 Files

efa17a6

Q

Go to file

> Campaigns

> Collection

> Command and Control

C2-NamedPipe.md

Connection to Rare DNS Hosts....

DNSPattern [Nobelium].md

Device network events w low co...

EncodedDomainURL [Nobelium]...

Tor.txt

c2-bluekeep.md

check-for-shadowhammer-activ...

python-use-by-ransomware-m...

recon-with-rundll.md

reverse-shell-ransomware-maco...

> Credential Access

> Defense evasion

> Delivery

> Discovery

> Email Queries

> Execution

> Exfiltration

> Exploits

> Fun

> General queries

> Impact

> Initial access

> Lateral Movement

> M365-PowerBi Dashboard

> Network

> Notebooks

> Persistence


> Privilege escalation


> Protection events


> Ransomware

> TVM




Microsoft-365-Defender-Hunting-Queries / Command and Control / C2-NamedPipe.md



 Iveco Update C2-NamedPipe.md19253ac · 3 years ago

 History

PreviewCodeBlame97 lines (87 loc) · 6.6 KB

Raw








Detects malicious SMB Named Pipes (used by common C2 frameworks)

Detects the creation of a [named pipe](#) used by known APT malware.

Query

```
// maximum lookback time
let minTimeRange = ago(7d);
// this is what should be constantly tweaked with default C2 framework n
let badPipeNames = pack_array(
    '\\psexec', // PSexec default pi
    '\\paexec', // PSexec default pi
    '\\remcom', // PSexec default pi
    '\\csexec', // PSexec default pi
    '\\isapi_http', // Uroburos Malware |
    '\\isapi_dg', // Uroburos Malware |
    '\\isapi_dg2', // Uroburos Malware |
    '\\sdlrpc', // Cobra Trojan Name
    '\\ahexec', // Sofacy group malw
    '\\winsession', // Wild Neutron APT |
    '\\lsassw', // Wild Neutron APT |
    '\\46a676ab7f179e511e30dd2dc41bd388', // Project Sauron ht
    '\\9f81f59bc58452127884ce513865ed20', // Project Sauron ht
    '\\e710f28d59aa529d6792ca6ff0ca1b34', // Project Sauron ht
    '\\rpchlp_3', // Project Sauron ht
    '\\NamePipe_MoreWindows', // Cloud Hopper Anne
    '\\pcheap_reuse', // Pipe used by Equa
    '\\gruntsvc', // Covenant default
    '\\583da945-62af-10e8-4902-a8f205c72b2e', // SolarWinds SUNBUR
    '\\bizkaz', // Snatch Ransomware
    '\\atctl', // https://www.virus
    '\\userpipe', // ruag apt case
    '\\iehelper', // ruag apt case
    '\\sdlrpc', // project cobra htt
    '\\comnap', // https://www.gdata
    '\\lsadump', // Cred Dump-Tools N
    '\\cachedump', // Cred Dump-Tools N
    '\\wceservicepipe', // Cred Dump-Tools N
    '\\jaccdpqnvbrrxlaf', // PoshC2 default na
    '\\svcctl', // CrackMapExec defa
    '\\csexecsvc', // CSEXEC default na
    '\\status_', // CS default named
    '\\MSSE-', // CobaltStrike defa
    '\\status_', // CobaltStrike defa
    '\\msagent_', // (target) CobaltSt
    '\\postex_ssh_', // CobaltStrike defa
    '\\postex_', // CobaltStrike defa
```

Page 1 of 3

- >  Troubleshooting
- >  Webcasts
-  .gitignore
-  00-query-submission-template.md
-  CODE_OF_CONDUCT.md
-  LICENSE
-  MTPAHCheatSheetv01-dark.pdf

```
'\\Posh' // PoshC2 default na
);
DeviceEvents
| where ActionType == "NamedPipeEvent" and Timestamp > minTimeRange
| extend ParsedFields=parse_json(AdditionalFields)
| where ParsedFields.FileOperation == "File created"
| where ParsedFields.PipeName has_any (badPipeNames)
| project Timestamp, ActionType, DeviceName, InitiatingProcessAccountDom
```

Category

This query can be used to detect the following attack techniques and tactics ([see MITRE ATT&CK framework](#)) or security configuration states.

Technique, tactic, or state	Covered? (v=yes)	Notes
Initial access		
Execution		
Persistence		
Privilege escalation		
Defense evasion		
Credential Access		
Discovery		
Lateral movement		
Collection		
Command and control	v	
Exfiltration		
Impact		
Vulnerability		
Misconfiguration		
Malware, component		

Contributor info

Contributor: [@xknow_infosec](#)

This detection is a summary of knowledge already known. Credits only to original authors. Defender for Endpoint lately just added a new ActionType for SMB named pipes (NamedPipeEvent), which would allow new equal usecases now based on the same telemetry (for example replicating all Sysmon EventID 17/18 detections).

Original Authors / Credits / Ressources:

- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/pipe_created/sysmon_psexec_pipes_artifacts.yml
- https://drive.google.com/file/d/1IKya3_mLnR3UQuCoiYruO3qgu052_iS_/view
- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/pipe_created/sysmon_mal_namedpipes.yml
- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/pipe_created/sysmon_mal_cobaltstrike.yml
- <https://twitter.com/d4rksystem/status/1357010969264873472>
- <https://labs.f-secure.com/blog/detecting-cobalt-strike-default-modules-via-named-pipe-analysis/>
- [SigmaHQ/sigma#253](#)

- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/pipe_created/sysmon_cred_dump_tools_named_pipes.yml
- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/pipe_created/sysmon_apr_turla_namedpipes.yml
- <https://twitter.com/rpargman/status/1359961601160351744>