Threat Category: APT / ICS Malware

Threat Description: The YARA rule is designed to detect IronGate malware, a highly targeted ICS (Industrial Control Systems) attack focused on Step7ProSim, a Siemens PLC simulation software. IronGate is considered a proof-of-concept or nation-state malware, similar to Stuxnet, used to manipulate industrial automation processes.

Indicators of Compromise (IoCs)

Code execution artifacts:

Step7ProSim.Interfaces

PackagingModule.Step7ProSim.dll

RunPlcSim

Malware behavior signatures:

"\\obj\\Release\\Step7ProSim.pdb" ascii

"Step7ProSim.Interfaces" fullword ascii

"payloadExecutionTimeInMilliSeconds" fullword ascii

"PackagingModule.Step7ProSim.dll" fullword wide

"<KillProcess>b__0" fullword ascii

"newDllFilename" fullword ascii

"PackagingModule.exe" fullword wide

"$863d8af0-cee6-4676-96ad-13e8540f4d47" fullword ascii

"RunPlcSim" fullword ascii

"$ccc64bc5-ef95-4217-adc4-5bf0d448c272" fullword ascii

"InstallProxy" fullword ascii

"DllProxyInstaller" fullword ascii

"FindFileInDrive" fullword ascii

Detection Mechanism:

Must be a Windows PE file with MZ (0x5A4D) header

File size must be < 50KB

Must contain at least three Step7ProSim-related artifacts

hash1 = "0539af1a0cc7f231af8f135920a990321529479f6534c3b64e571d490e1514c3"

hash2 = "fa8400422f3161206814590768fc1a27cf6420fc5d322d52e82899ac9f49e14f"

hash3 = "5ab1672b15de9bda84298e0bb226265af09b70a9f0b26d6dfb7bdd6cbaed192d"

Possible Attribution & Use Cases:

Targets ICS/SCADA systems used in industrial automation

Linked to threat actors aiming to disrupt critical infrastructure

Recommended Actions:

Investigate: Inspect PLC activity logs for unauthorized manipulations

Contain & Mitigate: Restrict Step7ProSim to authorized users only

Threat Hunting: Deploy proactive scanning across industrial control networks

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Version: 1

Reference ID: a73cf9e2-c24f-5553-92e2-3a1a882a4a06