

Forum:[Hack Forums](#)

Thread: [Sharing New attack technique that uses YouTube and Office documents to spread malware](#)

cloudykoosh - November 15, 2018, 8:30 am

New attack technique uses YouTube and Office documents to spread malware

A successful attack could allow an attacker to execute any malicious code on a targeted computer.

This attack could be executed using other kinds of video into Word documents, instead of YouTube.

A new attack technique that allows attackers to embed malicious code into videos in Microsoft Word documents has been discovered by security experts. The technique allows malicious JavaScript code execution when a user clicks on a YouTube video thumbnail attached within a Word document.

A hacker could also conduct this attack without alerting the user or requesting user consent about executing malicious code. A successful attack could allow an attacker to execute any malicious code on a targeted computer.

The attack technique was discovered by researchers, who also developed a proof-of-concept attack utilizing a YouTube video link and a Microsoft Word document. However, researchers also said that this attack could also be executed using other kinds of video into Word documents, instead of YouTube, but did not test this attack vector.

Attack method

Researchers were able to perform this attack by exploiting the video-embedding feature that creates an HTML script behind the video image. This, in turn, gets executed by Internet Explorer when the thumbnail inside the document is clicked by the user. This HTML code could also be modified by attackers to point to the malware instead of the YouTube video.

A file called 'document.xml', which is a default XML file used by Microsoft Word, could be extracted and edited to perform the attack. The configuration for the embedded video is made available with the 'embeddedHTML' file and an iFrame for the YouTube video, which can be replaced along with a preferred malicious HTML.

The proof-of-concept showed an HTML replacement that contained a Base64-encoded malware binary that opens the download manager for Internet Explorer, which, in turn installs the malware payload.

According to the researcher, this method requires some phishing skills to make a user click on the video thumbnail. "But keep in mind that the video image in the document will not show any trace of not being a legitimate YouTube video," he added.

Microsoft dismisses bug

The bug report along with the proof-of-concept was submitted to Microsoft three months ago but the method was not acknowledged as a vulnerability by Microsoft. Instead, Microsoft gave the go-ahead to publish the findings.

