PLC Worms Can Pose Serious Threat to Industrial Networks

By Eduard Kovacs

Published: 2016-05-09 · Archived: 2026-04-02 12:03:52 UTC

Researchers have created an experimental worm that is capable of spreading from one programmable logic controller (PLC) to another without needing a PC or a server.

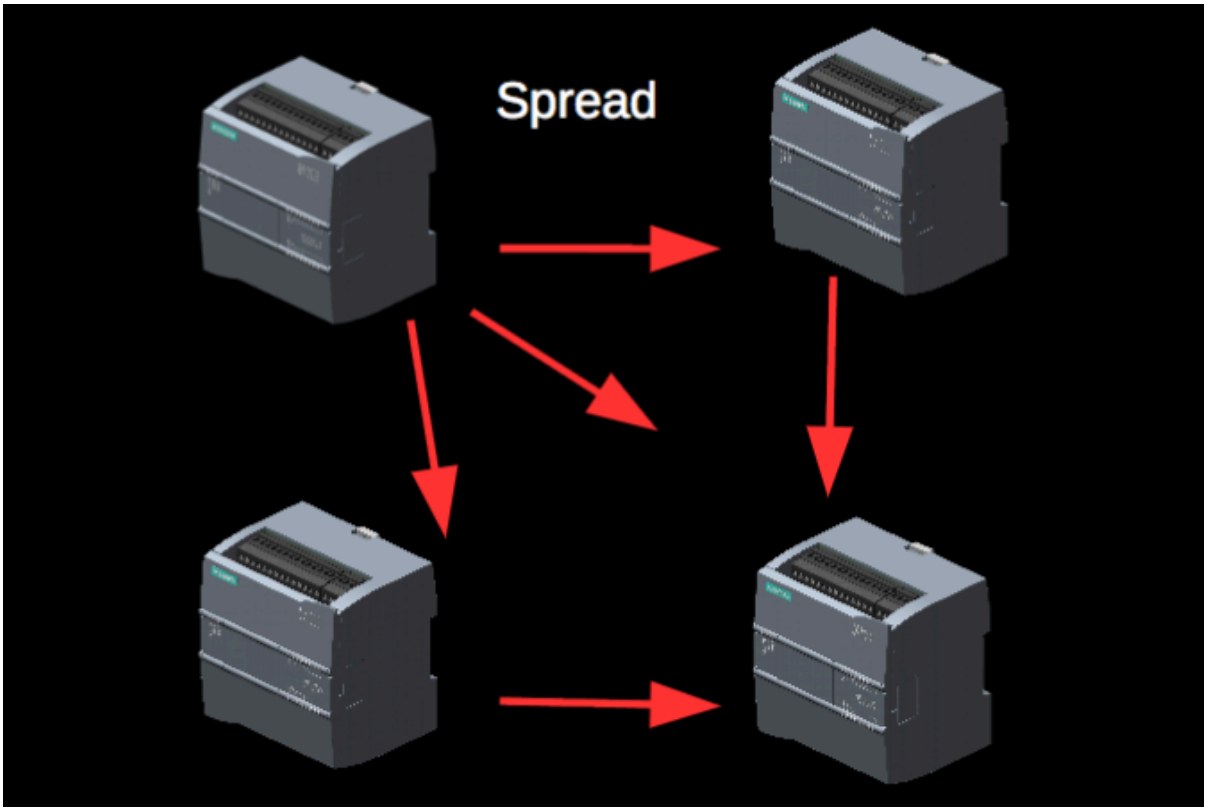
The worm, detailed at the recent Black Hat Asia conference by researchers from OpenSource Security, is dubbed "PLC-Blaster" and it's designed to target Siemens SIMATIC S7-1200v3 controllers.

Building on previous research showing that a piece of malware can run on a PLC, experts used the Structured Text (ST) language to develop a worm that leverages the PLC's communication features to spread from one device to another.

PLC-Blaster was written like a regular worm, but with some constraints that are specific to PLCs. Experts believe that the most likely infection vector involves distribution of the worm by an industrial component supplier, or infection of the device during transport.

Once an infected Siemens SIMATIC device is installed on a network, the worm starts scanning TCP port 102 for other similar systems. If the identified PLC is not already infected, the worm stops it for roughly 10 seconds, transfers its code to the target, and starts it again. This process is then repeated for every possible target.

According to researchers, their worm replicates itself on the targeted PLC by mimicking the Siemens TIA-Portal. The malware leverages a vulnerability in SIMATIC S7-1200 CPUs that Siemens patched with the release of version 4.



Researchers also implemented some malicious functionality to demonstrate the impact of PLC-Blaster. The malware can contact a command and control (C&C) server, it can act as a Socks4 proxy, it can cause a denial-of-service (DoS) condition on the infected PLC, and it can manipulate outputs.

OpenSource Security researchers noted that the worm can be detected based on the 10-second interruptions caused to the PLC during infection or the unusual network traffic generated by the threat. Since it's stored on the PLC, the malware is persistent across a restart of the device, but it does get removed after a factory reset or if the organization block (OB) it's stored in is overwritten.

Related: Registration for 2016 ICS Cyber Security Conference Now Open

"Attacking industrial systems by means of malware or worms is not a new technique. This form of attack has been demonstrated previously in other research projects such as Rockwell and Stuxnet, although the PLC worm is the first of its kind to be utilised without a large budget behind it," Jalal Bouhdada, founder and principal ICS security consultant at Applied Risk, told *SecurityWeek*. "This worm demonstrates that both hackers and the security community is now increasingly focussed on industrial control systems and its associated vulnerabilities."

PLC worms in the wild and other implications

Bouhdada believes these types of PLC worms will likely be seen in the wild.

"It is just matter of time until we see the first worm in the wild exploiting these vulnerabilities," the expert said. "Hacking industrial systems was previously reserved for the few with access to very expensive equipment, and while the PLC worm targets OT directly, IT systems remain the main point of access for any potential breach due to their compatibility with existing malware packages."

Martin Jartelius, CSO of vulnerability management company Outpost24, pointed out that there are other aspects that need to be taken into consideration.

“The research is interesting and of course fascinating. It should however be noted that most of the time RCE (Remote Code Execution) vulnerabilities in network-exposed services always give an opening for a worm, but the use of those is today more rare. It is noisy, your operations will be detected, and the portscanner component very quickly draws attention to the infected devices, leading to cleanups. It is simply not a good investment of time and effort from most attackers’ perspective,” Jartelius said via email.

“Propagation on the local network however makes more sense, i.e. if one device is Internet-exposed, other similar devices on the internal networks can be breached via the first. In essence, the code has justification from an attacker perspective, but if we see it used properly, it is not in the worm format,” he added.

“We will see worms every now and then of course – kids will be kids – but the remote installation and command/control component is more serious than the potential of creating a worm,” the expert noted.

Mitigating the threat

“In order to minimise the damage that can be caused by malware such as the PLC worm, organisations must solidify the security of their supply chains, ensure their industrial assets are identified and undertake embedded security assessments,” Bouhdada explained. “The PLC worm is a strong signal to industry that critical infrastructure requires significant protection, with suppliers and asset owners working closely together to ensure the safe and reliable operation of these environments.”

Jartelius advises organizations to protect their systems against such threats by following the recommendations from the Center for Internet Security’s Critical Security Controls (CSC). These include inventorying devices and software, ensuring that both hardware and software systems have secure configurations, controlled use of administrative privileges, and continuous vulnerability assessment and remediation.

Related: Concerns Raised Over Malware in German Nuclear Plant

---