ElastAlert: Persistence via Startup Folder

1 message

<rangammabokka46@gmail.com> Sat, May 24, 2025 at 7:13 PM
Reply-to: rangammabomma46@gmail.com
To: rangammabomma46@gmail.com

ðŸ"' Persistence Detected

âžˆ Host: {host.name}
âžˆ User: {user.name}
âžˆ Event ID: {event.code}
âžˆ Path: {file.path}

At least 1 events occurred between 2025-05-24 18:51 India Standard Time and 2025-05-24 18:56 India Standard Time

@timestamp: 2025-05-24T13:26:49.394Z
_id: KdF5ApcBfXkZTUU6mPJO
_index: .ds-winlogbeat-8.10.2-2025.05.14-000001
agent: {
"ephemeral_id": "5a79e404-042a-4cf1-888f-502ab2c43c2c",
"id": "e5e3a761-acc3-41a2-88c5-ee2b2b236970",
"name": "Viticm-SOC",
"type": "winlogbeat",
"version": "8.10.2"
}
ecs: {
"version": "1.12.0"
}
event: {
"action": "Process Create (rule: ProcessCreate)",
"category": [
"process"
],
"code": "1",
"created": "2025-05-24T13:26:52.547Z",
"ingested": "2025-05-24T13:26:52.742809700Z",
"kind": "event",
"module": "sysmon",
"provider": "Microsoft-Windows-Sysmon",
"type": [
"start"
]
}
host: {
"architecture": "x86_64",
"hostname": "viticm-soc",
"id": "7e25c1a1-4745-47c6-abe9-ec7f50bf1d98",
"ip": [
"fe80::2674:6aaf:881:b09b",
"192.168.52.131"
],
"mac": [
"00-0C-29-C5-7F-10"
],
"name": "viticm-soc",
"os": {
"build": "19045.5854",
"family": "windows",
"kernel": "10.0.19041.5848 (WinBuild.160101.0800)",
"name": "Windows 10 Home",
"platform": "windows",
"type": "windows",
"version": "10.0"
}
}
log: {
"level": "information"

}
message: Process Create:
RuleName: -
UtcTime: 2025-05-24 13:26:49.394
ProcessGuid: {7e25c1a1-c919-6831-ff00-000000002800}
ProcessId: 7068
Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
FileVersion: 136.0.3240.76
Description: Microsoft Edge
Product: Microsoft Edge
Company: Microsoft Corporation
OriginalFileName: msedge.exe
CommandLine: "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store
.mojom.AssetStoreService --lang=en-US --service-sandbox-type=asset_store_service --no-pre-read-main-dll --skip-read-main-dll --
field-trial-handle=2384,i,5386439097223761735,9916251049940614 06,262144 --variations-seed-version --mojo-platform-channel-
handle=5400 /prefetch:8
CurrentDirectory: C:\Program Files (x86)\Microsoft\Edge\Application\136.0.3240.76\
User: VITICM-SOC\ranga
LogonGuid: {7e25c1a1-c666-6831-ce25-040000000000}
LogonId: 0x425CE
TerminalSessionId: 1
IntegrityLevel: Low
Hashes: MD5=521170F343FC5A4E725232663AEF57C0,SHA256=014FE0D805E6255B8BD7B9FAF1A50B847208B551F90536
E92640ED9E8204A7B4,IMPHASH=23FF41140CBD1050F401744A4BF949D3
ParentProcessGuid: {7e25c1a1-c6a1-6831-7700-000000002800}
ParentProcessId: 5508
ParentImage: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
ParentCommandLine: "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start
ParentUser: VITICM-SOC\ranga
num_hits: 20
num_matches: 20
process: {
  "args": [
    "C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe",
    "--type=utility",
    "--utility-sub-type=asset_store.mojom.AssetStoreService",
    "--lang=en-US",
    "--service-sandbox-type=asset_store_service",
    "--no-pre-read-main-dll",
    "--skip-read-main-dll",
    "--field-trial-handle=2384,i,5386439097223761735,9916251049940614 06,262144",
    "--variations-seed-version",
    "--mojo-platform-channel-handle=5400",
    "/prefetch:8"
  ],
  "args_count": 11,
  "command_line": "\"C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe\" --type=utility --utility-sub-
type=asset_store.mojom.AssetStoreService --lang=en-US --service-sandbox-type=asset_store_service --no-pre-read-main-dll --skip-
read-main-dll --field-trial-handle=2384,i,5386439097223761735,9916251049940614 06,262144 --variations-seed-version --mojo-
platform-channel-handle=5400 /prefetch:8",
  "entity_id": "{7e25c1a1-c919-6831-ff00-000000002800}",
  "executable": "C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe",
  "hash": {
    "md5": "521170f343fc5a4e725232663aef57c0",
    "sha256": "014fe0d805e6255b8bd7b9faf1a50b847208b551f90536e92640ed9e8204a7b4"
  },
  "name": "msedge.exe",
  "parent": {
    "args": [
      "C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe",
      "--no-startup-window",
      "--win-session-start"
    ],
    "args_count": 3,
    "command_line": "\"C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe\" --no-startup-window --win-session-
start",
    "entity_id": "{7e25c1a1-c6a1-6831-7700-000000002800}",
    "executable": "C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe",
    "name": "msedge.exe",
    "pid": 5508
  },
  "pe": {
    "company": "Microsoft Corporation",
    "description": "Microsoft Edge",

```
      "file_version": "136.0.3240.76",
      "imphash": "23ff41140cbd1050f401744a4bf949d3",
      "original_file_name": "msedge.exe",
      "product": "Microsoft Edge"
    },
    "pid": 7068,
    "working_directory": "C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\136.0.3240.76\\"
}
related: {
    "hash": [
      "014fe0d805e6255b8bd7b9faf1a50b847208b551f90536e92640ed9e8204a7b4",
      "521170f343fc5a4e725232663aef57c0",
      "23ff41140cbd1050f401744a4bf949d3"
    ],
    "user": [
      "ranga"
    ]
}
user: {
    "domain": "VITICM-SOC",
    "id": "S-1-5-18",
    "name": "ranga"
}
winlog: {
    "api": "wineventlog",
    "channel": "Microsoft-Windows-Sysmon/Operational",
    "computer_name": "Viticm-SOC",
    "event_data": {
      "Company": "Microsoft Corporation",
      "Description": "Microsoft Edge",
      "FileVersion": "136.0.3240.76",
      "IntegrityLevel": "Low",
      "LogonGuid": "{7e25c1a1-c666-6831-ce25-040000000000}",
      "LogonId": "0x425ce",
      "ParentUser": "VITICM-SOC\\ranga",
      "Product": "Microsoft Edge",
      "TerminalSessionId": "1"
    },
    "event_id": "1",
    "opcode": "Info",
    "process": {
      "pid": 2428,
      "thread": {
        "id": 3216
      }
    },
    "provider_guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
    "provider_name": "Microsoft-Windows-Sysmon",
    "record_id": "28411",
    "task": "Process Create (rule: ProcessCreate)",
    "user": {
      "domain": "NT AUTHORITY",
      "identifier": "S-1-5-18",
      "name": "SYSTEM",
      "type": "User"
    },
    "version": 5
}
```