CAR-2013-05-002: Suspicious Run Locations

Submission Date: 2013/05/07
Update Date:
Information Domain: Host
Data Subtypes: Process
Analytic Type: TTP
Applicable Platforms: Windows
Contributors: MITRE

In Windows, files should never execute out of certain directory locations. Any of these locations may exist for a variety of reasons, and executables may be present in the directory but should not execute. As a result, some defenders make the mistake of ignoring these directories and assuming that a process will never run from one. There are known TTPs that have taken advantage of this fact to go undetected. This fact should inform defenders to monitor these directories more closely, knowing that they should never contain running processes.

Monitors the directories

- `*:\RECYCLER`
- `*:\SystemVolumeInformation`
- `%systemroot%\Tasks`
- `%systemroot%\debug`

ATT&CK Detections

Technique	Subtechnique(s)	Tactic(s)	Level of Coverage
Masquerading	N/A	Defense Evasion	Low

D3FEND Techniques

ID	Name
D3-PSA	Process Spawn Analysis

Data Model References

Object	Action	Field
process	create	image_path

Implementations

Pseudocode

The RECYCLER and SystemVolumeInformation directories will be present on every drive. Replace %systemroot% and %windir% with the actual paths as configured by the endpoints.

```
processes = search Process:Create
suspicious_locations = filter process where (
 image_path == "*:\RECYCLER\*" or
 image_path == "*:\SystemVolumeInformation\*" or
 image_path == "%windir%\Tasks\*" or
 image_path == "%systemroot%\debug\*"
)
output suspicious_locations
```

Dnif, Sysmon native

DNIF version of the above pseudocode.

```
_fetch * from event where $LogName=WINDOWS-SYSMON AND $EventID=1 AND $Process=regex(.*(\:\\recycler\\|\:\\systemvolumeinfor
```

Sigma

Sigma version of the above pseudocode, with some modifications.

Logpoint, LogPoint native

LogPoint version of the above pseudocode.

```
norm_id=WindowsSysmon event_id=1 image IN ["*:\RECYCLER\*", "*:\SystemVolumeInformation\*", "C:\Windows\Tasks\*", "C:\Windc
```

Unit Tests

Test Case 1

Configurations: Windows 7

- Typically %systemroot% is C:\Windows but you can check this by running “echo %systemdrive%” at the command line.
- Copy C:\Windows\system32\notepad to C:\Windows\Tasks.
- Run notepad. The analytic should fire.
- Delete the executable to clean up from the test.

```
copy C:\windows\system32\notepad.exe C:\windows\tasks
start C:\windows\tasks\notepad.exe
del C:\windows\tasks\notepad.exe
```