4-CyberScoop-Leaked NSA hacking tools

Leaked NSA hacking tools are a hit on the dark web

Share

Apr 20, 2017 | CyberScoop

Written by Chris Bing Apr 20, 2017 | CYBERSCOOP

UndergroundÂ hackers are now sharing, promoting and working to adopt executable computer code evident in NSA documents that were published last week by the Shadow Brokers, private sector intelligence analysts tell CyberScoop.

Tutorials on how to utilize some of the tools began appearing the same day the NSA documents were originally published, according to researchers at Israel-based dark web intelligence firm SenseCy. Forum members have shown a particular interest in a leaked framework similar to Metasploit thatâ€™s unique to the NSA called Fuzzbunch.

SenseCy, a firm focused on the dark web staffed by former intelligence officials, identified a series of conversations occurring in a hidden Russian cybercrime forum discussing how members could exploit a bug in Windows Server Message Block, a network file sharing protocol.

â€œHackers [have] shared the leaked [NSA] information on various platforms, including explanations [for how to use the tools]Â published by Russian-language blogs,â€ said SenseCy Director Gilles Perez. â€œWe identified [one] discussion dealing with the SMB exploit [ETERNALBLUE], where hackers expressed interest in its exploitation and share instruction on how to do so.â€

Perez declined to name the dark web forums surveilled by SenseCy, but provided CyberScoop with screenshots of conversations between members discussing the matter inÂ discussion boards â€” â€œWe can never provide the names of the forums as that could jeopardize our operations,â€ he wrote in an email.

One of the powerful tools shared by the Shadow Brokers last week, and addressed by a March Microsoft security update, is codenamed ETERNALBLUE in the leaked documents â€” it is also referred to as vulnerability MS17-010 by Microsoft.

ETERNALBLUE allows for an attacker to remotely cause older versions of Windows to execute code.

Here is a video showing ETERNALBLUE being used to compromise a Windows 2008 R2 SP1 x64 host in under 120 seconds with FUZZBUNCH #0day ğŸ˜‰ pic.twitter.com/I9aUF530fU

â€” Hacker Fantastic (@hackerfantastic) April 14, 2017

Security researcher Matthew Hickey was able to show in a video that ETERNALBLUE is effective against machines running Windows Server 2008 R2 SP1, an old but popular version of Windows Server.

SenseCy researchers told CyberScoop theyâ€™ve already seen cybercriminals attempt to utilize the MS17-010 vulnerability in ransomeware-style attacks.

â€œWe are now seeing a trend, that most likely will gain momentum in the following weeks, of infecting Windows servers with Ransomware utilizing the [NSA] leaked exploits,â€ Gilles said.

Some security researchers believe that exploiting MS17-010 will become popular amongst cybercrime gangs because it allows for a more damaging ransomware infection .

Prediction: ransomware worm. E.g. SMB. Somebody uses Equation Group exploit to worm across world and encrypt in process.

â€” Kevin Beaumont (@GossiTheDog) April 19, 2017

Researchers at cyber intelligence firm Recorded Future told CyberScoop that they too have spotted separate discussions in several Russian and Chinese hacker forums in which users successfully reversed engineered some of the Windows tools and were openly sharing their findings.

â€œThe surprising recent release â€” one of the most comprehensive and up to date â€” of hacking tools and exploits by the notorious Shadow Brokers group stirred up great interest among Russian-speaking cyber criminals,â€ said Andrei Barysevich, Recorded Futureâ€™s director of advanced collection. â€œOnly three days after the data was leaked, we identified a discussion among members of an elite dark web community sharing expertise in weaponizing the EternalBlue exploit as well as the DoublePulsar kernel payload.â€

He added, â€œconsidering that Microsoft patched the EternalBlue vulnerability as recently as March 14, the number of potentially affected systems could still be tremendous *[Worry]*.â€

Recorded Future similarly declined to name the forums where they discovered this content.

â€œ[In the Chinese forum], they were particularly interested in the exploit framework (named FUZZBUNCH), the SMB malware (ETERNALBLUE) and privilege escalation tool (ETERNALROMANCE),â€ members of Recorded Futureâ€™s research team wrote in an email. â€œActors were focused on the unique trigger point for [ETERNALBLUE] and some claimed that the patches for CVE-2017-0143 through -0148 were insufficient because they did not address the base code weaknesses.â€

These discussions indicate that thereâ€™s broad interest in the unique malware triggers published by the Shadow Brokers and a belief that the underlying vulnerabilities being exploited had not been completely mitigated by Microsoftâ€™s patches, according to Recorded Future. â€œThese two factors combine to increase the risk that malicious Chinese actors may reuse or repurpose this malware in the future *[Worry]*,â€ a spokesperson explained.

Hickey was able to demonstrate how FUZZBUNCH can deploy malware

Most of the exploits and implants mentioned in the latest release are designed to exploit software vulnerabilities apparent in older Microsoft products, including Office and various operating systems. The technology giant stated in a blog post over the weekend that it had patched most of the exploits. Discontinued, end of life version of Windows, such as XP and 2003, remain vulnerable as they did not receive a security patch.

More than 65 percent of desktop computers connected to the internet last month ran on older versions of Windows like Vista, according to estimates from the tracking firm Net Market Share.

While many of the Microsoft Windows-specific exploits contain remote code execution vulnerabilities, they need to be deployed against a host in order to be successful. In other words, a connection to the organization must already be established for many of these exploits to work â€" as port 445, which is used in Microsoftâ€™s SMB, is typically blocked internet-wide.

Microsoft declined to answer questions pertaining to how the company originally became aware of the aforementioned vulnerabilities, which were supposedly once exploited by the NSA.

Though it remains unclear whether anyone has been able to successfully leverage any of the leaked hacking tools to launch their own computer intrusion, security researchers fully expect and are preparing for a barrage of new attacks supported by NSAâ€™s quality engineering *[Worry]*.

â€œEven though the vulnerabilities released were patched, we feel confident that it will only be a matter of time before we see exploitation in the wild *[Worry]*,â€ said Cylance Chief Research Officer Jon Miller. â€œThe scale will be on par with any other known and patched vulnerability. Only those that arenâ€™t judicious in patching their systems will be affected, mitigating the risk that comes from a true zero-day.â€

Liam Oâ€™Murchu, the director of Symantecâ€™s security technology and response group, said he expects it will take a â€œlittle longerâ€ for attackers to begin incorporating the leaked tools into their own attacks.

â€œFrom a defensive perspective, one of the main problems is the volume of data released,â€ said Oâ€™Murchu. â€œWe need to analyze all the files to understand how they could be changed or used to fit in with current cybercrime attacks â€¦ with ~7000 files disclosed, it is very resource intensive to understand all of the tools, the full capabilities and how they can be used. That is what we are working on now.â€

A cohort of independent researchers and security firms are finding new capabilities and targeted software vulnerabilities hidden in the massive trove of documents on a near daily basis since Fridayâ€™s release.

[Worry]

â€œWe have only begun to scratch the surface on these tools and now that they are out there itâ€™s important we can analyze them to determine servers that are impacted as well as what steps can be taken to protect against them,â€ Hickey wrote in a blog post , Wednesday.

image of a conversation occurring on a hidden forum, where users report Â â€“ provided by SenseCy

â€œThe tools are released in binary format and as reverse engineering efforts are underway. We will likely discover more interesting features about the attacks,â€ wrote Hickey. â€œWe are under no illusion that such a huge data trove will not be completely analyzed in its first few days of discovery and neither should you. *[Worry]*â€

-In this Story-