DeTT&CT

Mapping your blue team to ATT&CK™

23-10-2019

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

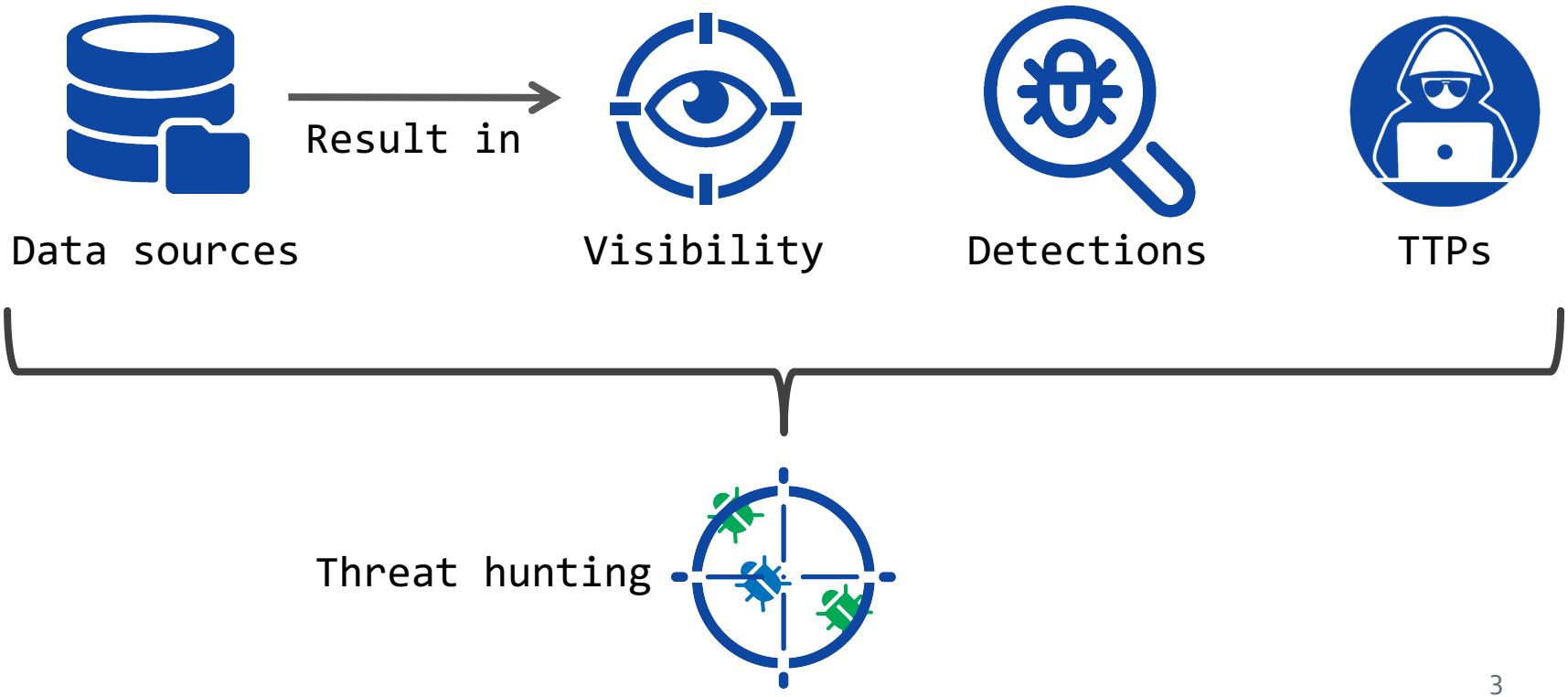
Marcus Bakker

- 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

Where to start hunting?

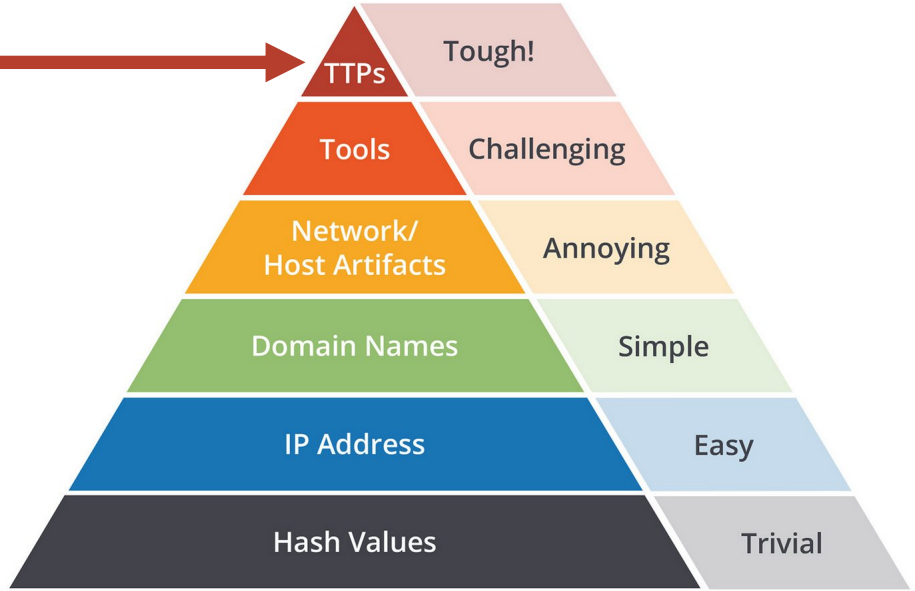
- Intelligence-driven approach with a focus on TTPs



Pyramid of Pain

ATT&CK™

"Wikipedia on cyber attacks"



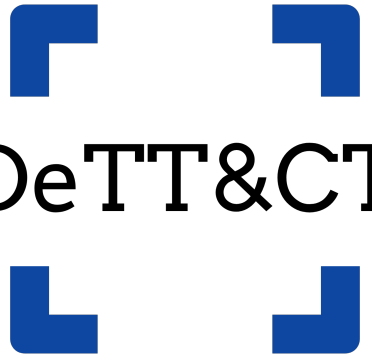
Source: David J. Bianco / http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

ATT&CK Matrix

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

- 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



github.com/rabobank-cdc/DeTTECT

Disclaimer

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

What do we log?

- Identify data sources

  Process injection

  ID: T1055

  Tactic: Defense Evasion, Privilege Escalation

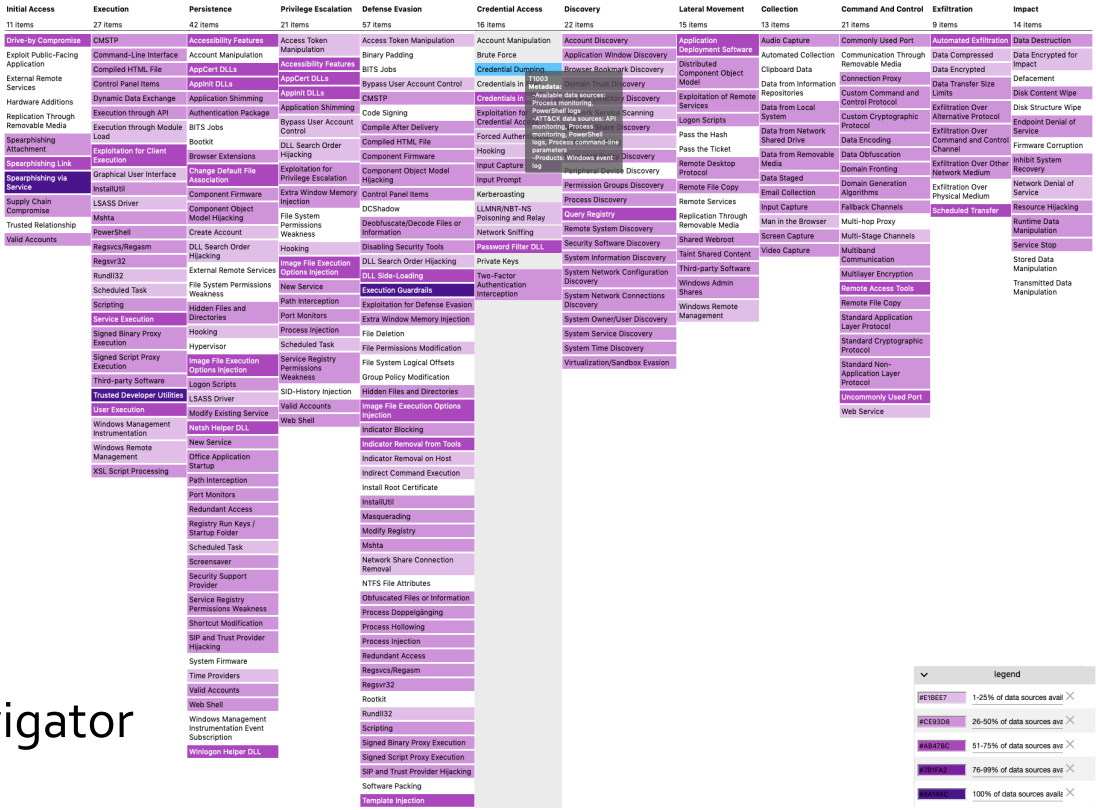
  Platform: Linux, macOS, Windows

  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

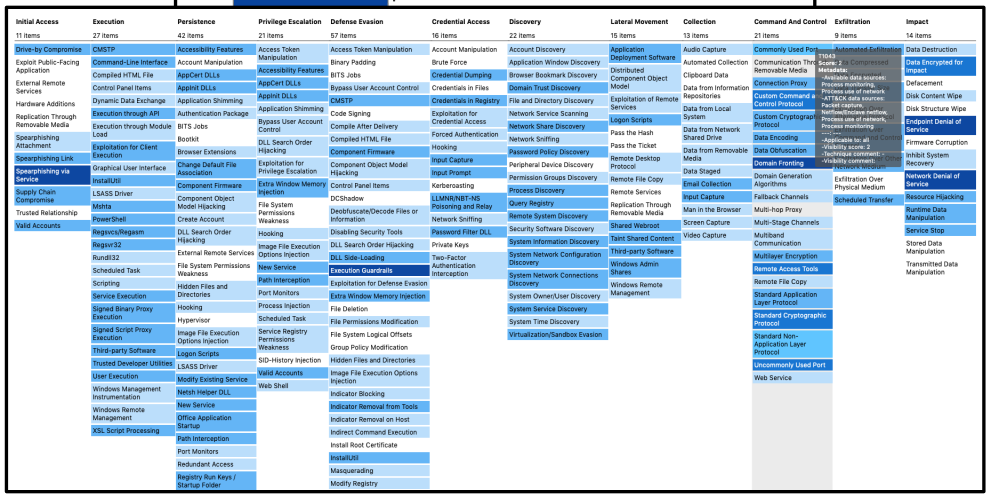


What can we see?

- 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.

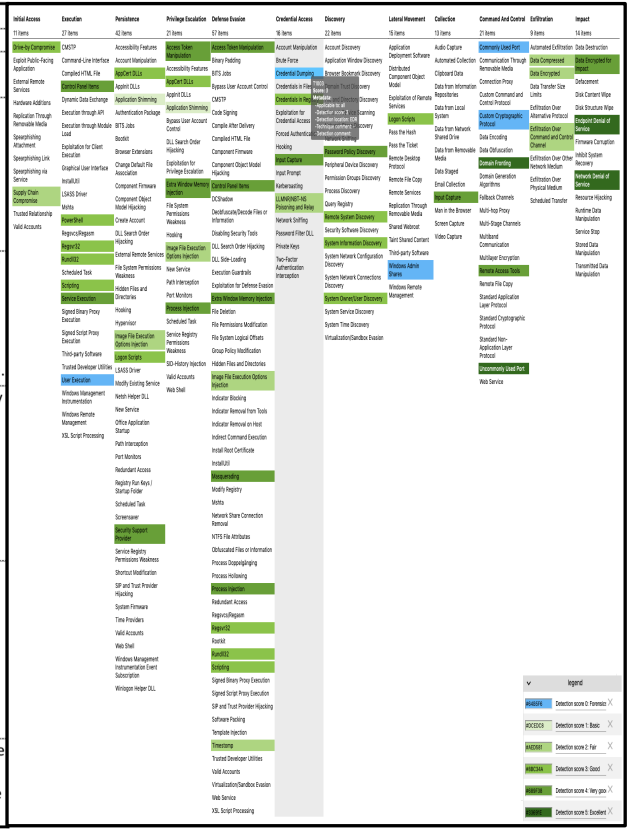


What is our detection coverage?

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

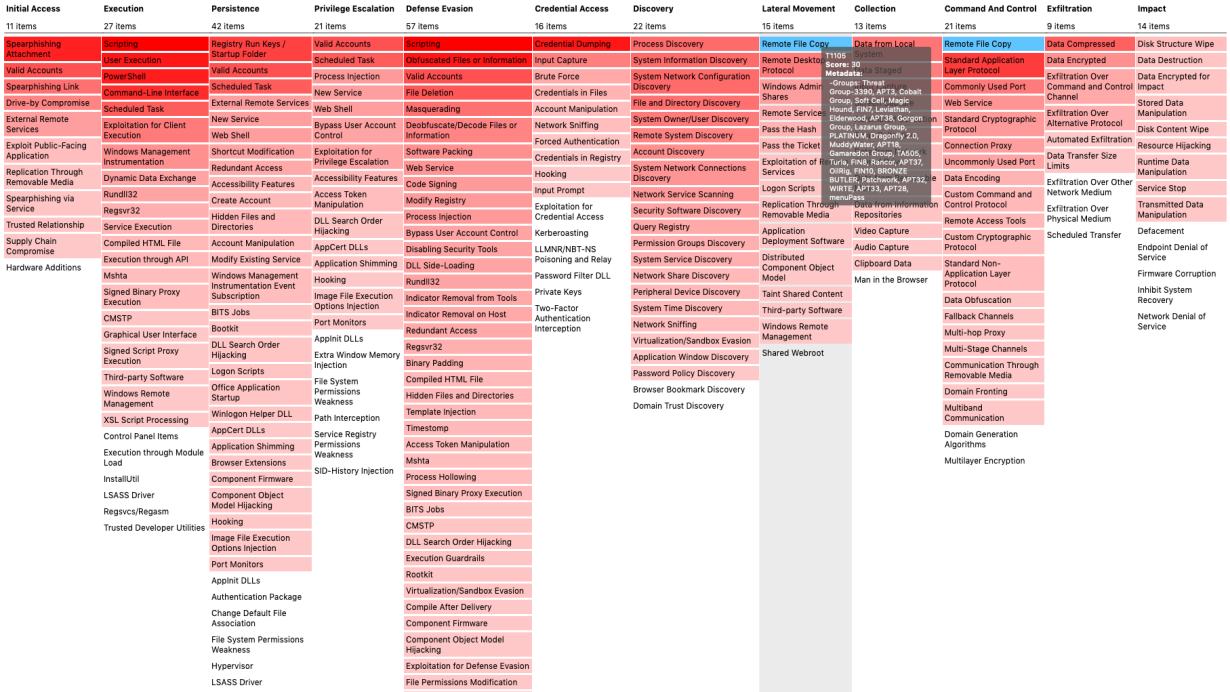
Detection scores

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".



What are attackers doing?

- 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



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

What are attackers doing?

- 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
%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
```

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

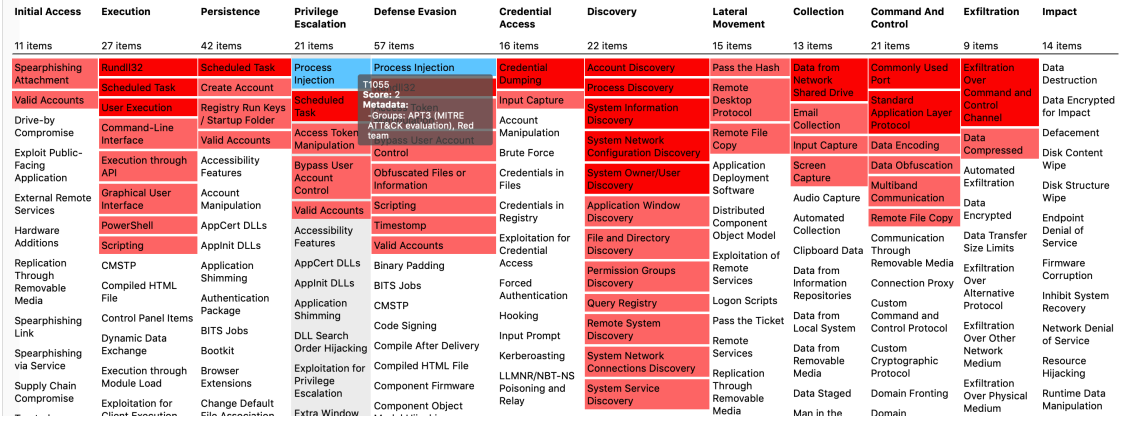
Groups

What are attackers doing?

- 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

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

```yaml
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
```



Prioritise your hunting efforts

- 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	Logon Scripts	Process Injection	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	Regsvr32	Image File Execution Options Injection	AppCert DLLs	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	Rundll32	Application Shimming	Image File Execution Options Injection	Process Injection	Account Manipulation	Account Discovery	Exploitation of Remote Services	Automated Collection	Data Obfuscation	Data Transfer Size Limits	Defacement
Hardware Additions	Scripting	Scheduled Task	Application Shimming	Regsvr32	Brute Force	Process Discovery	Pass the Ticket	Clipboard Data	Standard Application Layer Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Replication Through Removable Media	Scheduled Task	Accessibility Features	Scheduled Task	Rundll32	Credentials in Files	System Network Configuration Discovery	Remote Desktop Protocol	Data from Information Repositories	Communication Through Removable Media	Exfiltration Over Other Network Medium	Disk Structure Wipe
Spearphishing Link	User Execution	Account Manipulation	Accessibility Features	Scripting	Exploitation for Credential Access	Application Window Discovery	Remote File Copy	Data from Local System	Connection Proxy	Exfiltration Over Physical Medium	Firmware Corruption
Spearphishing via Service	CMSTP	AppInit DLLs	AppInit DLLs	Image File Execution Options Injection	Forced Authentication	Browser Bookmark Discovery	Remote Services	Data from Removable Media	Custom Command and Control Protocol		Inhibit System Recovery
	Command-Line Interface	Authentication Package		Timestomp	Hooking	Domain Trust Discovery	Replication Through	Data Staged			Resource
	Compiled HTML File			Obfuscated Files or Information		File and Directory					
	Dynamic Data Exchange			Binary Padding							
	Execution through API										

Endgame's EQL integration in DeTT&CT

- 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 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

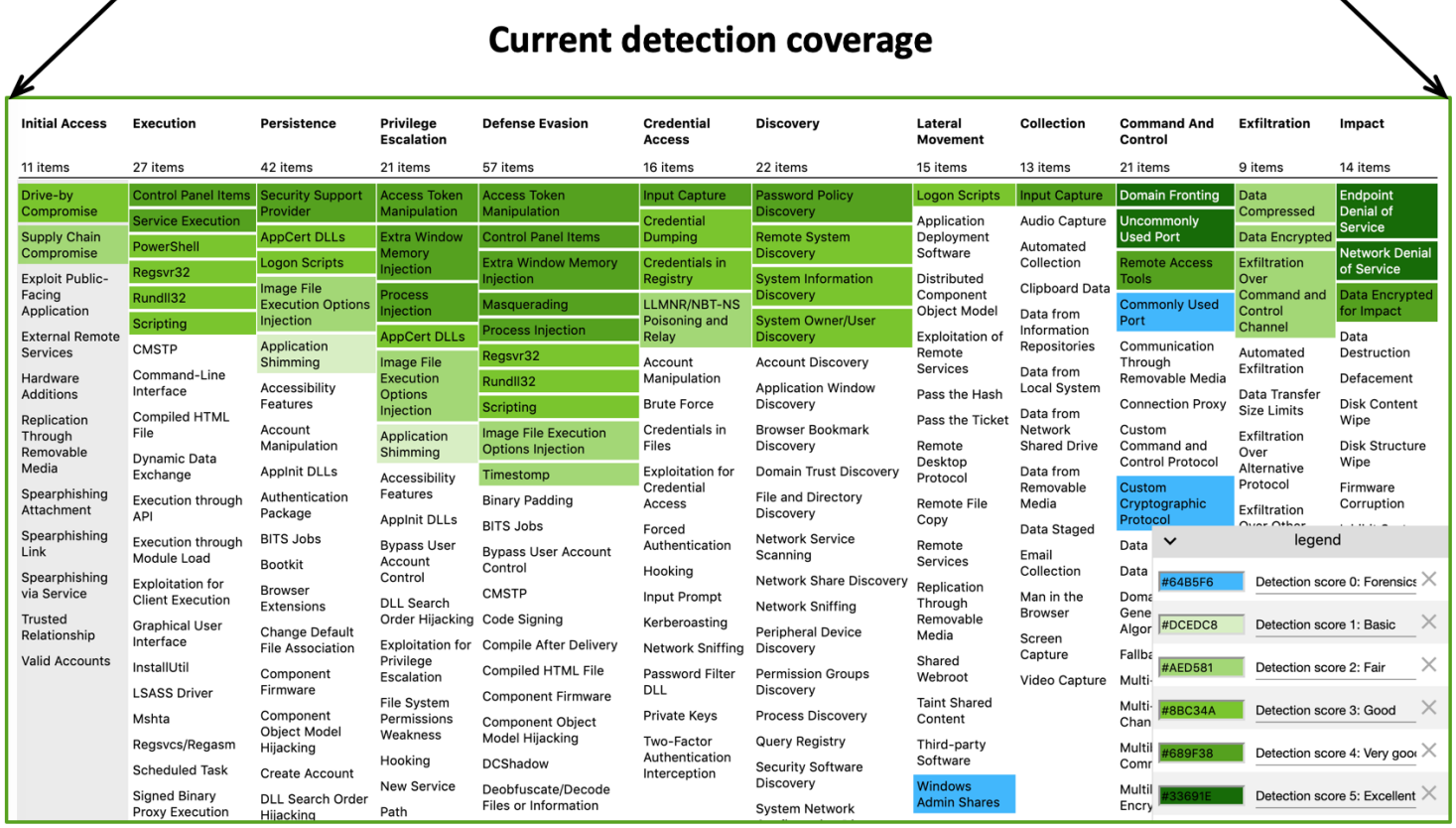
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Supply Chain Compromise	CMSTP	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	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Account Manipulation	Remote System Discovery	Distributed Component Object Model	Automated 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	AppInit DLLs	AppInit 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 Shimming	Application Shimming	CMSTP	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	Code Signing	Credentials in Registry	Application Window Discovery	Pass the Ticket	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Browser Bookmark Discovery	Remote Desktop Protocol	Data from Removable Media	Data Encoding	Exfiltration Over Other Network Medium	Disk Structure Wipe
Spearphishing Link	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication	Domain Trust Discovery	Remote File Copy	Data Staged	Data Obfuscation	Exfiltration Over Physical Medium	Firmware Corruption
Spearphishing via Service	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	File and Directory Discovery	Remote Services	Email Collection	Domain Fronting	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Capture	Network Service Scanning	Replication Through Removable Media	Input Capture	Domain Generation Algorithms		Network Denial of Service
Valid Accounts	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Input Prompt	Network Share Discovery	Shared Webroot	Man in the Browser	Fallback Channels		Resource Hijacking
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Kerberoasting	Network Sniffing	Taint Shared Content	Screen Capture	Multi-hop Proxy		Runtime Data Manipulation
	PowerShell	Create Account	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	Peripheral Device Discovery	Third-party Software	Video Capture	Multi-Stage Channels		Service Stop
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	Permission Groups Discovery	Windows Admin Shares		Multilayer Encryption		Stored Data Manipulation
	Regsvr32	External Remote Services	Port Monitors	DLL Search Order Hijacking	Private Keys	Process Discovery			Remote Access Tools		Transmitted Data Manipulation
	Rundll32	File System Permissions Weakness		DLL Side-Loading	Two-Factor Authentication Interception	Query Registry			Standard Application Layer Protocol		
	Scheduled Task	Hidden Files and		Execution Guardrails		Security Software Discovery			Standard Cryptographic Protocol		
	Scripting			Exploitation for Defense Evasion		System Network					
	Service Execution			Extra Window Memory Injection							
	Signed Binary Proxy Execution			File Deletion							

legend

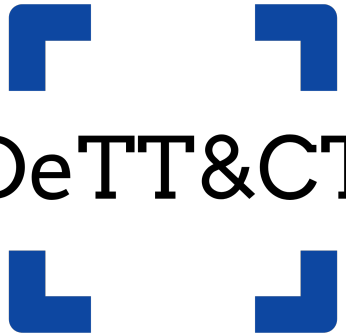
#64B5F6	Detection score 0: Forensics
#DCEDC8	Detection score 1: Basic
#AED581	Detection score 2: Fair
#8BC34A	Detection score 3: Good
#689F38	Detection score 4: Very good
#33691E	Detection score 5: Excellent

Detection coverage over time

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



End



github.com/rabobank-cdc/DeTTECT

Questions?

@Bakk3rM
@RubenB_2