Issued 4/11/17

Microsoft Zero-Day Attacks See Hackers Target Word Users

A new zero-day vulnerability that affects all supported versions of Microsoft Word has been uncovered and security researchers claim that hackers have already launched attacks in the wild, leveraging the bug. A patch is yet to be issued out for this particular vulnerability, which security experts believe, allows attackers to secretly infect systems with different kinds of malware.

The zero-day bug was disclosed by both McAfee and FireEye, who claimed to have notified Microsoft. However, the tech giant is slated to issue out a patch this week to coincide with Patch Tuesday, a Microsoft spokesperson confirmed, ZDNet reported. According to McAfee researchers, the "earliest attack" detected dates back to January. "The samples we have detected are organized as Word files (more specially, RTF files with '.doc' extension name). The exploit works on all Microsoft Office versions, including the latest Office 2016 running on Windows 10," McAfee researchers said.

The bug is triggered when users open a trick Word document, which then downloads a malicious HTML file. The file runs a script that hackers can use to install malware. FireEye researchers said, "The Microsoft HTA application loads and executes the malicious script. In both observed documents the malicious script terminated the winword.exe process, downloaded additional payload(s), and loaded a decoy document for the

user to see. The original winword.exe process is terminated in order to hide a user prompt generated by the OLE2link." In other words, hackers can attack affected systems, all the while bypassing security detecting mechanisms designed to prevent such attacks.

The most alarming aspect of this bug is that it does not rely on enabling macros to infect systems. This means that potential victims may likely not receive Office's alert to users when opening macro-enabled files. In other words, any Word file may potentially contain malicious content.