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 names, sear
let badPipeNames = pack_array(
    '\\psexec',                                    // PSexec default pipe
    '\\paexec',                                    // PSexec default pipe
    '\\remcom',                                    // PSexec default pipe
    '\\csexec',                                    // PSexec default pipe
    '\\isapi_http',                                // Uroburos Malware Named Pipe
    '\\isapi_dg',                                   // Uroburos Malware Named Pipe
    '\\isapi_dg2',                                  // Uroburos Malware Named Pipe
    '\\sdlrpc',                                     // Cobra Trojan Named Pipe htt
    '\\ahexec',                                     // Sofacy group malware
    '\\winsession',                                 // Wild Neutron APT malware ht
    '\\lsassw',                                     // Wild Neutron APT malware ht
    '\\46a676ab7f179e511e30dd2dc41bd388',           // Project Sauron https://goo.
    '\\9f81f59bc58452127884ce513865ed20',           // Project Sauron https://goo.
    '\\e710f28d59aa529d6792ca6ff0ca1b34',           // Project Sauron https://goo.
    '\\rpchlp_3',                                   // Project Sauron https://goo.
    '\\NamePipe_MoreWindows',                       // Cloud Hopper Annex B https:
    '\\pcheap_reuse',                               // Pipe used by Equation Group
    '\\gruntsvc',                                   // Covenant default named pipe
    '\\583da945-62af-10e8-4902-a8f205c72b2e',       // SolarWinds SUNBURST malware
    '\\bizkaz',                                     // Snatch Ransomware https://t
    '\\atctl',                                      // https://www.virustotal.com/
    '\\userpipe',                                   // ruag apt case
    '\\iehelper',                                   // ruag apt case
    '\\sdlrpc',                                     // project cobra https://www.g
    '\\comnap',                                     // https://www.gdatasoftware.c
    '\\lsadump',                                    // Cred Dump-Tools Named Pipes
    '\\cachedump',                                  // Cred Dump-Tools Named Pipes
    '\\wceservicepipe',                             // Cred Dump-Tools Named Pipes
    '\\jaccdpqnvbrrxlaf',                           // PoshC2 default named pipe
    '\\svcctl',                                     // CrackMapExec default named
    '\\csexecsvc'                                   // CSEXEC default named pipe
    '\\status_',                                    // CS default named pipes http
    '\\MSSE-',                                      // CobaltStrike default named
    '\\status_',                                    // CobaltStrike default named
    '\\msagent_',                                   // (target) CobaltStrike defau
    '\\postex_ssh_',                                // CobaltStrike default named
    '\\postex_',                                    // CobaltStrike default named
    '\\Posh'                                        // PoshC2 default named pipe
);
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, InitiatingProcessAccountDomain, Initi
```

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/1lKya3_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_apt_turla_namedpipes.yml
- https://twitter.com/rpargman/status/1359961601160351744