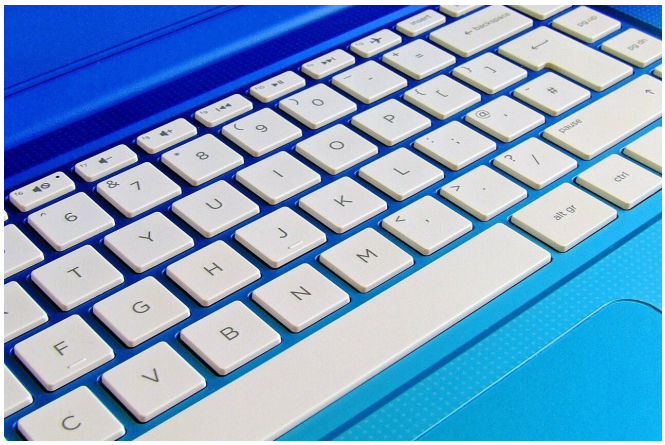
# BlueKeep exploit in the wild is not devastating but sleuths stay cautious

5 November 2019, by Nancy Cohen



Credit: CC0 Public Domain

A security exploit called BlueKeep is in the wild. Security watchers on numerous sites all reported that researchers had spotted evidence of exploitation. *HotHardware* said that so far the signs were that affected machines were being used to mine cryptocurrency.

(The bug in Microsoft's Remote Desktop Protocol, said *Wired*, "allows a hacker to gain full remote code execution on unpatched machines.")

Davey Winder. who covers cybersecurity, told readers in Forbes: The BlueKeep vulnerability that exists in unpatched versions of Windows Server 2003, Windows XP, Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2 has taken on a new bit of news: "it's now been confirmed that a BlueKeep exploit attack is currently ongoing."

As *Wired* said, the researchers have found evidence "that their so-called honeypots—bait machines designed to help detect and analyze malware outbreaks—are being compromised en masse using the BlueKeep vulnerability."

Paul Lilly in *HotHardware* said security researcher Kevin Beaumont had noticed "multiple honeypots in his EternalPort RDP network crashing and rebooting."

Back in July, Lilly had delivered a report that security researchers at Sophos created a proof-of-concept demonstration showing how easy it would be for an unpatched RDP (Remote Desktop Protocol) server to be compromised by BlueKeep, a Windows bug. Back then, the researchers had hoped the demo would scare companies into patching Windows.

So, fast-forward to this month. What is BlueKeep's target? Andy Greenberg in *Wired* said that "the widespread BlueKeep hacking merely installs a cryptocurrency miner, leeching a victim's processing power to generate cryptocurrency."

Not that security experts did not see this coming. Forbes provided an account of events.

"On June 4," wrote Winder, "the National Security Agency (NSA) took the unusual step of publishing an advisory urging Microsoft Windows administrators to update their operating system or risk a 'devastating' and 'wide-ranging impact' in the face of a growing threat.

"This warning was given even more gravitas on June 17 when the U.S. Government, via the Cybersecurity and Infrastructure Security Agency (CISA), issued an 'update now' activity alert. At much the same time, security researchers were predicting that a 'devastating' BlueKeep exploit was only weeks away."

Now that we are into November, Kryptos Logic has found it curious "that this publicly known wormable vulnerability, known to everyone who would care to know for at least six months, took this long to get detectably weaponized. One might theorize that attackers know they have essentially one shot at

using it at scale, and it becomes a game of chicken as to who will do it first."

Lilly said the good news here is it did not self-propagate.

*Threatpost* shared its observation. "The first attacks that exploit the zero-day Windows vulnerability install cryptominers and scan for targets rather than a worm with WannaCry potential." *Threatpost* found the attacks to be "Initially underwhelming," not nearly as bad as it could have been. As *Wired* explained, Rather than a worm that jumps unassisted from one computer to the next, these attackers appear to have scanned the internet for vulnerable machines to exploit."

Kryptos Logic has concluded that the alleged activity was concerning, {the Kryptos Logic blog posted a Twitter thread reporting BSODs, blue screens of death, across Beaumont's network of BlueKeep Honeypots] but consider that the information security community had predicted worse potential scenarios.

"Based on our data we are not seeing a spike in indiscriminate scanning on the vulnerable port like we saw when EternalBlue was wormed across the Internet in what is now known as the WannaCry attack."

Rather, said Kryptos Logic, it seemed likely "a low-level actor scanned the Internet and opportunistically infected vulnerable hosts using out-of-the-box penetration testing utilities."

Elizabeth Montalban in *Threatpost*, nonetheless, summarized why "this doesn't mean security administrators can rest easy just yet. This lackluster initial performance could represent more the unsophistication of the hackers than the nature of the vulnerability itself, observers noted."

Greenberg also preferred not to forget potential scenarios, of machines hit with a more serious—and more virulent—specimen of malware that exploits Microsoft's lingering RDP vulnerability. "That could take the form of a ransomware worm in the model of NotPetya or also WannaCry, which infected almost a quarter million computers when it spread in May of 2017, causing somewhere between $4 and $8 billion damage."

**More information:**
www.kryptoslogic.com/blog/2019 … spotted-in-the-wild/

APA citation: BlueKeep exploit in the wild is not devastating but sleuths stay cautious (2019, November 5) retrieved 7 December 2021 from https://techxplore.com/news/2019-11-bluekeep-exploit-wild-devastating-sleuths.html