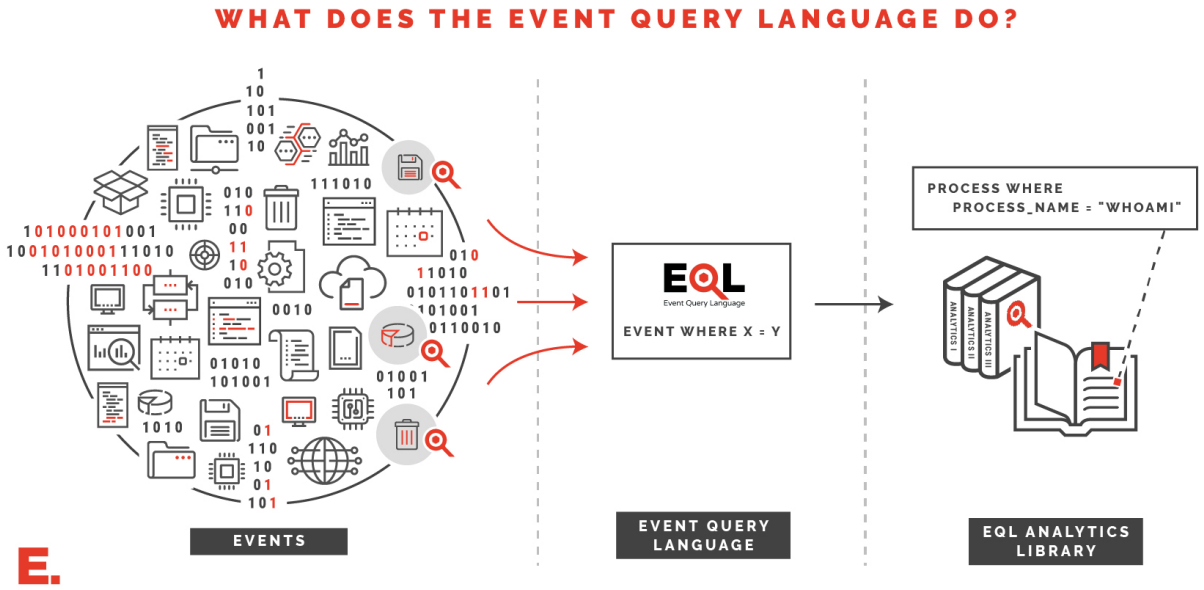
EQL Analytics Library

endgame

May 06, 2019

Contents



eqllib is a library of event based analytics, written in EQL to detect adversary behaviors identified in MITRE ATT&CK™.

CHAPTER 1

Resources

- *Get started* with EQL on your own computer
- Explore the *analytics* that map to ATT&CK.
- Learn how to write queries in EQL syntax
- Browse our *schemas* and existing normalizations
- Check the *license* status

1.1 Getting Started

The EQL library current supports Python 2.7 and 3.5 - 3.7. Assuming a supported Python version is installed, run the command:

```
$ git clone https://github.com/endgameinc/eqllib
$ cd eqllib
$ python setup.py install
```

If Python is configured and already in the PATH, then `eqllib` will be readily available, and can be checked by running the command:

```
$ eqllib -h
usage: eqllib [-h] {convert-query,convert-data,query,survey} ...

EQL Analytics

positional arguments:
  {convert-query,convert-data,query,survey}
                        Sub Command Help
    convert-query       Convert a query to specific data source
    convert-data        Convert data from a specific data source
    query               Query over a data source
    survey              Run multiple analytics over JSON data
```

1.1.1 `eqllib` Command-Line Interface

The EQL Analytics Library comes with a utility that can search, normalize, and survey JSON data. See *Getting Started* for instructions on installing `eqllib` locally.

convert-data

eqllib *convert-data* [*OPTIONS*] <*input-json-file*> <*output-json-file*>

The **`convert-data`** command normalizes data, generating a new JSON file that matches the schema.

Arguments

`output-json-file`
Path to an output JSON file to store normalized events.

Options

`-h`
Show the help message and exit

`--file, -f`
Path to a JSON file of unnormalized events. Defaults to stdin if not specified

`--format`
Format for the input file. One of `json`, `json.gz`, `jsonl`, `jsonl.gz`

`-s` `<data-source>`, **`--source`** `<data-source>`
Required: the source schema for the events. (e.g. `"Microsoft Sysmon"`)

`-e` `<encoding>`
Source file encoding. (e.g. `ascii`, `utf8`, `utf16`, etc.)

convert-query

eqllib *convert-query* [*OPTIONS*] <*eql-query*>

The **`convert-query`** command takes an EQL query that matches a normalized schema, and will print out the query converted to match a different schema.

Arguments

`eql-query`
Input EQL query written for the normalization schema

Options

`-h`
Show the help message and exit

`-s` `<data-source>`, **`--source`** `<data-source>`
Required: the source schema for the events. (e.g. `"Microsoft Sysmon"`)

query

The **query** command reads JSON events and print matching output events back as JSON. Unless specified with *-s*, data is assumed to already be normalized against the schema.

eqllib *query* [*OPTIONS*] <*input-query*> <*json-file*>

Arguments

input-query
Query in EQL syntax that matches the common schema.

Options

-h
Show the help message and exit

--file, -f
Path to a JSON file of unnormalized events. Defaults to stdin if not specified

--format
Format for the input file. One of `json`, `json.gz`, `jsonl`, `jsonl.gz`

-s `<data-source>`, **--source** `<data-source>`
Required: the source schema for the events. (e.g. `"Microsoft Sysmon"`)

-e `<encoding>`
Source file encoding. (e.g. `ascii`, `utf8`, `utf16`, etc.)

survey

eqllib *survey* [*OPTIONS*] <*json-file*> <*analytic-path*> [*analytic-path*, ...]

The **survey** command can be used to run multiple analytics against a single JSON file. Unless specified with *-s*, data is assumed to already be normalized against the schema.

Arguments

analytic-path `[analytic-path, ...]`
Path(s) to analytic TOML files or a directory of analytics.

Options

-h
Show the help message and exit

--file, -f
Path to a JSON file of unnormalized events. Defaults to stdin if not specified

--format
Format for the input file. One of `json`, `json.gz`, `jsonl`, `jsonl.gz`

-s `<data-source>`, **--source** `<data-source>`
Required: the source schema for the events. (e.g. `"Microsoft Sysmon"`)

-e <encoding>
Source file encoding. (e.g. `ascii`, `utf8`, `utf16`, etc.)

-c
Output counts per analytic instead of the individual hits.

View usage for the related EQL utility.

1.1.2 Guide to Microsoft Sysmon

Microsoft Sysmon is a freely available tool provided by SysInternals for endpoint logging.

Installing Sysmon

`Download` Sysmon from SysInternals.

To install Sysmon, from a terminal, simply change to the directory where the unzipped binary is located, then run the following command as an Administrator

To capture all default event types, with all hashing algorithms, run

```
Sysmon.exe -AcceptEula -i -h * -n -l
```

To configure Sysmon with a specific XML configuration file, run

```
Sysmon.exe -AcceptEula -i myconfig.xml
```

Full details of what each flag does can be found on the Microsoft Sysmon page

Warning: Depending on the configuration, Sysmon can generate a significant amount of data. When deploying Sysmon to production or enterprise environments, it is usually best to tune it to your specific environment. There are several Sysmon configuration files in common use which can be used or referenced for this purpose.

- @SwiftOnSecurity's scalable config file.
- @olafhartong's more verbose config file.

Getting Sysmon logs with PowerShell

Helpful PowerShell functions for parsing Sysmon events from Windows Event Logs are found in the Github at utils/scrape-events.ps1

Getting logs into JSON format can be done by piping to PowerShell cmdlets within an elevated `powershell.exe` console.

```
# Import the functions provided within scrape-events
Import-Module .\utils\scrape-events.ps1

# Save the most recent 5000 Sysmon logs
Get-LatestLogs  | ConvertTo-Json | Out-File -Encoding ASCII -FilePath my-sysmon-data.
↪json

# Save the most recent 1000 Sysmon process creation events
Get-LatestProcesses | ConvertTo-Json | Out-File -Encoding ASCII -FilePath my-sysmon-
↪data.json
```

To get *all* Sysmon logs from Windows Event Logs, run the powershell command

```
Get-WinEvent -filterhashtable @{logname="Microsoft-Windows-Sysmon/Operational"} -
↪Oldest | Get-EventProps | ConvertTo-Json | Out-File -Encoding ASCII -FilePath my-
↪sysmon-data.json
```

Warning: Use this with caution as it will process all events, which may take time and likely generate a large file

Example searches with EQL

Once you have logs in JSON format, they can now be queried using EQL. To do so, either the *query* or the *data* will need to be converted (normalized). Because EQL is built to be able to be flexible across all data sources, it is necessary to translate the query to match the underlying data, or to change the data to match the query. The conversion functionality is described in more detail in the *eqllib Command-Line Interface* guide.

For example, to find suspicious reconnaissance commands over the generated data

```
eqllib query -f my-sysmon-data.json --source "Microsoft Sysmon" "process where␣
↪process_name in ('ipconfig.exe', 'netstat.exe', 'systeminfo.exe', 'route.exe')"
```

1.2 Analytics

1.2.1 AD Dumping via Ntdsutil.exe

Identifies usage of `ntdsutil.exe` to export an Active Directory database to disk.

id 19d59f40-12fc-11e9-8d76-4d6bb837cda4

categories detect

confidence medium

os windows

created 01/07/2019

updated 01/07/2019

MITRE ATT&CK™ Mapping

tactics Credential Access

techniques T1003 Credential Dumping

Query

```
file where file_name == "ntds.dit" and process_name == "ntdsutil.exe"
```

Detonation

Atomic Red Team: T1003

Contributors

- Tony Lambert

1.2.2 Audio Capture via PowerShell

Detect attacker collecting audio via PowerShell Cmdlet.

id ab7a6ef4-0983-4275-a4f1-5c6bd3c31c23

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Collection

techniques T1123 Audio Capture

Query

```
process where subtype.create and
  process_name == "powershell.exe" and command_line == "* WindowsAudioDevice-
↪Powershell-Cmdlet *"
```

Detonation

Atomic Red Team: T1123

Contributors

- Endgame

1.2.3 Audio Capture via SoundRecorder

Detect audio collection via SoundRecorder application.

id f72a98cb-7b3d-4100-99c3-a138b6e9ff6e

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Collection

techniques T1123 Audio Capture

Query

```
process where subtype.create and
  process_name == "SoundRecorder.exe" and command_line == "* /FILE*"
```

Detonation

Atomic Red Team: T1123

Contributors

- Endgame

1.2.4 Bypass UAC via CMSTP

Detect child processes of automatically elevated instances of Microsoft Connection Manager Profile Installer (`cmstp.exe`).

id e584f1a1-c303-4885-8a66-21360c90995b

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion, Execution

techniques T1191 CMSTP, T1088 Bypass User Account Control

Query

```
sequence
  [ process where subtype.create and
     process_name == "cmstp.exe" and command_line =="*/s*" and command_line =="*/au*
↪"] by unique_pid
  [ process where subtype.create ] by unique_ppid
```

Detonation

Atomic Red Team: T1191

Contributors

- Endgame

1.2.5 Change Default File Association

Detect changes to default File Association handlers.

id 26f0ebab-b315-492d-a5be-aa665fba2f35

categories hunt

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Persistence

techniques T1042 Change Default File Association

Query

```
sequence by unique_pid with maxspan=1s
    [ registry where key_path == "*\\SOFTWARE\\Classes\\*\\*"]
    [ registry where key_path ==
↪"*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\GlobalAssocChangedCounter
↪"]

| unique_count process_name, key_path
```

Detonation

Atomic Red Team: T1042

Contributors

- Endgame

1.2.6 Clearing Windows Event Logs with wevtutil

Identifies attempts to clear Windows event logs with the command `wevtutil`.

id 5b223758-07d6-4100-9e11-238cfdd0fe97

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1070 Indicator Removal on Host

Query

```
process where subtype.create and
  process_name == "wevtutil.exe" and command_line == "* cl *"
```

Detonation

Atomic Red Team: T1070

Contributors

- Endgame

1.2.7 COM Hijack via Script Object

Identifies COM hijacking using the script object host `scrobj.dll`, which allows for stealthy execution of scripts in legitimate processes.

id 9d556fd6-76a3-45d5-9d8d-cb8edf0282f2

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Persistence, Defense Evasion

techniques T1122 Component Object Model Hijacking

Query

```
registry where
  key_path == "*_Classes\\CLSID\\{*}\\InprocServer32*" and
  (bytes_written_string == "scrobj*" or bytes_written_string == "*\\scrobj*")
```

Detonation

Atomic Red Team: T1122

Contributors

- Endgame

1.2.8 Command-Line Creation of a RAR file

Detect compression of data into a RAR file using the `rar.exe` utility.

id 1ec33c93-3d0b-4a28-8014-dbdaae5c60ae

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Exfiltration

techniques T1002 Data Compressed

Query

```
process where subtype.create and process_name == "rar.exe" and
  command_line == "* a *"
```

Detonation

Atomic Red Team: T1002

Contributors

- Endgame

1.2.9 Delete Volume USN Journal with fsutil

Identifies use of the fsutil command to delete the volume USNJRNL. This technique is used by attackers to eliminate evidence of files created during post-exploitation activities.

id c91f422a-5214-4b17-8664-c5fcf115c0a2

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1070 Indicator Removal on Host

Query

```
process where subtype.create and
    process_name == "fsutil.exe" and command_line == "* usn *" and command_line == "*␣
↪deletejournal*"
```

Detonation

Atomic Red Team: T1070

Contributors

- Endgame

1.2.10 Discovery of a Remote System's Time

Identifies use of various commands to query a remote system's time. This technique may be used before executing a scheduled task or to discover the time zone of a target system

id fcdb99c2-ac3c-4bde-b664-4b336329bed2

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Discovery

techniques T1124 System Time Discovery

Query

```
process where subtype.create and process_name == "net.exe" and
  command_line == "* time *" and command_line == "*\\\\*"
| unique parent_process_path, command_line
```

Detonation

Atomic Red Team: T1124

Contributors

- Endgame

1.2.11 Encoding or Decoding Files via CertUtil

Find execution of the Windows tool certutil.exe to decode or encode files.

id c6facc54-4894-4722-b873-062baaae851f

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1140 Deobfuscate/Decode Files or Information

Query

```
process where subtype.create and
  process_name == "certutil.exe" and
  (command_line == "*encode *" and command_line == "*decode *")
```

Detonation

Atomic Red Team: T1140

Contributors

- Endgame

1.2.12 Enumeration of Local Shares

Identifies enumeration of local shares with the builtin Windows tool `net.exe`.

id bc1944cd-97fc-4b9a-b068-46203b6bbcde

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Discovery

techniques T1135 Network Share Discovery

Query

```
process where subtype.create and
  (process_name == "net.exe" or (process_name == "net1.exe" and parent_process_name !
↪= "net.exe")) and
  command_line == "* share*" and command_line != "* * *"
```

Contributors

- Endgame

1.2.13 Enumeration of Mounted Shares

Identifies enumeration of mounted shares with the builtin Windows tool `net.exe`.

id 4d2e7fc1-af0b-4915-89aa-03d25ba7805e

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Discovery

techniques T1049 System Network Connections Discovery

Query

```
process where subtype.create and
  (process_name == "net.exe" or (process_name == "net1.exe" and parent_process_name !
↪= "net.exe")) and
  (command_line == "* use" or command_line == "* use *") and

  // since this command is looking for discovery only, we want to ignore mounting␣
↪shares
  command_line != "* \\\\*"
| unique parent_process_path, command_line, user_name
```

Detonation

Atomic Red Team: T1049

Contributors

- Endgame

1.2.14 Enumeration of Remote Shares

Identifies enumeration of remote shares with the builtin Windows tool `net.exe`.

id e61f557c-a9d0-4c25-ab5b-bbc46bb24deb

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Discovery

techniques T1135 Network Share Discovery

Query

```
process where subtype.create and
  (process_name == "net.exe" or (process_name == "net1.exe" and parent_process_name !
↪= "net.exe")) and
  command_line == "* view*" and command_line == "*\\\\*"
```

Detonation

Atomic Red Team: T1135

Contributors

- Endgame

1.2.15 Execution of a Command via a SYSTEM Service

Detect the usage of an intermediate service used to launch a SYSTEM-level command via `cmd.exe` or `powershell.exe`.

id dcb72010-c3f5-42bc-bc5e-f4f015aed1e8

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Privilege Escalation

techniques T1035 Service Execution, T1050 New Service

Query

```
registry where
    key_path == "*\\System\\*ControlSet*\\Services\\*\\ImagePath"
    and wildcard(bytes_written_string, "*%COMSPEC%*", "*cmd.exe*", "*powershell*",
↪"*cmd *")
```

Detonation

Atomic Red Team: T1035

Contributors

- Endgame

1.2.16 Image Debuggers for Accessibility Features

The Debugger registry key allows an attacker to launch intercept the execution of files, causing an a different process to be executed. This functionality is used by attackers and often targets common programs to establish persistence.

id 279773ee-7c69-4043-870c-9ed731c7989a

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Persistence, Privilege Escalation, Defense Evasion

techniques T1015 Accessibility Features, T1183 Image File Execution Options Injection

Query

```
registry where wildcard(key_path,
  "*\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution␣
↪Options\\*\\Debugger",
  "*\\Software\\Wow6432Node\\Microsoft\\Windows NT\\CurrentVersion\\Image File␣
↪Execution Options\\*\\Debugger"
  )

  and wildcard(key_path,
    // Accessibility Features
    "*\\sethc.exe\\*",
    "*\\utilman.exe\\*",
    "*\\narrator.exe\\*",
    "*\\osk.exe\\*",
    "*\\magnify.exe\\*",
    "*\\displayswitch.exe\\*",
    "*\\atbroker.exe\\*",
  )
```

Detonation

Atomic Red Team: T1015

Contributors

- Endgame

1.2.17 Indirect Command Execution

Detect indirect command execution via Program Compatibility Assistant `pcalua.exe` or `forfiles.exe`.

id 884a7ccd-7305-4130-82d0-d4f90bc118b6

categories hunt

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1202 Indirect Command Execution

Note: These processes can be used in legitimate scripts, so `| unique_count` and `| filter` are used to focus on outliers as opposed to commonly seen artifacts.

Query

```
process where subtype.create and
  parent_process_name in ("pcalua.exe", "forfiles.exe")
| unique_count command_line, process_name
| filter count < 10
```

Detonation

Atomic Red Team: T1202

Contributors

- Endgame

1.2.18 Installing Custom Shim Databases

Identifies the installation of custom Application Compatibility Shim databases.

id 0e9a0a32-acf4-4969-9828-215a692c436e

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Persistence, Privilege Escalation

techniques T1138 Application Shimming

Query

```
registry where key_path == "*\\SOFTWARE\\Microsoft\\Windows␣
↪NT\\CurrentVersion\\AppCompatFlags\\Custom\\*.sdb"
  and not event of [process where subtype.create and

                      // Ignore legitimate usage of sdbinst.exe
                      not (process_name == "sdbinst.exe" and parent_process_name ==
↪"msiexec.exe")
                    ]
```

Detonation

Atomic Red Team: T1138

Contributors

- Endgame

1.2.19 Interactive AT Job

Detect an interactive AT job, which may be used as a form of privilege escalation.

id d8db43cf-ed52-4f5c-9fb3-c9a4b95a0b56

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Privilege Escalation

techniques T1053 Scheduled Task

Note:

As of Windows 8, the `at.exe` command was deprecated and prints the error message The AT command has been deprecated. Please use schtasks.exe instead.

Query

```
process where subtype.create and
  process_name == "at.exe" and command_line == "* interactive *"
```

Detonation

Atomic Red Team: T1053

Contributors

- Endgame

References

- https://blogs.technet.microsoft.com/supportingwindows/2013/07/05/whats-new-in-task-scheduler-for-windows-8-server-2012/

1.2.20 Logon Scripts with UserInitMprLogonScript

Detect modification of Windows logon scripts stored in `HKCU\Environment\UserInitMprLogonScript` and trigger when a user logs in.

id 54fff7e8-f81d-4169-b820-4cbff0133e2d

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Persistence

techniques T1037 Logon Scripts

Query

```
registry where key_path == "*\\Environment\\UserInitMprLogonScript"
```

Detonation

Atomic Red Team: T1037

Contributors

- Endgame

1.2.21 LSASS Memory Dumping

Detect creation of dump files containing the memory space of lsass.exe, which contains sensitive credentials.

id 210b4ea4-12fc-11e9-8d76-4d6bb837cda4

categories detect

confidence high

os windows

created 01/07/2019

updated 01/07/2019

MITRE ATT&CK™ Mapping

tactics Credential Access

techniques T1003 Credential Dumping

Query

```
file where file_name == "lsass*.dmp" and process_name != "werfault.exe"
```

Detonation

Atomic Red Team: T1003

Contributors

- Tony Lambert

1.2.22 LSASS Memory Dumping via ProcDump.exe

Identifies usage of Sysinternals `procdump.exe` to export the memory space of lsass.exe which contains sensitive credentials.

id 1e1ef6be-12fc-11e9-8d76-4d6bb837cda4

categories detect

confidence high

os windows

created 01/07/2019

updated 01/07/2019

MITRE ATT&CK™ Mapping

tactics Credential Access

techniques T1003 Credential Dumping

Query

```
process where subtype.create and
  process_name == "procdump*.exe" and command_line == "*lsass*"
```

Detonation

Atomic Red Team: T1003

Contributors

- Tony Lambert

1.2.23 Modification of Boot Configuration

Identifies use of the bcdedit command to delete boot configuration data. This tactic is sometimes used as by malware or an attacker as a destructive technique.

id c4732632-9c1d-4980-9fa8-1d98c93f918e

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1107 File Deletion

Query

```
process where subtype.create and
  process_name == "bcdedit.exe" and command_line == "*set *" and
  (command_line == "* bootstatuspolicy *ignoreallfailures*" or command_line == "*␣
↪recoveryenabled* no*")
```

Detonation

Atomic Red Team: T1107

Contributors

- Endgame

1.2.24 Modifications of .bash_profile and .bashrc

Detect modification of .bash_profile and .bashrc files for persistent commands

id 3567621a-1564-11e9-8e67-d46d6d62a49e

categories hunt

confidence low

os linux, macos

created 01/10/2019

updated 01/10/2019

MITRE ATT&CK™ Mapping

tactics Persistence

techniques T1156 .bash_profile and .bashrc

Query

```
file where subtype.modify and
  (file_name == ".bash_profile" or file_name == ".bashrc")
```

Detonation

Atomic Red Team: T1156

Contributors

- Tony Lambert

1.2.25 Mounting Hidden Shares

Identifies enumeration of mounted shares with the builtin Windows tool `net.exe`.

id 9b3dd402-891c-4c4d-a662-28947168ce61

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Lateral Movement

techniques T1077 Windows Admin Shares

Query

```
process where subtype.create and
  (process_name == "net.exe" or (process_name == "net1.exe" and parent_process_name !
↪= "net.exe")) and
  (command_line == "* use" or command_line == "* use *") and

  // since this command is looking for discovery only, we want to ignore mounting␣
↪shares
  command_line == "* \\\\*"
| unique parent_process_path, command_line, user_name
```

Detonation

Atomic Red Team: T1077

Contributors

- Endgame

1.2.26 Mshta Network Connections

Identifies suspicious `mshta.exe` commands that make outbound network connections.

id 6bc283c4-21f2-4aed-a05c-a9a3ffa95dd4

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Execution, Defense Evasion, Command and Control

techniques T1170 Mshta

Query

```
sequence by unique_pid
  [process where subtype.create and process_name == "mshta.exe" and command_line ==
↪"*javascript*"]
  [network where process_name == "mshta.exe"]
```

Detonation

Atomic Red Team: T1170

Contributors

- Endgame

1.2.27 Persistence via AppInit DLL

Detect registry modifications of the AppInit_Dlls key, which is used by attackers to maintain persistence. AppInit DLLs are loaded into every process that users the common library `user32.dll`.

id 822dc4c5-b355-4df8-bd37-29c458997b8f

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Persistence, Privilege Escalation

techniques T1103 AppInit DLLs

Query

```
registry where wildcard(key_path,
    "*\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows\\AppInit_Dlls",
    "*\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows␣
↪NT\\CurrentVersion\\Windows\\AppInit_Dlls"
  )
  and not wildcard(process_path, "*\\system32\\msiexec.exe", "*\\syswow64\\msiexec.exe
↪")
| unique bytes_written_string
```

Detonation

Atomic Red Team: T1103

Contributors

- Endgame

1.2.28 Persistence via NetSh Key

The tool NetShell allows for the creation of helper DLLs, which are loaded into `netsh.exe` every time it executes. This is used by attackers to establish persistence.

id 5f9a71f4-f5ef-4d35-aff8-f67d63d3c896

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Persistence

techniques T1128 Netsh Helper DLL

Query

```
registry where key_path == "*\\Software\\Microsoft\\NetSh\\*"
```

Detonation

Atomic Red Team: T1128

Contributors

- Endgame

1.2.29 Persistence via Screensaver

Detect persistence via screensaver when attacker writes payload to registry within screensaver key path.

id dd2eee76-9b44-479e-9860-435357e82db8

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Persistence

techniques T1180 Screensaver

Query

```
registry where key_path == "*\\Control Panel\\Desktop\\SCRNSAVE.EXE"

  // Ignore when the screensaver is legitimately set via the dialog
  and not event of [ process where subtype.create
                       and process_path == "*\\system32\\rundll32.exe"
                       and parent_process_path == "*\\explorer.exe"
                       and command_line == "* shell32.dll,Control_RunDLL desk.cpl,
↪ScreenSaver,*"
                     ]
```

Detonation

Atomic Red Team: T1180

Contributors

- Endgame

References

- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1180/T1180.yaml

1.2.30 Registry Preparation of Event Viewer UAC Bypass

Identifies preparation for User Account Control (UAC) bypass via Event Viewer registry hijacking. Attackers bypass UAC to stealthily execute code with elevated permissions.

id f90dd84d-6aa1-4ffd-8f0e-933f51c20fbe

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Privilege Escalation

techniques T1088 Bypass User Account Control

Query

```
registry where
  key_path == "*\\MSCFile\\shell\\open\\command\\" and

  // Ignore cases where the original avalue is restored
  bytes_written_string != '*\\system32\\mmc.exe \"%1\"*'

  // SYSTEM will never need to bypass uac
  and not user_sid in ("S-1-5-18", "S-1-5-19", "S-1-5-20")
```

Detonation

Atomic Red Team: T1088

Contributors

- Endgame

1.2.31 RegSvr32 Scriplet Execution

Detect regsvr32 loading a script object (scrobj).

id 82200c71-f3c3-4b6c-aead-9cafeab602f5

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Execution

techniques T1117 Regsvr32

Query

```
process where subtype.create and
  process_name == "regsvr32.exe" and
  wildcard(command_line, "*scrobj*", "*/i:*", "*-i:*", "*.sct*")
```

Detonation

Atomic Red Team: T1117

Contributors

- Endgame

1.2.32 Remote Execution via WMIC

Identifies use of `wmic.exe` to run commands on remote hosts.

id 07b1481c-2a20-4274-a64e-effcd40941a5

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Lateral Movement, Execution

techniques T1047 Windows Management Instrumentation

Query

```
process where subtype.create and process_name == "wmic.exe" and
  (command_line == "* /node:*" or command_line == "* -node:*") and
  (command_line == "* *process* call *")
```

Contributors

- Endgame

1.2.33 SAM Dumping via Reg.exe

Identifies usage of `reg.exe` to export registry hives which contain the SAM and LSA secrets.

id aed95fc6-5e3f-49dc-8b35-06508613f979

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Credential Access

techniques T1003 Credential Dumping

Query

```
process where subtype.create and
  process_name == "reg.exe" and
  (command_line == "* save *" or command_line == "* export *") and
  (command_line == "*hklm*" or command_line == "*hkey_local_machine*" ) and
  (command_line == "*\\sam *" or command_line == "*\\security *" or command_line ==
↪"*\\system *")
```

Detonation

Atomic Red Team: T1003

Contributors

- Endgame

1.2.34 Suspicious ADS File Creation

Detect suspicious creation or modification of NTFS Alternate Data Streams.

id 6624038b-05e6-4f9b-9830-346af38de870

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1096 NTFS File Attributes

Query

```
file where
  file_name == "*:*" and (file_name == "*.dll*" or file_name == "*.exe*")
```

Detonation

Atomic Red Team: T1096

Contributors

- Endgame

1.2.35 Suspicious Bitsadmin Job via bitsadmin.exe

Detect download of BITS jobs via bitsadmin.exe.

id ef9fe5c0-b16f-4384-bb61-95977799a84c

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion, Persistence

techniques T1197 BITS Jobs

Query

```
process where subtype.create and
  process_name == "bitsadmin.exe" and command_line == "* /download *"
```

Detonation

Atomic Red Team: T1197

Contributors

- Endgame

1.2.36 Suspicious Bitsadmin Job via PowerShell

Detect download of BITS jobs via PowerShell.

id ec5180c9-721a-460f-bddc-27539a284273

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion, Persistence

techniques T1197 BITS Jobs

Query

```
process where subtype.create and
  process_name == "powershell.exe" and command_line == "*Start-BitsTransfer*"
```

Detonation

Atomic Red Team: T1197

Contributors

- Endgame

1.2.37 Suspicious Script Object Execution

Identifies scrobj.dll loaded into unusual Microsoft processes, often indicating a *Squiblydoo* attack.

id a792cb37-fa56-43c2-9357-4b6a54b559c7

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion, Execution

techniques T1117 Regsvr32

Query

```
image_load where image_name == "scrobj.dll" and
  process_name in ("regsvr32.exe", "rundll32.exe", "certutil.exe")
```

Detonation

Atomic Red Team: T1117

Contributors

- Endgame

References

- https://web.archive.org/web/20170427203617/http://subt0x10.blogspot.com/2017/04/bypass-application-whitelisting-script.html
- https://gist.github.com/subTee/24c7d8e1ff0f5602092f58cbb3f7d302

1.2.38 System Information Discovery

Detect enumeration of Windows system information via `systeminfo.exe`

id 4b9c2df7-87e2-4bbc-9123-9779ecb2dbf2

categories hunt

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Discovery

techniques T1082 System Information Discovery

Query

```
process where subtype.create and process_name == "systeminfo.exe"
| unique user_name, command_line
```

Detonation

Atomic Red Team: T1082

Contributors

- Endgame

1.2.39 Unload Sysmon Filter Driver with fltmc.exe

Detect the unloading of the Sysinternals Sysmon filter driver via the `unload` command line parameter.

id 1261d02a-ee99-4954-8404-8376a8d441b2

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1089 Disabling Security Tools

Note: The Sysmon driver can be installed with various service names. The analytic should be changed to reflect the installed service name if Sysmon is installed with a different name.

Query

```
process where subtype.create and
  process_name == "fltmc.exe" and command_line == "* unload *sysmon*"
```

Detonation

Atomic Red Team: T1089

Contributors

- Endgame

1.2.40 Unusual Child Process

Identifies processes launched with suspicious parents.

id 3b1b9720-179b-47e2-930e-d3757bbe345e

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion, Execution

techniques T1093 Process Hollowing, T1055 Process Injection

Query

```
process where subtype.create and
(
  (process_name == "smss.exe" and not parent_process_name in ("System", "smss.exe")) or
  (process_name == "csrss.exe" and not parent_process_name in ("smss.exe", "svchost.exe")) or
  (process_name == "wininit.exe" and parent_process_name != "smss.exe") or
  (process_name == "winlogon.exe" and parent_process_name != "smss.exe") or
  (process_name == "lsass.exe" and parent_process_name != "wininit.exe") or
  (process_name == "LogonUI.exe" and not parent_process_name in ("winlogon.exe", "wininit.exe")) or
  (process_name == "services.exe" and parent_process_name != "wininit.exe") or
  (process_name == "svchost.exe" and parent_process_name != "services.exe" and
      // When a 32-bit DLL is loaded, the syswow64\svchost.exe service will be called
      not (parent_process_path == "*\\system32\\svchost.exe" and process_path == "*\\syswow64\\svchost.exe")
  ) or
  (process_name == "spoolsv.exe" and parent_process_name != "services.exe") or
  (process_name == "taskhost.exe" and not parent_process_name in ("services.exe", "svchost.exe")) or
  (process_name == "taskhostw.exe" and not parent_process_name in ("services.exe", "svchost.exe")) or
  (process_name == "userinit.exe" and not parent_process_name in ("dwm.exe", "winlogon.exe"))
)
```

Contributors

- Endgame

References

- https://web.archive.org/web/20140119132337/https://sysforensics.org/2014/01/know-your-windows-processes.html

1.2.41 User Account Creation

Identifies creation of local users via the `net.exe` command.

id 014c3f51-89c6-40f1-ac9c-5688f26090ab

categories detect, hunt

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Persistence, Credential Access

techniques T1136 Create Account

Query

```
process where subtype.create and
  (process_name == "net.exe" or (process_name == "net1.exe" and parent_process_name !
↪= "net.exe")) and
  command_line == "* user */ad*"
```

Detonation

Atomic Red Team: T1136

Contributors

- Endgame

1.2.42 Volume Shadow Copy Deletion via VssAdmin

Identifies suspicious use of vssadmin.exe to delete volume shadow copies.

id d3a327b6-c517-43f2-8e97-1f06b7370705

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1107 File Deletion

Query

```
process where subtype.create and
    process_name == "vssadmin.exe" and command_line == "*delete* *shadows*"
```

Detonation

Atomic Red Team: T1107

Contributors

- Endgame

1.2.43 Volume Shadow Copy Deletion via WMIC

Identifies use of wmic for shadow copy deletion on endpoints. This commonly occurs in tandem with ransomware or other destructive attacks.

id 7163f069-a756-4edc-a9f2-28546dcb04b0

categories detect

confidence medium

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1107 File Deletion

Query

```
process where subtype.create and
  process_name == "wmic.exe" and command_line == "* *shadowcopy* *delete*"
```

Detonation

Atomic Red Team: T1107

Contributors

- Endgame

1.2.44 Windows Network Enumeration

Identifies attempts to enumerate hosts in a network using the built-in Windows `net.exe` tool.

id b8a94d2f-dc75-4630-9d73-1edc6bd26fff

categories detect

confidence low

os windows

created 11/30/2018

updated 11/30/2018

MITRE ATT&CK™ Mapping

tactics Discovery

techniques T1018 Remote System Discovery

Query

```
process where subtype.create and
    process_name == "net.exe" and command_line == "* view*" and command_line !=
↪"*\\\\*"
```

Detonation

Atomic Red Team: T1018

Contributors

- Endgame

Analytic	Contributors	Updated	Tactics	Techniques
AD Dumping via Ntdsutil.exe	Tony Lambert	01/07/2019	Credential Access	T1003 Credential Dumping
Audio Capture via PowerShell	Endgame	11/30/2018	Collection	T1123 Audio Capture
Audio Capture via SoundRecorder	Endgame	11/30/2018	Collection	T1123 Audio Capture
Bypass UAC via CMSTP	Endgame	11/30/2018	Defense Evasion Execution	T1191 CMSTP T1088 Bypass User Account Control
Change Default File Association	Endgame	11/30/2018	Persistence	T1042 Change Default File Association
Clearing Windows Event Logs with wevtutil	Endgame	11/30/2018	Defense Evasion	T1070 Indicator Removal on Host
COM Hijack via Script Object	Endgame	11/30/2018	Persistence Defense Evasion	T1122 Component Object Model Hijacking
Command-Line Creation of a RAR file	Endgame	11/30/2018	Exfiltration	T1002 Data Compressed
Delete Volume USN Journal with fsutil	Endgame	11/30/2018	Defense Evasion	T1070 Indicator Removal on Host

Continued on next page

Table 1 – continued from previous page

Analytic	Contributors	Updated	Tactics	Techniques
Discovery of a Remote System's Time	Endgame	11/30/2018	Discovery	T1124 System Time Discovery
Encoding or Decoding Files via CertUtil	Endgame	11/30/2018	Defense Evasion	T1140 Deobfuscate/Decode Files or Information
Enumeration of Local Shares	Endgame	11/30/2018	Discovery	T1135 Network Share Discovery
Enumeration of Mounted Shares	Endgame	11/30/2018	Discovery	T1049 System Network Connections Discovery
Enumeration of Remote Shares	Endgame	11/30/2018	Discovery	T1135 Network Share Discovery
Execution of a Command via a SYSTEM Service	Endgame	11/30/2018	Privilege Escalation	T1035 Service Execution T1050 New Service
Image Debuggers for Accessibility Features	Endgame	11/30/2018	Persistence Privilege Escalation Defense Evasion	T1015 Accessibility Features T1183 Image File Execution Options Injection
Indirect Command Execution	Endgame	11/30/2018	Defense Evasion	T1202 Indirect Command Execution
Installing Custom Shim Databases	Endgame	11/30/2018	Persistence Privilege Escalation	T1138 Application Shimming
Interactive AT Job	Endgame	11/30/2018	Privilege Escalation	T1053 Scheduled Task
Logon Scripts with UserInitMprLogonScript	Endgame	11/30/2018	Persistence	T1037 Logon Scripts
LSASS Memory Dumping	Tony Lambert	01/07/2019	Credential Access	T1003 Credential Dumping
LSASS Memory Dumping via ProcDump.exe	Tony Lambert	01/07/2019	Credential Access	T1003 Credential Dumping
Modification of Boot Configuration	Endgame	11/30/2018	Defense Evasion	T1107 File Deletion
Modifications of .bash_profile and .bashrc	Tony Lambert	01/10/2019	Persistence	T1156 .bash_profile and .bashrc
Mounting Hidden Shares	Endgame	11/30/2018	Lateral Movement	T1077 Windows Admin Shares
Mshta Network Connections	Endgame	11/30/2018	Execution Defense Evasion Command and Control	T1170 Mshta
Persistence via AppInit DLL	Endgame	11/30/2018	Persistence Privilege Escalation	T1103 AppInit DLLs
Persistence via NetSh Key	Endgame	11/30/2018	Persistence	T1128 Netsh Helper DLL

Continued on next page

Table 1 – continued from previous page

Analytic	Contributors	Updated	Tactics	Techniques
Persistence via Screensaver	Endgame	11/30/2018	Persistence	T1180 Screensaver
Registry Preparation of Event Viewer UAC Bypass	Endgame	11/30/2018	Privilege Escalation	T1088 Bypass User Account Control
RegSvr32 Scriplet Execution	Endgame	11/30/2018	Execution	T1117 Regsvr32
Remote Execution via WMIC	Endgame	11/30/2018	Lateral Movement Execution	T1047 Windows Management Instrumentation
SAM Dumping via Reg.exe	Endgame	11/30/2018	Credential Access	T1003 Credential Dumping
Suspicious ADS File Creation	Endgame	11/30/2018	Defense Evasion	T1096 NTFS File Attributes
Suspicious Bitsadmin Job via bitsadmin.exe	Endgame	11/30/2018	Defense Evasion Persistence	T1197 BITS Jobs
Suspicious Bitsadmin Job via PowerShell	Endgame	11/30/2018	Defense Evasion Persistence	T1197 BITS Jobs
Suspicious Script Object Execution	Endgame	11/30/2018	Defense Evasion Execution	T1117 Regsvr32
System Information Discovery	Endgame	11/30/2018	Discovery	T1082 System Information Discovery
Unload Sysmon Filter Driver with fltmc.exe	Endgame	11/30/2018	Defense Evasion	T1089 Disabling Security Tools
Unusual Child Process	Endgame	11/30/2018	Defense Evasion Execution	T1093 Process Hollowing T1055 Process Injection
User Account Creation	Endgame	11/30/2018	Persistence Credential Access	T1136 Create Account
Volume Shadow Copy Deletion via VssAdmin	Endgame	11/30/2018	Defense Evasion	T1107 File Deletion
Volume Shadow Copy Deletion via WMIC	Endgame	11/30/2018	Defense Evasion	T1107 File Deletion
Windows Network Enumeration	Endgame	11/30/2018	Discovery	T1018 Remote System Discovery

1.3 Atomic Blue Detections

Analytic	Contributors	Updated	Tactics	Techniques
AD Dumping via Ntdsutil.exe	Tony Lambert	01/07/2019	Credential Access	T1003 Credential Dumping
Audio Capture via PowerShell	Endgame	11/30/2018	Collection	T1123 Audio Capture
Audio Capture via SoundRecorder	Endgame	11/30/2018	Collection	T1123 Audio Capture
Bypass UAC via CMSTP	Endgame	11/30/2018	Defense Evasion Execution	T1191 CMSTP T1088 Bypass User Account Control
Change Default File Association	Endgame	11/30/2018	Persistence	T1042 Change Default File Association
Clearing Windows Event Logs with wevtutil	Endgame	11/30/2018	Defense Evasion	T1070 Indicator Removal on Host
COM Hijack via Script Object	Endgame	11/30/2018	Persistence Defense Evasion	T1122 Component Object Model Hijacking
Command-Line Creation of a RAR file	Endgame	11/30/2018	Exfiltration	T1002 Data Compressed
Delete Volume USN Journal with fsutil	Endgame	11/30/2018	Defense Evasion	T1070 Indicator Removal on Host
Discovery of a Remote System's Time	Endgame	11/30/2018	Discovery	T1124 System Time Discovery
Encoding or Decoding Files via CertUtil	Endgame	11/30/2018	Defense Evasion	T1140 Deobfuscate/Decode Files or Information
Enumeration of Mounted Shares	Endgame	11/30/2018	Discovery	T1049 System Network Connections Discovery
Enumeration of Remote Shares	Endgame	11/30/2018	Discovery	T1135 Network Share Discovery
Execution of a Command via a SYSTEM Service	Endgame	11/30/2018	Privilege Escalation	T1035 Service Execution T1050 New Service
Image Debuggers for Accessibility Features	Endgame	11/30/2018	Persistence Privilege Escalation Defense Evasion	T1015 Accessibility Features T1183 Image File Execution Options Injection
Indirect Command Execution	Endgame	11/30/2018	Defense Evasion	T1202 Indirect Command Execution
Installing Custom Shim Databases	Endgame	11/30/2018	Persistence Privilege Escalation	T1138 Application Shimming
Interactive AT Job	Endgame	11/30/2018	Privilege Escalation	T1053 Scheduled Task
Logon Scripts with UserInitMprLogonScript	Endgame	11/30/2018	Persistence	T1037 Logon Scripts

Continued on next page

Table 2 – continued from previous page

Analytic	Contributors	Updated	Tactics	Techniques
LSASS Memory Dumping	Tony Lambert	01/07/2019	Credential Access	T1003 Credential Dumping
LSASS Memory Dumping via ProcDump.exe	Tony Lambert	01/07/2019	Credential Access	T1003 Credential Dumping
Modification of Boot Configuration	Endgame	11/30/2018	Defense Evasion	T1107 File Deletion
Modifications of .bash_profile and .bashrc	Tony Lambert	01/10/2019	Persistence	T1156 .bash_profile and .bashrc
Mounting Hidden Shares	Endgame	11/30/2018	Lateral Movement	T1077 Windows Admin Shares
Mshta Network Connections	Endgame	11/30/2018	Execution Defense Evasion Command and Control	T1170 Mshta
Persistence via AppInit DLL	Endgame	11/30/2018	Persistence Privilege Escalation	T1103 AppInit DLLs
Persistence via NetSh Key	Endgame	11/30/2018	Persistence	T1128 Netsh Helper DLL
Persistence via Screensaver	Endgame	11/30/2018	Persistence	T1180 Screensaver
Registry Preparation of Event Viewer UAC Bypass	Endgame	11/30/2018	Privilege Escalation	T1088 Bypass User Account Control
RegSvr32 Scriplet Execution	Endgame	11/30/2018	Execution	T1117 Regsvr32
SAM Dumping via Reg.exe	Endgame	11/30/2018	Credential Access	T1003 Credential Dumping
Suspicious ADS File Creation	Endgame	11/30/2018	Defense Evasion	T1096 NTFS File Attributes
Suspicious Bitsadmin Job via bitsadmin.exe	Endgame	11/30/2018	Defense Evasion Persistence	T1197 BITS Jobs
Suspicious Bitsadmin Job via PowerShell	Endgame	11/30/2018	Defense Evasion Persistence	T1197 BITS Jobs
Suspicious Script Object Execution	Endgame	11/30/2018	Defense Evasion Execution	T1117 Regsvr32
System Information Discovery	Endgame	11/30/2018	Discovery	T1082 System Information Discovery
Unload Sysmon Filter Driver with fltmc.exe	Endgame	11/30/2018	Defense Evasion	T1089 Disabling Security Tools
User Account Creation	Endgame	11/30/2018	Persistence Credential Access	T1136 Create Account
Volume Shadow Copy Deletion via VssAdmin	Endgame	11/30/2018	Defense Evasion	T1107 File Deletion

Continued on next page

Table 2 – continued from previous page

Analytic	Contributors	Updated	Tactics	Techniques
Volume Shadow Copy Deletion via WMIC	Endgame	11/30/2018	Defense Evasion	T1107 File Deletion
Windows Network Enumeration	Endgame	11/30/2018	Discovery	T1018 Remote System Discovery

1.4 Enterprise ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc • *Modification of .bash_profile and .bashrc*	Exploitation for Privilege Escalation • *Elevated Execution*	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture • *Audio Capture via PowerShell* • *Audio Capture via SoundRecorder*	Automated Exfiltration	Commonly Used Port

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Exploit Public-Facing Application	Command-Line Interface	Accessibility Features • *Image Debuggers for Accessibility Features*	Image File Execution Options Injection • *Image Debuggers for Accessibility Features*	BITS Jobs • *Suspicious Bitsadmin Job via bitsadmin.exe* • *Suspicious Bitsadmin Job via PowerShell*	Bash History	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed • *Command-Line Creation of a RAR file*	Communication Through Removable Media • *Command-Line Creation of a RAR file*
Hardware Additions	Dynamic Data Exchange	AppCert DLLs	SID-History Injection	Binary Padding	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Spearphishing Attachment	Execution through API	AppInit DLLs • *Persistence via AppInit DLL*	Setuid and Setgid	Bypass User Account Control • *Bypass UAC via CMSTP*	Credential Dumping • *LSASS Memory Dumping* • *AD Dumping via Ntdsutil.exe* • *LSASS Memory Dumping via ProcDump.exe* • *SAM Dumping via Reg.exe*	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Link	Execution through Module Load	Application Shimming • *Installing Custom Shim Databases*	Sudo	CMSTP • *Bypass UAC via CMSTP*	Credentials in Files	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Spearphishing via Service	Exploitation for Client Execution	Authentication Package	Sudo Caching	Clear Command History	Credentials in Registry	Network Share Discovery • *Enumeration of Local Shares* • *Enumeration of Remote Shares*	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Supply Chain Compromise	Graphical User Interface	Bootkit		Code Signing	Exploitation for Credential Access	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Trusted Relationship	LSASS Driver	Browser Extensions		Compiled HTML File	Forced Authentication	Peripheral Device Discovery	Remote Services	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
	PowerShell	Change Default File Association • *Change Default File Association*		Component Firmware	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Email Collection	Scheduled Transfer	Fallback Channels

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Scheduled Task	Create Account • *User Account Creation*		Component Object Model Hijacking • *COM Hijack via Script Object*	Kerberoasting	Process Discovery	SSH Hijacking	Input Capture		Multi-Stage Channels
	Service Execution	DLL Search Order Hijacking		Control Panel Items	Keychain	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	Source	Dylib Hijacking		DCShadow	LLMNR/NBT-NS Poisoning	Remote System Discovery • *Windows Network Enumeration*	Taint Shared Content	Screen Capture		Multiband Communication
	Third-party Software	External Remote Services		DLL Side-Loading	Network Sniffing	Security Software Discovery	Windows Admin Shares • *Mounting Hidden Shares*	Video Capture		Multilayer Encryption

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Trap	File System Permissions Weakness		Deobfuscate/Decode Files or Information • *Encoding or Decoding Files via CertUtil*	Password Filter DLL	System Information Discovery • *System Information Discovery*				Remote Access Tools
	User Execution	Hooking		Disabling Security Tools • *Unload Sysmon Filter Driver with fltmc.exe*	Private Keys	System Network Configuration Discovery				Remote File Copy
	Windows Management Instrumentation • *Remote Execution via WMIC*	Hypervisor		Exploitation for Defense Evasion	Securityd Memory	System Network Connections Discovery • *Enumeration of Mounted Shares*				Standard Application Layer Protocol

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Windows Remote Management	Kernel Modules and Extensions		Extra Window Memory Injection	Two-Factor Authentication Interception	System Owner/User Discovery				Standard Cryptographic Protocol
		LC_LOAD_DYLIB Addition		File Deletion • *Volume Shadow Copy Deletion via WMIC* • *Modification of Boot Configuration* • *Volume Shadow Copy Deletion via VssAdmin*		System Service Discovery				Standard Non-Application Layer Protocol

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Launch Agent		File Permissions Modification		System Time Discovery • *Discovery of a Remote System's Time*				Uncommonly Used Port
		Launch Daemon		File System Logical Offsets						Web Service
		Local Job Scheduling		Gatekeeper Bypass						
		Login Item		HISTCONTROL						
		Modify Existing Service		Hidden Files and Directories						
		Netsh Helper DLL • *Persistence via NetSh Key*		Hidden Users						
		New Service		Hidden Window						
		Office Application Startup		Indicator Blocking						

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Path Interception		Indicator Removal from Tools						
		Port Monitors		Indicator Removal on Host • *Delete Volume USN Journal with fsutil* • *Clearing Windows Event Logs with wevtutil*						
		Rc.common		Indirect Command Execution • *Indirect Command Execution*						

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Re-opened Applications		Install Root Certificate						
		Registry Run Keys / Startup Folder		InstallUtil						
		Screensaver • *Persistence via Screensaver*		LC_MAIN Hijacking						
		Security Support Provider		Launchctl						
		Service Registry Permissions Weakness		Masquerading						
		Shortcut Modification		Modify Registry						
		Startup Items		Mshta • *Mshta Network Connections*						

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		System Firmware		NTFS File Attributes • *Suspicious ADS File Creation*						
		Time Providers		Network Share Connection Removal						
		Web Shell		Obfuscated Files or Information						
		Windows Management Instrumentation Event Subscription		Plist Modification						
		Winlogon Helper DLL		Port Knocking						
				Process Doppelgänging						

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
				Process Hollowing • *Unusual Child Process*						
				Process Injection • *Unusual Child Process*						
				Redundant Access						
				Regsvcs/Regasm						
				Regsvr32 • *Suspicious Script Object Execution*						
				Rootkit						
				Rundll32						
				SIP and Trust Provider Hijacking						
				Scripting						
				Signed Binary Proxy Execution						

Continued on next page

Table 3 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
				Signed Script Proxy Execution						
				Software Packing						
				Space after Filename						
				Template Injection						
				Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				XSL Script Processing						

1.4.1 Linux

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc • *Modification of .bash_profile and .bashrc*	Exploitation for Privilege Escalation • *Execution*	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Setuid and Setgid	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Graphical User Interface	Browser Extensions	Sudo	Disabling Security Tools	Credential Dumping	File and Directory Discovery	Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Spearphishing Attachment	Source	Create Account	Sudo Caching	Exploitation for Defense Evasion	Credentials in Files	Network Service Scanning	SSH Hijacking	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Link	Third-party Software	Kernel Modules and Extensions		File Deletion	Exploitation for Credential Access	Password Policy Discovery		Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing via Service	Trap	Local Job Scheduling		File Permissions Modification	Network Sniffing	Permission Groups Discovery		Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Supply Chain Compromise	User Execution	Web Shell		HISTCONTROL	Private Keys	Process Discovery		Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Trusted Relationship				Hidden Files and	Two-Factor Au-	Remote System Dis-		Data from Re-	Exfiltration Over Phys-	Domain Fronting

1.4.2 macOS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	bash_profile and .bashrc • *Modification of .bash_profile and .bashrc*	Exploitation for Privilege Escalation • *Elevation*	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Browser Extensions	Setuid and Setgid	Clear Command History	Brute Force	Application Window Discovery	Exploitation of Remote Services	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Exploitation for Client Execution	Create Account	Sudo	Code Signing	Credential Dumping	Browser Bookmark Discovery	Logon Scripts	Clipboard Data	Data Encrypted	Custom Command and Control Protocol
Spearphishing Attachment	Graphical User Interface	Dylib Hijacking	Sudo Caching	Disabling Security Tools	Credentials in Files	File and Directory Discovery	Remote Services	Data Staged	Data Transfer Size Limits	Custom Cryptographic Protocol
Spearphishing Link	Source	Kernel Modules and Extensions		Exploitation for Defense Evasion	Exploitation for Credential Access	Network Service Scanning	SSH Hijacking	Data from Information Repositories	Exfiltration Over Alternative Protocol	Data Encoding
Spearphishing via Service	Third-party Software	LC_LOAD_DYLIB Addition		File Deletion	Input Prompt	Network Share Discovery		Data from Local System	Exfiltration Over Command and Control Channel	Data Obfuscation
Supply Chain Compromise	Trap	Launch Agent		File Permissions Modification	Keychain	Password Policy Discovery		Data from Network Shared Drive	Exfiltration Over Other Network Medium	Domain Fronting
Trusted Rela-	User Execu-	Launch Dae-		Gatekeeper Bypass	Network Sniff-	Permission Groups		Data from	Exfiltration Over	Fallback Chan-

1.4.3 Windows

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command-Line Interface	Accessibility Features • *Image Debuggers for Accessibility Features*	Exploitation for Privilege Escalation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture • *Audio Capture via PowerShell* • *Audio Capture via SoundRecorder*	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Dynamic Data Exchange	AppCert DLLs	Image File Execution Options Injection • *Image Debuggers for Accessibility Features*	BITS Jobs • *Suspicious Bitsadmin Job via bitsadmin.exe* • *Suspicious Bitsadmin Job via PowerShell*	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed • *Command-Line Creation of a RAR file*	Communication Through Removable Media

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Hardware Additions	Execution through API	AppInit DLLs • *Persistence via AppInit DLL*	SID-History Injection	Binary Padding	Credential Dumping • *LSASS Memory Dumping* • *AD Dumping via Ntdsutil.exe* • *LSASS Memory Dumping via ProcDump.exe* • *SAM Dumping via Reg.exe*	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Custom Command and Control Protocol
Spearphishing Attachment	Execution through Module Load	Application Shimming • *Installing Custom Shim Databases*		Bypass User Account Control • *Bypass UAC via CMSTP*	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Cryptographic Protocol

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Spearphishing Link	Exploitation for Client Execution	Authentication Package		CMSTP • *Bypass UAC via CMSTP*	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Data Encoding
Spearphishing via Service	Graphical User Interface	Bootkit		Code Signing	Exploitation for Credential Access	Network Share Discovery • *Enumeration of Local Shares* • *Enumeration of Remote Shares*	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Obfuscation
Supply Chain Compromise	LSASS Driver	Browser Extensions		Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Domain Fronting
Trusted Relationship	PowerShell	Change Default File Association • *Change Default File Association*		Component Firmware	Kerberoasting	Peripheral Device Discovery	Remote Services	Data from Removable Media	Exfiltration Over Physical Medium	Fallback Channels

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Scheduled Task	Create Account • *User Account Creation*		Component Object Model Hijacking • *COM Hijack via Script Object*	LLMNR/NBT-NS Poisoning	Permission Groups Discovery	Replication Through Removable Media	Email Collection	Scheduled Transfer	Multi-Stage Channels
	Service Execution	DLL Search Order Hijacking		Control Panel Items	Network Sniffing	Process Discovery	Shared Webroot	Input Capture		Multi-hop Proxy
	Third-party Software	External Remote Services		DCShadow	Password Filter DLL	Query Registry	Taint Shared Content	Man in the Browser		Multiband Communication
	User Execution	File System Permissions Weakness		DLL Side-Loading	Private Keys	Remote System Discovery • *Windows Network Enumeration*	Windows Admin Shares • *Mounting Hidden Shares*	Screen Capture		Multilayer Encryption

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Windows Management Instrumentation • *Remote Execution via WMIC*	Hooking		Deobfuscate/Decode Files or Information • *Encoding or Decoding Files via CertUtil*	Two-Factor Authentication Interception	Security Software Discovery		Video Capture		Remote Access Tools
	Windows Remote Management	Hypervisor		Disabling Security Tools • *Unload Sysmon Filter Driver with fltmc.exe*		System Information Discovery • *System Information Discovery*				Remote File Copy
		Modify Existing Service		Exploitation for Defense Evasion		System Network Configuration Discovery				Standard Application Layer Protocol

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Netsh Helper DLL • *Persistence via NetSh Key*		Extra Window Memory Injection		System Network Connections Discovery • *Enumeration of Mounted Shares*				Standard Cryptographic Protocol
		New Service		File Deletion • *Volume Shadow Copy Deletion via WMIC* • *Modification of Boot Configuration* • *Volume Shadow Copy Deletion via VssAdmin*		System Owner/User Discovery				Standard Non-Application Layer Protocol

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Office Application Startup		File Permissions Modification		System Service Discovery				Uncommonly Used Port
		Path Interception		File System Logical Offsets		System Time Discovery • *Discovery of a Remote System's Time*				Web Service
		Port Monitors		Hidden Files and Directories						
		Registry Run Keys / Startup Folder		Indicator Blocking						
		Screensaver • *Persistence via Screensaver*		Indicator Removal from Tools						

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Security Support Provider		Indicator Removal on Host • *Delete Volume USN Journal with fsutil* • *Clearing Windows Event Logs with wevtutil*						
		Service Registry Permissions Weakness		Indirect Command Execution • *Indirect Command Execution*						
		Shortcut Modification		Install Root Certificate						
		System Firmware		InstallUtil						
		Time Providers		Masquerading						

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Web Shell		Modify Registry						
		Windows Management Instrumentation Event Subscription		Mshta • *Mshta Network Connections*						
		Winlogon Helper DLL		NTFS File Attributes • *Suspicious ADS File Creation*						
				Network Share Connection Removal						
				Obfuscated Files or Information						
				Process Doppelgänging						

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
				Process Hollowing • *Unusual Child Process*						
				Process Injection • *Unusual Child Process*						
				Redundant Access						
				Regsvcs/Regasm						
				Regsvr32 • *Suspicious Script Object Execution*						
				Rootkit						
				Rundll32						
				SIP and Trust Provider Hijacking						
				Scripting						
				Signed Binary Proxy Execution						

Continued on next page

Table 4 – continued from previous page

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
				Signed Script Proxy Execution						
				Software Packing						
				Template Injection						
				Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				XSL Script Processing						

1.5 Schemas

1.5.1 Microsoft Sysmon

This is the mapping from Microsoft Sysmon native fields to the *security schema*.

Timestamp

field `UtcTime`

format `%Y-%m-%d %H:%M:%S.%f`

Globally provided mapping

hostname `split(ComputerName, ".", 0)`

pid `number(ProcessId)`

process_name `baseName(Image)`

process_path `Image`

unique_pid `ProcessGuid`

user `User`

user_domain `split(User, "\\", 0)`

user_name `split(User, "\\", 1)`

Event specific mappings

file

`EventId in (11, 15)`

fields

file_name `baseName(TargetFilename)`

file_path `TargetFilename`

image_load

`EventId == 7`

fields

image_name `baseName(ImageLoaded)`

image_path `ImageLoaded`

network

`EventId == 3`

subtype mapping

incoming `Initiated == 'false'`

outgoing `Initiated == 'true'`

fields

destination_address `DestinationIp`

destination_port `DestinationPort`

protocol `Protocol`

source_address `SourceIp`

source_port `SourcePort`

process

`EventId in (1, 5)`

subtype mapping

create `EventId == 1`

terminate `EventId == 5`

fields

command_line `CommandLine`

logon_id `number(LogonId)`

parent_process_name `baseName(ParentImage)`

parent_process_path `ParentImage`

ppid `number(ParentProcessId)`

unique_ppid `ParentProcessGuid`

registry

`EventId in (12, 13, 14)`

hive mapping

hklm `TargetObject == "HKLM\\*"`

hku `TargetObject == "HKU\\*"`

fields

registry_key `dirName(TargetObject)`

registry_path `TargetObject`

registry_value `baseName(TargetObject)`

1.5.2 MITRE Cyber Analytics Repository

This is the mapping from MITRE Cyber Analytics Repository native fields to the *security schema*.

Timestamp

field `@timestamp`

format `%Y-%m-%dT%H:%M:%S.%fZ`

Globally provided mapping

hostname `hostname`

pid `pid`

process_name `exe`

process_path `image_path`

unique_pid `process_guid`

user `user`

user_domain `split(user, "\\", 0)`

user_name `split(user, "\\", 1)`

Event specific mappings

file

`data_model.object = 'file'`

subtype mapping

- **create** `arrayContains(data_model.actions, "create")`
- **delete** `arrayContains(data_model.actions, "delete")`
- **modify** `arrayContains(data_model.actions, "modify")`

fields

- **file_name** `file_name`
- **file_path** `file_path`

network

`data_model.object == 'flow'`

subtype mapping

- **incoming** `not initiated`
- **outgoing** `initiated`

fields

- **destination_address** `dest_ip`
- **destination_port** `dest_port`
- **protocol** `transport`
- **source_address** `src_ip`
- **source_port** `src_port`

process

`data_model.object = 'process'`

subtype mapping

- **create** `arrayContains(data_model.action, 'create')`
- **terminate** `arrayContains(data_model.action, 'terminate')`

fields

- **command_line** `command_line`
- **parent_process_name** `parent_exe`
- **parent_process_path** `parent_image_path`
- **ppid** `ppid`
- **unique_ppid** `parent_process_guid`

registry

```
data_model.object == "registry" and not arrayContains(data_model.actions,
"remove")
```

registry_type mapping

> **binary** `type == "REG_BINARY"`
>
> **dword** `type = "REG_DWORD"`
>
> **expand_string** `type = "REG_EXPAND_SZ"`
>
> **multi_string** `type = "REG_MULTI_SZ"`
>
> **qword** `type = "REG_QWORD"`
>
> **string** `type = "REG_SZ"`

hive mapping

> **hklm** `hive == "HKEY_LOCAL_MACHINE"`
>
> **hku** `hive == "HKEY_USERS"`

fields

> **registry_data** `data`
>
> **registry_key** `dirName(key_path)`
>
> **registry_path** `key_path`
>
> **registry_value** `value`

1.5.3 Security Events

This is the primary schema used for normalizing across data sources. Queries are written to match this schema, and data sources are converted to this schema. This unifies sources to a unified by a common language and a common data model, so analytics can be written generically and are easy shareable.

Globally provided fields

- hostname
- pid
- process_name
- process_path
- unique_pid
- user
- user_domain
- user_name
- user_sid

file

subtype options

- create
- modify
- delete

fields

- file_name
- file_path

image_load

fields

- image_name
- image_path

network

subtype options

- incoming
- outgoing
- disconnect

fields

- destination_address
- destination_port
- protocol
- source_address
- source_port
- total_in_bytes
- total_out_bytes

process

subtype options

- create
- terminate

fields

- command_line
- logon_id

- parent_process_name
- parent_process_path
- ppid
- unique_ppid

registry

hive options

- hku
- hklm

registry_type options

- dword
- qword
- string
- expand_string
- multi_string
- binary

fields

- registry_data
- registry_key
- registry_path
- registry_value

1.6 License

Note: The Event Query Language has an AGPL License

Index

Symbols

A

C

E

I

O

Q

S