How Leaked NSA Spy Tool 'EternalBlue' Became a Hacker Favorite

Lily Hay Newman ⋮ 5-6 minutes ⋮ 3/7/2018

An elite Russian hacking team, a historic ransomware attack, an espionage group in the Middle East, and countless small time cryptojackers all have one thing in common. Though their methods and objectives vary, they all lean on leaked NSA hacking tool EternalBlue to infiltrate target computers and spread malware across networks.

Leaked to the public not quite a year ago, EternalBlue has joined a long line of reliable hacker favorites. The Conficker Windows worm infected millions of computers in 2008, and the Welchia remote code execution worm wreaked havoc 2003. EternalBlue is certainly continuing that tradition—and by all indications it's not going anywhere. If anything, security analysts only see use of the exploit diversifying as attackers develop new, clever applications, or simply discover how easy it is to deploy.

"When you take something that's weaponized and a fully developed concept and make it publicly available you're going to have that level of uptake," says Adam Meyers, vice president of intelligence at the security firm CrowdStrike. "A year later there are still organizations that are getting hit by EternalBlue—still organizations that haven't patched it."

The One That Got Away

EternalBlue is the name of both a software vulnerability in Microsoft's Windows operating system and an exploit the National Security Agency developed to weaponize the bug. In April 2017, the exploit leaked to the public, part of the fifth release of alleged NSA tools by the still mysterious group known as the Shadow Brokers. Unsurprisingly, the agency has never confirmed that it created EternalBlue, or anything else in the Shadow Brokers releases, but numerous reports corroborate its origin—and even Microsoft has publicly attributed its existence to the NSA.

The tool exploits a vulnerability in the Windows Server Message Block, a transport protocol that allows Windows machines to communicate with each other and other devices for things like remote services and file and printer sharing. Attackers manipulate flaws in how SMB handles certain packets to remotely execute any code they want. Once they have that foothold into that initial target device, they can then fan out across a network.

Microsoft released its EternalBlue patches on March 14 of last year. But security update adoption is spotty, especially on corporate and institutional networks. Within two months, EternalBlue was the centerpiece of the worldwide WannaCry ransomware attacks that were ultimately traced to North Korean government hackers. As WannaCry hit, Microsoft even took the "highly unusual step" of issuing patches for the still popular, but long-unsupported Windows XP and Windows Server 2003 operating systems.

In the aftermath of WannaCry, Microsoft and others criticized the NSA for keeping the EternalBlue vulnerability a secret for years instead of proactively disclosing it for patching. Some reports estimate that the NSA used and continued to refine the EternalBlue exploit for at least five years, and only warned Microsoft when the agency discovered that the exploit had been stolen. EternalBlue can also be used in concert with other NSA exploits released by the Shadow Brokers, like the kernel backdoor known as DarkPulsar, which burrows deep into the trusted core of a computer where it can often lurk undetected.

Eternal Blues

The versatility of the tool has made it an appealing workhorse for hackers. And though WannaCry raised EternalBlue's profile, many attackers had already realized the exploit's potential by then.

Within days of the Shadow Brokers release, security analysts say that they began to see bad actors using EternalBlue to extract passwords from browsers, and to install malicious cryptocurrency miners on target devices. "WannaCry was a big splash and made all the news because it was ransomware, but before that attackers had actually used the same EternalBlue exploit to infect machines and run miners on them," says Jérôme Segura, lead malware intelligence analyst at the security firm Malwarebytes. "There are definitely a lot of machines that are exposed in some capacity."

Even a year after Microsoft issued a patch, attackers can still rely on the EternalBlue exploit to target victims, because so many machines remain defenseless to this day. "EternalBlue will be a go-to tool for attackers for years to come," says Jake Williams, founder of the security firm Rendition Infosec, who formerly worked at the NSA. "Particularly in air-gapped and industrial networks, patching takes a lot of time and machines get missed. There are many XP and Server 2003 machines that were taken off of patching programs before the patch for EternalBlue was backported to these now-unsupported platforms."