Threat Actors · July 04, 2019 · Cyware News

Chinese threat groups bank on improved RTF weaponizer to exploit security flaw

- The flaw in question is a stack buffer overflow vulnerability in Microsoft's Equation Editor.
- It was reported that this flaw was exploited since 2018 through an updated RTF weaponizer.

Security researchers from Anomali came across an improved version of a Rich Text Format (RTF) weaponizer used by multiple Chinese threat actors. As part of their analysis of this weaponized script, it was found that the updated version was used solely to exploit CVE-2018-0798 - a stack buffer overflow flaw in Microsoft's Equation Editor.

The earlier version of this "Royal Road" weaponizer was used to exploit two remote code execution vulnerabilities(CVE-2017-11882, CVE-2018-0802) in the same Equation Editor. Anomali researchers suggest that the groups now relied on CVE-2018-0798 due to its 'reliability' in all versions of Equation Editor.

The big picture

- Malware samples analyzed by the researchers were attributed to five Chinese threat actor groups. They are Conimes, KeyBoy, Emissary Panda, Rancor, and Temp.Trident.
- The campaigns using the improved RTF weaponizer were discovered from June 25, 2019, onwards.
- The earlier version of the weaponizer was used for approximately one year, starting from December 2017. After this period, it was reportedly used by other threat actors indicating that the creator of this weaponizer was selling it to others.
- Anomali researchers also came across various exploitation techniques that leveraged CVE-2018-0798 to drop malicious payloads.
- Some of these techniques included OLE package objects, DLL Sideloading and dropping malicious '.wlf' files in Windows startup folders.

Worth noting

The researchers indicate the reason on why threat actors opted for CVE-2018-0798 exploitation. "CVE-2017-11882 is only exploitable on an unpatched version prior to its fix, and CVE-2018-0802 is only exploitable on the version released to fix CVE-2017-11882. In contrast, a threat actor utilizing CVE-2018-0798 has a higher chance of success because it is not limited by version," they said.

RANCOR | Microsoft Office Equation Editor | Weaponized RTF Document | Chinese APT Groups | KeyBoy

READ PREVIOUS
Fake Android app serves bogus 'Samsung firmware updates ...
Malware and Vulnerabilities

READ NEXT
Lenovo servers contained major security vulnerabilities
Malware and Vulnerabilities