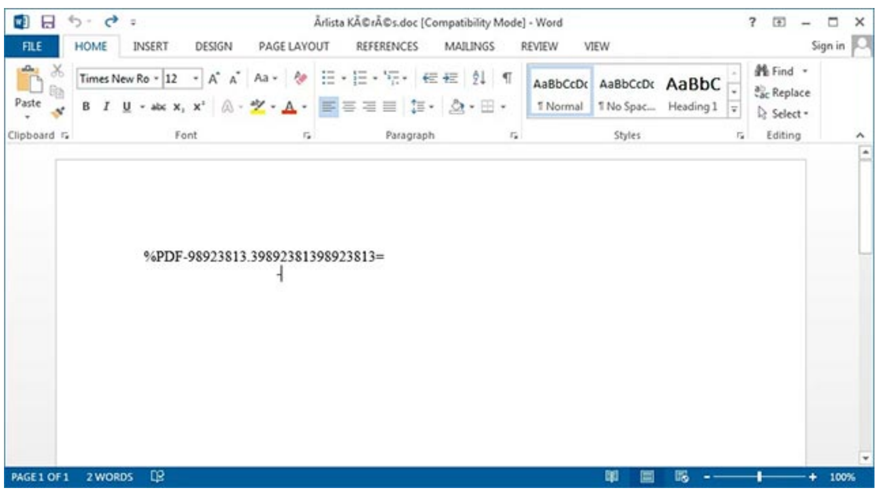
Microsoft warned about malicious spam campaigns using vulnerabilities in Office and Wordpad

Microsoft recently issued an emergency warning about an online spam campaign targeting European countries, currently using an exploit can easily infect users by simply opening an attachment. .

Microsoft recently issued an emergency warning about an online spam campaign targeting European countries, currently using an exploit can easily infect users by simply opening an attachment. .

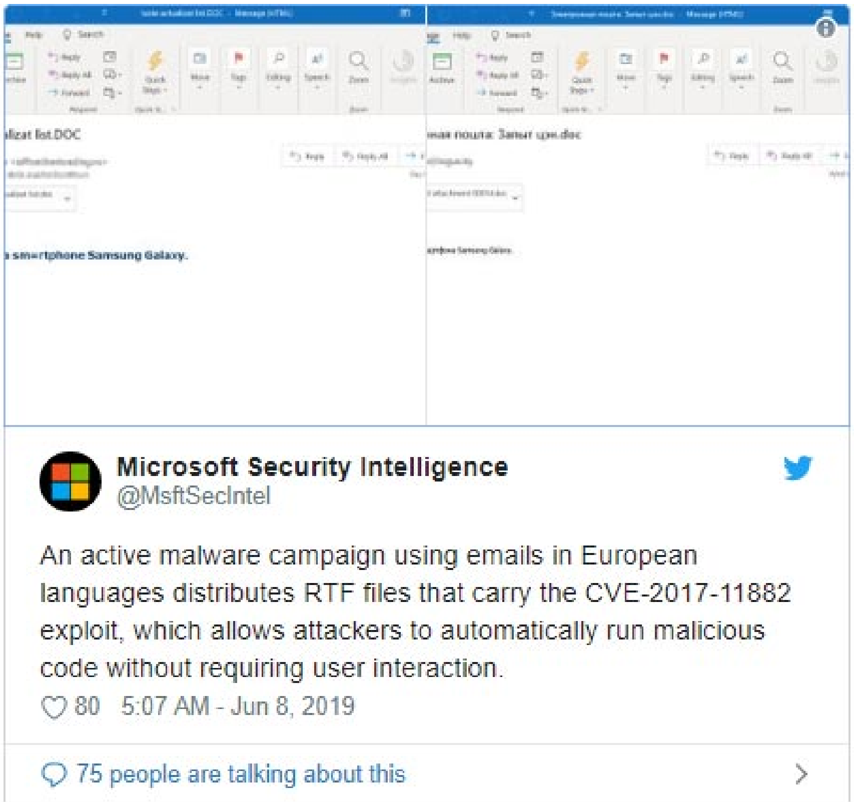
In a series of tweets posted from Microsoft Security Intelligence accounts on Twitter, Microsoft has repeatedly issued warnings that it has discovered a malicious campaign containing RTF attachments that abuse the CVE-2017 vulnerability. -11882 in Microsoft Office and Wordpad.



Example attached to the CVE-2017-11882 exploit

1. Hacker revealed the second Zero-Day, broke Windows' EoP vulnerability patch

When successfully exploited, this vulnerability can automatically infect users by simply opening a malicious attachment.



Microsoft Security Intelligence Alerts on Twitter

1. GoldBrute botnet campaign is trying to hack 1.5 million RDP servers worldwide

The CVE-2017-11882 vulnerability allows RTF and Word documents to be created to automatically execute certain commands after opening. This vulnerability has been successfully patched in 2017, but in fact, Microsoft continues to record small exploits used in attacks, especially showing signs of increasing. both in quantity and scope of impact in the past few weeks. Originally written by Microsoft as follows:

"Notably, Microsoft's security team has recorded a rapid increase in the number of malicious activities related to the CVE-2017-11882 vulnerability in the past few weeks. We really recommend you. Should apply the latest security updates to ensure the safety of your system ".

According to Microsoft experts, when the attachment is opened, it will "execute a large number of scripts of different types (VBScript, PowerShell, PHP, and others) to download the payload to the system. victim '.

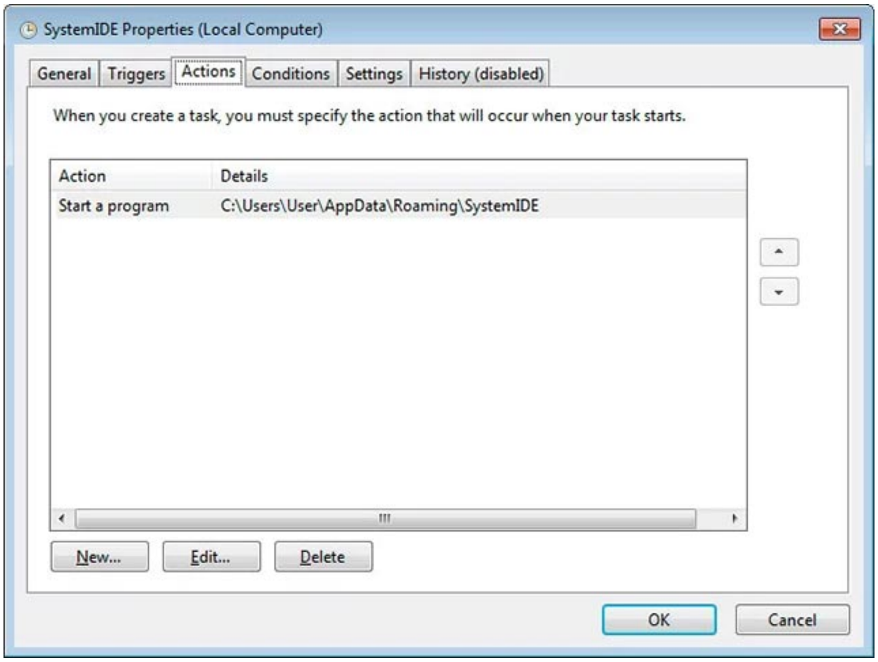
Researchers conducted one of the sample documents, when opening the document, it immediately began executing a script downloaded from Pastebin, executing the PowerShell command. This PowerShell command will then download an encrypted file named base64 and save the file to **% temp% bakdraw.exe.**

#	Result	Proto...	Host	URL	Body	Caching	Content-...	Process
16	200	HTTPS	pastebin.com	/raw/JVMDDmap	1,512	public, ...	text/plain...	eqnedt32:2124
18	200	HTTPS	s.put.re	/hvbE8LKw.exe	379,...	public, ...	applicatio...	powershell:4732
22	200	HTTPS	paste.ee	/r/t8PKG	201,...	public, ...	text/plain...	systemide:4260

Script and malware are being downloaded

1. Microsoft Azure is being used to host malware and C2 servers

Next, a copy of bakdraw.exe will be copied to the **% UserProfile% AppDataRoamingSystemIDE address** , and at the same time a scheduled task (Scheduled Task) named SystemIDE will be configured to start executing as well as modifying add sustainability.



Scheduled Task

1. Discovery of Trojan scattering steals virtual money through YouTube

The Microsoft side claims that this executable file is a backdoor currently configured to connect to a malicious domain that is no longer accessible. This means that although the computer will be infected, the backdoor will still not be able to communicate with its own command and control server (C2 server) to receive the command.

However, this payload can still easily be used for other forms of attack, so Microsoft recommends that all Windows users install the latest security update for this vulnerability as soon as possible.

The recent CVE-2017-11882 vulnerability has also been discovered by the FireEye team, and is currently being used in a campaign targeting several Central Asian regions, and establishing a new backdoor called HawkBall. . It is still unclear whether these campaigns are linked.

You finished reading the article "**Microsoft warned about malicious spam campaigns using vulnerabilities in Office and Wordpad**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.