PolySwarm Threat Bulletin:

Incontroller Targets ICS

April 20 2022

ANOMALI

Background

Mandiant recently reported on Incontroller, a malware family targeting industrial control systems.

What is Incontroller?

Earlier this year, Mandiant partnered with Schneider Electric to analyze a tool targeting industrial control systems (ICS). The malware, dubbed Incontroller or Pipedream, targets machine automation devices. Incontroller specifically targets OPC servers, Schneider Electric Modicon M251, Modicon M258, Modicon M221 Nano PLCs, Omron NX1P2m NJ501 PLCs, and R88D-1SN10F-ECT servo drive. According to Mandiant, other devices that use Modbus and Codesys and other NJ and NX PLC series devices may also be affected.

Incontroller has three components: TAGRUN, CODECALL, and OMSHELL. TAGRUN scans for OPC servers, enumerates them, brute forces credentials, and can read and write OPC tag values. Mandiant assessed TAGRUN was likely used for reconnaissance purposes, even though it also allows modification of data. Accessing OPC data gives threat actors a detailed overview of production systems and control processes.

CODECALL uses Modbus and Codesys protocols to communicate and can interact with, scan, and attack multiple Schneider Electric programmable logic controllers (PLCs). Threat actors can use CODECALL to identify Schneider Electric and Modbus-enabled devices, connect to those devices, and execute commands. Possible commands include but are not limited to brute forcing credentials using a dictionary file, uploading and downloading files to the PLC device, retrieving files, deleting files, disconnecting sessions, launching a DDoS attack, using a specially crafted packet to crash a device, and sending custom packets.

The OMSHELL framework facilitates interaction with and scanning of certain Omron PLCs via HTTP, Telnet, and the Omron FINS protocol. OMSHELL can be used to wipe and reset a device, load a backup configuration, restore data, activate telnet, connect to a backdoor, allow arbitrary command execution, kill processes, and transfer files. OMSHELL also allows interaction with Omron's servo drives.

Mandiant listed three hypothetical but realistic scenarios in which these tools could be used. The first use is to disrupt controllers and shutdown operations. The second is to reprogram controllers in order to sabotage industrial processes. The third is to disable safety controllers, resulting in physical destruction.

Mandiant notes it is also tracking two potentially related tools targeting Windows systems. The first exploits CVE-2020-15368 in the AsrDrv103.sys driver, which results in installation and exploitation of a vulnerable driver. The second, dubbed ICECORE, is a backdoor used for reconnaissance and C2 interaction.

Based on the malware's sophistication, Mandiant assesses it was likely created by a state sponsored threat actor. They did not attribute the malware to a particular threat actor. Mandiant compared Incontroller to Triton, Industroyer, and Stuxnet in terms of sophistication and potential impact on industrial systems.

IOCs

PolySwarm has a sample of Incontroller.

69296ca3575d9bc04ce0250d734d1a83c1348f5b6da756944933af0578bd41d2

You can use the following CLI command to search for all Incontroller samples in our portal:
$ polyswarm link list -f Incontroller

Don’t have a PolySwarm account? Go here to sign up for a free Community plan or to subscribe.