Hacker revealed the second Zero-Day, broke Windows' EoP vulnerability patch

A security researcher with a nickname SandboxEscaper recently publicly shared a second zero-day exploit, which can be used to break up an advanced security patch for a privileged vulnerability that is only currently available. Here in Microsoft Windows operating system.

A security researcher with a nickname SandboxEscaper recently publicly shared a second zero-day exploit, which can be used to break up an advanced security patch for a privileged vulnerability that is only currently available. Here in Microsoft Windows operating system.

1. Microsoft Azure is being used to host malware and C2 servers

SandboxEscaper is one of the most famous hackers in hunting for vulnerabilities on Windows. This security researcher has repeatedly published zero-day exploits towards unpatched Windows vulnerabilities. In 2018 alone, SandboxEscaper revealed a total of more than half a dozen zero-day vulnerabilities in the Windows operating system without really bothering to tell Microsoft about the product's problems in advance. they.

1. GoldBrute botnet campaign is trying to hack 1.5 million RDP servers worldwide

In just two weeks ago, SandboxEscaper revealed four new exploits of Windows exploits, one of which exploits could allow an attacker to bypass an advanced security patch for privileged vulnerabilities (CVE-2019-0841).) in Windows, exists when Windows AppX Deployment Service (AppXSVC) handles hard links incorrectly.

Now, the hacker once again claims to have found a new way to bypass the security patch Microsoft released for the same vulnerability, allowing a malicious application specifically designed to automatically escalates privileges for itself, and eventually takes complete control of the targeted Windows computer even though the system has been updated to the latest Microsoft patch.

1. Microsoft rushed to release security updates for Windows XP, Server 2003

This new exploit is named ByeBear, and as you can see in the demo video above, ByeBear will abuse the Microsoft Edge browser to write an optional access control list (DACL) as a system privilege (SYSTEM privilege).

The next patch for the flaw is likely to be released by Microsoft according to the Tuesday update schedule, scheduled for June 11. Please wait and see if the Windows team has acknowledged that their system had problems in the previous 4 exploits, and whether they can provide a specific security fix to resolve this vulnerability neatly. is not.