# DeTT&CT

## Mapping your blue team to ATT&CK

***10-05-2019***

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

Rabobank

# A threat hunter's conversation 1/2

Where do we start **hunting**?

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

What are those things?

Uh…

# A threat hunter's conversation 2/2

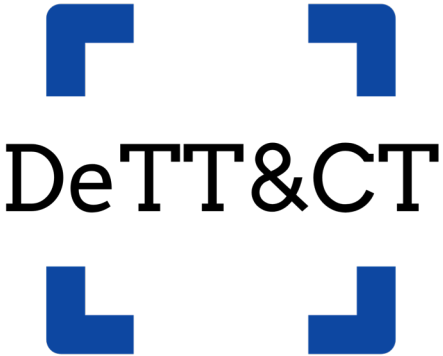
Okay, once we know where to start, what should we do first?

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




`github.com/rabobank-cdc/DeTTACT`

# Disclaimer

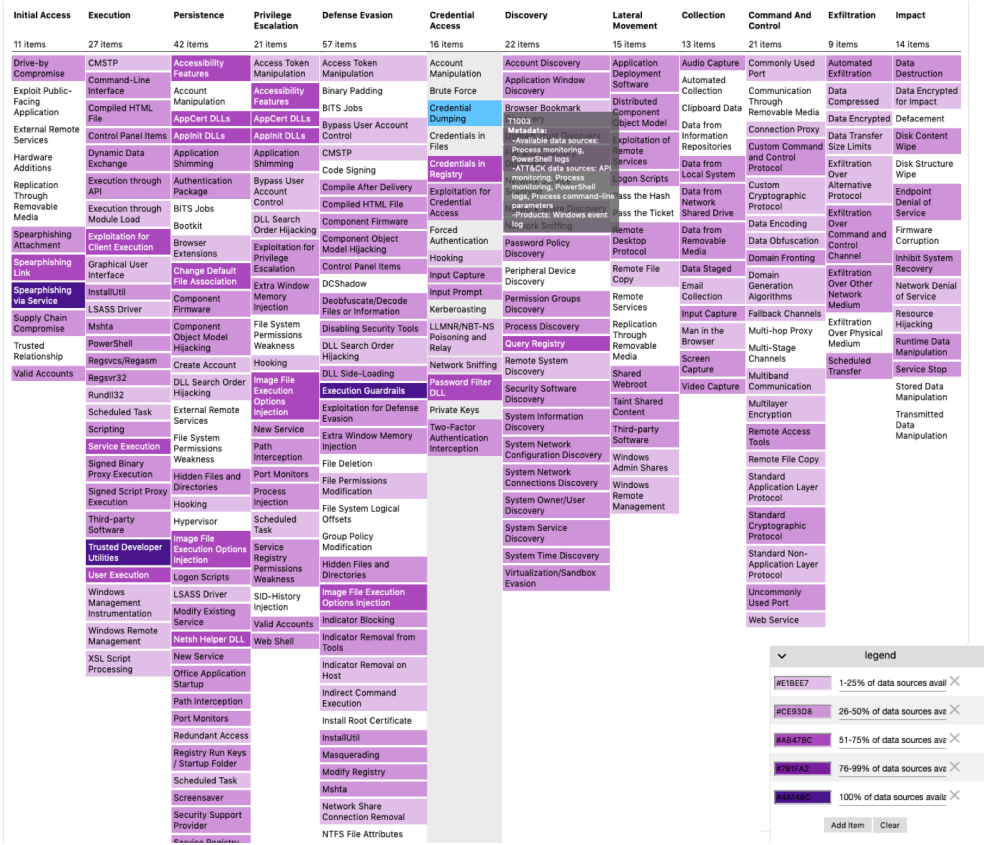
- All shown data and visualisation regarding data quality, visibility, detection and threat actor group are based on sample data.

# What can we see? 1/2

Where do we start hunting?

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

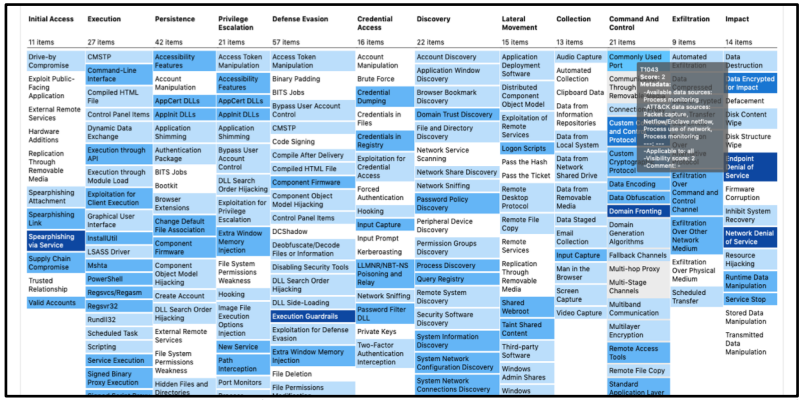
- Identify data sources
- Score data quality (DQ)
- Export DQ to Excel
- Visualise in the ATT&CK Navigator



# What can we see? 2/2

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

## 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?

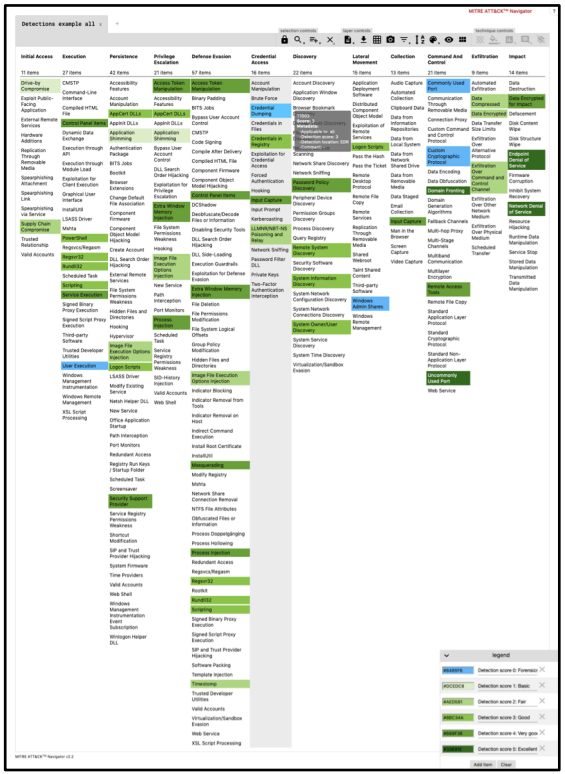
Where do we start hunting?

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". |



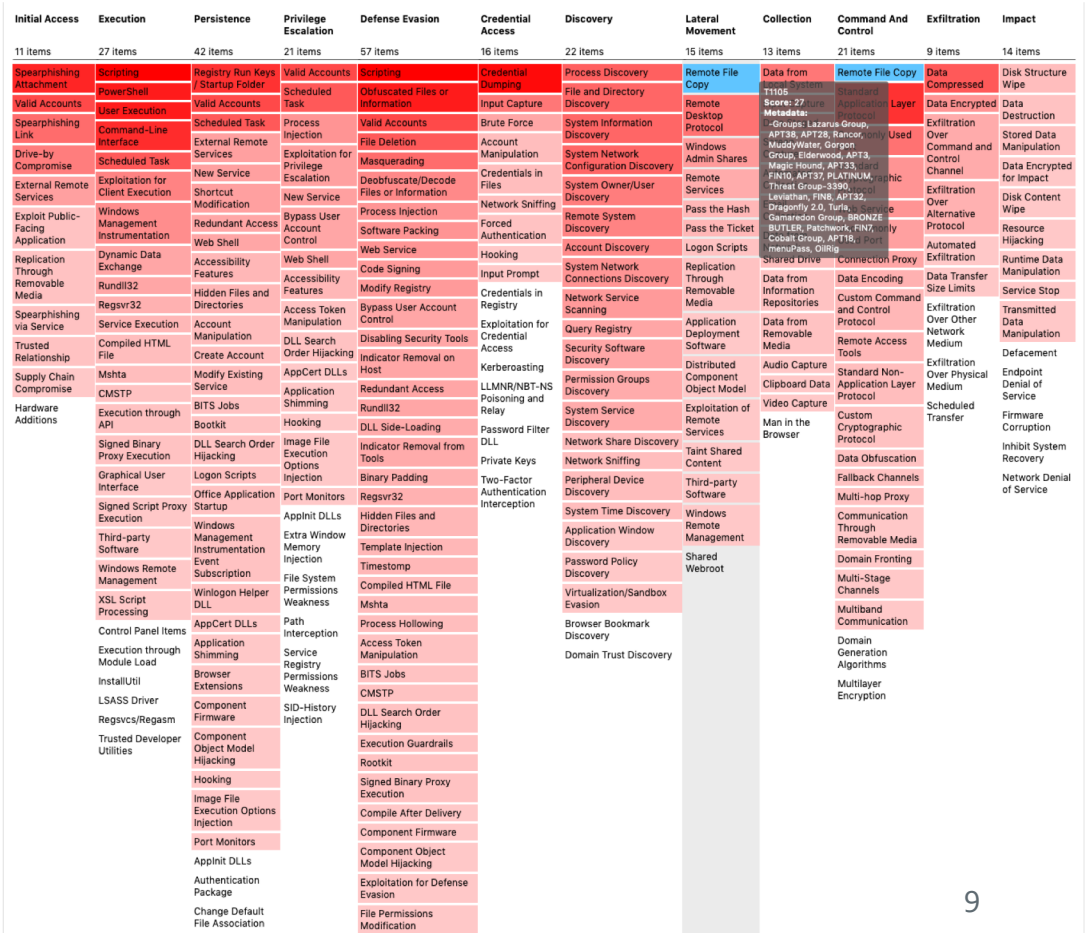
# What are attackers doing?

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



# What are attackers doing?

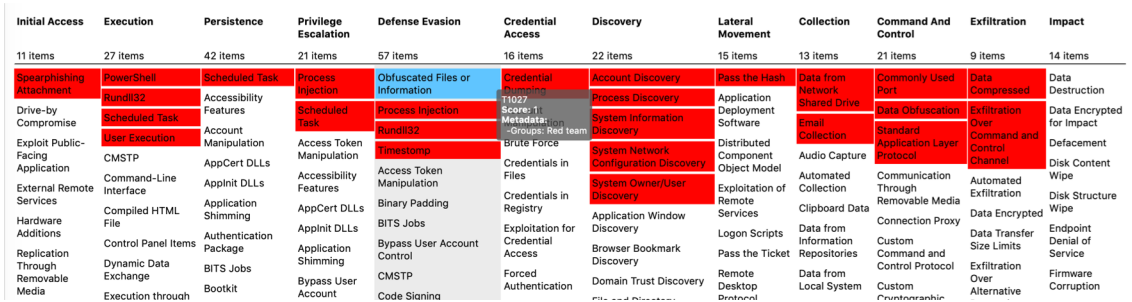
Okay, once we know where to start, what should we do first?

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

```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
```



# Groups

## What are attackers doing?

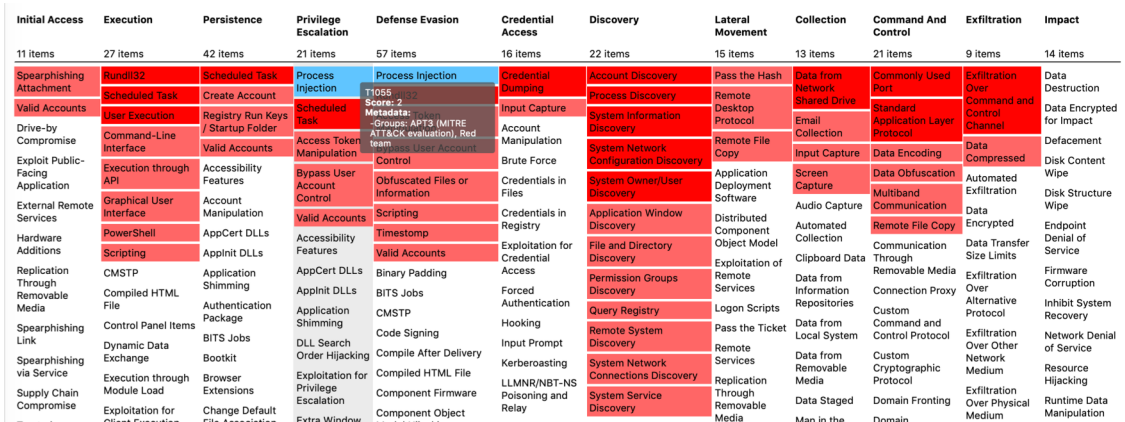
Okay, once we know where to start, what should we do first?

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

```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

Where do we start **hunting**?

**Legend**

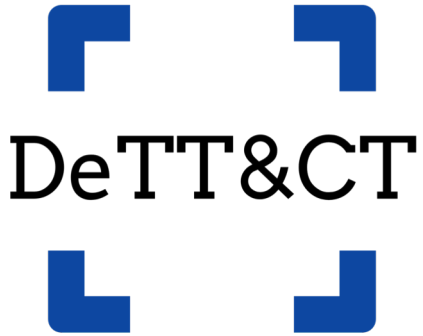
- Technique only present in group
- We have some level of detection
- We have detection and used by group

| 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 Discovery | Logon Scripts | Input Capture | Domain Fronting | Data Compressed | Endpoint Denial of Service |
| Drive-by Compromise | Service Execution | AppCert DLLs | Extra Window Memory Injection | Control Panel Items | Credential Dumping | System Network 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 | Network Share 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 | 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 | | Firmware Corruption |
| | 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 | | |
| | Command-Line Interface | Authentication Package | | Timestomp | | Domain Trust Discovery | | | | | |
| | Compiled HTML File | | | Obfuscated Files or Information | | File and Directory | | | | | |
| | Dynamic Data Exchange | | | Binary Padding | | | | | | | |
| | Execution through | | | | | | | | | | |

T1056
**Score:** 5
**Metadata:**
-Applicable to: client endpoints
-Detection score: 4
-Overlay: Detection

legend

# End




`github.com/rabobank-cdc/DeTTACT`

## Questions?

@bakk3rm
@rubenb_2