SearchSecurity.com

10 years after Stuxnet, new zero-days discovered

By Alexander Culafi

The threat of Stuxnet is still alive, thanks to the discovery of new zero-day vulnerabilities connected to an old Microsoft Windows flaw.

SafeBreach Labs security researcher Peleg Hadar and research team manager Tomer Bar discovered new vulnerabilities related to a the Windows Print Spooler exploited by the legendary Stuxnet worm that was never fully fixed. The Stuxnet used the print spooler flaw, along with other zero-days, to spread through Iran's nuclear facilities and physically damage uranium enrichment centrifuges.

"Stuxnet is considered by many to be one of the most complex and well-engineered computer worms ever seen," Bar said during his and Hadar's Black Hat USA 2020 panel Thursday. "In our opinion, a decade after Stuxnet, the most interesting part is the propagation capabilities, which is still relevant to almost any targeted attack."

During the panel, titled "A Decade After Stuxnet's Printer Vulnerability: Printing is Still the Stairway to Heaven," Bar explained that the original Stuxnet worm could be broken down into three parts: the propagation capabilities, which used five zero-day vulnerabilities; the evasion capabilities, which used rootkits and stolen digital certificates; and the final payload, which attacked Siemens industrial control systems. The zero-days were patched in the aftermath of Stuxnet, and the only one that wasn't reexploited was the Windows Print Spooler vulnerability, he said.

Microsoft patched the spooler flaw in 2010. But SafeBreach Labs recently used fuzzing to determine the printer spooler flaw was still exploitable and could be used for local privilege escalation attacks. "Microsoft did not fix this bug," Bar said.

Fast forward to 2020, Hadar and Bar discovered new vulnerabilities stemming from the print spooler flaw.

One allowed a threat actor to use the print spool to elevate privileges by logging onto an affected system and running a "specially crafted script or application". As with other escalation of privilege vulnerabilities, this would allow the attacker to read, alter or delete data, create accounts or install programs. Another vulnerability would allow the threat actor to crash the print spool service using a DoS condition.

After SafeBreach alerted Microsoft in January, the latter patched the elevation of privileges vulnerability (CVE-2020-1048) in May. However, the following month, Hadar and Bar discovered a new way to bypass the patch and, on the latest Windows version, reexploit the vulnerability. This vulnerability (CVE-2020-1337) will be fixed in Microsoft's upcoming Patch Tuesday, as revealed at the Black Hat session.

Hadar said coupling the vulnerabilities and bypasses together could potentially create a threat with "Stuxnet 2.0 propagation power." Because these new vulnerabilities are zero-days and have not been patched yet, SafeBreach Labs is withholding technical details regarding exploitation, he said.

But the company did release some of its research, as well as several proof of concept (POC) exploits for the vulnerabilities, which Bar said should offer real-time defense, on the vendor's GitHub page. "We believe in a loud security mitigation approach," he said of the POCs.

07 Aug 2020