EQL Analytics Library

endgame

Sep 26, 2019
1 Next Steps
1.1 Getting Started ................................................................. 3
1.2 Analytics ................................................................. 7
1.3 Atomic Blue Detections .................................................. 93
1.4 Enterprise ATT&CK Matrix ............................................ 96
1.5 Schemas ................................................................. 143
1.6 Resources ................................................................. 149
1.7 License ................................................................. 149

Index ...................................................................... 151
eqlib is a library of event based analytics, written in EQL to detect adversary behaviors identified in MITRE ATT&CK™.
Next Steps

- 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
- View additional resources
- 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

(continues on next page)
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.

eqlib 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

eqlib 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.

```powershell
# 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

```powershell
```

**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

```bash
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 Access of Outlook Email Archives

Collection of sensitive information via .ost and .pst outlook archive files.

<table>
<thead>
<tr>
<th>id</th>
<th>15d87029-42c1-4992-a49b-aac74d451c06</th>
</tr>
</thead>
<tbody>
<tr>
<td>categories</td>
<td>enrich</td>
</tr>
<tr>
<td>confidence</td>
<td>low</td>
</tr>
<tr>
<td>os</td>
<td>windows</td>
</tr>
<tr>
<td>created</td>
<td>7/26/2019</td>
</tr>
<tr>
<td>updated</td>
<td>7/26/2019</td>
</tr>
</tbody>
</table>
Query

```
process where subtype.create and wildcard(command_line, ".ost *", ".pst *")
```

Contributors

- Endgame

### 1.2.2 Account Discovery via Built-In Tools

Adversaries may use built-in applications to get a listing of local system or domain accounts

```
id 56fd859-b2a7-4009-88e0-69fec4c3deef
categories enrich
category low
os windows, macos, linux
created 7/26/2019
updated 7/26/2019
```

Query

```
process where subtype.create and (  
  process_name == "net.exe" and wildcard(command_line, "* user*", "*localgroup *"),  
  =$"*group *") or
  process_name in ("groups", "id") or
  process_name == "dsc1" and command_line == "list /groups*" or
  process_name == "dscacheutil" and command_line == "*group*" or
  wildcard(command_line, "*/etc/passwd*", "*/etc/master.passwd")
}
```

Contributors

- Endgame
1.2.3 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

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

Detonation

Atomic Red Team: T1003

Contributors

- Tony Lambert

1.2.4 Adding the Hidden File Attribute with via attrib.exe

Adversaries can add the hidden attribute to files to hide them from the user in an attempt to evade detection

id 9051814c-a142-4b1c-965b-76a09dace760
categories enrich
confidence low
os windows
created 7/26/2019
updated 7/26/2019

MITRE ATT&CK™ Mapping

tactics Defense Evasion, Persistence
techniques T1158 Hidden Files and Directories
Query

```sql
process where subtype.create and
    process_name == "attrib.exe" and
    command_line == "* +h:*"
```

Contributors

- Endgame

1.2.5 AppCert DLLs Registry Modification

Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.

```plaintext
id 14f90406-10a0-4d36-a672-31cabe149f2f
categories enrich
certainty low
os windows
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

- tactics Privilege Escalation, Persistence
- techniques T1182 AppCert DLLs

Query

```sql
registry where registry_path == "*\System\ControlSet\*\Control\SessionManager\AppCertDLLs\*"
```

Contributors

- Endgame

1.2.6 Audio Capture via PowerShell

Detect attacker collecting audio via PowerShell Cmdlet.

```plaintext
id ab7a6ef4-0983-4275-a4f1-5c6bd3c31e23
categories detect
certainty medium
os windows
```
MITRE ATT&CK™ Mapping

tactics Collection

Techniques T1123 Audio Capture

Query

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

Detonation

Atomic Red Team: T1123

Contributors

• Endgame

1.2.7 Audio Capture via SoundRecorder

Detect audio collection via SoundRecorder application.

id f72a98cb-7b3d-4100-99c3-a138b6e9ff6e
categories detect
category medium
os windows
created 11/30/2018
updated 11/30/2018

MITRE ATT&CK™ Mapping

<table>
<thead>
<tr>
<th>Tactics</th>
<th>Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Techniques</td>
<td>T1123 Audio Capture</td>
</tr>
</tbody>
</table>

Query

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

Atomic Red Team: T1123

Contributors

• Endgame

1.2.8 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
1.2.9 Bypass UAC via Fodhelper.exe

Identifies use of Fodhelper.exe to bypass User Account Control. Adversaries use this technique to execute privileged processes.

```
id  e491ce22-792f-11e9-8f5c-d46d6d62a49e
categories  detect
confidence  high
os  windows
created  05/17/2019
updated  05/17/2019
```

MITRE ATT&CK™ Mapping

- tactics  Privilege Escalation
- techniques  T1088 Bypass User Account Control

Query

```
process where subtype.create and
  parent_process_name == "fodhelper.exe"
```

Detonation

Atomic Red Team: T1088

Contributors

- Tony Lambert

1.2.10 Bypass UAC via WSReset.exe

Identifies use of WSReset.exe to bypass User Account Control. Adversaries use this technique to execute privileged processes.

```
id  532b5ed4-7930-11e9-8f5c-d46d6d62a49e
categories  detect
confidence  high
os  windows
created  05/17/2019
updated  05/17/2019
```
MITRE ATT&CK™ Mapping

**tactics** Privilege Escalation
**techniques** T1088 Bypass User Account Control

**Query**

```sql
process where subtype.create and
parent_process_name == "wsreset.exe" and process_name != "conhost.exe"
```

**Detonation**

Atomic Red Team: T1088

**Contributors**

- Tony Lambert

### 1.2.11 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**

```sql
sequence by unique_pid with maxspan=1s
[ registry where registry_path == "*\\SOFTWARE\\Classes\\*\\*"]
[ registry where registry_path == "*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\GlobalAssocChangedCounter ..."]
| unique_count process_name, registry_path
```
Detonation

Atomic Red Team: T1042

Contributors

• Endgame

1.2.12 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

1.2.13 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
MITRE ATT&CK™ Mapping

**tactics**  Persistence, Defense Evasion

**techniques**  T1122 Component Object Model Hijacking

**Query**

```plaintext
registry where
  registry_path == "*_Classes\CLSID\{}\InprocServer32*" and
  (registry_data == "scrobj*" or registry_data == "\scrobj")
```

**Detonation**

Atomic Red Team: T1122

**Contributors**

• Endgame

### 1.2.14 Command-Line Creation of a RAR file

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

```plaintext
id 1ec33c93-3d0b-4a28-8014-dbdaae5c60ae
categories detect
category medium
os windows
created 11/30/2018
updated 11/30/2018
```

MITRE ATT&CK™ Mapping

**tactics**  Exfiltration

**techniques**  T1002 Data Compressed

**Query**

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

Atomic Red Team: T1002

Contributors

• Endgame

1.2.15 Control Panel Items

Windows Control Panel items are utilities that allow users to view and adjust computer settings. Adversaries can use Control Panel items as execution payloads to execute arbitrary commands.

```
id 3b9bbf6b-dde2-4f82-b1ad-b3b625f44a26
categories enrich
confidence low
os windows
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

- tactics Defense Evasion, Execution
- techniques T1196 Control Panel Items

Query

```
process where subtype.create and
process_name in ("control.exe", "rundll32.exe") and
command_line == ".cpl *
```

Contributors

• Endgame

1.2.16 Creation of an Archive with Common Archivers

Adversaries may collect and stage data in a central location or directory in preparation of exfiltration.

```
id f43f66f3-7e86-4cd1-9850-df7b4ac7822e
categories enrich
confidence low
os macos, linux
created 7/26/2019
updated 7/26/2019
```
EQL Analytics Library

MITRE ATT&CK™ Mapping

tactics Collection

techniques T1074 Data Staged

Query

```
sequence by unique_pid with maxspan=1m
    [ process where subtype.create and process_name in ("zip", "tar", "gzip", "hdiutil \n") ]
    [ file where wildcard(file_name, ".*\.[z][i][p]\", ".*\.[t][a][r]\", ".*\.[g][z][i][p]\", ".*\.[g][z]\") ]
```

Contributors

- Endgame

1.2.17 Creation of Kernel Module

Identify activity related to loading kernel modules on Linux via creation of new ko files in the LKM directory

```
id 9e711823-72f1-4c5c-843d-9afc90c4e6a1
categories enrich
certainty low
os linux
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

```
tactics Persistence

techniques T1215 Kernel Modules and Extensions
```

Query

```
file where subtype.create and
    file_path == "/lib/modules/*" and file_name == "*.ko"
```

Contributors

- Endgame
1.2.18 Creation of Scheduled Task with `schtasks.exe`

A scheduled task can be used by an adversary to establish persistence, move laterally, and/or escalate privileges.

```
id 9583e2ff-508d-4ebb-8b89-712b0a4d3186
categories hunt
category confidence low
os windows
created 7/26/2019
updated 7/26/2019
```

**MITRE ATT&CK™ Mapping**

- **tactics** Privilege Escalation, Execution, Persistence
- **techniques** T1053 Scheduled Task

**Query**

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

**Contributors**

- Endgame

1.2.19 Creation or Modification of Systemd Service

Systemd services can be used to establish persistence on a Linux system. The systemd service manager is commonly used for managing background daemon processes (also known as services) and other system resources.

```
id 1a568233-9ca1-4c2c-b2e7-b15b90e2c954
categories enrich
category confidence low
os linux
created 7/26/2019
updated 7/26/2019
```

**MITRE ATT&CK™ Mapping**

- **tactics** Persistence
- **techniques** T1501 Systemd Service
Query

```sql
file where not subtype.delete and
file_name == "+.service*" and
wildcard(file_path, "/etc/systemd/system/*","/usr/lib/systemd/system/*")
```

Contributors

- Endgame

1.2.20 Credential Enumeration via Credential Vault CLI

Identifies use of the Credential Vault command line interface to enumerate a user’s saved credentials.

```plaintext
id  11968244-6db0-4e03-886c-e3983f9d9024
categories  detect
confidence  high
os  windows
created  8/16/2019
updated  8/16/2019
```

MITRE ATT&CK™ Mapping

- tactics  Credential Access
- techniques  T1003 Credential Dumping

Query

```sql
process where subtype.create and
process_name == "vaultcmd.exe" and
command_line == "* /list*"
```

Contributors

- David French

References

1.2.21 Delete Volume USN Journal with fsutil

Identifies use of the fsutil command to delete the volume USNJRNJL. 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

1.2.22 Disconnecting from Network Shares with net.exe

Identifies attempts to remove network shares with the Windows built-in command net.exe

```
   id   7d328c61-8f63-4411-9ae7-e5b502a80e7e
   categories enrich
   confidence low
   os   windows
   created 7/26/2019
   updated 7/26/2019
```
MITRE ATT&CK™ Mapping

tactics Defense Evasion
techniques T1126 Network Share Connection Removal

Query

```plaintext
process where subtype.create and
  process_name == "net.exe" and command_line == "* /d*"
```

Contributors

• Endgame

1.2.23 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

```plaintext
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
1.2.24 Discovery of Domain Groups

Identify usage of known commands for discovery of local groups

```
id  cd2124cb-718d-4ecf-bc96-5571f8e3dbce
categories  enrich
classification  low
os  linux, macos
created  7/26/2019
updated  7/26/2019
```

MITRE ATT&CK™ Mapping

- tactics  Discovery
- techniques  T1069 Permission Groups Discovery

Query

```
process where subtype.create and (
  process_name in ("ldapsearch", "dscacheutil") or
  process_name == "dscl" and command_line == "*-list*"
)
```

Contributors

- Endgame

1.2.25 Discovery of Network Environment via Built-in Tools

Build-in tools can be used to enumerate and discover network environment on unix systems.

```
id  fd7a0c56-60fa-4f14-8c8e-0e41ad955725
categories  enrich
classification  low
os  macos, linux
created  7/26/2019
updated  7/26/2019
```

MITRE ATT&CK™ Mapping

- tactics  Discovery
- techniques  T1016 System Network Configuration Discovery
Query

```sql
process where subtype.create and {
    process_name in ("ifconfig", "arp", "networkctl", "netstat", "route", "ntop") or {
        process_name in ('cat', 'more', 'less', 'vim', 'vi', 'nano', 'gedit') and
        command_line == "* /etc/hosts*"
    }
}
```

Contributors

- **Endgame**

1.2.26 Discovery of Network Environment via Built-in Tools

Built-in tools can be used to enumerate and discover network environment on windows systems.

- **id** 3a78a9fb-3714-43fa-90ca-7cf85da5a710
- **categories** enrich
- **confidence** low
- **os** windows
- **created** 7/26/2019
- **updated** 7/26/2019

**MITRE ATT&CK™ Mapping**

- **tactics** Discovery
- **techniques** T1016 System Network Configuration Discovery

Query

```sql
process where subtype.create and 
    process_name in ("ipconfig.exe", "route.exe", "nbtstat.exe", "arp.exe")
| unique command_line
```

Contributors

- **Endgame**

1.2.27 DLL Search Order Hijacking with known programs

Detects writing DLL files to known locations associated with Windows files vulnerable to DLL search order hijacking.

- **id** afd1fba7-5301-4d5c-ae66-f8608bc98ae9
- **categories** detect
- **confidence** low
os windows
created 7/26/2019
updated 7/26/2019

MITRE ATT&CK™ Mapping

tactics  Privilege Escalation, Defense Evasion, Persistence
techniques  T1038 DLL Search Order Hijacking

Query

```sql
file where not subtype.delete and
not user_sid in ("S-1-5-18", "S-1-5-19", "S-1-5-20") and {
    file_path == "*\windows\ehome\cryptbase.dll" or
    file_path == "*\windows\system32\sysprep\cryptbase.dll" or
    file_path == "*\windows\system32\sysprep\cryptsp.dll" or
    file_path == "*\windows\system32\sysprep\rpcrtremote.dll" or
    file_path == "*\windows\system32\sysprep\uxtheme.dll" or
    file_path == "*\windows\system32\sysprep\dwmapi.dll" or
    file_path == "*\windows\system32\sysprep\oleacc.dll" or
    file_path == "*\windows\system32\ntwdblib.dll"
} | unique process_path, file_path
```

Contributors

- Endgame

1.2.28 Domain Trust Discovery

Detect commands used to enumerate a list of trusted domains.

```plaintext
id bccb1c48-305c-4b1f-affb-a7a50bf4654b
categories enrich
category low
os windows
created 7/26/2019
updated 7/26/2019

MITRE ATT&CK™ Mapping

tactics  Discovery
techniques  T1482 Domain Trust Discovery
```
Query

```plaintext
process where subtype.create and (  
  (process_name == "dsquery.exe") and command_line == "*(objectClass=trustedDomain)*"  
  or  
  (process_name == "nltest.exe") and command_line == "*domain_trusts*"
)
```

Contributors

- Endgame

1.2.29 Domain Trust Discovery via Nltest.exe

Identifies execution of nltest.exe for domain trust discovery. This technique is used by attackers to enumerate Active Directory trusts.

```
id 03e231a6-74bc-467a-acb1-e5676b0fb55e
categories hunt
classification low
os windows
created 05/17/2019
updated 05/17/2019
```

MITRE ATT&CK™ Mapping

- **tactics** Discovery
- **techniques** T1482 Domain Trust Discovery

Query

```plaintext
process where subtype.create and
  process_name == "nltest.exe" and command_line == "*domain_trusts*"
```

Detonation

Atomic Red Team: T1482

Contributors

- Tony Lambert
1.2.30 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

1.2.31 Enumeration of Local Shares

Identifies enumeration of local shares with the built-in Windows tool `net.exe`.

```
id bc194cd-97fc-4b9a-b068-46203b6bbcd
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**

```sql
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

### 1.2.32 Enumeration of Mounted Shares

Identifies enumeration of mounted shares with the built-in Windows tool `net.exe`.

```sql
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**

```sql
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 *")
// since this command is looking for discovery only, we want to ignore mounting shares
  command_line != "* \ \ \ \ *"
| unique parent_process_path, command_line, user_name
```
1.2.33 Enumeration of Remote Shares

Identifies enumeration of remote shares with the built-in Windows tool net.exe.

```
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

1.2.34 Enumeration of System Information

System information enumeration and discovery via built-in tools.

```
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
**Query**

```plaintext
process where subtype.create and {
  process_name == "uname" or {
    process_name in ("cat", "more", "less") and 
    wildcard(command_line, 
      "+ /etc/issue*", "+ /proc/version*", "+ /etc/profile*", "+ /etc/services*", "+ /proc/cpuinfo*")
  
})
```

**Contributors**

- Endgame

### 1.2.35 Enumeration of System Information

Windows contains several built-in commands to report system information. These may be used by an actor to gain detailed information about the target machine.

```plaintext
id 507f19c1-dfa9-475b-925e-61e417a10967
categories enrich
confidence low
os windows
created 7/26/2019
updated 7/26/2019
```
process where subtype.create and
    process_name in ("systeminfo", "hostname") or (  
        process_name == "cmd.exe" and command_line == "* ver*"
    )

Contributors

- Endgame

1.2.36 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-c3f5-42be-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
    registry_path == "*\System\*\ControlSet*\Services\*\ImagePath"
    and wildcard(registry_data, "%COMSPEC%", "cmd.exe", "powershell", "cmd *")

Detonation

Atomic Red Team: T1035

Contributors

- Endgame
1.2.37 Execution of Existing Service via Command

Identifies attempts to execute an existing service by running a built-in Windows command.

```
id 45861478-8ba3-4302-9600-1970d5d8b074
categories enrich
category confidence low
os windows
created 7/26/2019
updated 7/26/2019
```

**MITRE ATT&CK™ Mapping**

- tactics Execution
- techniques T1035 Service Execution

**Query**

```plaintext
process where subtype.create and (  
  process_name == "sc.exe" and command_line == "* start *" or  
  process_name == "net.exe" and match(command_line, ?".*? start *\[s].*") or  
  process_name == "powershell.exe" and wildcard(command_line, "*Start-Service*") or  
  process_name == "wmic.exe" and wildcard(command_line, "*service*call*startservice*")  
)
```

**Contributors**

- Endgame

1.2.38 Execution via cmstp.exe

Identifies potentially stealthy execution via the Microsoft Connection Manager Profile Installer.

```
id 56c64a8c-a787-488a-a7f2-b992d332679d
categories enrich
category confidence low
os windows
created 7/26/2019
updated 7/26/2019
```

**MITRE ATT&CK™ Mapping**

- tactics Defense Evasion, Execution
- techniques T1191 CMSTP
Query

```sql
process where subtype.create and
    process_name == "cmstp.exe" and
    command_line == "* /s *"
```

Contributors

- Endgame

1.2.39 HH.exe execution

Identifies usage of hh.exe executing recently modified .chm files.

- id b25aa548-7937-11e9-8f5c-d46d6d62a49e
- categories detect
- confidence medium
- os windows
- created 08/08/2019
- updated 09/26/2019

MITRE ATT&CK™ Mapping

- tactics Defense Evasion, Execution
- techniques T1223 Compiled HTML File

Query

```sql
sequence with maxspan=1d
    [file where file_name == "*.chm"]
    [process where subtype.create and process_name == "hh.exe" and command_line == "*...
        "*.chm*"]
```

Detonation

Atomic Red Team: T1223

Contributors

- Dan Beavin
1.2.40 Host Artifact Deletion

Adversaries may delete artifacts on a host system, including logs, browser history, or directories.

```
id 339d4a19-dfb8-4d86-89c8-6a3ac807a57f
categories enrich
certainty low
os windows
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

- tactics Defense Evasion
- techniques T1070 Indicator Removal on Host

Query

```
process where subtype.create and (  
  (process_name == "rundll32.exe" and command_line == "*InetCpl.cpl,Clear*") or  
  (process_name == "reg.exe" and command_line == "* delete *") or  
  (process_name == "cmd.exe" and command_line == "* *rmdir *")  
)
```

Contributors

- Endgame

1.2.41 Image Debuggers for Accessibility Features

The Debugger registry key allows an attacker to launch intercept the execution of files, causing 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
certainty 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

```sql
registry where wildcard(registry_path,
    "*\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\*\Debugger",
    "*\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\*\Debugger"
) and wildcard(registry_path,
    // Accessibility Features
    "*\shtc.exe\*",
    "*\utilman.exe\*",
    "*\narrator.exe\*",
    "*\osk.exe\*",
    "*\magnify.exe\*",
    "*\displayswitch.exe\*",
    "*\atbroker.exe\*"
)
```

Detonation

Atomic Red Team: T1015

Contributors

- Endgame

1.2.42 Incoming Remote PowerShell Sessions

Incoming lateral movement via Windows Remote Management (WinRM)

- **id**: 3abf86e1-3ba3-4473-90ea-5fc37ff57d18
- **categories**: enrich
- **confidence**: low
- **os**: windows
- **created**: 7/26/2019
- **updated**: 7/26/2019

MITRE ATT&CK™ Mapping

- **tactics**: Lateral Movement, Execution
- **techniques**: T1028 Windows Remote Management

Query
sequence with maxspan=2s
    [network where subtype.incoming and destination_port in (5985, 5986)]
    [process where subtype.create and
        process_name == "wsmprovhost.exe" and parent_process_name == "svchost.exe"]

Contributors

- Endgame

1.2.43 Indirect Command Execution

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

id 884a7ccd-7305-4130-82d0-d4f90bc118b6
categories hunt
category 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
1.2.44 Installation of Port Monitor

A port monitors can be registered by calling the `AddMonitor` API with a path to a DLL. This functionality can be abused by attackers to establish persistence.

```
id  dce405ba-0f30-4278-b6c6-80d57847ba6b
categories  hunt
certainty  low
os  windows
created  7/26/2019
updated  7/26/2019
```

**MITRE ATT&CK™ Mapping**

- **tactics**: Privilege Escalation, Persistence
- **techniques**: T1013 Port Monitors

**Query**

```
registry where registry_path == "*ControlSet\Control\Print\Monitors*"
```

**Contributors**

- Endgame

1.2.45 Installation of Security Support Provider

Adversaries can establish persistence by modifying registry keys related to the Windows Security Support Provider (SSP) configuration.

```
id  43ecf8b8-e52d-4c1a-a110-3aecc09e6206
categories  enrich
certainty  low
os  windows
created  7/26/2019
updated  7/26/2019
```

**MITRE ATT&CK™ Mapping**

- **tactics**: Persistence
- **techniques**: T1101 Security Support Provider
Query

registry where
  wildcard(registry_path,
    "*\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages*",
    "*\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages*"
  )

Contributors

• Endgame

1.2.46 Installation of Time Providers

Attackers may establish persistence by registering a DLL with Windows as a valid time provider.

    id  3056a14a-59d9-43d3-84b5-738b4b8c3dd7
    categories  enrich
    confidence  low
    os  windows
    created  7/26/2019
    updated  7/26/2019

MITRE ATT&CK™ Mapping

    tactics  Persistence
    techniques  T1209 Time Providers

Query

registry where
  registry_path == "*\System\CurrentControlSet\Services\W32Time\TimeProviders\*"

Contributors

• Endgame

1.2.47 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
MITRE ATT&CK™ Mapping

- **tactics**: Persistence, Privilege Escalation
- **techniques**: T1138 Application Shimming

**Query**

```sql
registry where registry_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

### 1.2.48 InstallUtil Execution

InstallUtil may be abused to bypass process whitelisting or proxy the execution of code through a trusted Windows utility.

- **id**: b937f762-466f-4242-a461-d68e6e4bfc5a
- **categories**: hunt
- **confidence**: low
- **os**: windows
- **created**: 7/26/2019
- **updated**: 7/26/2019

MITRE ATT&CK™ Mapping

- **tactics**: Execution, Defense Evasion
- **techniques**: T1118 InstallUtil
1.2.49 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**

```sql
process where subtype.create and
  process_name == "installutil.exe" and
  command_line == "* *"
| unique parent_process_name, command_line
```

**Detonation**

Atomic Red Team: T1053

**Contributors**

- Endgame
1.2.50 Launch Daemon Persistence

An adversary can maintain persistence by installing a new launch daemon that can be configured to execute upon startup:

```plaintext
id 24cb8b7c-92fe-4d62-af0e-d3de993cd48b
categories enrich
category  low
os    macos
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

- **tactics**: Privilege Escalation, Persistence
- **techniques**: T1160 Launch Daemon

**Query**

```plaintext
process where subtype.create and
parent_process_name == "launchd"
```

**Contributors**

- Endgame

1.2.51 Loading Kernel Modules with kextload

Identify activity related to loading kernel modules on MacOS via the kextload command:

```plaintext
id deca3ab9-93f2-4e1e-b782-97863bc26089
categories hunt
category  low
os    macos
created 7/26/2019
updated 7/26/2019
```
**EQL Analytics Library**

**MITRE ATT&CK™ Mapping**

- **tactics**: Persistence
- **techniques**: T1215 Kernel Modules and Extensions

**Query**

```eql
process where subtype.create and
    process_name == "kextload"
```

**Contributors**

- Endgame

### 1.2.52 Local Job Scheduling Paths

On Linux and macOS systems, multiple methods are supported for creating pre-scheduled and periodic background jobs.

- **id**: 01fa72dc-5ce4-443b-96f9-703edfefa5d
- **categories**: enrich
- **confidence**: low
- **os**: macos, linux
- **created**: 7/26/2019
- **updated**: 7/26/2019

**MITRE ATT&CK™ Mapping**

- **tactics**: Execution, Persistence
- **techniques**: T1168 Local Job Scheduling

**Query**

```eql
file where wildcard(file_path, "/etc/crontab", "/etc/cron.d", "*LaunchDaemons*")
```

**Contributors**

- Endgame
1.2.53 Local Job Scheduling Process

On Linux and macOS systems, multiple methods are supported for creating pre-scheduled and periodic background jobs.

```
id 7f490015-20b2-43e3-acf7-e2f2d098505d
categories enrich
certainty low
os macos, linux
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

- tactics Execution, Persistence
- techniques T1168 Local Job Scheduling

Query

```
process where subtype.create and
    process_name in ("cron", "at", "launchd")
```

Contributors

- Endgame

1.2.54 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
certainty medium
os windows
created 11/30/2018
updated 11/30/2018
```

MITRE ATT&CK™ Mapping

- tactics Persistence
- techniques T1037 Logon Scripts
Query

```sql
registry where registry_path == "*\Environment\UserInitMprLogonScript"
```

Detonation

Atomic Red Team: T1037

Contributors

- Endgame

1.2.55 LSA Authentication Package

Adversaries can use the auto-start mechanism provided by LSA Authentication Packages for persistence.

- **id**: 077b1d1b-34ff-42d2-bd48-b0e6cdd1a359
- **categories**: enrich
- **confidence**: low
- **os**: windows
- **created**: 7/26/2019
- **updated**: 7/26/2019

MITRE ATT&CK™ Mapping

- **tactics**: Persistence
- **techniques**: T1131 Authentication Package

Query

```sql
registry where hive.hklm and
registry_path == "*\ControlSet\Control\Lsa\Authentication Packages*"
```

Contributors

- Endgame

1.2.56 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
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

**1.2.57 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
certainty 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*"
```
1.2.58 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  c4732632-9e1d-4980-9fa8-1d98c93f918e
categories detect
category confidence low
os  windows
created 11/30/2018
updated 05/17/2019
```

MITRE ATT&CK™ Mapping

- **tactics**: Impact
- **techniques**: T1490 Inhibit System Recovery

**Query**

```
process where subtype.create and
    process_name == "bcdedit.exe" and command_line == "*set *" and
    (command_line == "* bootstatuspolicy *ignoreallfailures*" or command_line == "* _
    _recoveryenabled* no*")
```
1.2.59 Modification of ld.so.preload

Identifies modification of ld.so.preload for shared object injection. This technique is used by attackers to load arbitrary code into processes.

```
id  fd9b987a-1101-4ed3-bda6-a70300eaf57e
categories  detect
confidence  medium
os  linux
created  05/17/2019
updated  05/17/2019
```

MITRE ATT&CK™ Mapping

```
tactics  Defense Evasion
techniques  T1055 Process Injection
```

Query

```
file  where  file_path="/etc/ld.so.preload"
```

Detonation

Atomic Red Team: T1055

Contributors

- Tony Lambert

1.2.60 Modification of Logon Scripts from Registry

Windows allows logon scripts to be run whenever a specific user or group of users log into a system.

```
id  af99d7ec-b1c7-4648-9188-063ca27544ac
categories  enrich
confidence  low
os  windows
created  7/26/2019
updated  7/26/2019
```

MITRE ATT&CK™ Mapping

```
tactics  Lateral Movement, Persistence
techniques  T1037 Logon Scripts
```
1.2.61 Modification of rc.common Script

During the boot process, macOS executes source /etc/rc.common, which is a shell script containing various utility functions. Adversaries can use the rc.common file as a way to hide code for persistence.

```
id 11db63f4-15eb-47f7-8e69-e4879bace2b0
categories enrich
certainty low
os macos
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

- Tactics: Persistence
- Techniques: T1163 Rc.common

```
Query

file where file_name == "rc.common"
```

1.2.62 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
certainty 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

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

Detonation

Atomic Red Team: T1156

Contributors

- Tony Lambert

1.2.63 Mounting Hidden Shares

Identifies enumeration of mounted shares with the built-in Windows tool `net.exe`.

```
id 9b3dd402-891c-4c4d-a662-28947168ce61
categories detect
certainty low
os windows
created 11/30/2018
updated 11/30/2018
```

MITRE ATT&CK™ Mapping


tactics Lateral Movement

techniques T1077 Windows Admin Shares

Query

```sql
process where subtype.create and
(review_name == "net.exe" or (review_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

1.2.64 Mounting Windows Hidden Shares with net.exe

Identifies hidden Windows Admin Network shares

id 8e7c9bce-565b-4ee1-bb70-37dc61afc8d0

categories hunt

confidence low

os windows

created 7/26/2019

updated 7/26/2019

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 \\*\*\*\*\*"

Contributors

• Endgame

1.2.65 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

```eql
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

1.2.66 Network Service Scanning via Port

Network Service Scanning via incoming network port scanning

```eql
id 4f64ef9e-ee9b-4245-a3f4-777e550ebb37
categories hunt
certainty low
os windows, macos, linux
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

tactics Discovery

techniques T1046 Network Service Scanning

Query

```eql
network where subtype.incoming
| unique unique_pid destination_port
| unique_count unique_pid
| filter count > 25
```
1.2.67 Office Application Startup via Template File Modification

Adversaries can modify default Microsoft Office templates in order to establish persistence.

```
file where not subtype.delete and
wildcard(file_path,
  "*:\Users\*\AppData\Roaming\Microsoft\Templates\Normal.dotm",
  "*:\Users\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB",
)
```

1.2.68 Office Application Startup via Template Registry Modification

Adversaries can modify Microsoft Office-related registry keys to establish persistence.

```
file where not subtype.delete and
wildcard(file_path,
  "*:\Users\*\AppData\Roaming\Microsoft\Templates\Normal.dotm",
  "*:\Users\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB",
)
```
MITRE ATT&CK™ Mapping

**tactics** Persistence

**techniques** T1137 Office Application Startup

Query

```sql
registry where wildcard(registry_path,
    "\Software\Microsoft\Office\Outlook\Today\UserDefinedUrl",
    "\Software\Microsoft\Office\Excel\Options\Open",
    "\Software\Microsoft\Office\PowerPoint\AddIns",
    "\Software\Microsoft\Office\Addins\*",
    "SOFTWARE\Microsoft\Office\Excel\Options",
    "Software\Microsoft\VBA\VBE\Addins\*"
)
```

Contributors

- Endgame

1.2.69 Password Policy Enumeration

Identifies enumeration of local or global password policies using built-in commands.

- **id** 94a5cbe1-851a-4b8f-bd9c-04c62097ae5e
- **categories** enrich
- **confidence** low
- **os** linux
- **created** 7/26/2019
- **updated** 7/26/2019

MITRE ATT&CK™ Mapping

**tactics** Discovery

**techniques** T1201 Password Policy Discovery

Query

```sql
process where subtype.create and (  
    process_name == "chage" and command_line == "-l *" or  
    process_name == "cat" and command_line == "*/etc/pam.d/common-password"
)
```

Contributors

- Endgame
1.2.70 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
classification 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(registry_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 registry_data
```

**Detonation**

Atomic Red Team: T1103

**Contributors**

- Endgame

1.2.71 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
classification 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 registry_path == "*\Software\Microsoft\NetSh\*"
```

**Detonation**

Atomic Red Team: T1128

**Contributors**

- Endgame

### 1.2.72 Persistence via Screensaver

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

- **id**: dd2ee76-9b44-479e-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 registry_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,*"
]
1.2.73 Persistent process via Launch Agent

An adversary can establish persistence by installing a new launch agent that executes at login by using launchd or launchctl to load a plist into the appropriate directories.

```
id 8b3a3f3b-f4f0-4cd4-82f4-28f79a3cf95b
categories enrich
confidence low
os macos
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

- **tactics**: Persistence
- **techniques**: T1159 Launch Agent

**Query**

```
file where not subtype.delete and
  file_path == "*/library/launchagents/*"
```

1.2.74 Plist Modification

Property list (plist) files contain all of the information that macOS and OS X uses to configure applications and services. Adversaries can modify these plist files to point to their own code, can use them to execute their code in the context of another user, bypass whitelisting procedures, or even use them as a persistence mechanism.

```
id 9424fa5e-466a-40df-bb69-7cf31b7bd398
categories enrich
```
1.2.75 Potential Gatekeeper Bypass

In macOS, when applications or programs are downloaded from the internet, there is a special attribute set on the file. This attribute is read by Apple’s Gatekeeper defense program at execution time.

```
| id          | a4fe6af5-bc33-4e72-8241-ee885b95c46 |
| categories  | detect                           |
| confidence  | low                              |
| os          | macos                            |
| created     | 7/26/2019                        |
| updated     | 7/26/2019                        |
```

MITRE ATT&CK™ Mapping

**tactics** Privilege Escalation, Defense Evasion, Persistence

**techniques** T1150 Plist Modification

Query

```
file where file_name == "Preferences/+.plist"
```

Contributors

- Endgame

1.2.75 Potential Gatekeeper Bypass

In macOS, when applications or programs are downloaded from the internet, there is a special attribute set on the file. This attribute is read by Apple’s Gatekeeper defense program at execution time.

```
id a4fe6af5-bc33-4e72-8241-ee885b95c46
categories detect
category confidence low
os macos
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

**tactics** Defense Evasion

**techniques** T1144 Gatekeeper Bypass

Query

```
process where subtype.create and
process_name == "xattr" and
command_line == "*com.apple.quarantine*"
| unique command_line
```
Contributors

- Endgame

### 1.2.76 Process Discovery via Built-In Applications

Built-in tools can be used to discover running processes on an endpoint

<table>
<thead>
<tr>
<th>id</th>
<th>737c7bed-364f-4b47-a0aa-763c80c8aa6c</th>
</tr>
</thead>
<tbody>
<tr>
<td>categories</td>
<td>enrich</td>
</tr>
<tr>
<td>confidence</td>
<td>low</td>
</tr>
<tr>
<td>os</td>
<td>macos, linux</td>
</tr>
<tr>
<td>created</td>
<td>7/26/2019</td>
</tr>
<tr>
<td>updated</td>
<td>7/26/2019</td>
</tr>
</tbody>
</table>

**MITRE ATT&CK™ Mapping**

- **tactics** Discovery
- **techniques** T1057 Process Discovery, T1063 Security Software Discovery

**Query**

```sql
process where subtype.create and
(process_name in ("ps", "pstree", "htop", "pgrep") or
match(command_line, ?".*? /proc/\d+"))
```

Contributors

- Endgame

### 1.2.77 Process Discovery via Windows Tools

Attackers will enumerate running processes to gain further comprehension of the environment.

<table>
<thead>
<tr>
<th>id</th>
<th>555a76e1-d5fe-44b9-a6bc-d275c4c446cc</th>
</tr>
</thead>
<tbody>
<tr>
<td>categories</td>
<td>enrich</td>
</tr>
<tr>
<td>confidence</td>
<td>low</td>
</tr>
<tr>
<td>os</td>
<td>windows</td>
</tr>
<tr>
<td>created</td>
<td>7/26/2019</td>
</tr>
<tr>
<td>updated</td>
<td>7/26/2019</td>
</tr>
</tbody>
</table>
MITRE ATT&CK™ Mapping

tactics Discovery

techniques T1057 Process Discovery, T1063 Security Software Discovery

Query

```eql
process where subtype.create and {
  process_name == "tasklist.exe" and not matchLite(?.* [-/]svc", command_line) or
  process_name == "quser.exe" or
  (process_name == "powershell.exe" and command_line == "*Get-Process")
}
```

Contributors

• Endgame

1.2.78 Processes Running with Unusual Extensions

Processes should always be executing with PE extensions, such as .exe, so any execution from non-PE extensions, such as .gif are immediately suspicious.

```
id 251c26ff-658b-42d1-a808-bafcd4b52284
(categories detect
  confidence low
  os windows
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

tactics Defense Evasion

techniques T1036 Masquerading

Query

```eql
process where subtype.create and wildcard(process_name,
  ".pif", ".pdf", ".docx", ".doc",
  ".xlsx", ".xls", ".pptx", ".ppt",
  ".txt", ".rtf", ".gif", ".jpg",
  ".png", ".bmp", ".vbs", ".vbe",
  ".bat", ".js", ".cmd",
  ".wsh", ".psi", ".",
)
```

1.2. Analytics
Contributors

- Endgame

1.2.79 Processes with Trailing Spaces

Identifies processes running with a trailing space, which can be used to look like an ordinary file while evading default file handlers.

<table>
<thead>
<tr>
<th>id</th>
<th>391c27cf-68d5-4416-9315-cdfde096a33b</th>
</tr>
</thead>
<tbody>
<tr>
<td>categories</td>
<td>detect</td>
</tr>
<tr>
<td>confidence</td>
<td>low</td>
</tr>
<tr>
<td>os</td>
<td>macos, linux</td>
</tr>
<tr>
<td>created</td>
<td>7/26/2019</td>
</tr>
<tr>
<td>updated</td>
<td>7/26/2019</td>
</tr>
</tbody>
</table>

MITRE ATT&CK™ Mapping

- tactics Defense Evasion, Execution
- techniques T1151 Space after Filename

Query

```
process where subtype.create
and process_name == "* "
```

Contributors

- Endgame

1.2.80 Proxied Execution via Signed Scripts

Signed script scripts such as PubPrn.vbs can be used to proxy execution from a remote site while bypassing signature validation restrictions and potentially application whitelisting.

<table>
<thead>
<tr>
<th>id</th>
<th>0d62a884-1052-44d0-a76c-1f4845e348d2</th>
</tr>
</thead>
<tbody>
<tr>
<td>categories</td>
<td>enrich</td>
</tr>
<tr>
<td>confidence</td>
<td>low</td>
</tr>
<tr>
<td>os</td>
<td>windows</td>
</tr>
<tr>
<td>created</td>
<td>7/26/2019</td>
</tr>
<tr>
<td>updated</td>
<td>7/26/2019</td>
</tr>
</tbody>
</table>
MITRE ATT&CK™ Mapping

tactics Defense Evasion, Execution

techniques T1216 Signed Script Proxy Execution

Query

```
process where subtype.create and
  process_name in ("cscript.exe", "wscript.exe") and
  command_line == "* *.vbs* *script:htp*"
```

Contributors

- Endgame

1.2.81 Reading the Clipboard with pbpaste

Adversaries may collect data stored in the clipboard from users copying information within or between applications.

id 4e026838-f673-4a5b-b380-615d624fbd00
categories enrich
c_confidence low
os macOS
created 7/26/2019
updated 7/26/2019

MITRE ATT&CK™ Mapping

tactics Collection

techniques T1115 Clipboard Data

Query

```
process where subtype.create and process_name == "pbpaste"
```

Contributors

- Endgame
1.2.82 Registration of a Password Filter DLL

Identifies the installation of password filter DLLs which may be used to steal credentials from LSA.

id ae6ae50f-69f3-4e85-bfe2-2db9d1422517
categories detect
confidence low
os windows
created 7/26/2019
updated 7/26/2019

MITRE ATT&CK™ Mapping

tactics Credential Access
techniques T1174 Password Filter DLL

Query

```
registry where hive.hklm and registry_path == "*SYSTEM\ControlSet\\Control\Lsa\Notification Packages*" | unique registry_path, process_path
```

Contributors

- Endgame

1.2.83 Registration of Winlogon Helper DLL

A winlogon registry key was modified to establish persistence.

id 46de6f8f-e30e-45f7-a136-7ab140c9af08
categories hunt
confidence low
os windows
created 7/26/2019
updated 7/26/2019

MITRE ATT&CK™ Mapping

tactics Persistence
techniques T1004 Winlogon Helper DLL
Query

```eql
registry where
  wildcard(registry_path,
    "*\Software[Wow6432Node]Microsoft\Windows NT\CurrentVersion\Winlogon\*",
    "*\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\*"
)
```

Contributors

- Endgame

### 1.2.84 Registry Persistence via Run Keys

Adversaries can establish persistence by adding an entry to the “run keys” in the registry or startup folder. The referenced program will be executed when a user logs in.

**id** c457d0c5-3ec8-4e9e-93f5-6ddcbfeec498  
**categories** enrich  
**confidence** low  
**os** windows  
**created** 7/26/2019  
**updated** 7/26/2019

**MITRE ATT&CK™ Mapping**

- **tactics** Persistence  
- **techniques** T1060 Registry Run Keys / Startup Folder

Query

```eql
registry where
  registry_path == "*\Software\Microsoft\Windows\CurrentVersion\Run*"
```

Contributors

- Endgame

### 1.2.85 Registry Persistence via Shell Folders

Adversaries can establish persistence by adding an entry to the “run keys” in the registry or startup folder. The referenced program will be executed when a user logs in.

**id** f8b1720c-7116-4ec3-b38a-402f984e4972  
**categories** detect
1.2.86 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**

```sql
registry where
  registry_path == "\Software\Microsoft\Windows\CurrentVersion\Explorer\*Shell*Folders*"
```

(...continues on next page)
// 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

1.2.87 RegSvr32 Scriptlet Execution

Detect regsrv32 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
1.2.88 Remote Desktop Protocol Hijack

Identifies possible Remote Desktop Protocol session hijacking

- id: 46ff4da0-2f55-4023-8de3-1709fbd33f1d
- categories: hunt
- confidence: low
- os: windows
- created: 7/26/2019
- updated: 7/26/2019

MITRE ATT&CK™ Mapping

- tactics: Lateral Movement
- techniques: T1076 Remote Desktop Protocol

Query

```
process where subtype.create and
    process_name == "tscon.exe" and command_line == ": :"
```

Contributors

- Endgame

1.2.89 Remote Execution via WMIC

Identifies use of \texttt{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

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

Contributors

- Endgame

### 1.2.90 Remote System Discovery Commands

Commands used to obtain information about the remote system.

- **id**: 9be90e44-c0f7-4fd2-9378-be00c25a02d7
- **categories**: enrich
- **confidence**: low
- **os**: windows
- **created**: 7/26/2019
- **updated**: 7/26/2019

**MITRE ATT&CK™ Mapping**

- **tactics**: Discovery
- **techniques**: T1018 Remote System Discovery

Query

```eql
process where subtype.create and (    
  process_name == "nbtstat.exe" and wildcard(command_line, "* -n*", "* -s*") or
  process_name == "arp.exe" and command_line == "* -a*"
)
```

Contributors

- Endgame

### 1.2.91 Remote Terminal Sessions

An adversary may use Valid Accounts to log into a service specifically designed to accept remote connections.

- **id**: 5c310aff-d4a8-43fb-beed-b17dab1f1df0
- **categories**: enrich
- **confidence**: low
- **os**: windows, macos, linux
MITRE ATT&CK™ Mapping

tactics Lateral Movement

techniques T1021 Remote Services

Query

```
process where subtype.create and
    process_name in ("telnet.exe", "putty.exe", "ssh")
| unique_count parent_process_name, command_line
```

Contributors

- Endgame

1.2.92 Resumed Application on Reboot

Starting in Mac OS X 10.7 (Lion), users can specify certain applications to be re-opened when a user reboots their machine.

```
id 491db9c2-8b06-4076-8f9b-de44b9bae8d0
categories enrich
classification low
os macos
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

tactics Persistence

techniques T1164 Re-opened Applications

Query

```
file where file_name == "*Library/Preferences/com.apple.loginwindow.*plist"
```

Contributors

- Endgame
1.2.93 Root Certificate Install

Identifies modifications to the local trusted root certificates via known Windows tools. The install of a malicious root certificate would allow an attacker the ability to masquerade malicious files as valid signed components from any entity (e.g. Microsoft). It could also allow an attacker to decrypt SSL traffic on this machine. However, software may also install root certificates for the purpose of inspecting SSL traffic.

```
id 7a2efe5-42d9-4bb1-8e53-6e6d47167a96
categories hunt
confidence low
os windows
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

- **tactics** Defense Evasion
- **techniques** T1130 Install Root Certificate

Query

```
registry where wildcard(registry_path,
  -"\Software\Microsoft\SystemCertificates\Root\Certificates\*\Blob",
  -"\Software\Microsoft\SystemCertificates\AuthRoot\Certificates\*\Blob",
  -"\Software\Policies\Microsoft\SystemCertificates\Root\Certificates\*\Blob",
  -"\Software\Policies\Microsoft\SystemCertificates\AuthRoot\Certificates\*\Blob
  -")
| unique process_path,registry_path
```

Contributors

- Endgame

1.2.94 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**

```sql
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

### 1.2.95 Scheduled Task Creation via Microsoft Office Application

Identifies the creation of a scheduled task via a Microsoft Office application to establish persistence.

- **id**: 8e98bf09-e662-4908-b68e-5c96ad5c6860
- **categories**: detect
- **confidence**: medium
- **os**: windows
- **created**: 8/16/2019
- **updated**: 8/16/2019

MITRE ATT&CK™ Mapping

**tactics**  Persistence

**techniques**  T1053 Scheduled Task

**Query**

```sql
image_load where
  process_name in ("excel.exe", "winword.exe", "powerpnt.exe", "outlook.exe") and
  image_name == "taskschd.dll"
```
1.2.96 Searching for Passwords in Files

Adversaries may search local file systems and remote file shares for files containing passwords.

```
process where subtype.create
    and process_name in ("cat", "grep")
    and wildcard(command_line, ".bash_history", "password", "passwd")
```

Contributors

- Endgame

1.2.97 Searching for Passwords in Files

Adversaries may search local file systems and remote file shares for files containing passwords.

```
process where subtype.create
    and process_name in ("cat", "grep")
    and wildcard(command_line, ".bash_history", "password", "passwd")
```

Contributors

- Endgame
Query

```plaintext
process where subtype.create and
    process_name == "findstr.exe" and command_line == "*password*"
| unique parent_process_name, command_line
```

Contributors

- Endgame

1.2.98 Service Path Modification with sc.exe

Identifies usage of the sc.exe command to modify existing services.

- **id**: 15c17f6b-29c5-43a4-8adc-d298f2c4c141
- **categories**: hunt
- **confidence**: low
- **os**: windows
- **created**: 7/26/2019
- **updated**: 7/26/2019

MITRE ATT&CK™ Mapping

- **tactics**: Persistence
- **techniques**: T1031 Modify Existing Service

Query

```plaintext
process where subtype.create and
    process_name == "sc.exe" and
    wildcard(command_line, "* config *", "*binPath*")
```

Contributors

- Endgame
1.2.99 Service Stop or Disable with sc.exe

Detects when running services are stopped with the sc.exe command

```
id  591da84a-0382-40e7-afc8-12bd58c40425
categories  enrich
certainty  low
os  windows
created  7/26/2019
updated  7/26/2019
```

MITRE ATT&CK™ Mapping

- tactics  Impact
- techniques  T1489 Service Stop

Query

```
process where subtype.create and
process_name == "sc.exe" and
wildcard(command_line, "* stop*", "* config *disabled*"
```

Contributors

- Endgame

1.2.100 Stopping Services with net.exe

Detects when running services are stopped with the net.exe command.

```
id  0b2ea07b-b2ef-4cf7-ae2f-564a63662e3b
categories  enrich
certainty  low
os  windows
created  7/26/2019
updated  7/26/2019
```

MITRE ATT&CK™ Mapping

- tactics  Impact
- techniques  T1489 Service Stop
Query

```
process where subtype.create and
   process_name == "net.exe" and
   command_line == "* stop *"
```

Contributors

- Endgame

1.2.101 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 == "*:*
   file_name != ":Zone.Identifier" and
   (file_name == "*.dll*" or file_name == "*.exe")
```

Detonation

Atomic Red Team: T1096

Contributors

- Endgame
1.2.102 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 wildcard(command_line, "* /download *", "*transfer*")
```

**Detonation**

Atomic Red Team: T1197

**Contributors**

- Endgame

1.2.103 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

strategies  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

1.2.104 Suspicious File Creation via Browser Extensions

Malicious browser extensions can be installed via app store downloads masquerading as legitimate extensions, social engineering, or by an adversary that has already compromised a system

id  7797d204-3205-4033-bac7-658fc203198d
categories  enrich
certainty  low
os  macos, windows
created  7/26/2019
updated  7/26/2019

MITRE ATT&CK™ Mapping

tactics  Persistence

strategies  T1176 Browser Extensions

Query

```
file where not subtype.delete and
wildcard(file_name, "*.exe", "*.dll", "*.ps1", "*.vbs", "*.bat") and
wildcard(file_path,
// windows
"*\AppData\Local\Google\Chrome\User Data\Default\Extensions",
"*:\Program Files\Mozilla Firefox\plugins\*",
"*:\Program Files\Internet Explorer\Plugins\*",
(continues on next page)
// macos
"/Applications/Firefox.app/Contents/MacOS/firefox/plugins/*",
"/Users/*/Library/Safari/Extensions/*",
"/Users/*/Library/Application Support/Google/Chrome/Default/Extensions/*"

Contributors

• Endgame

1.2.105 Suspicious Process Loading Credential Vault DLL

Identifies an unexpected process loading the Windows Credential Vault DLL in preparation of enumerating/stealing a user’s saved credentials.

```
id 679560ee-0ea0-4358-bf83-e4c478d9d1c8
categories detect
confidence high
os windows
created 8/16/2019
updated 8/16/2019
```

MITRE ATT&CK™ Mapping

- tactics Credential Access
- techniques T1003 Credential Dumping

Query

```
image_load where process_name != "vaultcmd.exe" and
image_name == "vaultcli.dll"
```

Contributors

• David French

References

• https://medium.com/threatpunter/detecting-adversary-tradecraft-with-image-load-event-logging-8de93338c16
1.2.106 Suspicious Script Object Execution

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

- **id**: a792eb37-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**

```plaintext
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://gist.github.com/subTee/24c7d8e1ff0f5602092f58cbb3f7d302

1.2.107 System Information Discovery

Detect enumeration of Windows system information via systeminfo.exe

- **id**: 4b9c2df7-87e2-4bcb-9123-9779ecb2dbf2
- **categories**: hunt
- **confidence**: medium
- **os**: windows
- **created**: 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

1.2.108 System Network Connections Discovery

Adversaries may attempt to get a listing of network connections to or from a compromised system.

```
id df696af0-8d3f-4557-8278-d10f40ba7c07
categories enrich
category confidence low
os macos, linux
created 7/26/2019
updated 7/26/2019
```

MITRE ATT&CK™ Mapping

tactics Discovery

techniques T1049 System Network Connections Discovery

Query

```
process where subtype.create and process_name in ("netstat", "lsof", "who", "w")
| unique command_line
```
1.2.109 System Owner and User Discovery

Windows contains several built-in commands to report the active user. These may be used by an actor to learn privileges levels or determine if a session is active.

```
query = process where subtype.create and (process_name in ("hostname.exe", "whoami.exe", "systeminfo.exe", "quser.exe") or process_name == "cmd.exe" and wildcard(command_line, "*echo *\%USERNAME\%", "*echo *\%USERDOMAIN\%")
```

1.2.110 Trap Signals Usage

The trap command allows programs and shells to specify commands that will be executed upon receiving interrupt signals.

```
id 3ecbba23-0d1e-4870-8b9e-016b423aebee
categories enrich
category confidence low
os macos, linux
created 7/26/2019
updated 7/26/2019
```
MITRE ATT&CK™ Mapping

tactics Execution, Persistence
techniques T1154 Trap

Query

```
process where subtype.create and
  process_name == "trap" and command_line == "* signals*"
```

Contributors

• Endgame

1.2.111 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
EQL Analytics Library

Contributors

• Endgame

1.2.112 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 == "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"))
}
```
1.2.113 User Account Creation

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

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

Detonation

Atomic Red Team: T1136

Contributors

- Endgame
1.2.114 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: 05/17/2019

MITRE ATT&CK™ Mapping

- tactics: Impact
- techniques: T1490 Inhibit System Recovery

Query

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

Detonation

Atomic Red Team: T1490

Contributors

- Endgame

1.2.115 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: 05/17/2019
MITRE ATT&CK™ Mapping

**tactics**  Impact
**techniques**  T1490 Inhibit System Recovery

Query

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

Detonation

Atomic Red Team: T1490

Contributors

- Endgame

1.2.116 Windows File Permissions Modification

File permissions are commonly managed by discretionary access control lists (DACLs) specified by the file owner. Adversaries may modify file permissions/attributes to evade intended DACLs.

```plaintext
id
a099cb16-1a92-4503-9102-56cc84a51ad1
categories  enrich
category  low
os  windows
created  7/26/2019
updated  7/26/2019
```

MITRE ATT&CK™ Mapping

**tactics**  Defense Evasion
**techniques**  T1222 File Permissions Modification

Query

```plaintext
process where subtype.create and (  
    process_name == "attrib.exe" and command_line == "* +h*" or  
    process_name == "takeown.exe" or  
    process_name == "icacls.exe" and command_line == "*grant*"
)
```
1.2.117 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
category 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

1.2.118 WMI Execution via Microsoft Office Application

Identifies the execution of Windows Management Instrumentation (WMI) via a Microsoft Office application.

```
id e6be5ffe-c765-4e13-962d-7eaae07aeaecc
categories detect
category medium
os windows
created 8/16/2019
updated 8/16/2019
```
MITRE ATT&CK™ Mapping

**tactics** Execution

**techniques** T1047 Windows Management Instrumentation

<table>
<thead>
<tr>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>image_load where process_name in (&quot;excel.exe&quot;, &quot;winword.exe&quot;, &quot;powerpnt.exe&quot;, &quot;outlook.exe&quot;) and image_name in (&quot;wbemdisp.dll&quot;, &quot;wbemcomn.dll&quot;, &quot;wbemprox.dll&quot;, &quot;wmiutils.dll&quot;, &quot;wbemsvc.dll&quot;, &quot;fastprox.dll&quot;)</code></td>
</tr>
</tbody>
</table>

Contributors

- David French

References


<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access of Outlook Email Archives</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Collection</td>
<td>T1114 Email Collection</td>
</tr>
<tr>
<td><strong>Account Discovery via Built-In Tools</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1087 Account Discovery</td>
</tr>
<tr>
<td><strong>AD Dumping via Ntdsutil.exe</strong></td>
<td>Tony Lambert</td>
<td>01/07/2019</td>
<td>Credential Access</td>
<td>T1003 Credential Dumping</td>
</tr>
<tr>
<td><strong>Adding the Hidden File Attribute with via attrib.exe</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Defense Evasion Persistence</td>
<td>T1158 Hidden Files and Directories</td>
</tr>
<tr>
<td><strong>AppCert DLLs Registry Modification</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Privilege Escalation Persistence</td>
<td>T1182 AppCert DLLs</td>
</tr>
<tr>
<td><strong>Audio Capture via PowerShell</strong></td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Collection</td>
<td>T1123 Audio Capture</td>
</tr>
<tr>
<td><strong>Audio Capture via SoundRecorder</strong></td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Collection</td>
<td>T1123 Audio Capture</td>
</tr>
<tr>
<td><strong>Bypass UAC via CMSTP</strong></td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion Execution</td>
<td>T1191 CMSTP T1088 Bypass User Account Control</td>
</tr>
<tr>
<td><strong>Bypass UAC via Fodhelper.exe</strong></td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Privilege Escalation</td>
<td>T1088 Bypass User Account Control</td>
</tr>
<tr>
<td><strong>Bypass UAC via Fodhelper.exe</strong></td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Privilege Escalation</td>
<td>T1088 Bypass User Account Control</td>
</tr>
<tr>
<td><strong>Bypass UAC via WSReset.exe</strong></td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Privilege Escalation</td>
<td>T1088 Bypass User Account Control</td>
</tr>
<tr>
<td><strong>Change Default File Association</strong></td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1042 Change Default File Association</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearing Windows Event Logs with wevtutil</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1070 Indicator Removal on Host</td>
</tr>
<tr>
<td>COM Hijack via Script Object</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1122 Component Object Model Hijacking</td>
</tr>
<tr>
<td>Command-Line Creation of a RAR file</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Exfiltration</td>
<td>T1002 Data Compressed</td>
</tr>
<tr>
<td>Control Panel Items</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Defense Evasion Execution</td>
<td>T1196 Control Panel Items</td>
</tr>
<tr>
<td>Creation of an Archive with Common Archivers</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Collection</td>
<td>T1074 Data Staged</td>
</tr>
<tr>
<td>Creation of Kernel Module</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1215 Kernel Modules and Extensions</td>
</tr>
<tr>
<td>Creation of Scheduled Task with scfats.exe</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Privilege Escalation</td>
<td>T1053 Scheduled Task</td>
</tr>
<tr>
<td>Creation or Modification of Systemd Service</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1501 Systemd Service</td>
</tr>
<tr>
<td>Credential Enumeration via Credential Vault CLI</td>
<td>David French</td>
<td>8/16/2019</td>
<td>Credential Access</td>
<td>T1003 Credential Dumping</td>
</tr>
<tr>
<td>Delete Volume USN Journal with fsutil</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1070 Indicator Removal on Host</td>
</tr>
<tr>
<td>Disconnecting from Network Shares with net.exe</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Defense Evasion</td>
<td>T1126 Network Share Connection Removal</td>
</tr>
<tr>
<td>Discovery of a Remote System's Time</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1124 System Time Discovery</td>
</tr>
<tr>
<td>Discovery of Domain Groups</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1069 Permission Groups Discovery</td>
</tr>
<tr>
<td>Discovery of Network Environment via Built-in Tools</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1016 System Network Configuration Discovery</td>
</tr>
<tr>
<td>Discovery of Network Environment via Built-in Tools</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1016 System Network Configuration Discovery</td>
</tr>
<tr>
<td>DLL Search Order Hijacking with known programs</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Privilege Escalation</td>
<td>T1038 DLL Search Order Hijacking</td>
</tr>
<tr>
<td>Domain Trust Discovery</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1482 Domain Trust Discovery</td>
</tr>
<tr>
<td>Domain Trust Discovery via Nltest.exe</td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Discovery</td>
<td>T1482 Domain Trust Discovery</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encoding or Decoding Files via CertUtil</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1140 Deobfuscate/Decode Files or Information</td>
</tr>
<tr>
<td>Enumeration of Local Shares</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1135 Network Share Discovery</td>
</tr>
<tr>
<td>Enumeration of Mounted Shares</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1049 System Network Connections Discovery</td>
</tr>
<tr>
<td>Enumeration of Remote Shares</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1135 Network Share Discovery</td>
</tr>
<tr>
<td>Enumeration of System Information</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1082 System Information Discovery</td>
</tr>
<tr>
<td>Execution of a Command via a SYSTEM Service</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Privilege Escalation</td>
<td>T1035 Service Execution</td>
</tr>
<tr>
<td>Execution of Existing Service via Command</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Execution</td>
<td>T1035 Service Execution</td>
</tr>
<tr>
<td>Execution via cmstp.exe</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Defense Evasion</td>
<td>T1191 CMSTP</td>
</tr>
<tr>
<td>HH.exe execution</td>
<td>Dan Beavin</td>
<td>09/26/2019</td>
<td>Defense Evasion</td>
<td>T1223 Compiled HTML File</td>
</tr>
<tr>
<td>Host Artifact Deletion</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Defense Evasion</td>
<td>T1070 Indicator Removal on Host</td>
</tr>
<tr>
<td>Image Debuggers for Accessibility Features</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1015 Accessibility Features</td>
</tr>
<tr>
<td>Installing Custom Shim Databases</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1138 Application Shimming</td>
</tr>
<tr>
<td>Installing Time Providers</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1209 Time Providers</td>
</tr>
<tr>
<td>InstallUtil Execution</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Execution</td>
<td>T1118 InstallUtil</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactive AT Job</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Privilege Escalation</td>
<td>T1053 Scheduled Task</td>
</tr>
<tr>
<td>Launch Daemon Persistence</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Privilege Escalation Persistence</td>
<td>T1160 Launch Daemon Persistence</td>
</tr>
<tr>
<td>Loading Kernel Modules with kextload</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1215 Kernel Modules and Extensions</td>
</tr>
<tr>
<td>Local Job Scheduling Paths</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Execution Persistence</td>
<td>T1168 Local Job Scheduling</td>
</tr>
<tr>
<td>Local Job Scheduling Process</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Execution Persistence</td>
<td>T1168 Local Job Scheduling</td>
</tr>
<tr>
<td>Logon Scripts with UserInitMprLogonScript</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1037 Logon Scripts</td>
</tr>
<tr>
<td>LSA Authentication Package</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1131 Authentication Package</td>
</tr>
<tr>
<td>LSASS Memory Dumping</td>
<td>Tony Lambert</td>
<td>01/07/2019</td>
<td>Credential Access</td>
<td>T1003 Credential Dumping</td>
</tr>
<tr>
<td>LSASS Memory Dumping via ProcDump.exe</td>
<td>Tony Lambert</td>
<td>01/07/2019</td>
<td>Credential Access</td>
<td>T1003 Credential Dumping</td>
</tr>
<tr>
<td>Modification of Boot Configuration</td>
<td>Endgame</td>
<td>05/17/2019</td>
<td>Impact</td>
<td>T1490 Inhibit System Recovery</td>
</tr>
<tr>
<td>Modification of ld.sopreload</td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Defense Evasion</td>
<td>T1055 Process Injection</td>
</tr>
<tr>
<td>Modification of Logon Scripts from Registry</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Lateral Movement Persistence</td>
<td>T1037 Logon Scripts</td>
</tr>
<tr>
<td>Modification of rc.common Script</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1163 Rc.common</td>
</tr>
<tr>
<td>Modifications of .bash_profile and .bashrc</td>
<td>Tony Lambert</td>
<td>01/10/2019</td>
<td>Persistence</td>
<td>T1156 .bash_profile and .bashrc</td>
</tr>
<tr>
<td>Mounting Hidden Shares</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Lateral Movement</td>
<td>T1077 Windows Admin Shares</td>
</tr>
<tr>
<td>Mounting Windows Hidden Shares with net.exe</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Lateral Movement</td>
<td>T1077 Windows Admin Shares</td>
</tr>
<tr>
<td>Mshta Network Connections</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Execution</td>
<td>T1170 Mshta</td>
</tr>
<tr>
<td>Network Service Scanning via Port</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1046 Network Service Scanning</td>
</tr>
<tr>
<td>Office Application Startup via Template File Modification</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1137 Office Application Startup</td>
</tr>
</tbody>
</table>

Continued on next page
Table 1 – continued from previous page

<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office Application Startup via Template Registry Modification</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1137 Office Application Startup</td>
</tr>
<tr>
<td><strong>Password Policy Enumeration</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1201 Password Policy Discovery</td>
</tr>
<tr>
<td><strong>Persistence via ApplInit DLL</strong></td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1103 ApplInit DLLs</td>
</tr>
<tr>
<td><strong>Persistence via NetSh Key</strong></td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1128 Netsh Helper DLL</td>
</tr>
<tr>
<td><strong>Persistence via Screensaver</strong></td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1180 Screensaver</td>
</tr>
<tr>
<td><strong>Persistent process via Launch Agent</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1159 Launch Agent</td>
</tr>
<tr>
<td><strong>Plist Modification</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Privilege Escalation</td>
<td>T1150 Plist Modification</td>
</tr>
<tr>
<td><strong>Potential Gatekeeper Bypass</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Defense Evasion</td>
<td>T1144 Gatekeeper Bypass</td>
</tr>
<tr>
<td><strong>Process Discovery via Built-In Applications</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1057 Process Discovery T1063 Security Software Discovery</td>
</tr>
<tr>
<td><strong>Processes Running with Unusual Extensions</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Defense Evasion</td>
<td>T1036 Masquerading</td>
</tr>
<tr>
<td><strong>Processes with Trailing Spaces</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Defense Evasion</td>
<td>T1151 Space after Filename</td>
</tr>
<tr>
<td><strong>Proxied Execution via Signed Scripts</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Defense Evasion</td>
<td>T1216 Signed Script Proxy Execution</td>
</tr>
<tr>
<td><strong>Reading the Clipboard with pbpaste</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Collection</td>
<td>T1115 Clipboard Data</td>
</tr>
<tr>
<td><strong>Registration of a Password Filter DLL</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Credential Access</td>
<td>T1174 Password Filter DLL</td>
</tr>
<tr>
<td><strong>Registration of Winlogon Helper DLL</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1004 Winlogon Helper DLL</td>
</tr>
<tr>
<td><strong>Registry Persistence via Run Keys</strong></td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1060 Registry Run Keys / Startup Folder</td>
</tr>
<tr>
<td><strong>Registry Persistence via Shell Folders</strong></td>
<td>Endgame</td>
<td>7/22/2019</td>
<td>Persistence</td>
<td>T1060 Registry Run Keys / Startup Folder</td>
</tr>
</tbody>
</table>

Continued on next page
Table 1 – continued from previous page

<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Preparation of Event Viewer UAC Bypass</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Privilege Escalation</td>
<td>T1088 Bypass User Account Control</td>
</tr>
<tr>
<td>RegSvr32 Scriptlet Execution</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Execution</td>
<td>T1117 Regsvr32</td>
</tr>
<tr>
<td>Remote Execution via WMIC</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Lateral Movement</td>
<td>T1047 Windows Management Instrumentation</td>
</tr>
<tr>
<td>Remote System Discovery Commands</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1018 Remote System Discovery</td>
</tr>
<tr>
<td>Remote Terminal Sessions</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Lateral Movement</td>
<td>T1021 Remote Services</td>
</tr>
<tr>
<td>Resumed Application on Reboot</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1164 Re-opened Applications</td>
</tr>
<tr>
<td>SAM Dumping via Reg.exe</td>
<td>David French</td>
<td>8/16/2019</td>
<td>Persistence</td>
<td>T1053 Scheduled Task</td>
</tr>
<tr>
<td>Scheduled Task Creation via Microsoft Office Application</td>
<td>David French</td>
<td>8/16/2019</td>
<td>Persistence</td>
<td>T1081 Credentials in Files</td>
</tr>
<tr>
<td>Searching for Passwords in Files</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Credential Access</td>
<td>T1081 Credentials in Files</td>
</tr>
<tr>
<td>Searching for Passwords in Files</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Credential Access</td>
<td>T1081 Credentials in Files</td>
</tr>
<tr>
<td>Service Path Modification with sc.exe</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1031 Modify Existing Service</td>
</tr>
<tr>
<td>Service Stop or Disable with sc.exe</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Impact</td>
<td>T1489 Service Stop</td>
</tr>
<tr>
<td>Stopping Services with net.exe</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Impact</td>
<td>T1489 Service Stop</td>
</tr>
<tr>
<td>Suspicious ADS File Creation</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1096 NTFS File Attributes</td>
</tr>
<tr>
<td>Suspicious Bitadmin Job via bitsadmin.exe</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion Persistence</td>
<td>T1197 BITS Jobs</td>
</tr>
<tr>
<td>Suspicious File Creation via Browser Extensions</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Persistence</td>
<td>T1176 Browser Extensions</td>
</tr>
<tr>
<td>Suspicious Process Loading Credential Vault DLL</td>
<td>David French</td>
<td>8/16/2019</td>
<td>Credential Access</td>
<td>T1003 Credential Dumping</td>
</tr>
<tr>
<td>Suspicious Script Object Execution</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion Execution</td>
<td>T1117 Regsvr32</td>
</tr>
</tbody>
</table>

Continued on next page
### Table 1 – continued from previous page

<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Information Discovery</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1082 System Information Discovery</td>
</tr>
<tr>
<td>System Network Connections Discovery</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1049 System Network Connections Discovery</td>
</tr>
<tr>
<td>System Owner and User Discovery</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Discovery</td>
<td>T1033 System Owner/User Discovery</td>
</tr>
<tr>
<td>Trap Signals Usage</td>
<td>Endgame</td>
<td>7/26/2019</td>
<td>Execution</td>
<td>T1154 Trap</td>
</tr>
<tr>
<td>Unload Sysmon Filter Driver with fltmc.exe</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1089 Disabling Security Tools</td>
</tr>
<tr>
<td>User Account Creation</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1136 Create Account</td>
</tr>
<tr>
<td>Volume Shadow Copy Deletion via VssAdmin</td>
<td>Endgame</td>
<td>05/17/2019</td>
<td>Impact</td>
<td>T1490 Inhibit System Recovery</td>
</tr>
<tr>
<td>Volume Shadow Copy Deletion via WMIC</td>
<td>Endgame</td>
<td>05/17/2019</td>
<td>Impact</td>
<td>T1490 Inhibit System Recovery</td>
</tr>
<tr>
<td>Windows Network Enumeration</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1018 Remote System Discovery</td>
</tr>
<tr>
<td>WMI Execution via Microsoft Office Application</td>
<td>David French</td>
<td>8/16/2019</td>
<td>Execution</td>
<td>T1047 Windows Management Instrumentation</td>
</tr>
</tbody>
</table>

### 1.3 Atomic Blue Detections

<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD Dumping via Ntdsutil.exe</td>
<td>Tony Lambert</td>
<td>01/07/2019</td>
<td>Credential Access</td>
<td>T1003 Credential Dumping</td>
</tr>
<tr>
<td>Audio Capture via PowerShell</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Collection</td>
<td>T1123 Audio Capture</td>
</tr>
<tr>
<td>Audio Capture via SoundRecorder</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Collection</td>
<td>T1123 Audio Capture</td>
</tr>
<tr>
<td>Bypass UAC via CMSTP</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1191 CMSTP T1088 Bypass User Account Control</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypass UAC via Fodhelper.exe</td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Privilege Escalation</td>
<td>T1088 Bypass User Account Control</td>
</tr>
<tr>
<td>Bypass UAC via Fodhelper.exe</td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Privilege Escalation</td>
<td>T1088 Bypass User Account Control</td>
</tr>
<tr>
<td>Bypass UAC via WSReset.exe</td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Privilege Escalation</td>
<td>T1088 Bypass User Account Control</td>
</tr>
<tr>
<td>Change Default File Association</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1042 Change Default File Association</td>
</tr>
<tr>
<td>Clearing Windows Event Logs with wevtutil</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1070 Indicator Removal on Host</td>
</tr>
<tr>
<td>COM Hijack via Script Object</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1122 Component Object Model Hijacking</td>
</tr>
<tr>
<td>Command-Line Creation of a RAR file</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Exfiltration</td>
<td>T1002 Data Compressed</td>
</tr>
<tr>
<td>Delete Volume USN Journal with fsutil</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1070 Indicator Removal on Host</td>
</tr>
<tr>
<td>Discovery of a Remote System’s Time</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1124 System Time Discovery</td>
</tr>
<tr>
<td>Domain Trust Discovery via Nltest.exe</td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Discovery</td>
<td>T1482 Domain Trust Discovery</td>
</tr>
<tr>
<td>Encoding or Decoding Files via CertUtil</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1140 Deobfuscate/Decode Files or Information</td>
</tr>
<tr>
<td>Enumeration of Mounted Shares</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1049 System Network Connections Discovery</td>
</tr>
<tr>
<td>Enumeration of Remote Shares</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1135 Network Share Discovery</td>
</tr>
<tr>
<td>Execution of a Command via a SYSTEM Service</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Privilege Escalation</td>
<td>T1035 Service Execution</td>
</tr>
<tr>
<td>HH.exe execution</td>
<td>Dan Beavin</td>
<td>09/26/2019</td>
<td>Defense Evasion</td>
<td>T1223 Compiled HTML File</td>
</tr>
<tr>
<td>Image Debuggers for Accessibility Features</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1015 Accessibility Features</td>
</tr>
<tr>
<td>Indirect Command Execution</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1202 Indirect Command Execution</td>
</tr>
<tr>
<td>Installing Custom Shim Databases</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1138 Application Shimming</td>
</tr>
<tr>
<td>Interactive AT Job</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Privilege Escalation</td>
<td>T1053 Scheduled Task</td>
</tr>
</tbody>
</table>

Continued on next page
Table 2 – continued from previous page

<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Scripts with UserInitMprLogon-Script</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1037 Logon Scripts</td>
</tr>
<tr>
<td>LSASS Memory Dumping</td>
<td>Tony Lambert</td>
<td>01/07/2019</td>
<td>Credential Access</td>
<td>T1003 Credential Dumping</td>
</tr>
<tr>
<td>LSASS Memory Dumping via Proc-Dump.exe</td>
<td>Tony Lambert</td>
<td>01/07/2019</td>
<td>Credential Access</td>
<td>T1003 Credential Dumping</td>
</tr>
<tr>
<td>Modification of Boot Configuration</td>
<td>Endgame</td>
<td>05/17/2019</td>
<td>Impact</td>
<td>T1490 Inhibit System Recovery</td>
</tr>
<tr>
<td>Modification of ld.so.preload</td>
<td>Tony Lambert</td>
<td>05/17/2019</td>
<td>Defense Evasion</td>
<td>T1055 Process Injection</td>
</tr>
<tr>
<td>Modifications of .bash_profile and .bashrc</td>
<td>Tony Lambert</td>
<td>01/10/2019</td>
<td>Persistence</td>
<td>T1156 .bash_profile and .bashrc</td>
</tr>
<tr>
<td>Mounting Hidden Shares</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Lateral Movement</td>
<td>T1077 Windows Admin Shares</td>
</tr>
<tr>
<td>Mshta Network Connections</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Execution</td>
<td>T1170 Mshta</td>
</tr>
<tr>
<td>Persistence via AppInit DLL</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence Privilege Escalation</td>
<td>T1103 AppInit DLLs</td>
</tr>
<tr>
<td>Persistence via NetSh Key</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1128 Netsh Helper DLL</td>
</tr>
<tr>
<td>Persistence via Screensaver</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1180 Screensaver</td>
</tr>
<tr>
<td>Registry Preparation of Event Viewer UAC Bypass</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Privilege Escalation</td>
<td>T1088 Bypass User Account Control</td>
</tr>
<tr>
<td>RegSvr32 Scriptlet Execution</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Execution</td>
<td>T1117 Regsvr32</td>
</tr>
<tr>
<td>SAM Dumping via Reg.exe</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Credential Access</td>
<td>T1003 Credential Dumping</td>
</tr>
<tr>
<td>Suspicious ADS File Creation</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1197 BITS Jobs</td>
</tr>
<tr>
<td>Suspicious Bitadmin Job via bitsadmin.exe</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1197 BITS Jobs</td>
</tr>
<tr>
<td>Suspicious Script Object Execution</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1117 Regsvr32</td>
</tr>
<tr>
<td>System Information Discovery</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1082 System Information Discovery</td>
</tr>
<tr>
<td>Unload Sysmon Filter Driver with fltmc.exe</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Defense Evasion</td>
<td>T1089 Disabling Security Tools</td>
</tr>
</tbody>
</table>

Continued on next page
### Table 2 – continued from previous page

<table>
<thead>
<tr>
<th>Analytic</th>
<th>Contributors</th>
<th>Updated</th>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account Creation</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Persistence</td>
<td>T1136 Create Account</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Credential Access</td>
<td></td>
</tr>
<tr>
<td>Volume Shadow Copy Deletion via VssAdmin</td>
<td>Endgame</td>
<td>05/17/2019</td>
<td>Impact</td>
<td>T1490 Inhibit System Recovery</td>
</tr>
<tr>
<td>Volume Shadow Copy Deletion via WMIC</td>
<td>Endgame</td>
<td>05/17/2019</td>
<td>Impact</td>
<td>T1490 Inhibit System Recovery</td>
</tr>
<tr>
<td>Windows Network Enumeration</td>
<td>Endgame</td>
<td>11/30/2018</td>
<td>Discovery</td>
<td>T1018 Remote System Discovery</td>
</tr>
</tbody>
</table>

### 1.4 Enterprise ATT&CK Matrix

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript .bash_profile and .bashrc</td>
<td>• Modifications for Privilege Elevation</td>
<td>• Access Token Manipulation</td>
<td>• Account Discovery</td>
<td>• Applied Deployment Software and Credential Discovery</td>
<td>• Audio Capture</td>
<td>• Automated Exfiltration</td>
<td>• Common Used Port</td>
<td>• Data Destruction</td>
<td></td>
</tr>
<tr>
<td>Initial Access</td>
<td>Executive Privilege</td>
<td>Defense Evasion</td>
<td>Credential Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Exfiltration</td>
<td>Command and Control</td>
<td>Impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------</td>
<td>-----------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>------------</td>
<td>-------------</td>
<td>---------------------</td>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Command Line Interface</td>
<td>Access Features</td>
<td>Image File Execution</td>
<td>BITS Jobs</td>
<td>Bash History</td>
<td>Suspicious BITS Job via min.exe (w)</td>
<td>Suspicious BITS Job via PowerShell (w)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suspect调试者 for Ac- cessibility Features (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>reDynamic Data Exchange</td>
<td>AppCert DLLs</td>
<td>SID-History Injection</td>
<td>AppCert DLLs Registry Modification (w)</td>
<td>Binary Padding</td>
<td>Brute Force</td>
<td>Browser Bookmark Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Clipboard Data</td>
<td>Data Encrypted for Impact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Continued on next page
<table>
<thead>
<tr>
<th>Table 3 – continued from previous page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Access</strong></td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>Spearphishing via Module Load</td>
</tr>
<tr>
<td>Spearphishing via Service</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access Discovery</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration Command and Control</th>
<th>Impact Supply Chain Compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply Chain Compromise</td>
<td>Graphic User Interface</td>
<td>Code Signing</td>
<td>Exploitation for Credential Access</td>
<td>Network Share Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Data from Network Shared Drive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Remote Desktop Protocol</td>
<td>Exfiltration Over Other Network Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Exfiltration Over Other Network Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Firmware Corruption</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Executable Persistence</th>
<th>Privilege Escala-</th>
<th>Defense Evasion</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection &amp; Exfiltration</th>
<th>Command &amp; Control</th>
<th>Impact</th>
<th>Trusted Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSASS Driver</td>
<td>Browser Extensions</td>
<td>Compile After Delivery</td>
<td>Forced Authentication</td>
<td>Password Policy Discovery</td>
<td>Remote Services</td>
<td>Data from Removable Media</td>
<td>Exfiltration Over Physical Medium</td>
<td>Domain Fronting</td>
<td>Inhibit System Recovery</td>
</tr>
<tr>
<td></td>
<td>• Suspicious File Creation via Browser Extensions (m, w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Privilege Escalation</th>
<th>Defense</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerShell</td>
<td>Change Default File Association</td>
<td>Compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Change Default File Association</td>
<td>compiled HTML File</td>
<td>Input Prompt</td>
<td>Peripheral Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithms</td>
<td>Network Denial of Service</td>
</tr>
</tbody>
</table>
### Table 3 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution of Existing Service</th>
<th>DLL Search Order Hijacking</th>
<th>Component Object Model Hijacking</th>
<th>Keychain Process Discovery</th>
<th>Shared Webroot</th>
<th>Man in the Browser</th>
<th>Multi-Stage Channels</th>
<th>Runtime Data Manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Dylib Hijacking</td>
<td>Control Panel Items</td>
<td>LLMNR NS Poisoning Control Panel Items</td>
<td>Process Discovery</td>
<td>Shared Content</td>
<td>Screen Capture</td>
<td>Multi-hop Proxy</td>
<td>Service Stop</td>
</tr>
<tr>
<td>Source</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 3 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Network Enumeration (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap</td>
<td>File System Tampering</td>
<td>DLL Side-Loading</td>
<td>Password Filter DLL</td>
<td>Process Discovery via Built-In Applications (l, m)</td>
<td>Multilayer Encryption</td>
<td>Transmitted Data Manipulation</td>
</tr>
<tr>
<td></td>
<td>System Permissions</td>
<td></td>
<td></td>
<td>Registration of a Password Filter DLL (w)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>File Permissions</td>
<td></td>
<td></td>
<td>Process Discovery via Windows Tools (w)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Execution</td>
<td>Hooking</td>
<td>Deobfuscation of Files or Information</td>
<td>Deobfuscation of Keys</td>
<td>System Information Discovery</td>
<td>System Information Discovery (I)</td>
<td>System Information Discovery (w)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encoding or Decoding Files via CertUtil (w)</td>
<td></td>
<td></td>
<td>• Enumeration of System Information (I)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Enumeration of System Information (w)</td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Executive Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery Lateral Movement</th>
<th>Collection Exfiltration and Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>• WMI Ex- ecution via Microsoft Office Application (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Remote Ex- ecution via WMIC (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Remote Management</td>
<td>Kernel Modules and Extensions</td>
<td><strong>Incoming Creation of Remote Kernel Module</strong></td>
<td><strong>Two-Factor Authentication Interception</strong></td>
<td><strong>System Network Connections Discovery</strong></td>
<td><strong>System Owner/User Discovery</strong></td>
<td><strong>Standard Application Layer Protocol</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Incoming Remote Power Shell Sessions</td>
<td>• Loading Kernel Modules with kextload</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(w)</td>
<td>(m)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial Access</td>
<td>Execution Persistence</td>
<td>Defense Evasion</td>
<td>Credential Access</td>
<td>Lateral Movement</td>
<td>Collection Exfiltration</td>
<td>Command and Control</td>
<td>Impact</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>-----------------</td>
<td>------------------------</td>
<td>--------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Launch Agent</td>
<td>Extra Window Memory Injection</td>
<td>System Service Discovery</td>
<td>System Time Discovery</td>
<td>Discovery of a Remote System’s Time (w)</td>
<td>Standard Non-Application Layer Protocol</td>
<td>Uncommonly Used Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch Daemon</td>
<td>File Deletion</td>
<td>System Time Discovery</td>
<td>System Time Discovery</td>
<td>Discovery of a Remote System’s Time (w)</td>
<td>Standard Non-Application Layer Protocol</td>
<td>Uncommonly Used Port</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 3 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Executable Persistence Privilege Escalation</th>
<th>Defense Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Job Scheduling&lt;br&gt;• Local Job Scheduling Paths (l, m)&lt;br&gt;• Local Job Scheduling Process (l, m)</td>
<td>File Permissions Modification&lt;br&gt;• Windows File Permissions Modification&lt;br&gt;• System Logical Offsets</td>
<td>Modify Existing Service&lt;br&gt;• Service Path Modification with sc.exe (w)</td>
<td>Gatekeeper Bypass&lt;br&gt;• Potential Gatekeeper Bypass (m)</td>
<td>Web Service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
</table>
| Netsh Helper DLL  •  
  *Persistence via NetSh Key (w)| Group Policy Modification | | | | | | | | |
| New Service | HISTCONTROL | | | | | | | | |

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Defense</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection &amp; Exfiltration</th>
<th>Command &amp; Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Application Startup</td>
<td>Hidden Files and Directories</td>
<td>Office Application Startup via Template File Modification (w)</td>
<td>Adding the Hidden File Attribute with via attrib.exe (w)</td>
<td>Path Interception</td>
<td>Hidden Users</td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 3 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port Monitors</strong></td>
<td><strong>Installation of Port Monitor (w)</strong></td>
<td><strong>Hidden Window</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Rc.common</strong></td>
<td><strong>Modification of rc.common Script (m)</strong></td>
<td><strong>Indicator Blocking</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Re-opened Applications</strong></td>
<td><strong>Resumed Application on Reboot (m)</strong></td>
<td><strong>Indicator Removal from Tools</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
## Table 3 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution of Persistent Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration and Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Run Keys / Startup Folder</td>
<td>Indicator Removal on Host</td>
<td>Delete Volume USN Journal with fsutil (v)</td>
<td>Host Artifact Deletion (v)</td>
<td>Clearing Windows Event Logs with wevtutil (v)</td>
<td>Continued on next page</td>
</tr>
<tr>
<td>Initial Access</td>
<td>Execution Persistence</td>
<td>Defense</td>
<td>Credential Discovery</td>
<td>Lateral Movement</td>
<td>Collection Exfiltration</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------</td>
<td>---------</td>
<td>-----------------------</td>
<td>------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Screensaver</td>
<td>Direct Command Execution</td>
<td>Indirect Command Execution</td>
<td>Security Support Provider</td>
<td>Root Certificate</td>
<td>InstallUtil Execution</td>
</tr>
<tr>
<td>Screensaver</td>
<td>Persistence via Screen saver (w)</td>
<td>Indirect Command Execution</td>
<td>Security Support Provider</td>
<td>InstallRootCertificate</td>
<td></td>
</tr>
<tr>
<td>Security Support Provider</td>
<td>Installation of Security Support Provider (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Registry Permissions Weakness</td>
<td>InstallUtil Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shortcut Modification</td>
<td>LC_MAIN Hijacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Startup Items</td>
<td>Launchctl</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Firmware</td>
<td>Masquerading</td>
<td>Processes Running with Unusual Extensions (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Service</td>
<td>Modify Registry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creation of Modification of System Service (l)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Installation of Time Providers (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mshta Network Connections (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mshta</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Shell</td>
<td>NTFS File Attributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Suspicious ADS File Creation (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Manage-</td>
<td>Network Share Con-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ment Instrumentation Event Sub-</td>
<td>nexion Removal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cription</td>
<td>• Disconnecting from Network Shares with net.exe (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Winlogon Helper DLL</td>
<td>Obfuscated Files or Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution of Privileged Services</th>
<th>Defense</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection and Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plist Modification</td>
<td>Port Knocking</td>
<td>Process Doppleganging</td>
<td>Process Hollowing</td>
<td>Process Injection</td>
<td>Modification of ld.so.preload</td>
<td>Unusual Child Process</td>
</tr>
<tr>
<td>• Plist Modification</td>
<td>• Port Knocking</td>
<td>• Process Doppleganging</td>
<td>• Unusual Child Process</td>
<td>• Modification of ld.so.preload</td>
<td>• Unusual Child Process</td>
<td>—</td>
</tr>
<tr>
<td>(m)</td>
<td></td>
<td></td>
<td>(w)</td>
<td>(l)</td>
<td>(w)</td>
<td>—</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redundant Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regsvcs/Regasm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regsvr32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Suspicious Script Object Execution (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rootkit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rundll32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP and Trust Provider Hijacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scripting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signed Binary Proxy Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signed Script Proxy Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Proxied Execution via Signed Scripts (w)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 3 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Executive/Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Software Packaging</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Space after Filename</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Processes with Trailing Spaces (I, m)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Template Injection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Timestomp</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Trusted Developer Utilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Valid Accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Virtualization/Sandbox Evasion</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>XSL Script Processing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

120 Chapter 1. Next Steps
1.4. Enterprise ATT&CK Matrix
### 1.4.1 Linux

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Executable</th>
<th>Privileged escalation</th>
<th>Defense Evasion</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>Command Line Interface</td>
<td>Bash_padding</td>
<td>Bash History</td>
<td>Account Discovery</td>
<td>Application Deployment Software</td>
<td>Audio Capture</td>
<td>Automatic Exfiltration</td>
<td>Common Used Port</td>
<td>Data Destruction</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Exploit for Client Execution</td>
<td>Libtoolkit</td>
<td>Setuid and Setgid</td>
<td>Clear Command History</td>
<td>Brute Force</td>
<td>Browser Bookmark Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Auto Collection</td>
<td>Encrypted for Impact</td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Graphic User Interface</td>
<td>Sudo</td>
<td>Compile After Delivery</td>
<td>Credential Dumping</td>
<td>aFile and Directory Discovery</td>
<td>Remote Services</td>
<td>Clipboard Data</td>
<td>Data Encrypted</td>
<td></td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Create Account</td>
<td>Sudo Caching</td>
<td>Disabling Security Tools</td>
<td>Credential in Files</td>
<td>aNetwork Service Scan- ning</td>
<td>Network Service Scanning</td>
<td>Data Staged</td>
<td>Data Trans fer Limits</td>
<td>Custom Command and Control Protocol</td>
</tr>
</tbody>
</table>

122 Chapter 1. Next Steps
# 1.4.2 macOS

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Executive Persistence Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript .login and .bashrc</td>
<td>Bash Profiling</td>
<td>Bash History</td>
<td>Account Discovery</td>
<td>Application Deploymen</td>
<td>Automated</td>
<td>Compressed</td>
</tr>
<tr>
<td>Exploits Public-Facing Application</td>
<td>Command-Line Interface</td>
<td>Browser Extensions</td>
<td>Setuid and Setgid</td>
<td>Clear Command History</td>
<td>Brute Force</td>
<td>Automated</td>
<td>Compressed</td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Exploit for Client Execution</td>
<td>Create Account</td>
<td>Sudo Code Signing</td>
<td>Credential Dumping</td>
<td>Browser Bookmark Discovery</td>
<td>Logon Scripts</td>
<td>Clipboard Data</td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>User Interface</td>
<td>Dylib Hijacking</td>
<td>Sudo Caching</td>
<td>Compile After Delivery</td>
<td>Credential in Files</td>
<td>Remote Services</td>
<td>Data Staged</td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>Kernel Module</td>
<td>Disabling Exploitation</td>
<td>Network Services</td>
<td>SSH Hijacking</td>
<td>Data from Memory</td>
<td>Exfiltration</td>
<td>Custom Crypto</td>
</tr>
</tbody>
</table>

EQL Analytics Library
### 1.4.3 Windows

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execute</th>
<th>Persistent Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Disability Management</th>
<th>Lateral Privilege Escalation</th>
<th>Forensics</th>
<th>Command and Control Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>Command Line Interface</td>
<td>Access Token Exploitation for Privilege Elevation</td>
<td>Access Token Manipulation</td>
<td>Account Discovery</td>
<td>Application Deployment</td>
<td>Application Deployment</td>
<td>Audio Capture</td>
<td>Audio Capture via SoundRecorder</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exploit Public-Facing Application

<table>
<thead>
<tr>
<th>Dynamic Data Exchange</th>
<th>AppCert DLLs</th>
<th>Image File Execution</th>
<th>BITS Jobs</th>
<th>Brute Force</th>
<th>Application Component Collection</th>
<th>Data Compressed</th>
<th>Communication Through Removable Media Encrypted for Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Constrained via Command-line</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 4 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Escalation</th>
<th>Defense</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Additions</td>
<td>Execu-</td>
<td>through API</td>
<td>nAppInit DLLs</td>
<td>SID-His-</td>
<td>Binary Padding</td>
<td>Creden-</td>
<td>Exploit</td>
<td>Pullboard</td>
<td>Data</td>
<td>Encrypted</td>
<td>Defacement</td>
</tr>
<tr>
<td></td>
<td>tion</td>
<td></td>
<td>tory DLL</td>
<td>tory DLL</td>
<td></td>
<td>tial Vault</td>
<td>of Re-</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DLL</td>
<td>mote</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spearphishing Attachment</td>
<td>Application Shimming through Module Load</td>
<td>Bypass User Account Control</td>
<td>Installing Custom Shim Databases</td>
<td>Domain Trust Discovery</td>
<td>Data Staged</td>
<td>Data Transfer Size Limits</td>
<td>Custom Command and Control Protocol</td>
<td>Disk Content Wipe</td>
</tr>
<tr>
<td></td>
<td>• Installing Custom Shim Databases</td>
<td>• Bypass UAC via CMSTP</td>
<td>• Searching for Passwords in Files</td>
<td>• Domain Trust Discovery via Nttest.exe</td>
<td>• Domain Trust Discovery from Registry</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing links for Client Execution</td>
<td>Authentication Package</td>
<td>CMSTP</td>
<td>• LSA Authentication Package</td>
<td>• LSA Authentication Package</td>
<td>• LSA Authentication Package</td>
<td>• LSA Authentication Package</td>
<td>• LSA Authentication Package</td>
<td>• LSA Authentication Package</td>
</tr>
<tr>
<td></td>
<td>• CMSTP.exe</td>
<td>• CMSTP.exe</td>
<td>• CMSTP.exe</td>
<td>• CMSTP.exe</td>
<td>• CMSTP.exe</td>
<td>• CMSTP.exe</td>
<td>• CMSTP.exe</td>
<td>• CMSTP.exe</td>
</tr>
<tr>
<td>Spearphishing via Service Interface</td>
<td>Code Signing</td>
<td>Exploits for Credential Access</td>
<td>Network Service Scanning</td>
<td>Pass the Ticket</td>
<td>Data from Local System</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Custom Cryptographic Protocol</td>
<td>Endpoint Denial of Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Network Service Scanning</td>
<td>• Network Service Scanning via Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Compile After Delivery</td>
<td>Forced Authentication</td>
<td>Network Share Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Data from Network Shared Drive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Executive</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted Relationship</strong></td>
<td>PowerShell</td>
<td>Change Default File Association</td>
<td>Compiled HTML File</td>
<td>Input Prompt</td>
<td>Password Policy Discovery</td>
<td>Remote Services</td>
<td>Data from Removable Media</td>
<td>Exfiltration Over Physical Medium</td>
<td>Inhibit System Recovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Change Default File Association</td>
<td>• HH.exe execution</td>
<td></td>
<td></td>
<td></td>
<td>• Removable Terminal Sessions</td>
<td></td>
<td>• Modification of Boot Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Volume Shadow Copy Deletion via VssAdm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Volume Shadow Copy Deletion via WMIC</td>
</tr>
<tr>
<td><strong>Scheduled Task</strong></td>
<td>Create Account Creation of User Scheduled Task Creation with atontask</td>
<td>Compiled Kerberos Firmware</td>
<td>Device Discovery</td>
<td>Replication Through Removable Media</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Domain Generation Algorithm</td>
<td>Network Denial of Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create Account Creation</td>
<td></td>
<td></td>
<td></td>
<td>• Access of Outlook Email Archives</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 4 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistent Privilege Escalation</th>
<th>Defense</th>
<th>Credential discovery</th>
<th>Lateral Movement</th>
<th>Collection &amp; Exfiltration</th>
<th>Command &amp; Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Execution</td>
<td>DLL Search Order Hijacking</td>
<td>DLL Search Order Hijacking</td>
<td>Component Object Model Hijacking</td>
<td>CMN NS Poisoning and Relay</td>
<td>LLMNR/NBT Poisoning and Relay</td>
<td>Shared Webroot</td>
<td>Input Capture</td>
<td>Fallback Channels</td>
</tr>
<tr>
<td>Third-party Software</td>
<td>External Remote Services</td>
<td>Control Panel Items</td>
<td>Network Sniffing</td>
<td>Process Discovery</td>
<td>Taint Shared Content</td>
<td>Man in the Browser</td>
<td>Multi-stage Channels</td>
<td>Runtime Data Manipulation</td>
</tr>
<tr>
<td>Initial Access</td>
<td>Execution</td>
<td>Defense</td>
<td>Privilege Escalation</td>
<td>Defense</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command and Control</td>
<td>Impact</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
<td>---------</td>
<td>----------------------</td>
<td>---------</td>
<td>------------------</td>
<td>------------</td>
<td>---------------------</td>
<td>--------</td>
</tr>
<tr>
<td>User Execution</td>
<td>File System Permissions Weakness</td>
<td>DCShadow Password Filter DLL</td>
<td>Query Registry</td>
<td>Windows Admin Shares</td>
<td>Screen Capture</td>
<td>Multihop Proxy</td>
<td>Service Stop</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Registration of a Password Filter DLL</td>
<td>• Mounting Hidden Shares</td>
<td>• Mounting Hidden Shares with net.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Executive Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection &amp; Exfiltration</th>
<th>Command and Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>• WMI Execution via Microsoft Office Application</td>
<td></td>
<td></td>
<td>• Windows Network Enumeration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Remote E-Ex-ecution via WMIC</td>
<td></td>
<td></td>
<td>• Remote System Discovery Commands</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Remote Management</td>
<td>Hypervisor</td>
<td>Deobfuscation/Decompression of Files or Information</td>
<td></td>
<td>Security Software Discovery</td>
<td></td>
<td></td>
<td>Multilayer Encryption</td>
</tr>
<tr>
<td>• Incoming Remote Power Shell Sessions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Manipulation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encrypted or Decoding Files via CertUtil</td>
<td></td>
<td>Process Discovery via Windows Tools</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify Existing Service</td>
<td></td>
<td>Disabling Security Tools</td>
<td></td>
<td>System Information Discovery</td>
<td></td>
<td></td>
<td>Remote Access Tools</td>
</tr>
<tr>
<td>• Service Path Modification with sc.exe</td>
<td></td>
<td>• Unload System Filter Driver with fltm.exe</td>
<td></td>
<td>Enumeration of System Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• System Information Discovery</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 4 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery Lateral Movement</th>
<th>Collection Exfiltration and Control</th>
<th>Command and Impact</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netsh Helper DLL</td>
<td>• Persistence via NetSh Key</td>
<td>Execution Guardrails</td>
<td>System Network Configuration Discovery</td>
<td>• Discovery of Network Environment via Built-in Tools</td>
<td>Remote File Copy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery Lateral Movement</th>
<th>Collection Exfiltration and Control</th>
<th>Command and Impact</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Service</td>
<td>Exploitation for Defense Evasion</td>
<td>System Network Connections Discovery</td>
<td>• Enumeration of Mounted Shares</td>
<td>Standard Application Layer Protocol</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Persistence</th>
<th>Privilege Escala-</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Applica-</td>
<td>Extra Win-</td>
<td>System Owner/</td>
<td>System Owner/</td>
<td>Standard Crypto-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tion Startup</td>
<td>dows Memory</td>
<td>User Discovery</td>
<td>and User Dis-</td>
<td>tographic Proto-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office Appli-</td>
<td>Injection</td>
<td>cov-</td>
<td>cove-</td>
<td>col</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cation Startup</td>
<td>via Tem-</td>
<td>ry</td>
<td>ry</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>via Tem-</td>
<td>plate File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>plate File</td>
<td>Modifi-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modification</td>
<td>cation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office Appli-</td>
<td>Extra Win-</td>
<td>System Owner/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cation Startup</td>
<td>dows Memory</td>
<td>User Discovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>via Tem-</td>
<td>Injection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>plate Reg-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>istry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path Inter-</td>
<td>File Dele-</td>
<td>System Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ception</td>
<td>tion</td>
<td>Discovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution of Persistent Privilege Escalation</th>
<th>Defense</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Monitors</td>
<td>File Permissions Modification</td>
<td>System Time Discovery</td>
<td>•</td>
<td>Uncommonly Used Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Installation of Port Monitor</td>
<td>• Windows File Permissions Modification</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registry Run Keys / Startup Folder</td>
<td>System Logarithmic Offsets</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Web Service</td>
<td></td>
</tr>
<tr>
<td>• Registry Persistence via Run Keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Registry Persistence via Shell Folders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial Access</td>
<td>Execution Persistence</td>
<td>Defense Evasion</td>
<td>Credential Discovery</td>
<td>Lateral Movement</td>
<td>Collection Exfiltration</td>
<td>Command and Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------</td>
<td>----------------</td>
<td>---------------------</td>
<td>-----------------</td>
<td>------------------------</td>
<td>---------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screensaver</td>
<td>Group Policy Modifica-</td>
<td>Security Sup-</td>
<td>Hidden Files and D-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>tion via Screen-</td>
<td>port Provider</td>
<td>ecrories</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>saver</td>
<td></td>
<td>• Installation of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provider</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Adding the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hidden File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Attribute with</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>attributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>via attribexe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Reg-</td>
<td>Indicator Blocking</td>
<td>Security Sup-</td>
<td>Indicator Removal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>istry Per-</td>
<td></td>
<td>port Provider</td>
<td>from Tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mis-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weakness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shortcut Mod-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 4 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution of Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection and Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Firmware</td>
<td>Indicator Removal on Host</td>
<td>* Delete Volume USN Journal with fsutil</td>
<td>* Host Artifact Deletion</td>
<td>* Clearing Windows Event Logs with wevtutil</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Providers</td>
<td>* Installation of Time Providers</td>
<td>Indirect Command Execution</td>
<td>* Indirect Command Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 4 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Defense Evasion</th>
<th>Credential Discovery</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Shell</td>
<td>Install Root Certificate • Root Certificate Install</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Manage-</td>
<td>InstallUtil • InstallUtil Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ment Instrumentation Event Subscription</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Winlogon Helper DLL • Registration of Winlogon Helper DLL</td>
<td>Masquerading • Processes Running with Unusual Extensions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modify Registry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
Table 4 – continued from previous page

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mshta</td>
<td>Mshta</td>
<td>Mshta</td>
<td>Mshta</td>
<td>Mshta</td>
<td>Mshta</td>
<td>Mshta</td>
</tr>
<tr>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
</tr>
<tr>
<td>Connections</td>
<td>Connections</td>
<td>Connections</td>
<td>Connections</td>
<td>Connections</td>
<td>Connections</td>
<td>Connections</td>
</tr>
<tr>
<td>NTFS File Attributes</td>
<td>NTFS File Attributes</td>
<td>NTFS File Attributes</td>
<td>NTFS File Attributes</td>
<td>NTFS File Attributes</td>
<td>NTFS File Attributes</td>
<td>NTFS File Attributes</td>
</tr>
<tr>
<td>Suspicious ADS File Creation</td>
<td>Suspicious ADS File Creation</td>
<td>Suspicious ADS File Creation</td>
<td>Suspicious ADS File Creation</td>
<td>Suspicious ADS File Creation</td>
<td>Suspicious ADS File Creation</td>
<td>Suspicious ADS File Creation</td>
</tr>
<tr>
<td>Disconnecting from Network Shares with net.exe</td>
<td>Disconnecting from Network Shares with net.exe</td>
<td>Disconnecting from Network Shares with net.exe</td>
<td>Disconnecting from Network Shares with net.exe</td>
<td>Disconnecting from Network Shares with net.exe</td>
<td>Disconnecting from Network Shares with net.exe</td>
<td>Disconnecting from Network Shares with net.exe</td>
</tr>
<tr>
<td>Obfuscated Files or Information</td>
<td>Obfuscated Files or Information</td>
<td>Obfuscated Files or Information</td>
<td>Obfuscated Files or Information</td>
<td>Obfuscated Files or Information</td>
<td>Obfuscated Files or Information</td>
<td>Obfuscated Files or Information</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th></th>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unusual Child Process Injection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspicious Script Object Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rootkit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP and Trust Provider Hijacking Scripting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Signed Binary Proxy Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Signed Script Proxy Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Proxied Execution via Signed Scripts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software Packing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Template Injection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timestomp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trusted Developer Utilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid Accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virtualization/Sandbox Evasion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>XSL Script Processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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)
original_file_name OriginalFileName
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**
EQL Analytics Library

```

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  key
    registry_path  key
    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
• original_file_name
• 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 Resources

1.6.1 Blogs

- EQL’s Highway to Shell
- Getting Started with EQL
- EQL For the Masses
- Introducing EQL

1.6.2 Presentations

- BlackHat 2019: Fantastic Red-Team Attacks and How to Find Them (slides)
- BSIDES SATX 2019: The Hunter Games: How to Find the Adversary with EQL (slides)
- Circle City Con 2019: The Hunter Games: How to Find the Adversary with EQL (slides)
- Atomic Friday: Endgame on EQL (slides, notebook)
- MITRE ATT&CKcon: From Technique to Detection

1.6.3 Additional Resources

- Atomic Red Team
- Microsoft Sysmon
- MITRE ATT&CK™
- Event Query Language (docs, code)
- EQL Analytics Library (docs, code)

1.7 License

MIT License

Copyright (c) 2018 Endgame, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
EQL Analytics Library

**Note:** The Event Query Language has an AGPL License
Symbols

- `–file, -f`
  convert-data command line option, 4
  query command line option, 5
  survey command line option, 6
- `–format`
  convert-data command line option, 4
  query command line option, 5
  survey command line option, 6
- `–c`
  survey command line option, 6
- `–e <encoding>`
  convert-data command line option, 4
  query command line option, 5
  survey command line option, 6
- `–h`
  convert-data command line option, 4
  convert-query command line option, 5
  query command line option, 5
  survey command line option, 6
- `–s <data-source>, –source <data-source>`
  convert-data command line option, 4
  convert-query command line option, 5
  query command line option, 5
  survey command line option, 6

A

analytic-path [analytic-path, ...]
  survey command line option, 5

C

convert-data command line option
  –file, -f, 4
  –format, 4
  –e <encoding>, 4
  –h, 4
  –s <data-source>, –source <data-source>, 4
  output-json-file, 4
convert-query command line option
  –h, 5
  –s <data-source>, –source <data-source>, 5
eql-query, 4

E

eql-query
  convert-query command line option, 4

I

input-query
  query command line option, 5

O

output-json-file
  convert-data command line option, 4

Q

query command line option
  –file, -f, 5
  –format, 5
  –e <encoding>, 5
  –h, 5
  –s <data-source>, –source <data-source>, 5
input-query, 5

S

survey command line option
  –file, -f, 6
  –format, 6
  –c, 6
  –e <encoding>, 6
  –h, 6
  –s <data-source>, –source <data-source>, 6
analytic-path [analytic-path, ...], 5