EDR/AV Evasion

WHITE PAPER

Table of Contents

Introduction

This whitepaper describes the importance of EDR security and gives a quick glimpse of EDR evasion techniques. The objective of this paper is to provide insights on endpoint security as an increasingly vital component of any organization's cybersecurity strategy.

Abbreviation

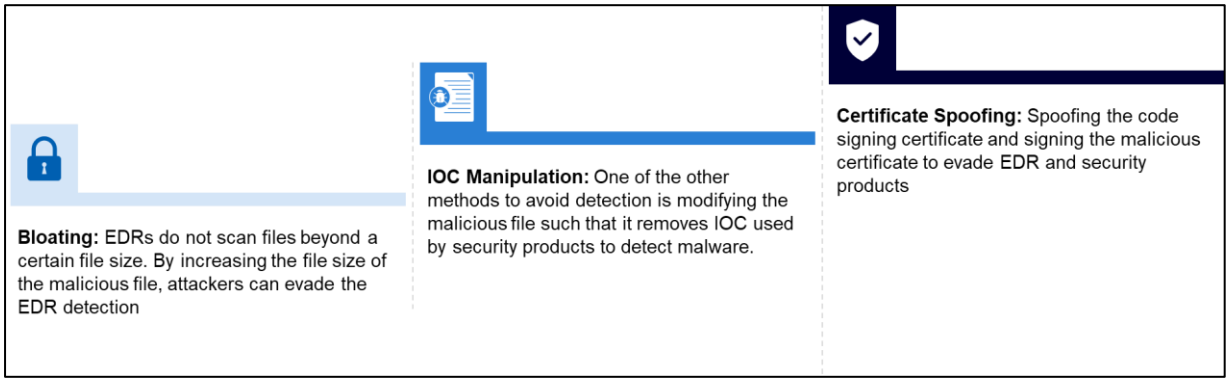
Sl. No.	Acronyms	Full Form
1.	EDR	Endpoint Detection and Response
2	AV	Antivirus
3	IOC	Indicator of compromise

Market Trends & Challenges

EDR evasion capabilities have grown significantly in the past several years. It is easy to find many publicly available approaches for defeating EDR tools. A strong endpoint security is an increasingly vital component of any organization's cybersecurity strategy. The information available on existing EDR evasion capabilities will be explored as this can aid threat hunters in detection. Deploying an effective EDR security solution is essential to protecting enterprises/organizations from cyber threats.

Let us look at the current methods that hackers use to evade EDR detection:

Different Methods to Evade EDR Detection:



1. **Bloating:** Cyber attackers can evade EDR detection by increasing the file size of the malicious file as EDRs do not scan files beyond a certain file size

2. **IOC Manipulation:** Attackers also use other methods such as modifying the malicious files in a manner that it removes IOC used by security products to detect the malware

3. **Certificate Spoofing:** Hackers also spoof code signing certificates and sign malicious files to evade EDR and security products

Shown below are some sample screenshots of the various stages of EDR evasion

1) Detection before bloating (Fig 1)

Ad-Aware	Trojan.GenericKD.62515700	AhnLab-V3	Malware/Win.Malware-gen.R525063
ALYac	Trojan.GenericKD.62515700	Antiy-AVL	Trojan/Generic.ASMalwS.5170
Arcabit	Trojan.Generic.D3B9E9F4	Avast	Win32:CrypterX-gen [Trj]
AVG	Win32:CrypterX-gen [Trj]	Avira (no cloud)	TR/Injector.mprib
BitDefender	Trojan.GenericKD.62515700	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.90de66	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Cerber.XHPT-9103
DrWeb	BackDoor.Siggen2.4144	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.GenericKD.62515700 (B)	eScan	Trojan.GenericKD.62515700
ESET-NOD32	A Variant Of Win32/Injector.ESCG	Fortinet	W32/GenKryptik.FSCS!tr
GData	Trojan.GenericKD.62515700	Google	Detected
Gridinsoft (no cloud)	Ransom.Win32.Wacatac.sa	Ikarus	Trojan-Spy
K7AntiVirus	Trojan (005991d21)	Kaspersky	UDS:Trojan.Win32.Agent.a
Kingsoft	Malware.kb.a.(kcloud)	Lionic	Trojan.Win32.Generic.4!c
Malwarebytes	Malware.AI.4278002693	MAX	Malware (ai Score=83)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	GenericRXAA-AAI3FFFA3952204
Microsoft	Ransom:Win32/CerberCrypt.PB!MTB	Palo Alto Networks	Generic.ml
Panda	Trj/RansomGen.A	Rising	Trojan.Generic@AI.85 (RDML:dd2hdPG…
Sangfor Engine Zero	Trojan.Win32.Agent.Vxhu	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Symantec	ML.Attribute.HighConfidence
Tencent	Win32.Trojan.Inject.Udkl	Trellix (FireEye)	Generic.mg.3fffa3952204057b
TrendMicro-HouseCall	TROJ_GEN.R053H0CJ622	VBA32	TScope.Trojan.Delf

Fig 1

2) Bloating the infected file (Fig 2)

```
mc@mc:/tmp/ezr$ ls -lh
total 7.0M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 4.8M Oct  7 15:05 infected
mc@mc:/tmp/ezr$ ./ezr --input infected --output infected_bloated --bloat 100

mc@mc:/tmp/ezr$ ls -lh
total 112M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 4.8M Oct  7 15:05 infected
-rwxrwxr-x 1 mc mc 105M Oct  7 21:40 infected_bloated
mc@mc:/tmp/ezr$
```

Fig 2

3) After bloating (Fig 3)

Acronis (Static ML)	Undetected	Alibaba	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	CrowdStrike Falcon	Undetected
Emsisoft	Undetected	F-Secure	Undetected
Gridinsoft (no cloud)	Undetected	Jiangmin	Undetected
K7GW	Undetected	Kaspersky	Undetected
Kingsoft	Undetected	Lionic	Undetected
Malwarebytes	Undetected	MaxSecure	Undetected
McAfee	Undetected	McAfee-GW-Edition	Undetected
Microsoft	Undetected	NANO-Antivirus	Undetected
Palo Alto Networks	Undetected	Panda	Undetected
QuickHeal	Undetected	Sangfor Engine Zero	Undetected
SecureAge	Undetected	Sophos	Undetected
SUPERAntiSpyware	Undetected	Symantec	Undetected
TACHYON	Undetected	TEHTRIS	Undetected
Tencent	Undetected	Trapmine	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
VirIT	Undetected	ViRobot	Undetected
Webroot	Undetected	Yandex	Undetected
Zillya	Undetected	ZoneAlarm by Check Point	Undetected
Zoner	Undetected	Avast-Mobile	Unable to process f
BitDefenderFalx	Unable to process file type	Cylance	Unable to process f

Fig 3

4) Before IOC Evasion (Fig 4)

Ad-Aware	Gen:Variant.Ransom.Hive.18	AhnLab-V3	Trojan/Win.Generic.C4991530
Alibaba	Trojan:Application/Redcap.1e5bc17d	ALYac	Gen:Variant.Ransom.Hive.18
Antiy-AVL	Trojan/Generic.ASMalwS.4D91	Arcabit	Trojan.Ransom.Hive.18
Avast	Win64:Trojan-gen	AVG	Win64:Trojan-gen
Avira (no cloud)	TR/Redcap.mirti	BitDefender	Gen:Variant.Ransom.Hive.18
Comodo	Malware@#395mahan0y3ht	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 99)
Cyren	W64/Agent.ECY.gen!Eldorado	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Ransom.Hive.18 (B)	eScan	Gen:Variant.Ransom.Hive.18
ESET-NOD32	A Variant Of WinGo/Agent.BE	Fortinet	W64/Agent.BE!tr
GData	Gen:Variant.Ransom.Hive.18	Google	Detected
Ikarus	Trojan.WinGo.Agent	Jiangmin	Trojan.Generic.hhcnf
K7AntiVirus	Trojan (0057dfcf1)	K7GW	Trojan (0057dfcf1)
Kaspersky	Trojan.Win32.Cobalt.eqz	Malwarebytes	Malware.AI.4192744535
MAX	Malware (ai Score=80)	MaxSecure	Trojan.Malware.119631590.susgen
McAfee	Artemis!127478CC9FEC	McAfee-GW-Edition	Artemis!Trojan
Microsoft	Trojan:Win64/Malgent!MSR	Panda	Trj/CI.A
Rising	Trojan.Agent!8.B1E (TFE:5:JVJTXwxksfP)	Sangfor Engine Zero	Trojan.WinGo.Agent.BE
SecureAge	Malicious	Symantec	Trojan.Gen.MBT
Tencent	Win32.Trojan.Cobalt.Dwjk	Trellix (FireEye)	Generic.mg.127478cc9fec34ee
TrendMicro	TROJ_GEN.R002C0WC122	TrendMicro-HouseCall	TROJ_GEN.R002C0WC122
VBA32	Trojan.Convagent	VIPRE	Gen:Variant.Ransom.Hive.18

Fig 4

5) Performing IOC Evasion (Fig 5)

```
mc@mc:/tmp/ezr$ ls -lh
total 4.5M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 2.3M Oct  7 16:35 infected
mc@mc:/tmp/ezr$ ./ezr --input infected --output infected_evaded --ioc

mc@mc:/tmp/ezr$ ls -lh
total 6.7M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 2.3M Oct  7 16:35 infected
-rwxrwxr-x 1 mc mc 2.3M Oct  7 22:10 infected_evaded
mc@mc:/tmp/ezr$
```

Fig 5

6) After IOC Evasion (Fig 6)

Ad-Aware	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	Comodo	Undetected
CrowdStrike Falcon	Undetected	Cybereason	Undetected
Cylance	Undetected	DrWeb	Undetected
Emsisoft	Undetected	eScan	Undetected
F-Secure	Undetected	GData	Undetected
Gridinsoft (no cloud)	Undetected	Ikarus	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kingsoft	Undetected	Lionic	Undetected
MAX	Undetected	McAfee	Undetected
McAfee-GW-Edition	Undetected	NANO-Antivirus	Undetected
Palo Alto Networks	Undetected	Panda	Undetected
QuickHeal	Undetected	Sangfor Engine Zero	Undetected
SentinelOne (Static ML)	Undetected	Sophos	Undetected
SUPERAntiSpyware	Undetected	Symantec	Undetected
TACHYON	Undetected	TEHTRIS	Undetected

Fig 6

7) Faking certificate (Fig 7)

```
mc@mc:/tmp/ezr$ ls -lh
total 8.2M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 4.8M Oct  7 15:05 infected
-rwxrwxrwx 1 mc mc 1.3M May 12 12:54 putty.exe
mc@mc:/tmp/ezr$ ./ezr --input infected --output infected_cert --cert-file putty.exe

mc@mc:/tmp/ezr$ ls -lh
total 13M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 4.8M Oct  7 15:05 infected
-rwxrwxr-x 1 mc mc 4.8M Oct  7 21:51 infected_cert
-rwxrwxrwx 1 mc mc 1.3M May 12 12:54 putty.exe
```

Fig 7

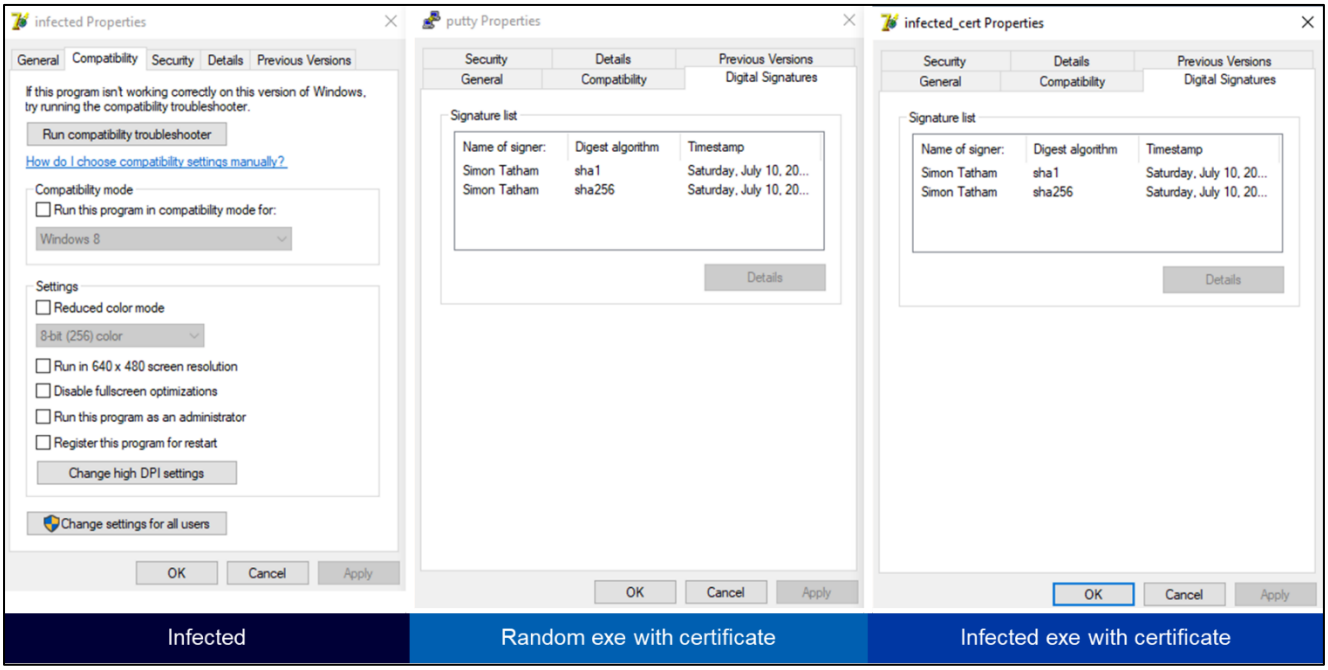


Fig 8

8) After certificate spoof (Fig 9)

Ad-Aware	Undetected	Alibaba	Undetected
ALYac	Undetected	Arcabit	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	CrowdStrike Falcon	Undetected
Cyren	Undetected	DrWeb	Undetected
Emsisoft	Undetected	eScan	Undetected
F-Secure	Undetected	GData	Undetected
Google	Undetected	Gridinsoft (no cloud)	Undetected
Ikarus	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kaspersky	Undetected
Kingsoft	Undetected	MAX	Undetected
McAfee	Undetected	McAfee-GW-Edition	Undetected
Microsoft	Undetected	NANO-Antivirus	Undetected
Palo Alto Networks	Undetected	Panda	Undetected
QuickHeal	Undetected	Sangfor Engine Zero	Undetected
SecureAge	Undetected	SentinelOne (Static ML)	Undetected
Sophos	Undetected	SUPERAntiSpyware	Undetected
Symantec	Undetected	TACHYON	Undetected
TEHTRIS	Undetected	Tencent	Undetected
Trapmine	Undetected	Trellix (FireEye)	Undetected

Fig 9

The following images show how hackers encrypt the Payload/Shell code using XOR

9) Common AV/EDR evasion methods for XOR shellcode (Fig 10)

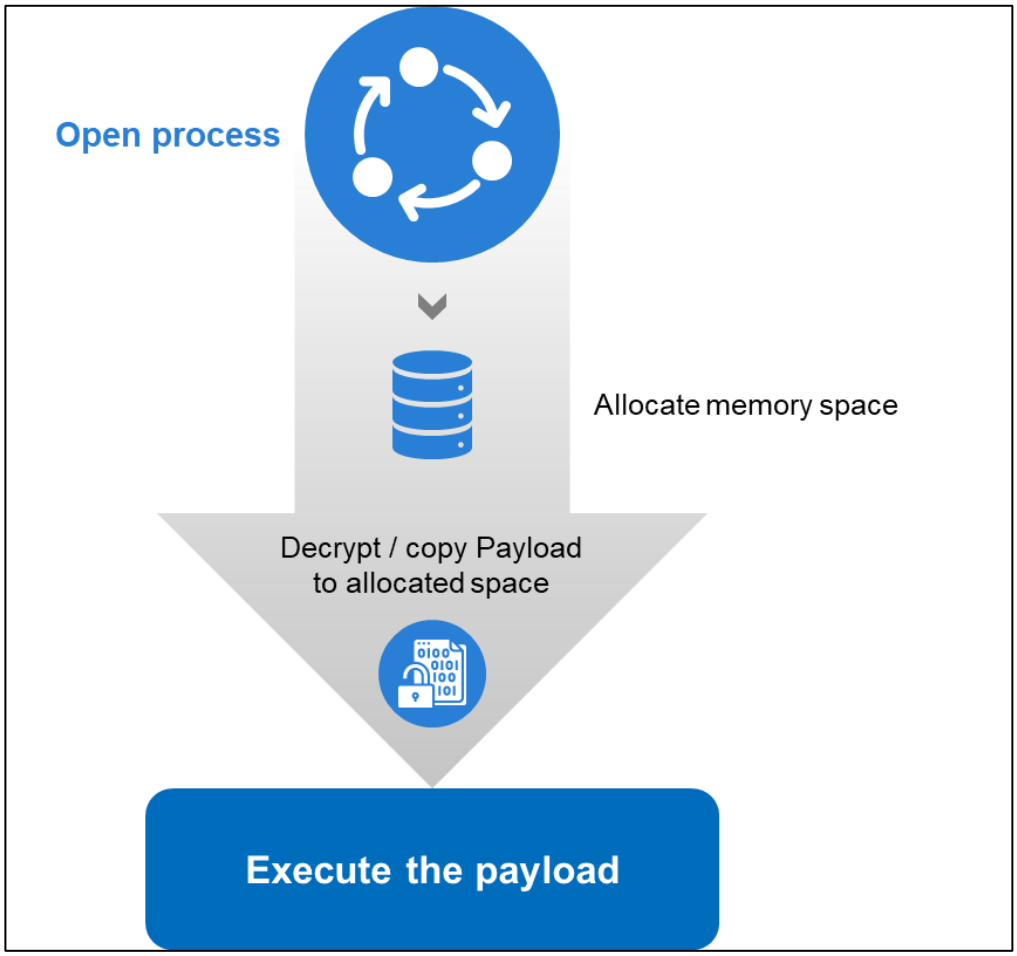


Fig 10

The drawback however is that common functions like memcpy, WriteProcessMemory are now detected on dynamic analysis by most AV's.

10) How the hackers encrypt the Payload/ Shell code using XOR (Fig 11)

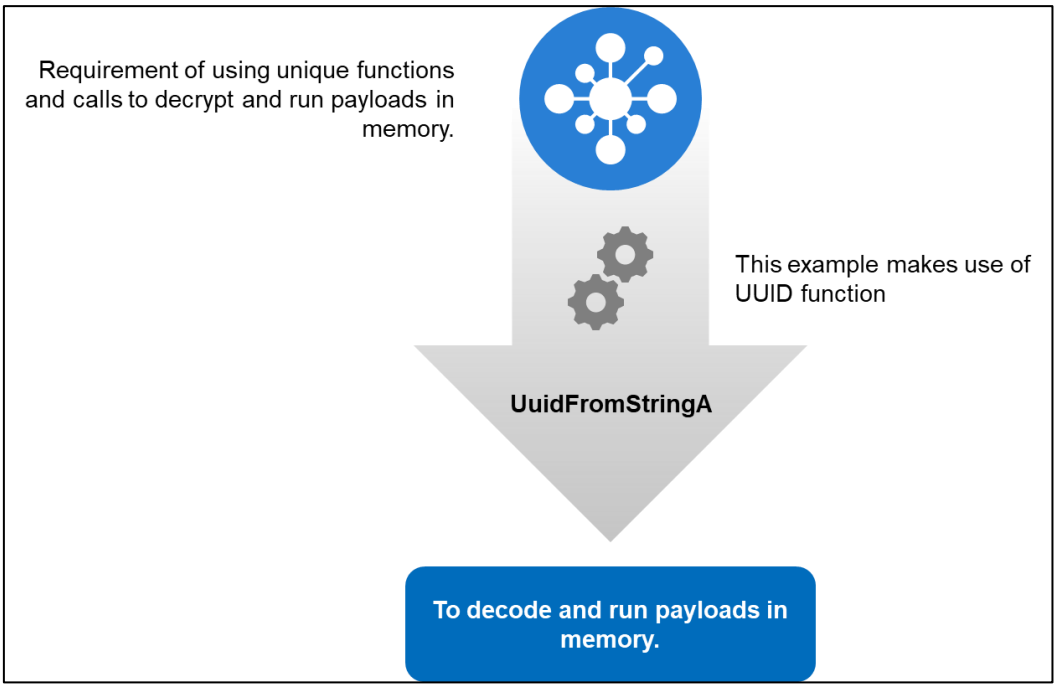


Fig 11

11) Steps to create the same (Fig 12)

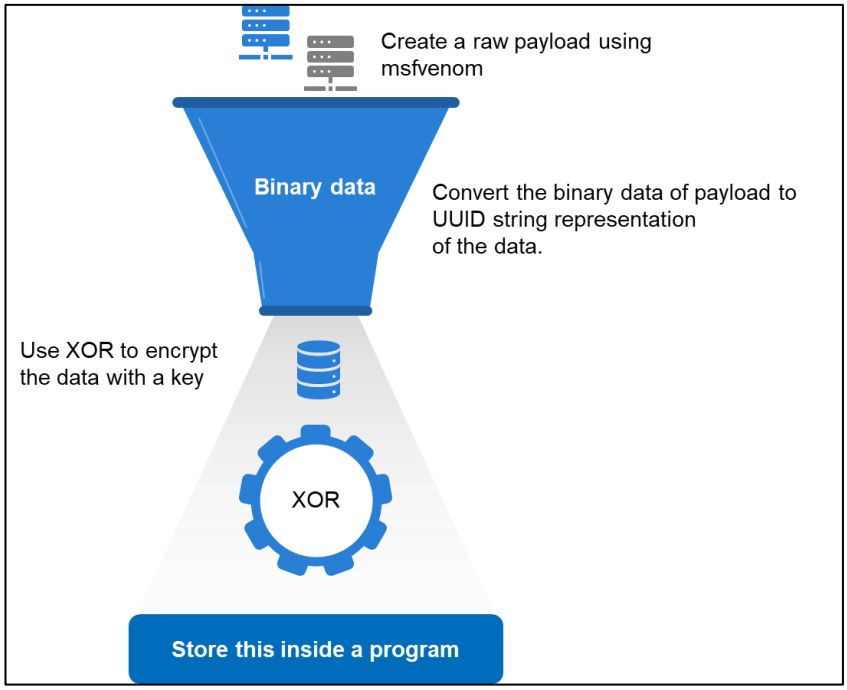


Fig 12

12) **Steps to execute payload from within program (Fig 13)**

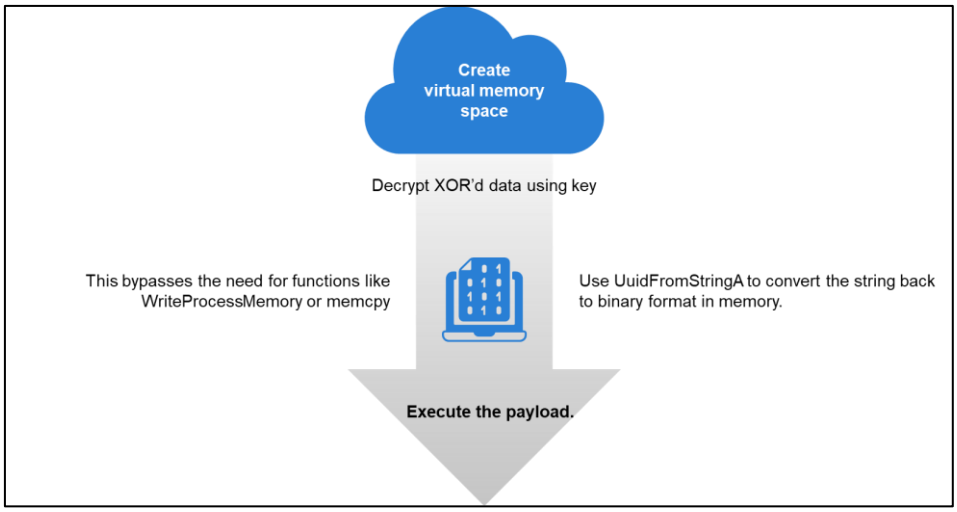


Fig 13

13) **Next few screenshots show how an executable is converted to an embedded zip file inside JScript (Fig 14)**

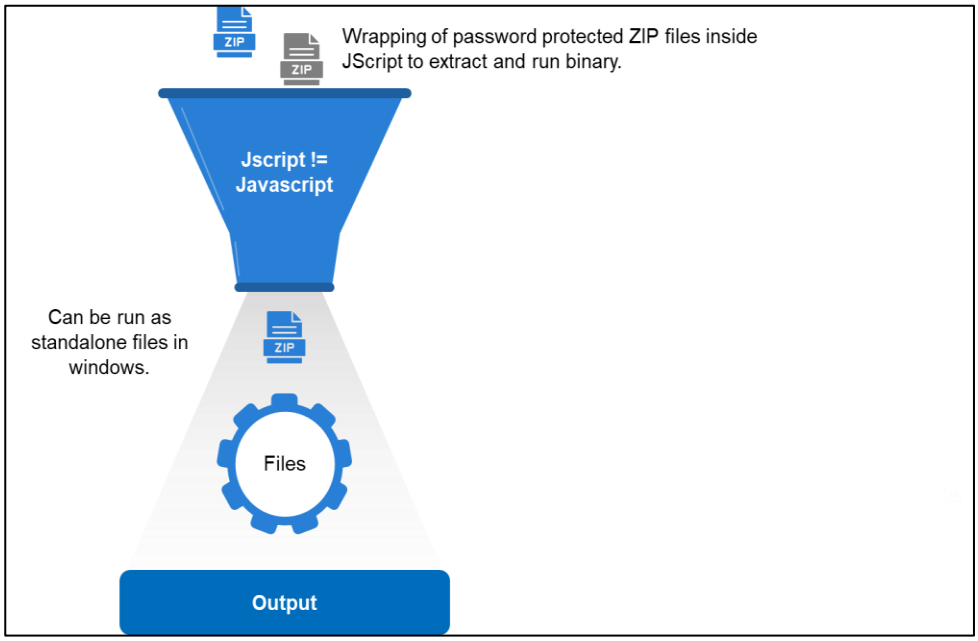


Fig 14

Steps to create (Fig 15)

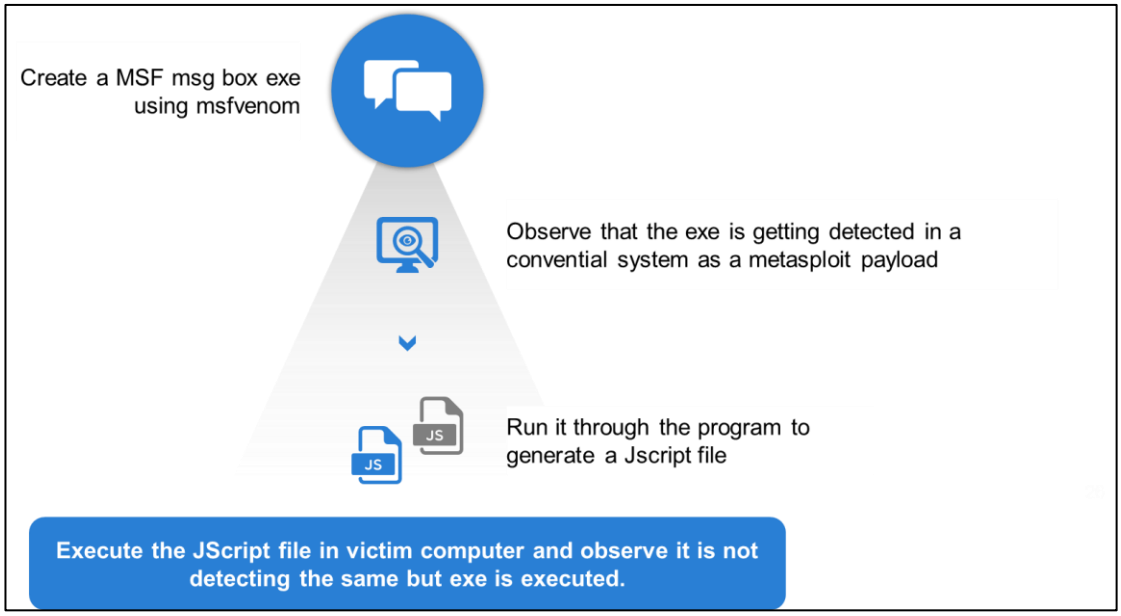


Fig 15

How the JScript code works (Fig 16)

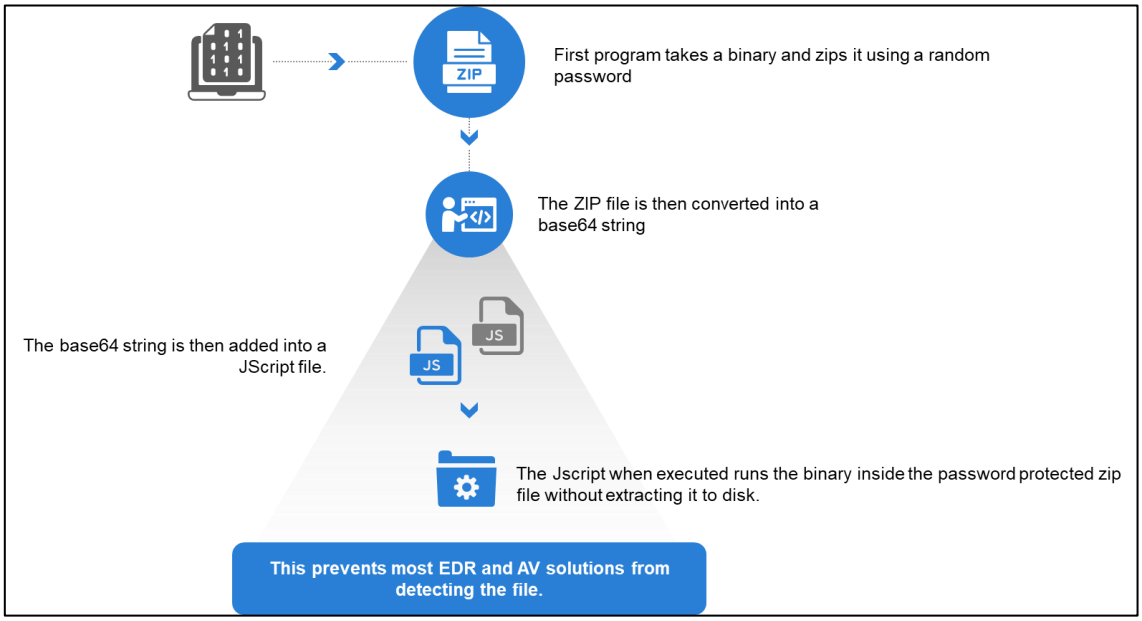


Fig 16

Analysis

Conclusion

To summarize, malicious actors are taking advantage of the situation, exploiting an unprecedented opportunity to breach organizations worldwide using endpoints as the top attack vector. As a result, the endpoint security solution should be based upon best practices for protecting organizations from preventing the most imminent threats to the endpoint.

While EDR & AV solutions are effective at blocking a high percentage of cyberattacks, some will slip through or bypass these defenses entirely. These solutions should be used in conjunction with application-level controls and the larger environment should be actively monitored for omissions.

Author Info

Mr. Suriya Prakash
Head-DARWIS SFS & Threat Intel API
CySecurity Corp

Mr. Sabari Selvan
Security Architect
CySecurity Corp