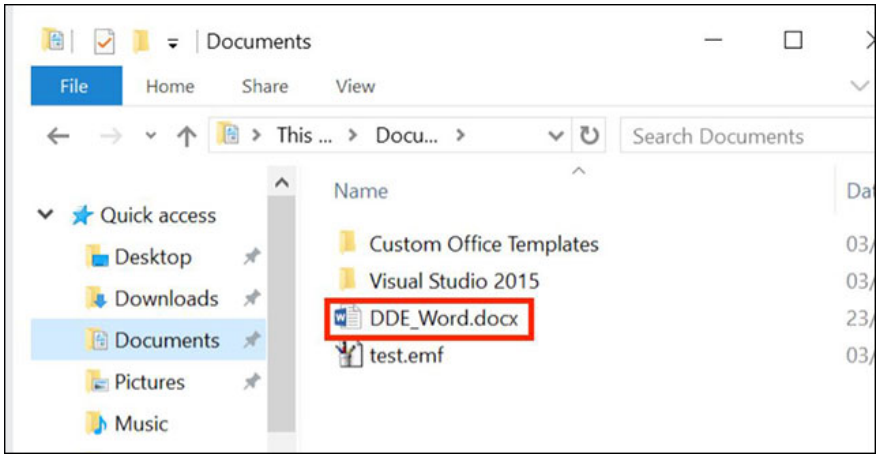
Features available on MS Office allow malware to enter without turning on the macro

Since cybercriminals appear more and more, traditional techniques become more mysterious when exploiting standard tools and protocols that are often overlooked.

Since cybercriminals appear more and more, traditional techniques become more mysterious when exploiting standard tools and protocols that are often overlooked.

Researchers at Cisco's Talos team have discovered an attack campaign that spreads Microsoft Word files with malware, executing code on a compromised machine without turning on Macros or affecting memory.

The Macro-less MSWord code execution technique is described by two researchers from Sensepost, Etienne Stalmans and Saif El-Sherei, using built-in MS Office features called Dynamic Data Exchange (DDE) to enforcement.



The file uses the DDE protocol, which is used to share data

The DDE protocol is one of the Microsoft methods that allows two applications to share the same data. Applications use this protocol to transfer data once and continue to exchange, whereby the application sends updates to each other when new data is available.

Thousands of applications are using the DDE protocol, including **Excel, MS Word, Quattro Pro and Visual Basic** .

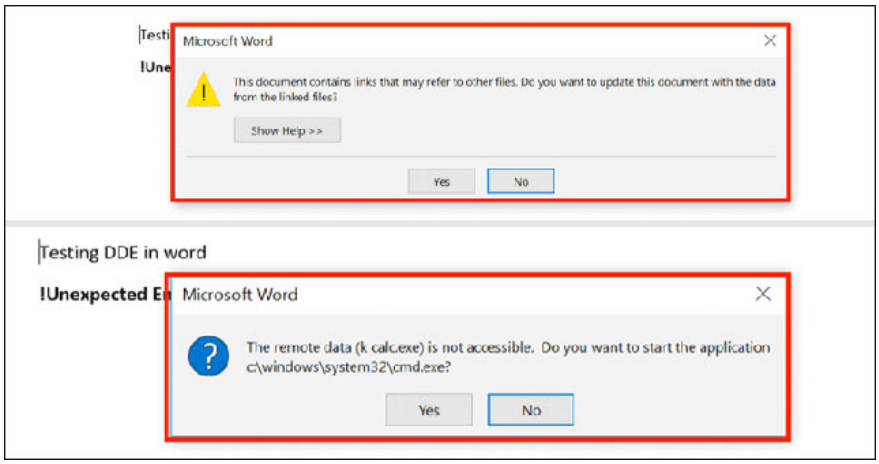
The mining technique described by the researchers does not show warnings to victims, except to ask if they want to execute the application in the command. However, this warning may also be 'modified syntax'.

MS Word DDE has been exploited in practice

According to Cisco's description, this technique has been exploited by hackers, targeting a number of organizations by using fake email of SEC (Securities Trading Commission).

> 'Emails containing malicious files [MS Word] can open up a complicated process of poisoning, leading to DNSMessenger malware infection,' Talos researchers said.

In early March, researchers at Talos discovered that DNSMessenger, a remote-access remote user, used a DNS query to execute a poisoned PowerShell command on the victim's machine.



Alerts direct users to another link

When opened, the victim receives a message that the file contains a link to the external file and asks for permission to deny or deny the content.

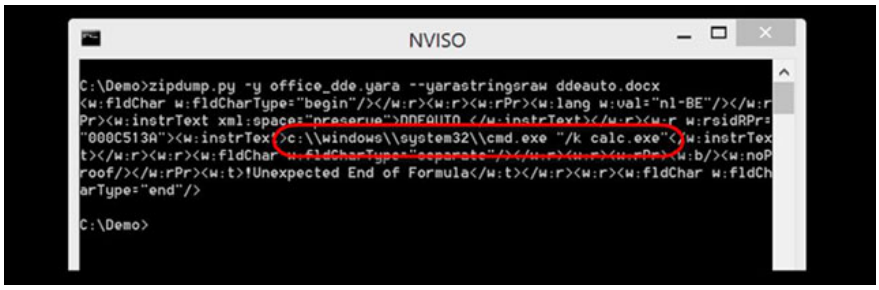
If allowed, the infected file will communicate with the content of the host attacker to retrieve the code and then execute this code to start the DNS malware infection.

'Interesting is that the DDEAUTO that this file uses to get the code is hosted on a Louisiana state website, may have been attacked and used for this purpose'.

How to detect MS Word DDE attack?

More worrisome is that MIcrosoft does not consider this a security issue, but according to them, the DDE protocol is a feature that cannot be deleted but can be improved to warn better in the future.

Although there is no direct way to disable the execution of DDE code, users can actively check the event history to see if it is exploited.



Instructions from NVISO to detect if the device has been attacked by malware

In addition, researchers at NVISO Labs also introduced 2 rules to detect DDE in Office Open XML file. *https://blog.nviso.be/2017/10/11/detecting-dde-in-ms-office-documents/*

You finished reading the article "**Features available on MS Office allow malware to enter without turning on the macro**" 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.
