JASK THREAT ADVISORY | TLP: WHITE | RISK FACTOR: HIGH

MICROSOFT OFFICE DDE PROTOCOL ABUSE DRIVING CRIMEWARE CAMPAIGNS

OVERVIEW

A number of crimeware campaigns observed in the field are using Microsoft DDE protocol as the main attack vector. Microsoft DDE is a software feature designed to transfer data between applications. "Dynamic Data Exchange (DDE) protocol sends messages between applications, uses shared memory to exchange data between applications. Applications can use the DDE protocol for data-transfers or continuous exchanges."*

This protocol is a feature of Microsoft software and can be used for things such as mail merges whereas a document has sometimes millions of addresses that need to be mixed and matched with printing content. The ability to transfer information also allows this protocol to execute commands as well; this function can be abused to allow command execution and bypass system protections designed to prevent Office applications to execute commands that allow attackers to run malicious payloads on victim computers. This exploit was recently demonstrated by recently by PwnDizzle and security firm SensePost.

The novelty of this type of attack is that current Microsoft Office security controls can be bypassed as they are mainly focused on preventing MACROS, which are portions of code used to expedite the application functions that can be used as well for malicious purposes. Current mitigation mechanism requires application of Active Directory Group Policy Object (GPO) which may take some time and latency depending on enterprise architecture. Several crimeware campaigns are being reported using this vector along with payloads such as Locky/Ransomware, fake Word document with alleged Windows product keys, Hancitor malspam, Vortex ransomware, phishing links embedded in Outlook body emails, and APT driven SEC spear phishing campaigns. This attack vector is not preventable by Antivirus.

INDICATORS

The principal delivery mechanism is via email; malicious actors can as well host documents with malicious code and use social engineering to drive users to download and execute DDE embedded content with malicious code. One of the characteristics of this attack is that users are presented some warnings before executing code, providing a window for this attack to be discovered or stopped. This means users must download the document, open it then go through a series of warnings before the code is executed. In the case of embedded invitations, the user must accept it (Click Yes) in order for the code to run.

Some of the observed delivery methods include:

– DDE Code embedded in Microsoft Word/Excel documents attached to an email

– Emails with misleading links to download DDE code embedded documents

– DDE code embedded in email message body in Outlook (Meeting/RTF body format)

LAB STUDY

The following are some screen captures of this attack vector, simply embedding commands to call up calc.exe by going into Insert tab -> Quick Parts -> Field and placing {DDEAUTO c:\\windows\\system32\\cmd.exe "/k calc.exe" }.

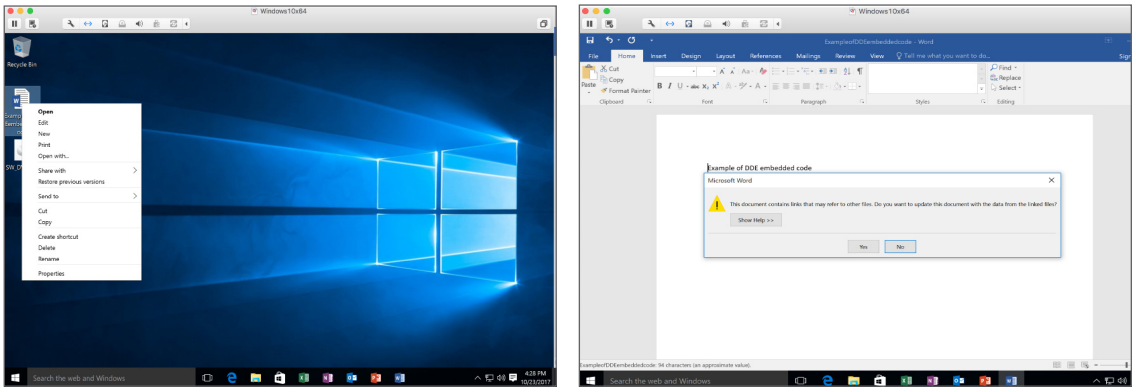

Fig 1.1 Warnings are displayed about subsequent execution of DDE embedded code on a Win 10 64Bit host with MS Office 2016.

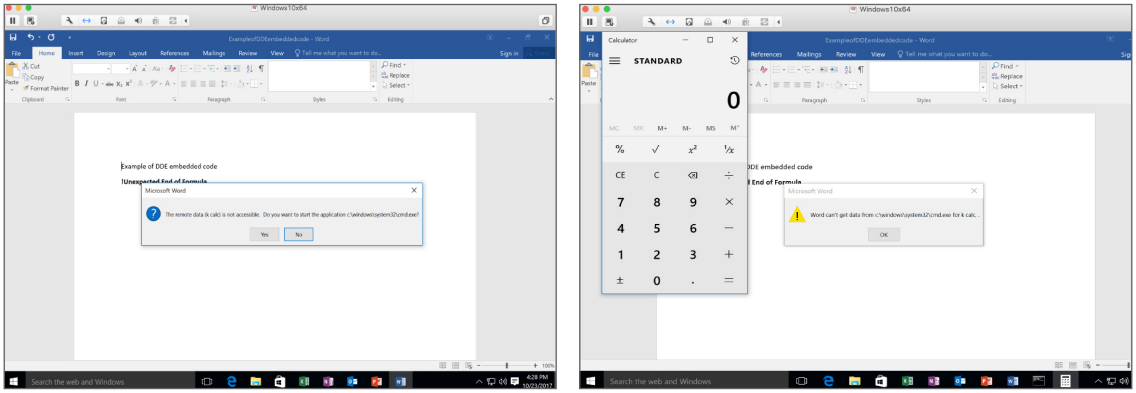

Fig 1.2 Subsequent warnings are presenting before finally executing code (calc.exe)

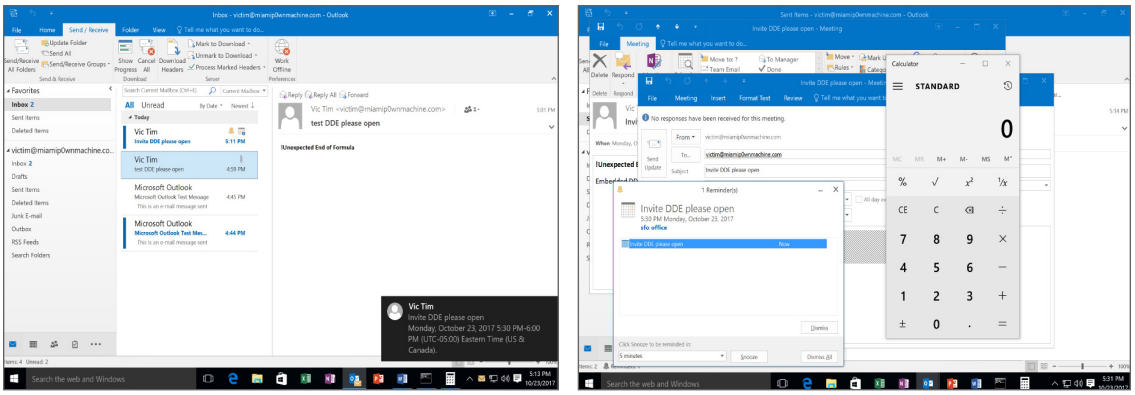

Fig 1.3 Shows Outlook embedded invitation variant.

The above simple examples can be used to download malicious payload onto the victim and take over the machine. Notice on Figure 1.3 that downloading or opening a document is not necessary as it is embedded into the body of email. It is also very likely that new variants and obfuscation techniques will add to this type of attack in order to bypass security controls.

JASK DETECTION

JASK Trident has several mechanisms to detect delivery of malicious documents via phishing links or malicious download, including the following:

- Password Zip protected file download
- Non TLD file download
- Presence of iframes, javascript, pagerank, source of images, redirects
- Presence of .exe, .pdf, .bat, ps1, ps, .bin, .bat, .jar, .bin, .zip

The above microbehaviors can help detect these types of attacks, considering the difficulty of detection by Antivirus (Not detected as of the writing of this advisory) and the nature of DDE of being a feature for documents sharing data between applications, not a bug or a vulnerability, it works as it is expected to work.

MITIGATION

First and foremost train users in spotting emails with suspicious content or sources. Users can effectively stop these attacks if they simply do not click on the warnings that allow code execution. This might be more difficult in the case of targeted spear phishing attacks, however a security conscious user can effectively avoid and prevent this type of attack. The links below provide items that can mitigate this type of attacks and should be used as guidance and tested for every specific environment in order to determine their effectiveness.

Apply GPO disabling DDE code execution via registry
http://blog.inquest.net/blog/2017/10/13/microsoft-office-dde-macro-less-command-execution-vulnerability/

Disable DDEAUTO
https://www.ghacks.net/2017/10/23/disable-office-ddeauto-to-mitigate-attacks/

Disable automatic view/open of DDE word documents/MS Word GPO
https://www.vertekmti.com/malware-distributed-via-ms-office-dde-feature-no-macros-required/

Select to view emails only in plain text in Outlook
https://support.office.com/en-us/article/Read-email-messages-in-plain-text-16dfe54a-fadc-4261-b2ce-19ad072ed7e3

Yara rules
https://blog.nviso.be/2017/10/11/detecting-dde-in-ms-office-documents/
https://github.com/InQuest/yara-rules/blob/master/Microsoft_Office_DDE_Command_Execution.rule

JASK

ABOUT JASK.AI

JASK monitors networks end to end, surfacing, triaging and mapping the most relevant attacks at unprecedented speed, using advanced AI. Analysts are empowered to make informed decisions faster and with more precision.

www.jask.ai