0-Ars Technica-NSA

Sign up or login to join the discussions!

Stay logged in

Sign up to comment and more Sign up

Biz & IT —

NSA-leaking Shadow Brokers just dumped its most damaging release yet

Windows zerodays, SWIFT bank hacks, slick exploit loader among the contents.

Apr 14, 2017 5:27 pm UTC

Enlarge / A screen shot showing EternalRomance, one of the NSA exploits leaked Friday.

Share on Reddit

Important Update 4/15/2017 11:45 AM California time None of the exploits reported below are, in fact, zerodays that work against supported Microsoft products. Readers should read this update for further details. What follows is the post as it was originally reported.

The Shadow Brokers—the mysterious person or group that over the past eight months has leaked a gigabyte worth of the National Security Agency's weaponized software exploits—just published its most significant release yet. Friday's dump contains potent exploits and hacking tools that target most versions of Microsoft Windows and evidence of sophisticated hacks on the SWIFT banking system of several banks across the world.

Further Reading

Group claims to hack NSA-tied hackers, posts exploits as proof

Friday's release—which came as much of the computing world was planning a long weekend to observe the Easter holiday—contains close to 300 megabytes of materials the leakers said were stolen from the NSA. The contents (a convenient overview is here) included compiled binaries for exploits that targeted vulnerabilities in a long line of Windows operating systems, including Windows 8 and Windows 2012. It also included a framework dubbed Fuzzbunch, a tool that resembles the Metasploit hacking framework that loads the binaries into targeted networks. Independent security experts who reviewed the contents said it was without question the most damaging Shadow Brokers release to date.

"It is by far the most powerful cache of exploits ever released," Matthew Hickey, a security expert and co-founder of Hacker House, told Ars. "It is very significant as it effectively puts cyber weapons in the hands of anyone who downloads it. A number of these attacks appear to be 0-day exploits which have no patch and work completely from a remote network perspective."

One of the Windows zerodays flagged by Hickey is dubbed Eternalblue . It exploits a remote code-execution bug in the latest version of Windows 2008 R2 using the server message block and NetBT protocols. Another hacking tool known as Eternalromance contains an easy-to-use interface and "slick" code. Hickey said it exploits Windows systems over TCP ports 445 and 139. The exact cause of the bug is still being identified. Friday's release contains several tools with the word "eternal" in their name that exploit previously unknown flaws in Windows desktops and servers.

The full list of tools documented by Hickey are:

ETERNALROMANCE—Remote privilege escalation (SYSTEM) exploit (Windows XP to Windows 2008 over TCP port 445)

ENTERNALCHAMPION, ETERNALSYSTEM—Remote exploit up to Windows 8 and 2012

ETERNALBLUE — Remote Exploit via SMB & NBT (Windows XP to Windows 2012)

EXPLODINGCAN—Remote IIS 6.0 exploit for Windows 2003

EWORKFRENZY—Lotus Domino 6.5.4 and 7.0.2 exploit

ETERNALSYNERGY—Windows 8 and Windows Server 2012

FUZZBUNCH—Exploit Framework (Similar to Metasploit) for the exploits.

A separate analysis by researcher Kevin Beaumont found three zerodays affecting Windows systems. They are Esteemaudit-2.1.0.exe , a Remote Desktop exploit that installs an implant on Windows Server 2003 and XP; Eternalchampion-2.0.0.exe , which also works against SMB; and the previously mentioned Eternalblue. Beaumont found four other exploits that he believes may be zerodays, including Eskimoroll-1.1.1.exe , a Kerberos attack targeting domain controllers running Windows Server 2000, 2003, 2008 and 2008 R2; Eternalromance-1.3.0.exe , Eternalromance-1.4.0.exe , an update of Eternalromance-1.3.0.exe; and Eternalsynergy-1.0.1.exe , a remote code-execution attack against SMBv3.

With the exception of Esteemaudit, the exploits should be blocked by most firewalls. And best practices call for remote desktop connections to require use of a virtual private network, a practice that should make the Estememaudit exploit ineffective. Microsoft also recommends that organizations disable SMBv1, unless they absolutely need to hang on to it for compatibility reasons, which may block Eternalblue. That means organizations that are following best practices are likely safe from external attacks using these exploits. There’s no indication any of the exploits work on Windows 10 and Windows Server 2016, although it’s possible the exploits could be modified to work on these operating systems.

Still, the public distribution of some of the NSA’s most prized hacking tools is sure to cause problems *[Worry]*. *[Disappointment]* In a post published by the Lawfare website , Nicholas Weaver, a security researcher at the

University of California at Berkeley and the International Computer Science Institute, wrote:

Normally, dumping these kinds of documents on a Friday would reduce their impact by limiting the news cycle. But Friday is the perfect day to dump tools if your goal is to cause maximum chaos; all the script kiddies are active over the weekend, while far too many defenders are offline and enjoying the Easter holiday. *[Worry]* I'm only being somewhat glib in suggesting that the best security measure for a Windows computer might be to just turn it off for a few days.

Besides the risk the exploit leaks pose to Windows users all over the world, they are likely to further tarnish the image of the NSA. The highly secretive agency reportedly had at least 96 days to warn Microsoft about the weaponized Windows exploits released today, according to this account from Emptywheel *[Disappointment]*. It points to a January 8 Shadow Brokers leak that references some of the same exploits.

We hack banks

Friday's dump also contains code for hacking into banks, particularly those in the Middle East. According to this analysis by Matt Suiche, a researcher and founder of Comae Technologies, Jeepflea_Market is the code name for a 2013 mission that accessed EastNets, the largest SWIFT service bureau in the Middle East. EastNets provides anti-money laundering oversight and related services for SWIFT transactions in the region. Besides specific data concerning specific servers, the archive also includes reusable tools to extract the information from Oracle databases such as a list of database users and SWIFT message queries.

"This would make a lot of sense that the NSA compromise this specific SWIFT Service Bureau for Anti-money laundering (AML) reasons in order to retrieve ties with terrorists groups," Suiche wrote. "But given the small number (74) of SWIFT Service Bureaus, and how easy it looks like to compromise them (e.g. 1 IP per Bank)—How many of those Service Bureau may have been or are currently compromised?"

Suiche also found evidence that Al Quds Bank for Development and Investment, a bank in Ramallah, Palestine, was specifically targeted.

The release also contains the software for “Oddjob”, an implant tool and backdoor for controlling hacked computers through an HTTP-based command server. Other implants have names such as Darkpulsar-1.1.0.exe, Mofconfig-1.0.0.exe, and PluginHelper.py. With the exception of minor generic detections for engines related to a “packer” that conceals Oddjob, none of the implants were detected by antivirus programs at the time this update was going live. AV companies are almost certainly in the process of pushing out updates.

Further Reading

NSA-leaking Shadow Brokers lob Molotov cocktail before exiting world stage

The Shadow Brokers have captured the attention of the intelligence community in the US and around the world. Some of the previous weapons-grade leaks, for instance, exploited unpatched vulnerabilities in Cisco Systems firewalls . Researchers from security firm Kaspersky Lab, meanwhile, have confirmed the leaked code they analyzed bears unique signatures tied to Equation Group, Kaspersky’s name for a state-sponsored group that operated one of the most advanced hacking operations ever seen. In January, Shadow Brokers claims it was suspending operations, after making one last inflammatory release . Friday’s dump shows the group was still holding plenty more incendiary material.

The Shadow Brokers have already prompted a major internal investigation inside the NSA with the arrest of at least one agent accused of stealing 75 percent of the hacking tools belonging to the NSA’s Tailored Access Operations group *[Legal Action]* . But so far, there’s no indication investigators have been able to tie the defendant to the Shadow Brokers. This latest dump is sure to make matters more urgent and will undoubtedly preempt the holiday plans for countless people in both government and private industry.

This post has been updated repeatedly over the course of several hours as new information became available. A claim that one of the exploits worked on Windows 10 has been removed after Qualys, the company that made the claim, withdrew it.

Listing image by Internet Archives

Promoted Comments