30-year-old file format behind MacOS hack

August 6 2020, by Peter Grad

Credit: CC0 Public Domain

A security expert revealed this week that an exploit commonly used against Windows users who own Microsoft Office can sneak into MacOS systems as well.

A former NSA security specialist who addressed the Black Hat security

conference this week summarized his research into the new use for a very old exploit.

Patrick Wardle explained that the exploit capitalizes on the use of macros in Microsoft Office. Hackers have long used the approach to trick users into granting permission to activate the macros, which in turn surreptitiously launch malicious code.

But Wardle noted that attacks against Mac systems using such macros began occurring around 2017. In 2018, the internet security company Kaspersky uncovered evidence that North Korean hackers infected a cryptocurrency exchange in what was believed to be the first such assault on a MacOS system. Hackers residing under the world's most repressive regime may have earned up to $2 billion in cryptocurrency hacks, according to a report released why the United Nations last year.

The hacks rely on the use of two additional weak spots, one a nearly 30-year-old file format little used in recent years. While Microsoft Office generally prompts users before a macro is executed, the old SYLK Excel file format (.SLK) does not trigger a prompt. Thus, it can be used to bypass a line of security.

Wardle noted that Microsoft Office handles code for old files differently than code for newer ones.

When researchers alerted Apple to the .SLK vulnerability last year, Wardle said, Microsoft declined to issue a patch, asserting that malicious code would be contained within the secure Microsoft Office sandbox environment.

Wardle, who slyly proclaimed, "Working at the NSA corrupted my mind and filled it with evil ideas," set out to test those boundaries of the sandbox protection. In a matter of days, he found a vulnerability.

By beginning a filename with the "$" character, he learned, a file can break out of the sandbox and avoid detection.

"Security researchers love these ancient file formats because they were created at a time when no one was thinking about security," Wardle told Motherboard.

Microsoft has patched the SYLK vulnerability and says it is communicating with Apple on addressing other issues raised by the research of Wardle and others.

Wardle fears these hacks may be just the tip of the iceberg.

"I was surprised how easy it was," to devise these hacks, Wardle told Wired magazine. "I do have experience doing this, but it would be arrogant for me to think that well-resourced hacker groups aren't looking at this and don't have similar talents, if not more so. It's a very broad attack vector. Sufficiently resourced and clever hackers will find ways to gain access and persist on Mac systems."

Dutch researcher Stan Hegt, who uncovered the SYLK macro vulnerability, praised Wardle's research but also cautioned there likely are more problems to come.

"The fact that he's now built a full exploit chain definitely proves a point," said Hegt. "I'm pretty sure if you dig deep in Office, especially on Macs, there's more" troublesome issues to uncover.

More information: objective-see.com/blog/blog_0x4B.html