Suspicious PowerShell Malware Simulation Detected

1 message

<rangammabokka46@gmail.com> Wed, May 21, 2025 at 10:27 PM
Reply-to: rangammabokka46@gmail.com
To: rangammabokka46@gmail.com

A suspicious PowerShell activity indicating malware simulation was detected.
Details:
- host.name
- user.name
- event.code
- process.name
- process.command_line
- file.path
- registry.path

```
@timestamp: 2025-05-21T16:56:33.090Z
_id: fwzG85YBk_68sXEUj-yJ
_index: .ds-winlogbeat-8.10.2-2025.05.14-000001
agent: {
   "ephemeral_id": "3c240ab4-063a-412b-b8e0-4cb9ca47742b",
   "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": "2025-05-21T16:56:34.412Z",
   "ingested": "2025-05-21T16:56:38.526111900Z",
   "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: 2025-05-21 16:56:33.090
ProcessGuid: {7e25c1a1-05c1-682e-fd01-000000002200}
ProcessId: 1536
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.19041.3996 (WinBuild.160101.0800)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass -File malware-simulation.ps1
CurrentDirectory: C:\Scripts\
User: VITICM-SOC\ranga
LogonGuid: {7e25c1a1-ef3c-682d-9689-040000000000}
LogonId: 0x48996
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=2E5A8590CF6848968FC23DE3FA1E25F1,SHA256=9785001B0DCF755EDDB8AF294A373C0B87B2498660F724E76C4D53F9C217C7A3,IMPHASH=3D08F4848535206D772DE145804FF4B6
ParentProcessGuid: {7e25c1a1-ef91-682d-8e00-000000002200}
ParentProcessId: 7068
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
ParentUser: VITICM-SOC\ranga
num_hits: 3
num_matches: 3
process: {
  "args": [
    "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
    "-ExecutionPolicy",
    "Bypass",
    "-File",
    "malware-simulation.ps1"
  ],
  "args_count": 5,
  "command_line": "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -ExecutionPolicy Bypass -File malware-simulation.ps1",
  "entity_id": "{7e25c1a1-05c1-682e-fd01-000000002200}",
  "executable": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
  "hash": {
    "md5": "2e5a8590cf6848968fc23de3fa1e25f1",
    "sha256": "9785001b0dcf755eddb8af294a373c0b87b2498660f724e76c4d53f9c217c7a3"
  },
  "name": "powershell.exe",
  "parent": {
    "args": [
      "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
    ],
    "args_count": 1,
    "command_line": "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" ",
    "entity_id": "{7e25c1a1-ef91-682d-8e00-000000002200}",
    "executable": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
    "name": "powershell.exe",
    "pid": 7068
  },
  "pe": {
    "company": "Microsoft Corporation",
    "description": "Windows PowerShell",
    "file_version": "10.0.19041.3996 (WinBuild.160101.0800)",
    "imphash": "3d08f4848535206d772de145804ff4b6",
    "original_file_name": "PowerShell.EXE",
    "product": "Microsoft® Windows® Operating System"
  },
  "pid": 1536,
  "working_directory": "C:\\Scripts\\"
}
related: {
  "hash": [
    "9785001b0dcf755eddb8af294a373c0b87b2498660f724e76c4d53f9c217c7a3",
    "2e5a8590cf6848968fc23de3fa1e25f1",
        "3d08f4848535206d772de145804ff4b6"
    ],
    "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": "Windows PowerShell",
        "FileVersion": "10.0.19041.3996 (WinBuild.160101.0800)",
        "IntegrityLevel": "High",
        "LogonGuid": "{7e25c1a1-ef3c-682d-9689-040000000000}",
        "LogonId": "0x48996",
        "ParentUser": "VITICM-SOC\\ranga",
        "Product": "Microsoft® Windows® Operating System",
        "TerminalSessionId": "1"
    },
    "event_id": "1",
    "opcode": "Info",
    "process": {
        "pid": 6444,
        "thread": {
            "id": 4576
        }
    },
    "provider_guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
    "provider_name": "Microsoft-Windows-Sysmon",
    "record_id": "22708",
    "task": "Process Create (rule: ProcessCreate)",
    "user": {
        "domain": "NT AUTHORITY",
        "identifier": "S-1-5-18",
        "name": "SYSTEM",
        "type": "User"
    },
    "version": 5
}
```