Microsoft Office files that contain VBA macros have opened the door to thousands of computers for attackers. Spear phishers frequently use macro-enabled files to run malicious code on your computer, leaving your device infected and our network compromised.

What to Look For

As of 2016, file attachments containing macros were the second most popular delivery method of malware for spear phishers. These files can be identified by the letter “m” at the end of the file extension. Filetypes include .docm, .xlsm, and .pptm.

What Happens When I Download?

Macro-enabled files often slip past email filters and antivirus scanners because the file contains no malware at the time of download. When you run the file, you will be prompted to enable macros, which are disabled by default.

This experience will be different on a Mac or a Windows PC.

98%

of Microsoft Office related threats exploit macros. [1]

What are Macros?

Macros allow Microsoft Office users to automate repetitive or time-consuming tasks by using Visual Basic scripts or code. Macro code that you’ve written yourself is typically safe. Macros downloaded from outside sources can be used to retrieve malware.

Always keep macros disabled. Enabling macros at this point is like opening a door to your computer to let the attacker in. The attackers can then trigger code to activate or retrieve malware, like keyloggers, banking Trojans, or encryption ransomware.

Keyloggers

Steal information you type into files and browsers

Banking Trojans

Monitor your activity to gather your online bank account

Encryption Ransomware

Locks away your files in exchange for a ransom

What About Mobile?

Currently, macros are not supported by Microsoft Office apps for mobile devices, but some third-party applications do support macros. If you encounter a macro-enabled file on your phone or tablet, treat the file with the same caution.

Don’t download unsolicited/strange files, especially if the filetype ends with “m”.

Check the sender address, and verify with a quick telephone call if you know the sender.

Never enable macros. If a file with macros makes it onto your device, do not enable macros in your Microsoft Office app.

If you suspect a spear phishing attack targeting our organization using file attachments with macros, be sure to report it immediately.

MALICIOUS MACROS AND PHISHING EMAILS

[1] https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

COFENSE