

Mapping your blue team to ATT&CK

10-05-2019

Marcus Bakker | twitter.com/bakk3rm
Ruben Bouman | twitter.com/rubenb_2



Rabobank

Where do we start **hunting**?

For the things we have **visibility** and poor or no **detection**.

What are those things?

Uh...

Okay, once we know where to start, what should we do first?

We should look at what **attackers** are doing.

So we must integrate **threat intelligence**, right?

Indeed, but how...

- 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



DeTT&CT



github.com/rabobank-cdc/DeTTACT

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

Where do we start hunting?

For the things we have **visibility** and poor or no detection.

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

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	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment 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 Object Model	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	Browser Bookmark Metadata	Clipboard Data	Clipboard Data	Data Encrypted	Defacement	
Hardware Additions	Control Panel Items	Appln DLLs	Appln DLLs	Credentials in Files	Credentials in Registry	T1003.001	Connection Proxy	Connection Proxy	Custom Command and Control Protocol	Custom Command and Control Protocol	Custom Command and Control Protocol
Execution through API	Dynamic Data Exchange	Application Shimming	Application Shimming	Code Signing	Code Signing	Exploitability of Application Services	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Command and Control Protocol	Custom Command and Control Protocol	Custom Command and Control Protocol
Execution Through Removable Media	Execution through API	Authentication Package	Bypass User Account Control	Compile After Delivery	Compromised Credentials	Exploitability of Application Services	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
Spearphishing Attachment	Execution through Removable Media	BITS Jobs	BITS Jobs	Exploitation for Credential Access	Component Firmware	Exploitability of Application Services	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
Spearphishing Link	Exploitation for Client Execution	Bootkit	Bootkit	Component Object Model Hijacking	Component Object Model Hijacking	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
Spearphishing Interface	Graphical User Interface	Change Default File Association	Change Default File Association	Control Panel Items	Control Panel Items	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
Spearphishing via Service	InstallUtil	Component Firmware	Extra Window Memory Injection	DCShadow	DCShadow	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
Supply Chain Compromise	LSASS Driver	Component Permissions	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
Trusted Relationship	PowerShell	Object Model Hijacking	File System Permissions Weakness	Disabling Security Tools	Disabling Security Tools	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
Valid Accounts	Regsvcs/Regasm	Create Account	Hooking	DLL Search Order Hijacking	DLL Side-Loading	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Regsv32	DLL Search Order Hijacking	Image File Execution Options Injection	Execution Guardrails	Execution Guardrails	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Rundll32	External Remote Services	New Service	File System Path Interception	File System Path Interception	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Scheduled Task	Scripting	Port Monitors	Extra Window Memory Injection	Extra Window Memory Injection	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Service Execution	File System Permissions Weakness	Port Monitors	File Deletion	File Deletion	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Signed Binary Proxy Execution	Hidden Files and Directories	File Permissions Modification	File Permissions Modification	File Permissions Modification	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Signed Script Proxy Execution	Process Injection	Injected Task	File System Logical Offsets	File System Logical Offsets	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Third-party Software	Hooks	Group Policy Modification	Group Policy Modification	Group Policy Modification	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Trusted Developer Utilities	Image File Execution Options Injection	Hidden Files and Directories	Indicator Blocking	Indicator Blocking	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	User Execution	Logon Scripts	Services Registry Permissions Weakness	Indicator Removal from Tools	Indicator Removal from Tools	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Windows Management Instrumentation	LSASS Driver	SID History Injection	Indicator Removal on Host	Indicator Removal on Host	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	Windows Remote Management	Modify Existing Service	Virtualization/Sandbox Evasion	Indirect Command Execution	Indirect Command Execution	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	XSL Script Processing	Netsh Helper DLL	Web Shell	Install Root Certificate	Install Root Certificate	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
		New Service	Indicator Removal on Host	Indicator Removal on Host	Indicator Removal on Host	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
		Office Application Startup	Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
		Path Interception	InstallUtil	Install Root Certificate	Install Root Certificate	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
		Port Monitors	Masquerading	Indicator Removal from Tools	Indicator Removal from Tools	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
		Redundant Access	Modify Registry	Indicator Removal on Host	Indicator Removal on Host	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
		Registry Run Keys / Startup Folder	Mohita	Indicator Removal on Host	Indicator Removal on Host	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
		Scheduled Task	Network Share Connection Removal	Network Share Connection Removal	Network Share Connection Removal	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
		Screensaver	NTFS File Attributes	NTFS File Attributes	NTFS File Attributes	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
		Security Support Provider	Custom Resolution	Custom Resolution	Custom Resolution	Forced Authentication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol

Legend

#E1BEE7	1-25% of data sources avail	X
#CE93D8	26-50% of data sources av	X
#AB47BC	51-75% of data sources av	X
#7B1FA2	76-99% of data sources av	X
#A1A8C0	100% of data sources avail	X

Add Item Clear

Where do we start hunting?

For the things we have **visibility** and poor or no detection.

- Manual score visibility
 - One source is more important than the other
 - Minimal set of data sources to have useful visibility
- 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	Application Deployment	Audio Capture	Commonly Used Port	Automated Collection	Data destruction	Exfiltration	
Exploit Public-Interface Application	Command-Line Interface	Account Enumeration	Access Token Manipulation	Application Window Manipulation	Automated Collection	Clipboard Data Removal	Community-based Threat Intelligence	Component Discovery	Data Encrypted in transit	File Encryption	
External Remote Services	Compiled HTML File	AppCert DLLs	AppCMD DLLs	Bypass User Account Control	Browser Bookmarks	Browser Detection	Browser Exploitation	Clipboard Data Removal	Custom	Custom Content	
Hardware Additions	Dynamic Data Exchange	Application Shimming	CMSTP	Credentials in Memory	Clipboard Data Removal	Cloud Services	Cloud Services	Cloud Storage	Custom	Custom Content	
Replication Through Removable Media	Execution through App	Authentication	Bypass User Control	Compile After Delivery	Component Discovery	Computer Discovery	Computer Discovery	Computer Discovery	Custom	Custom Content	
Screenprinting Attachment	Execution through Module Load	BITS Jobs	Component Firmware	Compromised File	Component Object Model Hijacking	Container Discovery	Container Discovery	Container Discovery	Custom	Custom Content	
Spearehishing via Service	Exploration for Client Execution	Browser Extensions	Execution for Privileges	Forced Authentication	Forced Logon	Forceful Takeover	Forceful Takeover	Forceful Takeover	Custom	Custom Content	
Supply Chain Compromise	Grabbing User Interface	Change Default File Association	Control Panel Items	Control Panel Item Escalation	Control Panel Item Escalation	Custom	Custom Content				
Trusted Relationship	Install/Uninstall Component Firmwares	Extra Window Injection	DCShadow	Device Driver	Device Driver	Device Driver	Device Driver	Device Driver	Custom	Custom Content	
Valid Accounts	LSASS Driver	File System Permissions Violations	Disk Shadowing	Disk Shadowing	Custom	Custom Content					
	Mitira	File System Permissions Violations	DLL Search Order Hijacking	DLL Side-Loading	Execution Guardrails	Execution Guardrails	Execution Guardrails	Execution Guardrails	Custom	Custom Content	
	PowerShell	File System Permissions Violations	File System Permissions Violations	Custom	Custom Content						
	Regexec/Regasm	Create Account	Hijacking	Image File Execution	Image File Execution	Image File Execution	Image File Execution	Image File Execution	Custom	Custom Content	
	Regver32	DLL Search Order Hijacking	Input Capture	Input Capture	Custom	Custom Content					
	Rundll32	External Remote Services	Input Decoder/Encoder	Input Decoder/Encoder	Custom	Custom Content					
	Scheduled Task Scripting	File Interception	Input Prompts	Input Prompts	Custom	Custom Content					
	Service Execution	File System Permissions Weakness	Interception	Interception	Interception	Interception	Interception	Interception	Custom	Custom Content	
	Signed Binary Proxy Execution	Hidden Files and Directories	Port Monitors	Port Monitors	Custom	Custom Content					

Visibility scores

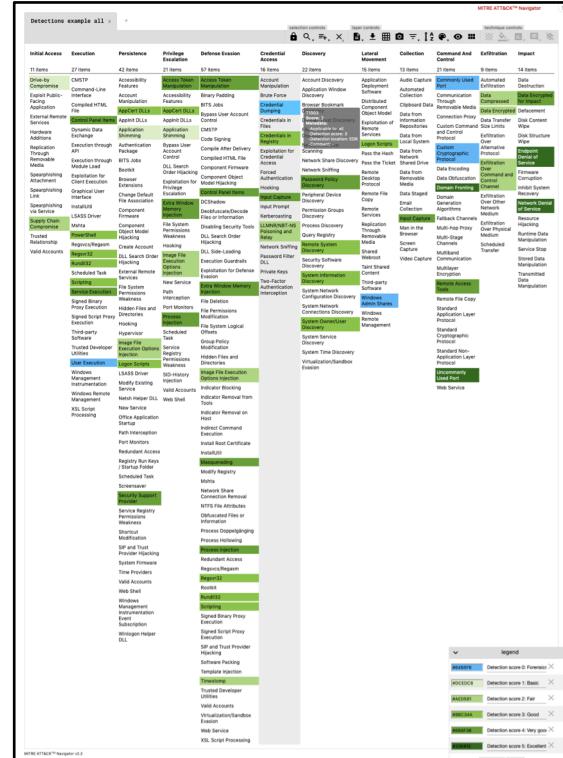
Score	Score name	Description
0	None	No visibility at all.
1	Minimal	Sufficient data sources with sufficient quality available to be able to see one aspect of the technique's procedures.
2	Medium	Sufficient data sources with sufficient quality available to be able to see more aspects of the technique's 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.

Where do we start hunting?

For the things we have visibility and poor or no detection.

- 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
-1	None	No detection.
0	Forensics / context	No detection, but the technique is being logged for forensic purposes and can be used to provide context.
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.
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.
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.
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.
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".



Groups

What are attackers doing?

Okay, once we know where to start, what should we do first?

We should look at what
attackers are doing.

So we must integrate **threat intelligence**, right?

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

Okay, once we know where to start, what should we do first?

We should look at what **attackers** are doing.

So we must integrate **threat intelligence**, right?

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

```
%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 Hunting	Account Discovery	Pass the Hash	Data from Network Shared Drive	Commonly Used Port	Data Compressed	Data Destruction
Rundll32		Accessibility Features		T1027		Process Discovery	Application Deployment Software				
Drive-by Compromise	Scheduled Task		Scheduled Task	Score: 1 Score: 100 - Groups: Red team		System Information Discovery					
Exploit Public-Facing Application	User Execution	Account Manipulation	Timestamp	Bride Force		System Network Configuration Discovery	Distributed Component Object Model	Email Collection	Standard Application Layer Protocol	Exfiltration Over Command and Control Channel	Data Encrypted for Impact Defacement
External Remote Services	CMSTP	AppCert DLLs	Access Token Manipulation	Credentials in Files			Audio Capture	Automated Collection	Communication Through Removable Media	Automated Exfiltration	Disk Content Wipe
Hardware Additions	Command-Line Interface	ApnInit DLLs	Accessibility Features	Binary Padding	Credentials in Registry	System Owner/User Discovery	Clipboard Data	Clipboard Data	Connection Proxy	Data Encrypted	Disk Structure Wipe
Replication Through Removable Media	Compiled HTML File	Application Shimming	AppInit DLLs	BITS Jobs	Exploitation for Credential Access	Application Window Discovery	Automated Collection	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Endpoint Denial of Service
	Control Panel Items	Authentication Package	AppInit DLLs	Bypass User Account Control	Forced Authentication	Browser Bookmark Discovery	Custom Command and Control Protocol	Custom Custom	Custom Custom	Exfiltration Over Alternative	Firmware Corruption
	Dynamic Data Exchange	BITS Jobs	BITS Jobs	CMSSTP	Domain Trust Discovery	Logon Scripts	Custom Custom	Custom Custom	Custom Custom		
	Execution through	Bootkit	Execution through	Code Signina		Pass the Ticket	Remote Desktop Driven	Data from Local System	Custom Custom		

Groups

What are attackers doing?

Okay, once we know where to start, what should we do first?

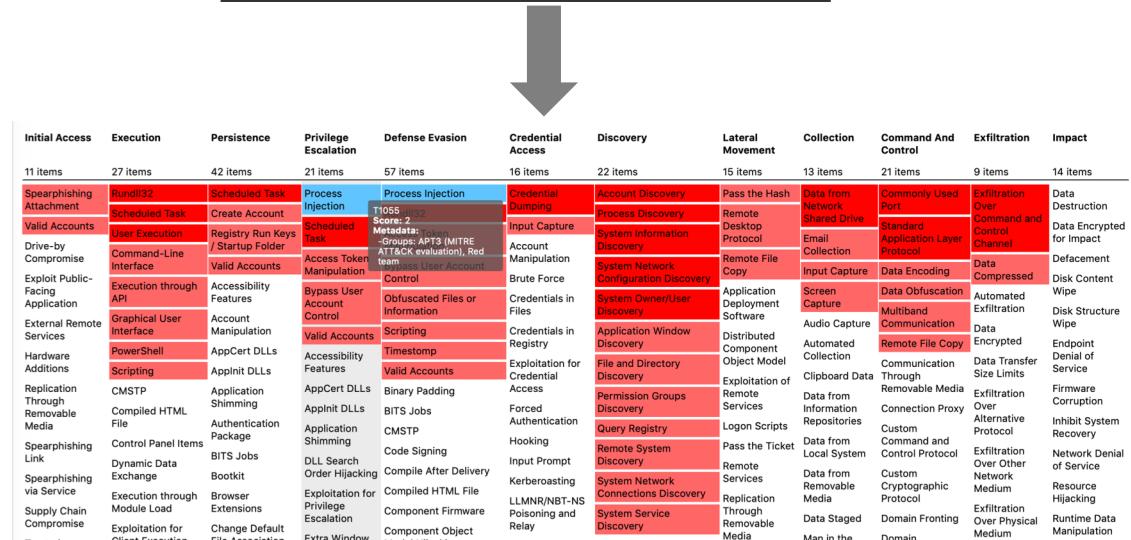
We should look at what
attackers are doing.

So we must integrate **threat intelligence**, right?

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

```
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
```



Where do we start hunting?

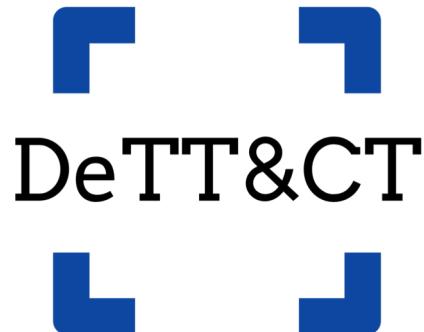
Legend

Technique only present in group

We have some level of detection

We have detection and used by 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
Supply Chain Compromise	Control Panel Items	Security Support Provider	Access Token Manipulation	Access Token Manipulation	Input Capture	Password Policy T1056 Score: 5 Metadata: -System -Applicable to: client endpoints -Detection score: 4 -Overlay: Detection	Logon Scripts	Input Capture	Domain Fronting	Data Compressed	Endpoint Denial of Service
	Service Execution	AppCert DLLs	Extra Window Memory Injection	Control Panel Items	Credential Dumping		Pass the Hash	Data from Network Shared Drive	Uncommonly Used Port	Data Encrypted	
Drive-by Compromise	PowerShell	Logon Scripts	Image File Execution Options	Extra Window Memory Injection	Credentials in Registry	Application Deployment Software	Application Deployment Software	Remote Access Tools	Exfiltration Over Command and Control Channel	Network Denial of Service	
	Regsvr32	Rundll32	Process Injection	Masquerading	LLMNR/NBT-NS Poisoning and Relay		Distributed Component Object Model	Commonly Used Port	Exfiltration Over Command and Control Channel		
Exploit Public-Facing Application	Scripting	Execution Options Injection	AppCert DLLs	Process Injection	Account Manipulation	System Owner/User Discovery	Audio Capture	Commonly Used Port	Command and Control Channel	Data Encrypted for Impact	
	Scheduled Task	Application Shimming	Image File Execution Options Injection	Regsvr32	Brute Force		Automated Collection	Data Obfuscation	Data Destruction		
External Remote Services	User Execution	Scheduled Task	Accessibility Features	Rundll32	Credentials in Files	Process Discovery	Clipboard Data	Standard Application Layer Protocol	Defacement	Data Transfer Size Limits	
	CMSTP	CMSTP	Application Shimming	Scripting	Exploitation for Credential Access		Data from Information Repositories	Communication Through Removable Media	Data Transfer Size Limits		
Hardware Additions	Command-Line Interface	Account Manipulation	Image File Execution Options Injection	Timestomp	Exploitation for Credential Access	System Network Configuration Discovery	Remote Desktop Protocol	Connection Proxy	Exfiltration Over Alternative Protocol	Disk Content Wipe	
Replication Through Removable Media	Compiled HTML File	Applnit DLLs	Scheduled Task	Obfuscated Files or Information	Forced Authentication	Application Window Discovery	Data from Local System	Custom Command and Control	Exfiltration Over Other	Disk Structure Wipe	
Spearphishing Link	Dynamic Data Exchange	Authentication Package	Accessibility Features	Binary Padding	Domain Trust Discovery	File and Directory	Remote File Copy	Remote Services	File and Directory	Firmware Corruption	
	Execution through BITS Jobs	Applnit DLLs	Applnit DLLs	Applnit DLLs	File and Directory	File and Directory	File and Directory	File and Directory	File and Directory	File and Directory	



github.com/rabobank-cdc/DeTTACT

Questions?



@bakk3rm
@rubenb_2