domain Trust Discovery	Communication Through Removable Media	Exfiltration Over Network Medium	Service Stop	
Third-party Software	Office Application Startup	File System Permissions Weakness	File System Permissions Weakness	Hidden Files and Directories	Template Injection	Browser Bookmark Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
Windows Remote Management	Winlogon Helper DLL	Path Interception	Path Interception	Time Stomp	Access Token Manipulation	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
XSL Script Processing	AppCert DLLs	Service Registry Weakness	Service Registry Weakness	Access Token Manipulation	MShta	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
Control Panel Items	Application Shimming	Browser Extensions	Browser Extensions	SID-History Injection	Process Hollowing	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
Execution through Module Load	Component Firmware	Component Firmware	Component Firmware	Signed Binary Proxy Execution	BITS Jobs	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
InstallUtil	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	BITS Jobs	CMSTP	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
LSASS Driver	Hooking	Hooking	Hooking	CMSTP	Image File Execution Options Injection	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
Regsvcs/Regasm	Image File Execution Options Injection	Image File Execution Options Injection	Image File Execution Options Injection	DLL Search Order Hijacking	Port Monitors	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
Trusted Developer Utilities	Port Monitors	Port Monitors	Port Monitors	Execution Guardrails	Appinit DLLs	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
	Authentication Package	Authentication Package	Authentication Package	Virtualization/Sandbox Evasion	Change Default File Association	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
	File System Permissions Weakness	File System Permissions Weakness	File System Permissions Weakness	Component Firmware	File System Permissions Weakness	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
	Hypervisor	Hypervisor	Hypervisor	Component Object Model Hijacking	Hypervisor	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	
	LSASS Driver	LSASS Driver	LSASS Driver	Exploitation for Defense Evasion	File Permissions Modification	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Generation Algorithms	Exfiltration Over Network Medium	Service Stop	

*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	T1027	System Discovery	Application Deployment Software	Data Obfuscation	Exfiltration Over Command and Control Channel	Data Encrypted for Impact	Data Encrypted for Impact
Exploit Public-Facing Application	User Execution	Account Manipulation	Access Token Manipulation	Rundll32	Score: 100	System Information Discovery	System Information Software	Email Collection	Standard Application Layer Protocol	Defacement	Defacement
External Remote Services	CMSTP	AppCert DLLs	Access Token Manipulation	Timestamp	Groups: Red team	System Network Configuration Discovery	Distributed Component Object Model	Automated Exfiltration	Communication Through Removable Media	Disk Content Wipe	Disk Content Wipe
Hardware Additions	Command-Line Interface	AppCert DLLs	Access Token Manipulation	Binary Padding	Credentials in Files	System Owner/User Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Disk Structure Wipe	Disk Structure Wipe
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	Access Token Manipulation	BITS Jobs	Credentials in Registry	Application Window Discovery	Application Window Discovery	Automated Exfiltration	Connection Proxy	Data Encrypted Wipe	Data Encrypted Wipe
	Control Panel Items	Authentication Package	Access Token Manipulation	Bypass User Account Control	Exploitation for Credential Access	Browser Bookmark Discovery	Logon Scripts	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Endpoint Denial of Service
	Dynamic Data Exchange	BITS Jobs	Access Token Manipulation	CMSTP	Forced Authentication	Domain Trust Discovery	Pass the Ticket	Remote Desktop Protocol	Custom Cryptographic	Exfiltration Over Alternative	Firmware Corruption
	Execution through	Bootkit	Access Token Manipulation	Code Signing							

*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

```
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, T1042, 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	Process Injection	Score 2 Metadata: -Groups: APT3 (MITRE ATT&CK evaluation), Red team	Input Capture	Process Discovery	Remote Desktop Protocol	Email Collection	Standard Application Layer Protocol		Data Encrypted for Impact
Drive-by Compromise	Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Access Token Manipulation	Account Manipulation	System Information Discovery	Remote File Copy	Input Capture	Data Encoding	Data Compressed	Defacement
Exploit Public-Facing Application	Execution through API	Accessibility Features	Bypass User Account Control	Obfuscated Files or Information	Brute Force	System Network Configuration Discovery	Screen Capture	Application Deployment Software	Data Obfuscation	Automated Wipe	Disk Content
External Remote Services	Graphical User Interface	Account Manipulation	Valid Accounts	Scripting	Credentials in Registry	System Owner/User Discovery	Audio Capture	Application Window Discovery	Multiband Communication	Data	Disk Structure
Hardware Additions	PowerShell	AppCert DLLs	Accessibility Features	Timestomp	Exploitation for Credential Access	File and Directory Discovery	Automated Collection	Distributed Component Object Model	Remote File Copy	Encrypted	Endpoint Denial of Service
Replication Through Removable Media	Scripting	Appinit DLLs	Valid Accounts	Valid Accounts	Forced Authentication	File and Directory Discovery	Clipboard Data	Exploitation of Remote Services	Communication Through Connection Proxy	Data Transfer Size Limits	Service
Spearphishing Link	Control Panel Items	Application Shimming	AppCert DLLs	Binary Padding	Authentication	Permission Groups Discovery	Information Repositories	Logon Scripts	Removable Media	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing via Service	Dynamic Data Exchange	Authentication Package	Application Shimming	BITS Jobs	Hooking	Query Registry	Logon Scripts	Pass the Ticket	Custom Command and Control Protocol	Exfiltration Over Other Network Protocol	Resource Hijacking
Supply Chain Compromise	Execution through Client Execution	Browser Extensions	Application Shimming	Code Signing	Input Prompt	Remote System Discovery	Remote Services	Remote Services	Data from Removable Media	Custom Cryptographic Protocol	Resource Hijacking
	Change Default File Association	Change Default File Association	Extra Window	Component Object Model	Component Object Model	System Network Connections Discovery	System Network Connections Discovery	System Service Discovery	Domain Staged	Exfiltration Over Physical Medium	Runtime Data Manipulation

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



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

- 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:DeTTECT mb$ python detect.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	Accessibility Features	Access Token Manipulation	Access Token Manipulation	LLMNR/NBT-NS Poisoning and Relay	Password Policy Discovery	Application Deployment	Audio Capture	Remote Access Tools	Data Compressed	Endpoint Denial of Service
Drive-by Compromise	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Account Manipulation	Remote System Discovery	Distributed Component Object Model	Automated Software Collection	Commonly Used Port	Data Encrypted	Network Denial of Service
Exploit Public-Facing Application	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	System Information Discovery	Exploitation of Remote Services	Clipboard Data	Communication Through Removable Media	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
External Remote Services	Control Panel Items	Appnit DLLs	Appnit DLLs	Bypass User Account Control	Credential Dumping	System Owner/User Discovery	Logon Scripts	Data from Information Repositories	Connection Proxy	Automated Exfiltration	Data Destruction
Hardware Additions	Dynamic Data Exchange	Application Shimmming	Application Shimmming	Code Signing	Credentials in Files	Account Discovery	Pass the Hash	Data from Local System	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Execution through API	Authentication Package	Bypass User Account Control	Compile After Delivery	Credentials in Registry	Application Window Discovery	Pass the Ticket	Data from Network Shared Drive	Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Component Firmware	Exploitation for Credential Access	Browser Bookmark Discovery	Remote Desktop Protocol	Data from Removable Media	Data Encoding	Exfiltration Over Other Channels	Disk Structure Wipe
Spearphishing Link	Exploitation for Client Execution	Browser Extensions	Exploitation for Privilege Escalation	Control Panel Items	Forced Authentication	Domain Trust Discovery	File and Directory Discovery	Data Staged	Data Obfuscation	Exfiltration Over Other Channels	Firmware Corruption
Spearphishing via Service	Graphical User Interface	Change Default File Association	Extra Window Memory Injection	DCShadow	Hooking	Network Service Scanning	Remote File Copy	Email Collection	Domain	Legend	
Trusted Relationship	InstallUtil	Component Firmware	File System Permissions Weakness	Disabling Security Tools	Input Capture	Network Share Discovery	Replication Through Removable Media	Input Capture	Man in the Browser	#64B5F6	Detection score 0: Forensics
Valid Accounts	LSASS Driver	Firmware	DLL Search Order Hijacking	DLL Search Order Hijacking	Kerberoasting	Network Sniffing	Peripheral Device Discovery	Screen Capture	Fallback	#DCEDC8	Detection score 1: Basic
	PowerShell	Create Account	Hooking	DLL Side-Loading	Network Sniffing	Permission Groups Discovery	Shared Webroot	Multi-Chan	Multi-Chan	#AED581	Detection score 2: Fair
	PowerShell	Create Account	Hooking	DLL Side-Loading	Network Sniffing	Permission Groups Discovery	Shared Webroot	Multi-Chan	Multi-Chan	#8BC34A	Detection score 3: Good
	PowerShell	Create Account	Hooking	DLL Side-Loading	Network Sniffing	Permission Groups Discovery	Shared Webroot	Multi-Chan	Multi-Chan	#689F38	Detection score 4: Very good
	PowerShell	Create Account	Hooking	DLL Side-Loading	Network Sniffing	Permission Groups Discovery	Shared Webroot	Multi-Chan	Multi-Chan	#33691E	Detection score 5: Excellent

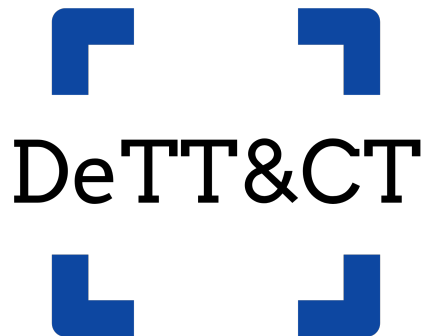
```
unknown:DeTTECT mb$ python dettect.py d -ft sample-data/techniques-administration-endpoints.yaml --layer
File written: output/detection_example.json
```

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 Memory Injection	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	PowerShell	Logon Scripts	Extra Window 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	Regsvr32	Image File Execution Options Injection	Process Injection	Masquerading	LLMNR/NBT-NS Poisoning and Relay	System Owner/User Discovery	Exploitation of Remote Services	Clipboard Data	Commonly Used Port	Communication Through Removable Media	Data Destruction
	Rundll32										
Hardware Additions	Scripting	CMSTP	Image File Execution Options Injection	Regsvr32	Brute Force	Application Window Discovery	Pass the Hash	Data from Network Shared Drive	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Command-Line Interface	Accessibility Features	Application Shimming	Rundll32	Credentials in Files	Browser Bookmark Discovery	Pass the Ticket	Desktop Protocol	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Compiled HTML File	Account Manipulation	Application Shimming	Image File Execution Options Injection	Exploitation of Credential Access	Domain Trust Discovery	Remote File Copy	Data from Removable Media	Custom Cryptographic Protocol	Exfiltration Over Other Protocol	Firmware Corruption
Spearphishing Link	Dynamic Data Exchange	Applnit DLLs	Accessibility Features	Timestamp	Binary Padding	File and Directory Discovery	Remote Services	Data Staged	Data		
Spearphishing via Service	Execution through API	Authentication Package	Applnit DLLs	BITS Jobs	BITS Jobs	Network Service Scanning	Replication Through Removable Media	Email Collection	Man in the Browser	Domain Gene	
Trusted Relationship	Execution through Module Load	Bootkit	Bypass User Account Control	Bypass User Account Control	Hooking	Network Share Discovery	Screen Capture	Man in the Browser	Algorithm	Fallba	
Valid Accounts	Exploitation for Client Execution	Browser Extensions	DLL Search Order Hijacking	Code Signing	Kerberoasting	Network Sniffing	Shared Webroot	Video Capture	Multi-Chan		
	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Compiled HTML File	Component Firmware	Private Keys	Taint Shared Content				
	InstallUtil	Component Firmware	File System Permissions Weakness	Component Object Model Hijacking	Two-Factor Authentication Interception	Query Registry	Third-party Software				
	LSASS Driver	Component Object Model Hijacking	Hooking	DCShadow	Deobfuscate/Decode Files or Information	Security Software Discovery	Windows Admin Shares				
	Mshst	Create Account	New Service Path			System Network					
	Regsvcs/Regasm	DLL Search Order Hijacking									
	Scheduled Task										
	Signed Binary Proxy Execution										

legend

- #64B5F6 Detection score 0: Forensic
- #DCEDC8 Detection score 1: Basic
- #AED581 Detection score 2: Fair
- #8BC34A Detection score 3: Good
- #689F38 Detection score 4: Very good
- #33691E Detection score 5: Excellent



`github.com/rabobank-cdc/DeTTECT`

Questions?



@Bakk3rM

@RubenB_2