Shades Of Stuxnet Spotted In Newly Found ICS/SCADA Malware

'IronGate' discovery underlines the risk of industrial attacks yet to come.

Newly discovered malware targeting industrial control systems has the researchers who discovered it intrigued and hungry for help from the ICS community to further unravel it.

FireEye researchers today detailed their findings on the so-called Irongate ICS/SCADA malware, which targets a Siemens PLC simulation (SIM) environment—not an operational one—via a man-in-the middle attack on a specific piece of custom PLC SIM code. SIM environments are where engineers test out their PLC code, which means Irongate as-is represents no actual threat to ICS operations, according to FireEye, and there's been no sign of any attacks or attempts thus far.

Irongate, which the researchers believe is a proof-of-concept, apparently has been under the radar for some time. It dates back to 2012, but wasn't discovered until late last year after a couple of its samples were uploaded to VirusTotal: even then, antivirus scanners missed it. FireEye reverse-engineered the samples after noticing some SCADA references in the code.

The ICS/SCADA security community has been awaiting a new wave of malware focused on manipulating or altering industrial processes since the infamous Stuxnet attack was first exposed and deconstructed in 2010. But there's been no similar ICS/SCADA attack or threat to emerge publicly despite predictions that Stuxnet was a harbinger of possible threats yet to come.

Irongate is no Stuxnet, but it resembles it in some ways: like Stuxnet, Irongate targets a specific Siemens control system, and it uses its own DLLs to alter a specific process. Each malware family does a little detective work of its own to evade detection: while Stuxnet searched for antivirus software to bypass, Irongate skirts sandboxes and other virtual environments so it won't get caught.

There are no ties to the codebases of the two malware families, and Irongate has no worm-like spreading function, nor any apparent ties to nation-state actors like Stuxnet does. In fact, Irongate isn't even a real attack as yet. The researchers don't have proof of any victims, but they say the creator had to have some detailed insight and knowledge about the specific custom simulation process that it targets. Irongate doesn't exploit any vulnerabilities in a Siemens PLC nor does it attack the PLC itself.

"Post-Stuxnet, everybody said this is going to unleash ICS malware. But we didn't see that. This is really the first example of control system malware that did copy those

techniques," says Rob Caldwell, ICS manager for FireEye Mandiant. Irongate is not as complex or sophisticated as Stuxnet, but it can evade sandboxes —something Stuxnet could not do, he says

could not do, he says.

The researchers say it's unclear whether Irongate is the handiwork of a nation-state, a cybercriminal, or a researcher testing threats to ICS. "The question for us is if it's a simulated environment, then what is it? Is someone trying this in a simulated [environment] before taking it to a production environment? Or is it a researcher saying 'look what I can do ... a Stuxnet-type thing,'" says Dan Scali, senior manager for FireEye Mandiant ICS Consulting.

Either way, the discovery of Irongate should be a wakeup call for the ICS/SCADA community, security experts say.

No New Stuxnet Here

Robert M. Lee, a SANS instructor and ICS/SCADA expert, says Irongate itself doesn't represent a next-generation Stuxnet or other threat per se, but it does underscore a basic problem with ICS/SCADA security. "It's not a sign of a specific [attack] capability, but it's a sign of the interest in this by pen testers, security companies, as well as adversaries," Lee says. "The problem I have ... is I am not confident that a majority of the industry could respond to it. We don't know what's out there; antivirus companies aren't finding it and even if they had, who would know what to do with it [the threat]?"

Lee says it's difficult to determine who is behind Irongate, but he's not sold that it's an actual attack. "This looks to be a security company put it together to demonstrate a security tool, or a pen test and researcher put it together for a project," he says. "It's not an adversary tool -- but it's still important."

The Irongate code was manually uploaded to VirusTotal from someone based in Israel, he notes.

FireEye, meanwhile, says some of Irongate's functions indeed could become part of future ICS/SCADA malware and attacks. "I would not be surprised to see sandbox evasion and file replacement attacks incorporated by future ICS malware deployed in the wild," says Sean McBride, attack synthesis lead for FireEye iSIGHT Intelligence.

Irongate, which goes after custom PLC logic code written and tested in Siemens Step 7 PLC simulation environment, wages a man-in-the-middle attack against the PLC test code and replaces the Dynamic Link Library (DLL) used in the Siemens system with a malicious one of its own. Some of Irongates droppers won't run if they detect a VMware or Cuckoo sandbox, FireEye found.

While the researchers say they don't know which PLC process Irongate is simulating, they were able to correlate some of data with pressure and temperature simulations.

"The vulnerability in this case is more of something that ICS operators need to think about when they write their own code: code that's not signed, so it can be replaced," Caldwell says.

Web Ties?

FireEye found code samples similar to the process that Irongate was attacking on a control engineering blog that covers PLC SIM issues. "The code seems to resemble some examples of PLC simulation code that's freely available on the Web, which also helped inform our hunch [Irongate] may be a proof-of-concept," Caldwell says. "It's very similar to some publicly available demo code out there."

FireEye released details of the malware here.

Related Content: