Issued 3/24/17

Vulnerability Allows Hackers to Hijack Antivirus Software on Any Windows Version

Security company Cybellum discovered a new zero-day attack that makes it possible for hackers to take control of the antivirus software running on a Windows system using a vulnerability that exists in all Windows versions out there, starting with Windows XP and ending with the most recent build of Windows 10.

The company explains in a blog published today that most major antivirus solutions are affected by this vulnerability, Including Avast, AVG, Avira, Bitdefender, Trend Micro, Comodo, ESET, F-Secure, Kaspersky, Malwarebytes, McAfee, Panda, Quick Heal, and Norton. Called DoubleAgent, the exploit relies on a legitimate tool that Microsoft itself is offering in Windows and is named “Microsoft Application Verifier.” Built to help developers find bugs in their applications, this tool can be hijacked to replace the standard verifier with a custom verifier, which enables an attacker to take full control of the app.

The next step is to register a compromised DLL for a process belonging to security software, which in turn opens the door to more malicious activities, such as installing backdoors, add exclusions, delete files or even encrypt them in the typical ransomware attack. Cybellum says it has already notified the affected security companies, but until now, only Malwarebytes and AVG released a patch. “The sad, but plain fact is that the vulnerability is yet to be patched by most of the antivirus vendors and could be used in

the wild to attack almost any organization that uses an antivirus. Once the attacker has gained control of the antivirus, he may command it to perform malicious operations on behalf of the attacker," the firm says. What's worse is that DoubleAgent has the capabilities of injecting code even after users reboot the systems or install patches and updates, making it very difficult to remove the malware. Being a new persistence technique, DoubleAgent bypasses AV, NGAV and other endpoint solutions, and giving an attacker ability to pperform his attack undetected with no time limit," the blog post reads.