# PLC-Blaster Worm Targets Industrial Control Systems

By Tom Spring

Published: 2016-08-05 · Archived: 2026-04-05 17:18:03 UTC

Researchers create a self-propagating worm that can infect a Siemens' PLC and can be programmed to bring an industrial control platform to its knees.

LAS VEGAS – Security researchers at Black Hat USA described a proof-of-concept worm that targets weaknesses within automated industrial control systems used to manage critical infrastructure and manufacturing. The worm, according to OpenSource Security, has the capability to autonomously search for and spread between networked programmable logic controllers (PLCs).

PLC-Blaster was designed to target Siemens SIMATIC S7-1200 PLCs. Siemens is Europe's biggest engineering company and a PLC market share leader. Siemens said in March shortly after the worm was unveiled at Black Hat Asia that the malware was not exploiting a vulnerability in Siemens gear. Maik Brüggemann, software developer and security engineer at OpenSource Security, said that worms like this one are a threat to any industrial network.

"These are new threats to industrial control companies that have traditionally been well protected against attacks from the outside," Brüggemann said. "It's not unimaginable a PLC worm could be distributed by a component supplier or internally. It's not just Siemens that should be concerned. Worms represents a new threat to any industrial network."

On Thursday at Black Hat USA, Brüggemann showed how an attacker with physical or network access to a PLC can manage to introduce the malware to the network and launch an attack. The worm can be programmed to carry out a number of different attacks. Or the infected PLCs can be programmed to automatically contact an attacker's command-and-control server and be remotely controlled – assuming the PLCs is connected to the public Internet. Attack scenarios include shutting off or tampering with volatile critical infrastructure components.

The worm's success is tied to PLC design flaws by Siemens that leave the PLC platform open to attack via the PLC's management console called TIA Portal, the researchers assert. The first two have to do with computer code used to manage PLC access passwords, and serial numbers called Knowhow Protection and Copy Protection. The features are missing integrity safeguards that allow an attacker to read, write and modify blocks of code pertaining to hashed passwords and serial numbers. Doing so cracks open a window for an attacker to bypass TIA Portal software protections in order to upload PLC-Blaster inside the environment.

"The built-in Knowhow protection forbids modifications of the user program on the PLC and prevents the extraction of the user program from the PLC. But we were able to figure out how to extract the user program, display the source code, modify it and reinstall the program," Brüggemann said.

With its defenses down, the malware can be uploaded to the PLC where it can wind its way through the network infecting others.

The one caveat to the above scenario, Brüggemann said, is a Siemens Access Protection option that limits the features of the protocol that is used to transfer software, or in this case the worm, to a PLC. The feature requires users to enter another password before uploading new software. “We found no security flaw in this protection. But the problem is this protection is off by default. If it is enabled, the worm needs to know the password and that’s usually not the case,” Brüggemann said.

Brüggemann said what needs to change is the TIA Portal password protection for uploading new software needs to be on by default so users are prompted for a password.

When OpenSource Security took its findings to Siemens, the researchers were told there were no flaws in its PLC platforms using its SIMATIC S7-1200 PLC. “We were told these were not vulnerabilities and that everything worked as expected,” Brüggemann said.

When Threatpost reached out to Siemens for comment it reiterated it didn’t view OpenSource Security’s research as conclusive evidence its SIMATIC S7-1200 PLCs were vulnerable. “The demonstration at Black Hat uses a prototype worm spread via modification of the user program of unprotected SIMATIC S7-1200 v3 PLCs (unprotected means: with disabled PLC-function access protection and without following Operational Guidelines),” the company said in a statement.

Siemens said its operational guidelines recommend enabling the Access Protection feature. However, Siemens in March did issue a security advisory (PDF) warning flaws “could possibly allow an attacker to circumvent user program block protections” in its SIMATIC S7-1200 PLCs.

“With respect to the additional issues reported, which are unrelated to the prototype worm, these were resolved (CVE-2016-2846) and communicated with acknowledgement and thanks to Maik Brüggemann and Ralf Spenneberg,” the company said in an email interview.

Brüggemann maintains the Access Protection configuration setting needs to be easier to find and that it also needs to be on by default to be safe.

“These are not Siemens-specific problems. All these industrial control companies have been doing things the same way for the past 30 years. They need to develop new attitudes toward security to make devices secure,” Brüggemann said.

---