

# Defender - Pretender

When Windows Defender Updates Become a Security Risk

Omer Attias  
Tomer Bar



# Tomer Bar

VP of Security Research @ SafeBreach

- **SafeBreach** has been qualified to speak **10** talks at **Black Hat USA**
- 20 years experience in security research
- Main focus in APT and vulnerability research
- Presented at many global security conferences  
Such as: Black Hat USA 2020, DEFCON 28-30
- 2023 - Qualified to speak 3 talks at Black Hat, DEFCON



# Omer Attias

Security Researcher @ SafeBreach

- 6 years of experience in cyber security
- Main focus in low level & vulnerability research
- Technology and science enthusiast



# Agenda

- Introduction
- Defender Update Process
- The vulnerability
- Attack vectors
- Takeaways
- Q & A

# Defender - Pretender



# Motivation - Flame

- Discovered by Kaspersky in 2012
- State-Sponsored
- 20 MB of code
- One of the most sophisticated Malware ever analyzed
- Signed with a fraudulent Microsoft [certificate](#)
- Flame Hijacked Microsoft updates  
For lateral movement



# Research Goal and challenges

Achieve similar capabilities running as an unprivileged user without possessing a forged certificate and without using MITM.

Resulting in turning the original Windows Defender process to our full control.

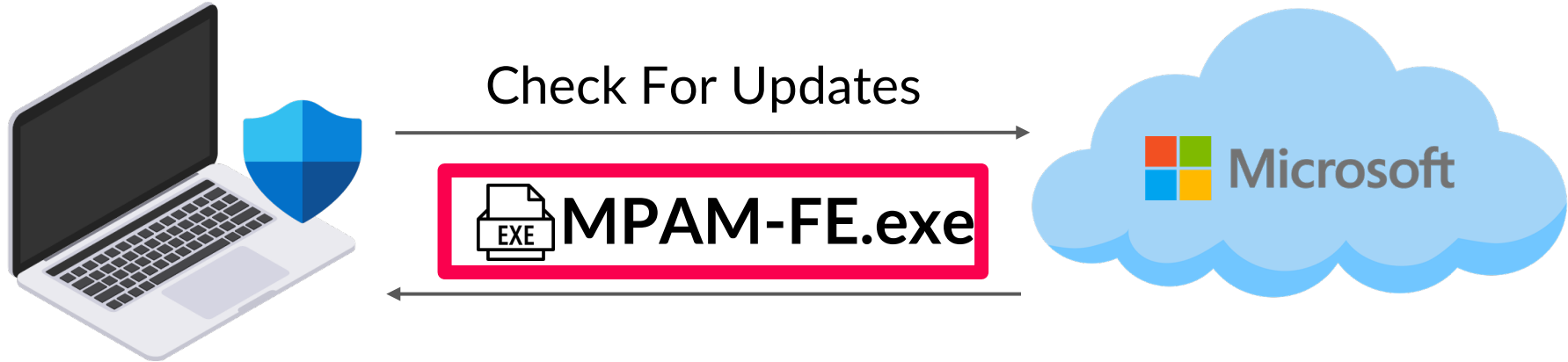


# Update Process

High Level Understanding

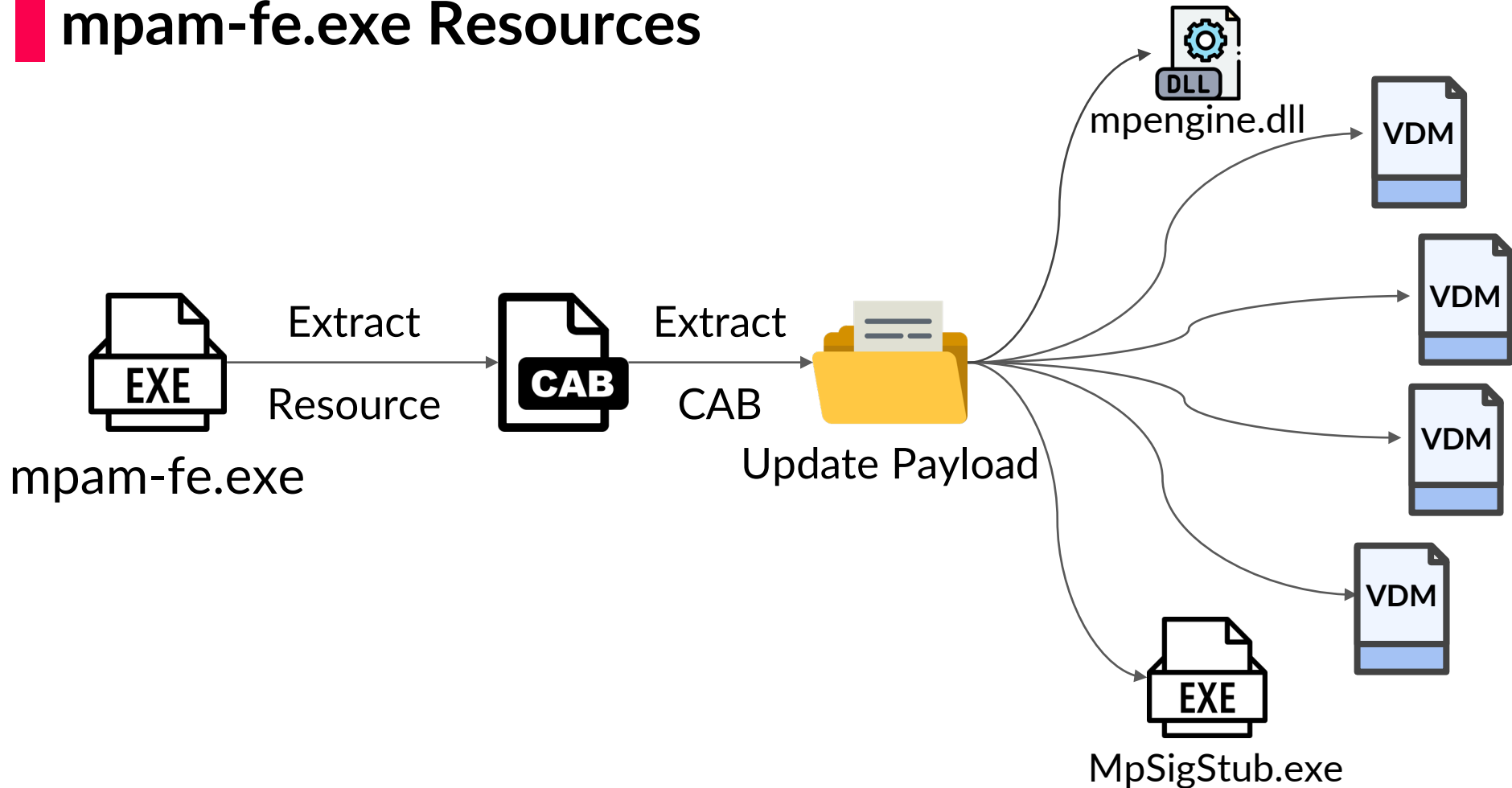


# What Windows Defender Pulls?



Microsoft **P**rotection **A**ntimalware **F**ront **E**nd.

# mpam-fe.exe Resources



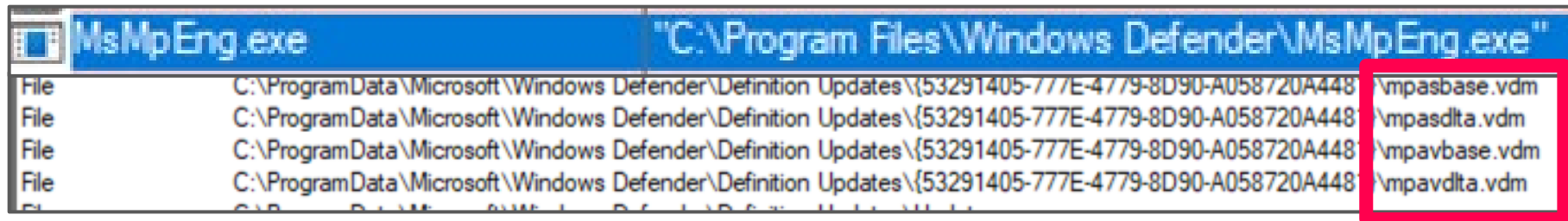
# mpam-fe.exe Execution

Procmon64.exe (11928)	Process Monitor	C:\Users\POTAT...	
<b>mpam-fe.exe (8828)</b>	AntiMalware Definition Up...	C:\Users\potatoh...	
MpSigStub.exe (8252)	Microsoft Malware Protecti...	C:\Users\POTAT...	
OneDrive.exe (10070)	Microsoft OneDrive	C:\Users\potatoh...	
GoogleCrashHandler.exe (1540)	Google Crash Handler	C:\Program Files (...)	
GoogleCrashHandler64.exe (10880)	Google Crash Handler	C:\Program Files (...)	

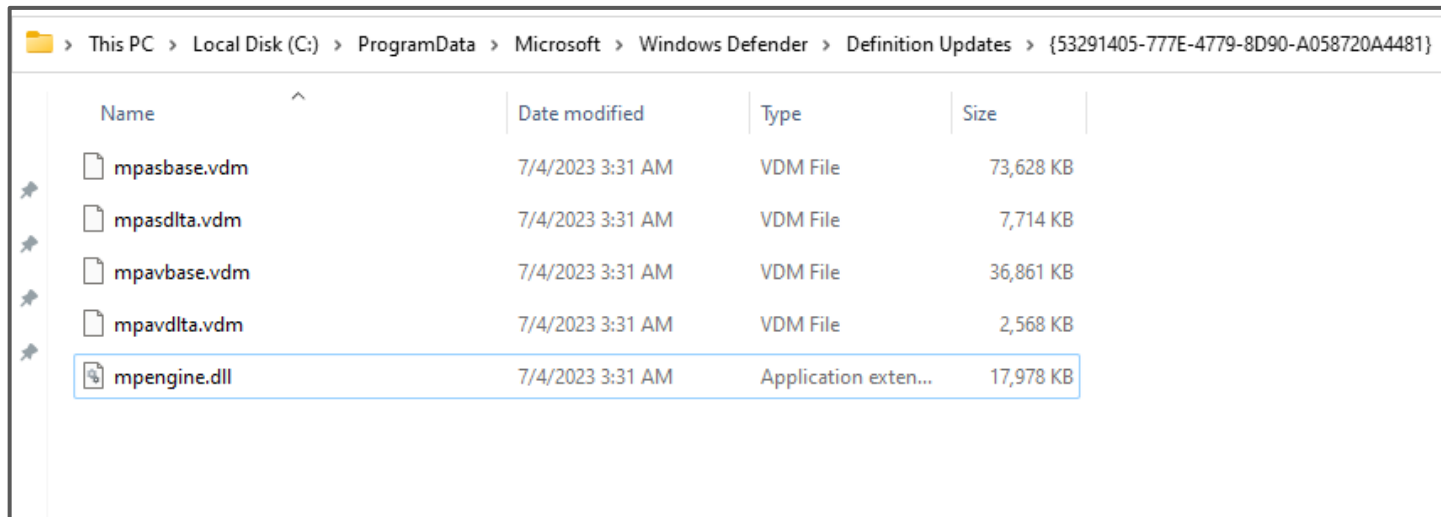
---

Description: Microsoft Malware Protection Signature Update Stub  
Company: Microsoft Corporation  
Path: C:\Users\POIAIU~1\AppData\Local\Temp\CE2CF71D-A77B-491F-8401-B82317A265EC\MpSigStub.exe  
**Command: :stub 1.1.18500.10 /payload 1.381.2904.0 /program C:\Users\potatohead\Desktop\mpam-fe.exe**  
User: toystory\potatohead  
PID: 8252      Started: 7/4/2023 7:15:39 AM  
                 Exited: 7/4/2023 7:15:39 AM

# Database Files & mpengine.dll



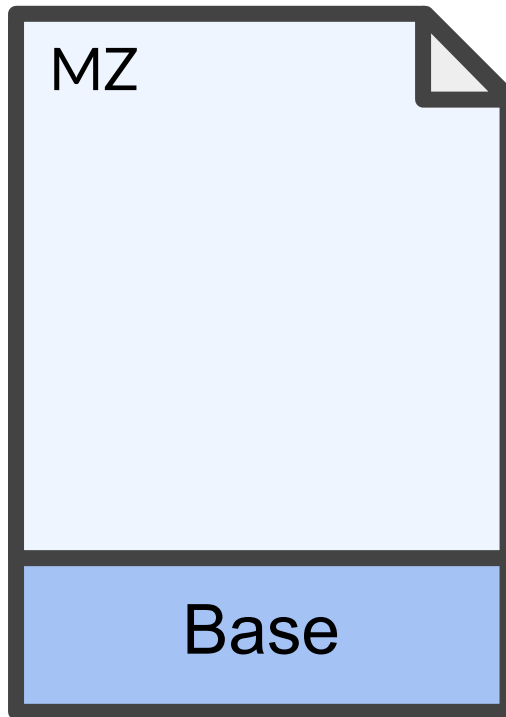
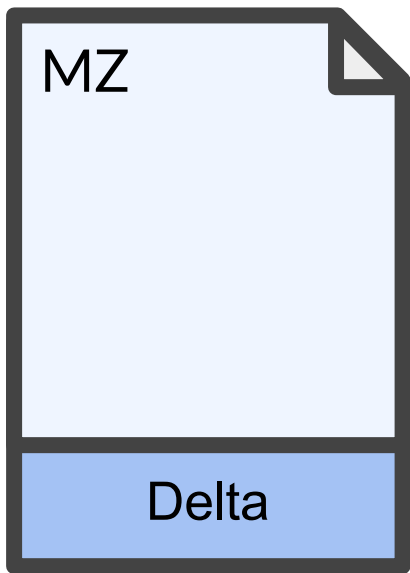
Process Name	Path
MsMpEng.exe	"C:\Program Files\Windows Defender\MsMpEng.exe"
File	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{53291405-777E-4779-8D90-A058720A448}\mpasbase.vdm
File	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{53291405-777E-4779-8D90-A058720A448}\mpasdlt.vdm
File	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{53291405-777E-4779-8D90-A058720A448}\mpavbase.vdm
File	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{53291405-777E-4779-8D90-A058720A448}\mpavdlt.vdm



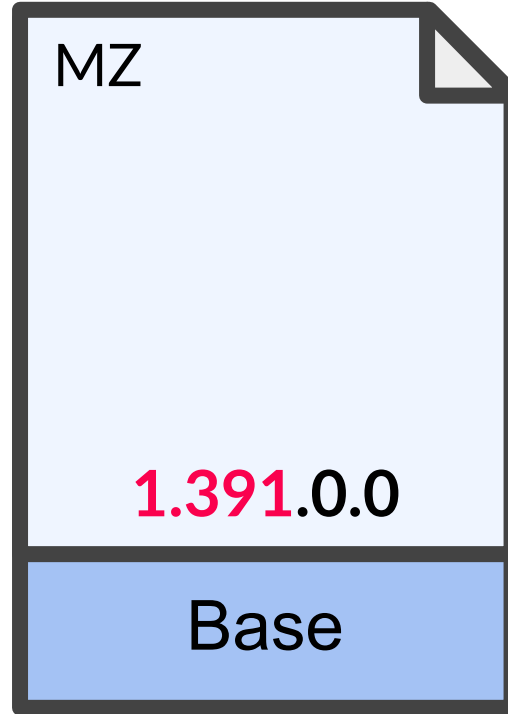
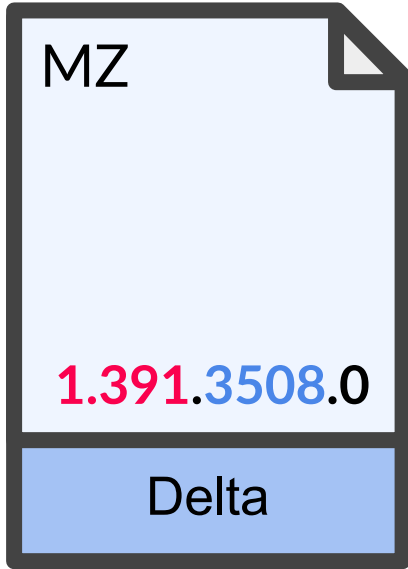
> This PC > Local Disk (C:) > ProgramData > Microsoft > Windows Defender > Definition Updates > {53291405-777E-4779-8D90-A058720A4481}

Name	Date modified	Type	Size
mpasbase.vdm	7/4/2023 3:31 AM	VDM File	73,628 KB
mpasdlt.vdm	7/4/2023 3:31 AM	VDM File	7,714 KB
mpavbase.vdm	7/4/2023 3:31 AM	VDM File	36,861 KB
mpavdlt.vdm	7/4/2023 3:31 AM	VDM File	2,568 KB
mpengine.dll	7/4/2023 3:31 AM	Application exten...	17,978 KB

# Base & Delta Files



# Base & Delta Versions



<major.minor.build.revision>

# Security Intelligence Version

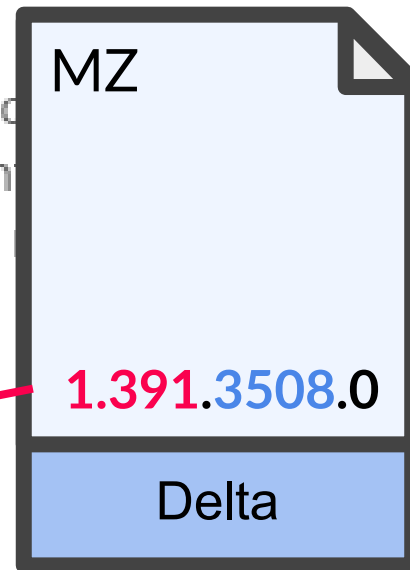
## Security intelligence

Microsoft Defender Antivirus uses security intelligence to help protect your device against the newest threats. We try to automatically download the most recent intelligence updates to your device against the newest threats. You can also manually download updates.

Security intelligence version: 1.391.3508.0

Version created on: 7/3/2023 5:41 PM

Last update: 7/4/2023 3:31 AM



# Digital Signature



Update Payload



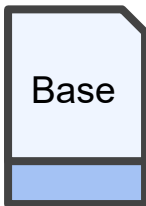
mpengine.dll



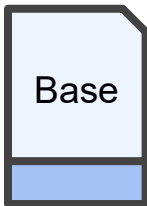
Delta



Delta



Base



Base

Digital Signature Details

General Advanced

**Digital Signature Information**  
This digital signature is OK.

Signer information

Name: Microsoft Windows

E-mail: Not available

Signing time: Friday, May 12, 2023 2:06:17 PM

View Certificate

Countersignatures

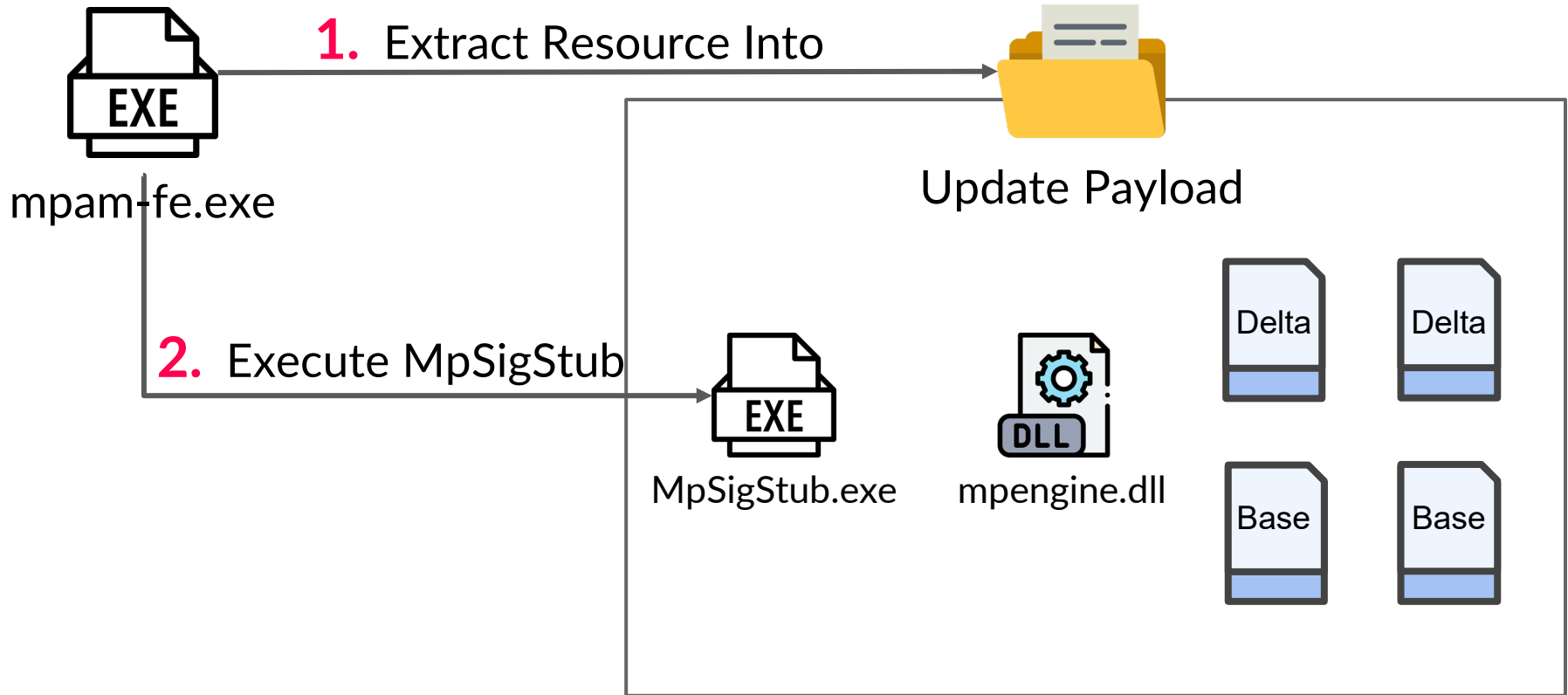
Name of signer:	E-mail address:	Timestamp
Microsoft Time-S...	Not available	Friday, May 12, 202...

Details

OK



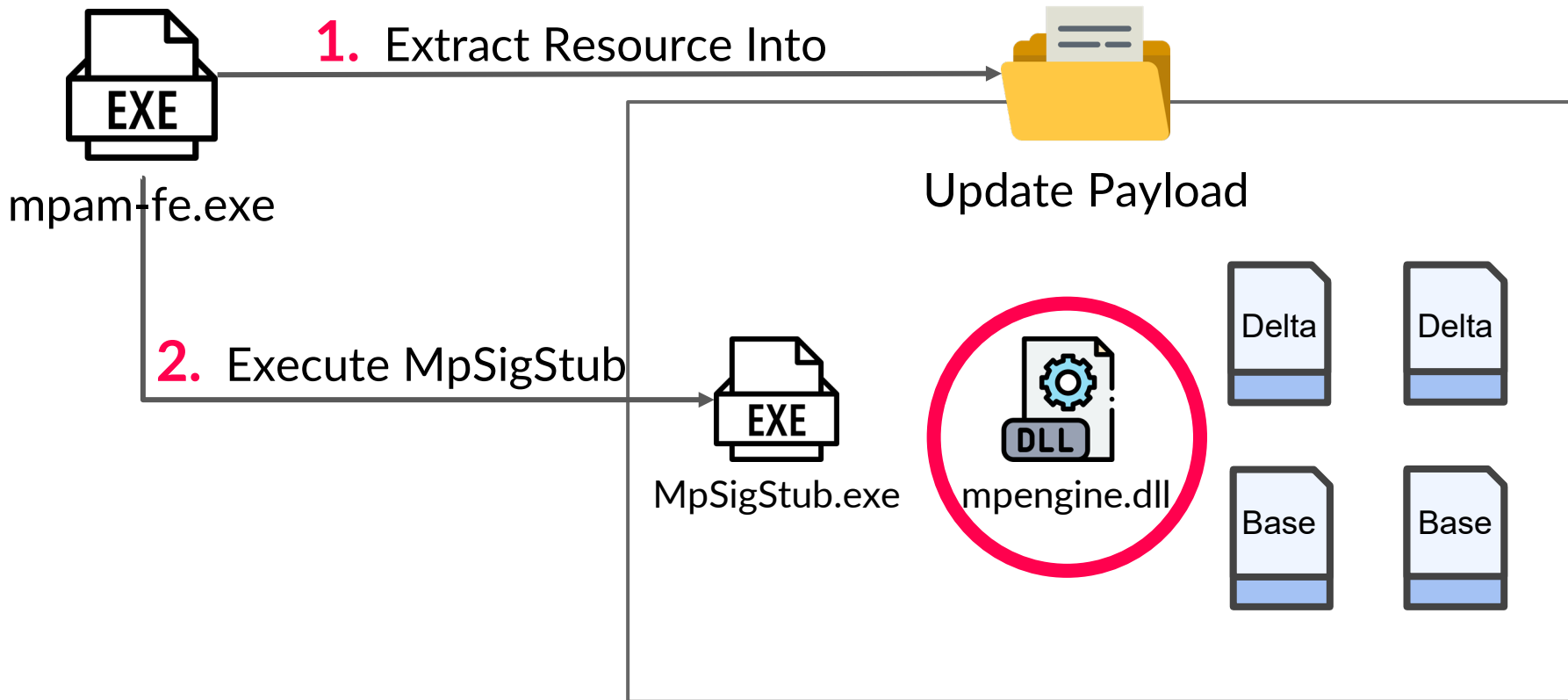
# Update Process Summary



# Playing Around With The Files

The First Clue That Something Is Fishy

# Pick a Target



# Trying To Modify MpEngine.dll



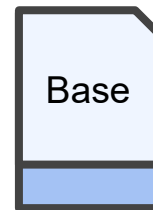
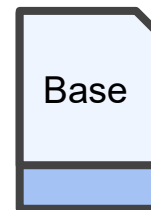
Update Payload



MpSigStub.exe



FAKE  
mpengine.dll



# Trying To Modify MpEngine.dll



Execute "Stub"



MpSigStub.exe

Update Payload



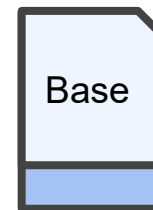
FAKE  
mpengine.dll



Delta



Delta



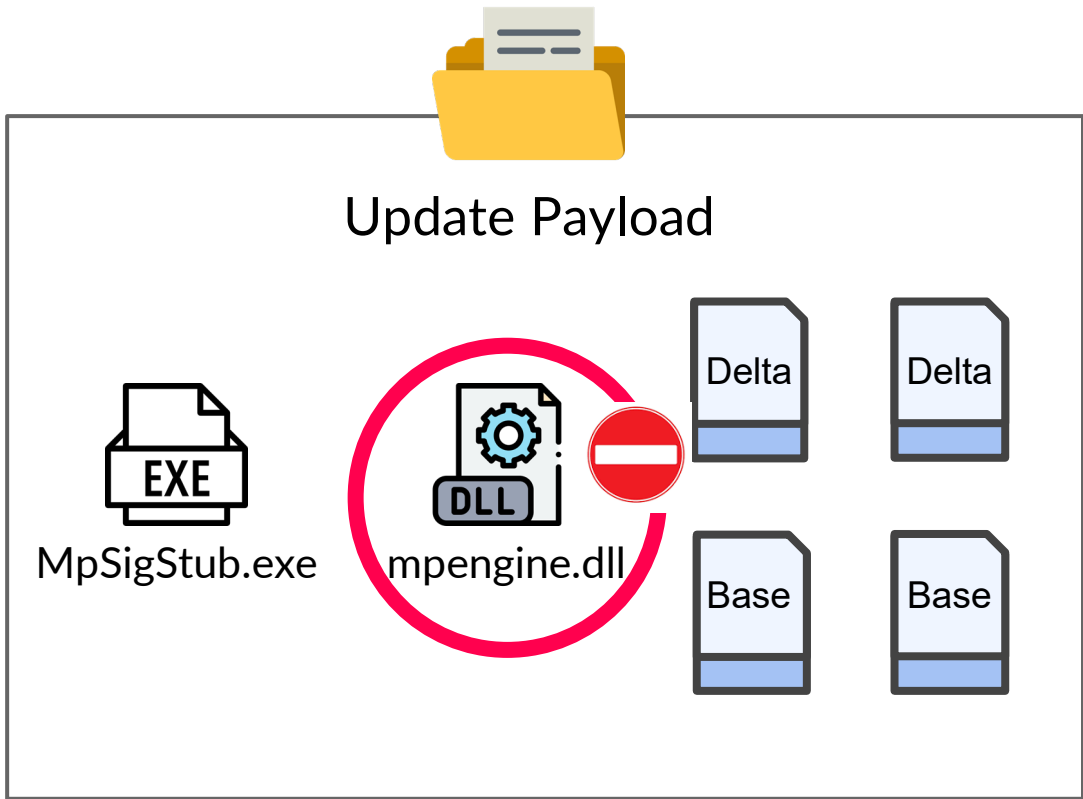
Base



Base

# Trying To Modify MpEngine.dll

```
*****  
* This break indicates this binary is not signed correctly:  
*****
```



# Trying To Modify the VDM files



Execute "Stub"

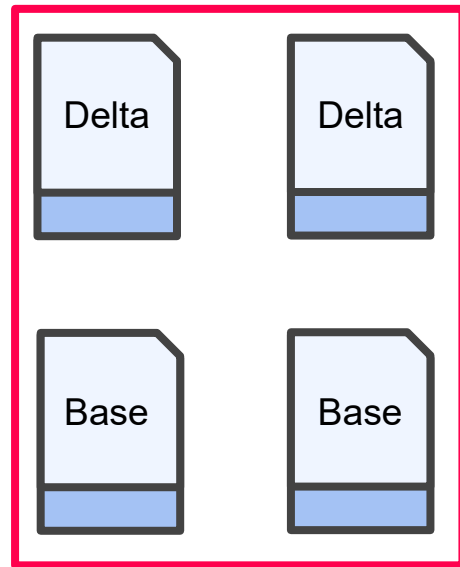


MpSigStub.exe

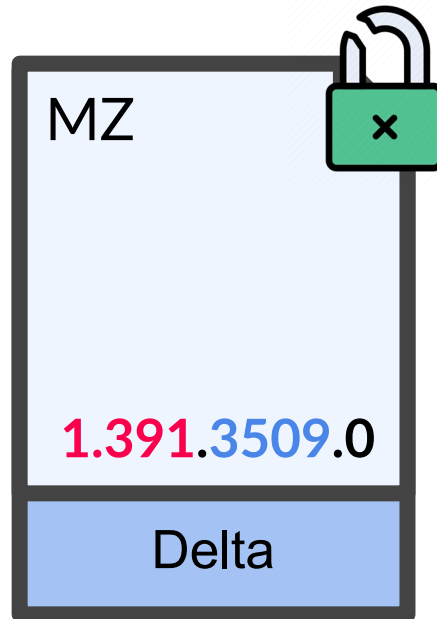
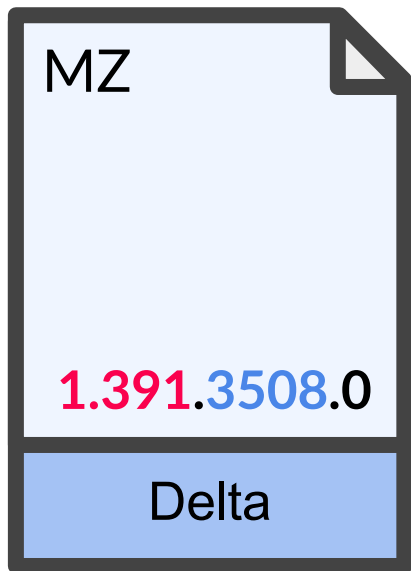
Update Payload



mpengine.dll

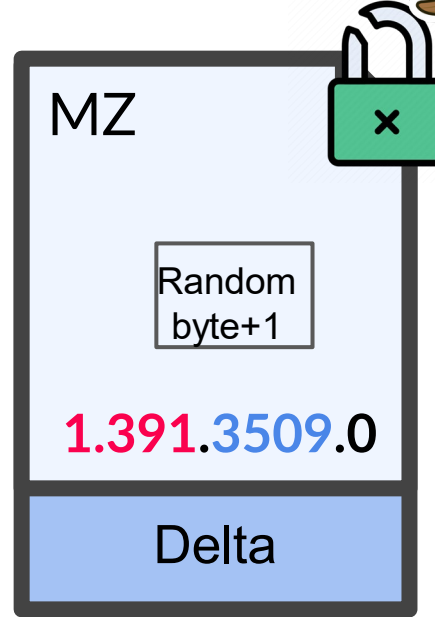
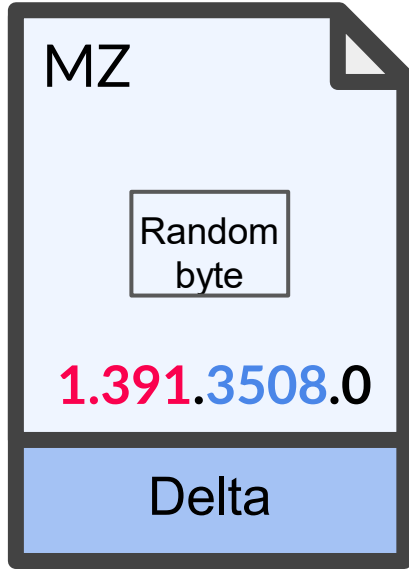


# First Clue That Something Is Fishy





# Trying To Modify Random Byte



# Summary

- We gained basic understanding of the update process
- Investigated each file involved
- We **failed** to modify mpengine.dll
- We **successfully** updated Defender with  
Using a modified 'VDM' file version
- A low privileged user can run an update
- We **failed** to update using random data modification

# MpSigStub to MsMpEng

Update With a Low Privilege User

# MpSigStub to MsMpEng

**MpSigStub.exe**

Malware Protection  
Signature Update Stub

???

**MsMpEng.exe**  
Microsoft Malware Protection  
Engine

Protected Process Light Process (PPL)

Black Box

Endpoints

Pid	Protocol	Name
800	ncacn_np	\pipe\lsass
800	ncalrpc	audit
800	ncalrpc	securityevent
800	ncalrpc	LSARPC_ENDPOINT
800	ncalrpc	lsacap
800	ncalrpc	LSA_IDPEXT_ENDPOINT
800	ncalrpc	LSA_EAS_ENDPOINT
800	ncalrpc	lsapolicylookup
800	ncalrpc	lsasspirpc
800	ncalrpc	protected_storage
800	ncalrpc	SidKey Local End Point
800	ncalrpc	samss_lpc

Processes

Name	Pid	Path
dllhost.exe	2620	C:\Windows\System32\dllhost.exe
msdtc.exe	2844	C:\Windows\System32\msdtc.exe
svchost.exe	2880	C:\Windows\System32\svchost.exe
SearchIndexer.exe	3296	C:\Windows\System32\SearchIndexer.exe
lsass.exe	800	C:\Windows\System32\lsass.exe
csrss.exe	704	
winlogon.exe	752	C:\Windows\System32\winlogon.exe
dwm.exe	608	C:\Windows\System32\dwm.exe
fontdrvhost.exe	1384	
explorer.exe	3188	C:\Windows\explorer.exe
vmtoolsd.exe	1420	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
cmd.exe	2172	C:\Windows\System32\cmd.exe
conhost.exe	3872	C:\Windows\System32\conhost.exe

# MpSigStub to MsMpEng

Manual reversing reveals RPC\_GUID which belongs to mpsvc.dll  
RPC func num:42

```
.rdata:0000000075B88DA8  
.rdata:0000000075B88DB0  
.rdata:0000000075B88DB1  
.rdata:0000000075B88DB2  
.rdata:0000000075B88DB3  
.rdata:0000000075B88DB4  
.rdata:0000000075B88DB8  
.rdata:0000000075B88DBA  
.rdata:0000000075B88DBC  
.rdata:0000000075B88DBD  
.rdata:0000000075B88DBE  
.rdata:0000000075B88DBF  
.rdata:0000000075B88DC0  
.rdata:0000000075B88DC1  
.rdata:0000000075B88DC2  
.rdata:0000000075B88DC3  
.rdata:0000000075B88DC4
```

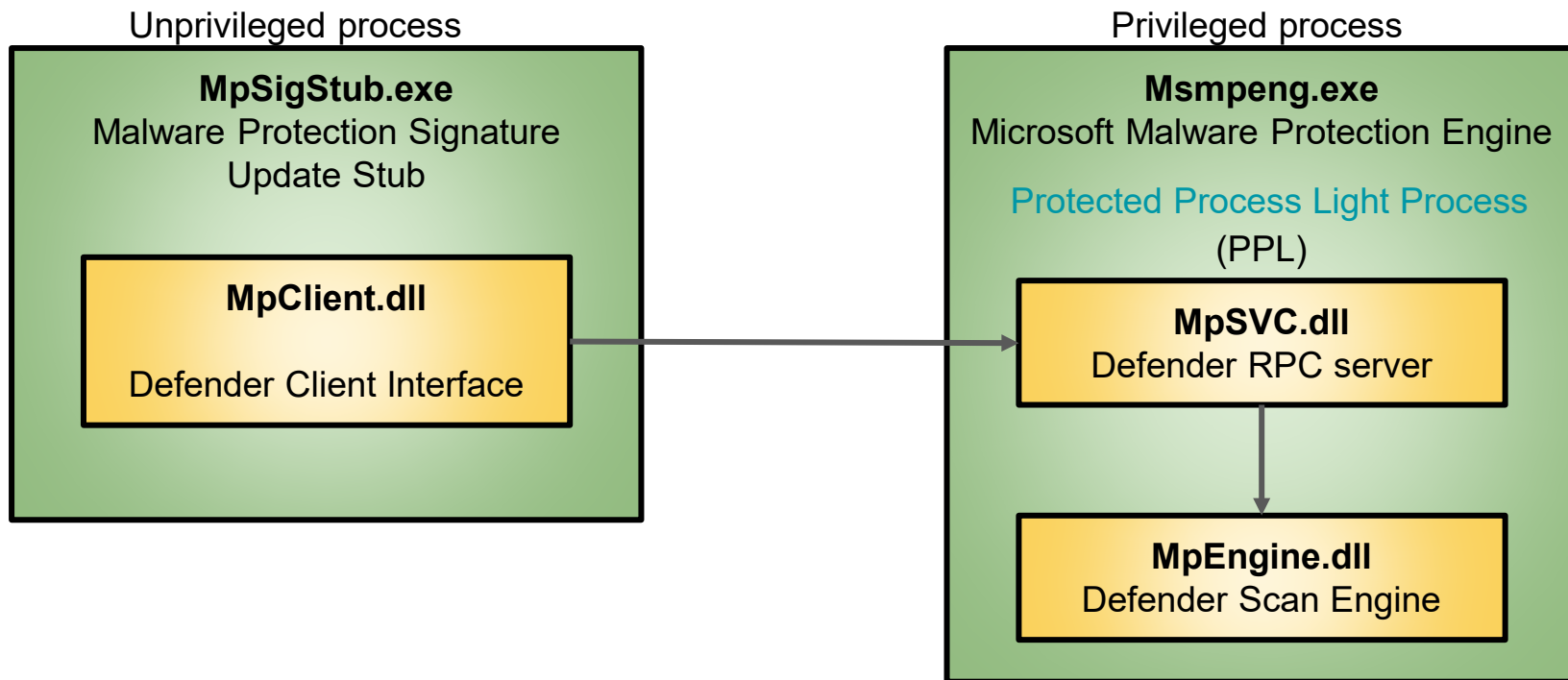
```
rp_d_guid dq offset unk_75B8BA1D0  
db 60h ;  
db 0  
db 0  
db 0  
dd 0C503F532h  
dw 443Ah  
dw 4C69h  
db 83h ; f  
db 0  
db 0CCh ; i  
db 0D1h ; N  
db 0FBh ; 0  
db 0DBh ; 0  
db 38h ; 8  
db 39h ; 9  
db 3
```

```
3736 RPC c503f532-443a-4c69-8300-ccd1fddb3839 (2.0) -- C:\Program Files\Windows Defender\mpsvc.dll  
3737 0 -> ServerMpEnableFeature  
3738 1 -> ServerMpDisableFeature  
3739 2 -> ServerMpQueryStatus  
3740 3 -> ServerMpEventOpen
```

```
41 -> ServerMpQueryEngineVersion  
42 -> ServerMpUpdateEngineSignature
```

```
42 -> ServerMpUpdateEngineSignature
```

# MpSigStub to MsMpEng



# Execution Flow - mpsvc to mpengine

**mpsvc::InitEngineContext**

↳ **mpengine::\_\_rsignal**

↳ **mpengine::StartMpEngine**

↳ **mpengine::DispatchSignalHelper**

↳ **mpengine::ksignalupper**

↳ **mpengine::ModProbelnit**

↳ **mpengine::modprobe\_init\_worker**

Called 4 times



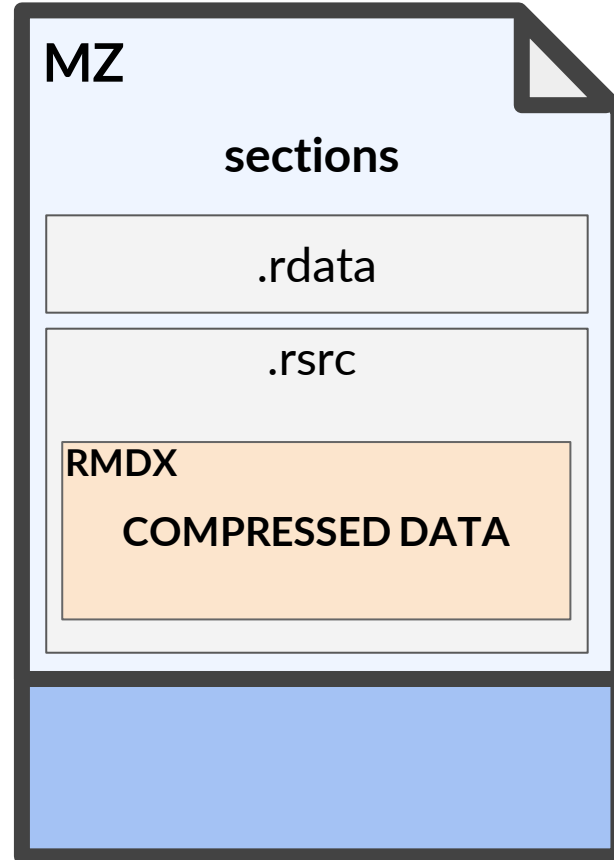
↳ **mpengine::LoadDatabase**

↳ **mpengine::ConsumeInputCompressed**

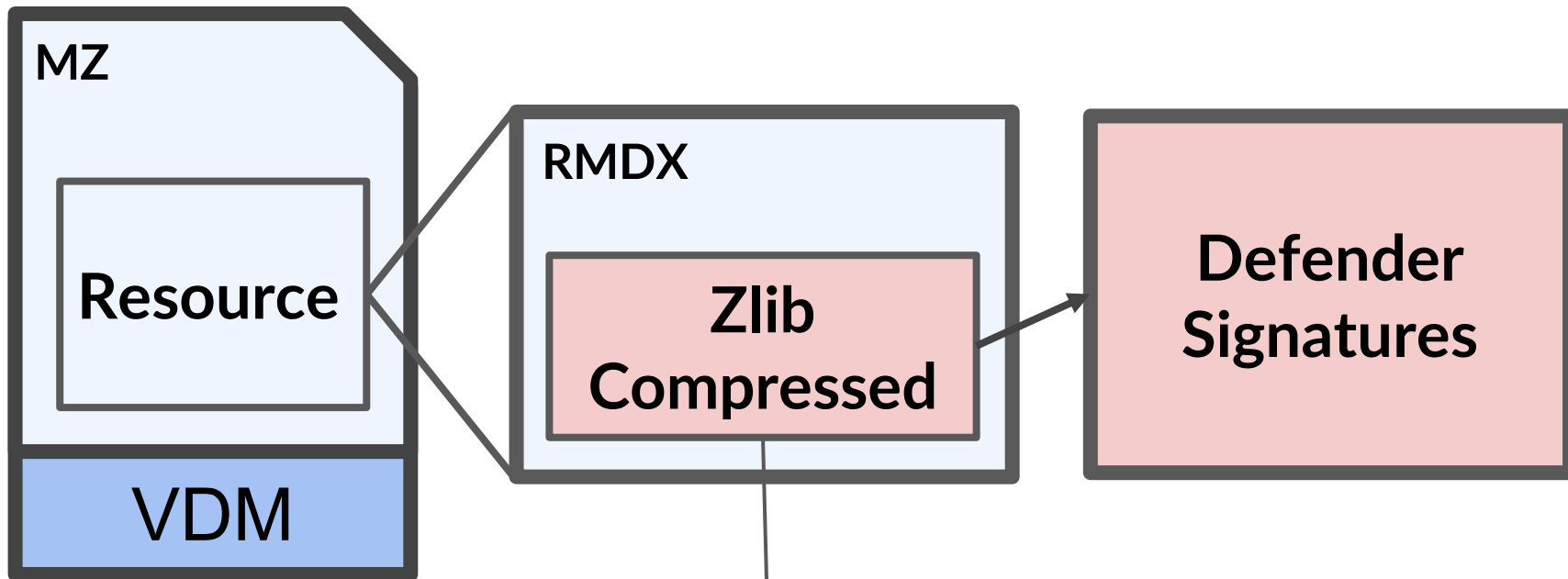
# VDM File Format



# VDM File Format



# VDM File Format



```
zlib.decompress('b\x78\x9c' + DecompressedData)
```

# The Signatures Are Not Encrypted!

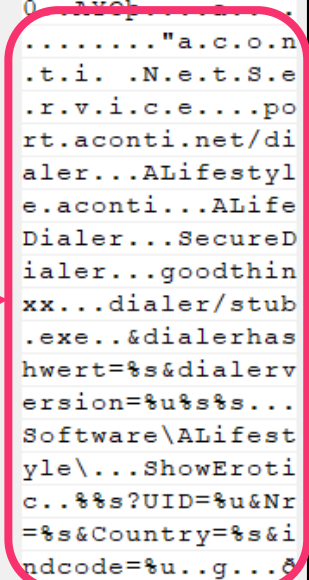
Base file

```
0001 0203 0405 0607 0809 0A0B 0C0D 0E0F 0123456789ABCDEF
0x00 5C1E 0000 4506 0000 0000 0100 0B00 0800 \...E.....
0x10 F421 4163 6F6E 7469 0000 0540 0582 2400 !Acont...@.,$.
0x20 0400 4045 0000 0400 0103 0000 0000 082A ..@E.....*
0x30 3000 0000 0000 0000 0000 0002 0000 0008 0.....
0x40 3000 0DDA FA83 7200 0000 0000 0000 0027 0..Úúfr.....'
0x50 3006 0B34 6BA2 924F EB36 0D00 0000 0045 0..4kç'œ6.....E
0x60 3000 08C1 59D2 FE00 0000 0061 0C01 0008 0..ívè.....
0x70 0008 000E 0000 0100 2261 0063 006F 006E ..... "a.c.o.n
0x80 0074 0069 0020 004E 0065 0074 0053 0065 .t.i. .N.e.t.S.e
0x90 0072 0076 0069 0063 0065 0001 0016 706F .r.v.i.c.e....po
0xA0 7274 2E61 636F 6E74 692E 6E65 742F 6469 rt.aconti.net/di
0xB0 616C 6572 0100 1141 4C69 6665 7374 796C aler...ALifestyl
0xC0 652E 6163 6F6E 7469 0100 0B41 4C69 6665 e.aconti...ALife
0xD0 4469 616C 6572 0100 0C53 6563 7572 6544 Dialer...Secured
0xE0 6961 6C65 7201 000A 676F 6F64 7468 696E ialer...goodthin
0xF0 7878 0100 0F64 6961 6C65 722F 7374 7562 xx...dialer/stub
x0100 2E65 7865 0100 2664 6961 6C65 7268 6173 .exe..&dialerhas
x0110 6877 6572 743D 2573 2664 6961 6C65 7276 hwert=%s&dialerv
x0120 6572 7369 6F6E 3D25 7525 7325 7301 0014 ersion=%u%s%s...
x0130 536F 6674 7761 7265 5C41 4C69 6665 7374 Software\ALifest
x0140 796C 655C 0100 0A53 686F 7745 726F 7469 yle\...ShowEroti
x0150 6301 0025 2573 3F55 4944 3D25 7526 4E72 c..%s?UID=%u&Nr
x0160 3D25 7326 436F 756E 7472 793D 2573 2669 =%s&Country=%s&i
x0170 6E64 636F 6465 3D25 7500 0067 1600 00F0 ndcode=%u..g...ç
x0180 1BB5 6E59 05AA 8CEC AFC0 BD00 4200 0000 .pnY.*@i A%.B...
```

proprietary structure

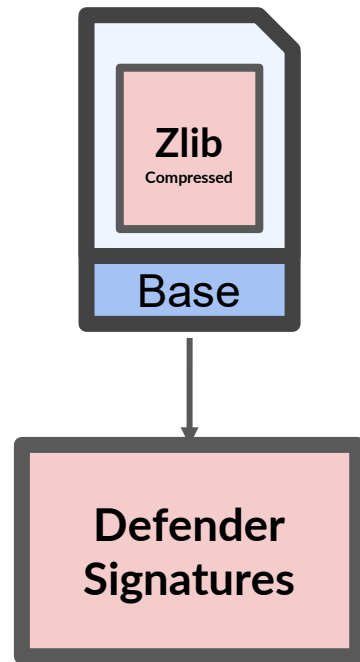
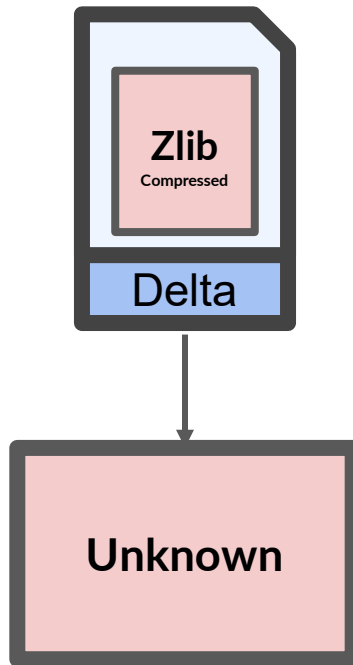
Threat Name

Signature Bytes



# Delta Decompressed Data

	0001	0203	0405	0607	0809	0A0B	0C0D	0E0F	0123456789ABCDEF
0x00	7450	0000	1300	0000	2702	0000	280A	0000	tP.....'... (...
0x10	2902	0000	4008	0000	5C54	0000	5D54	0000	)...@... \T..]T..
0x20	67B1	3600	6C01	0000	780F	0000	7A10	0000	g±6.l...x...z...
0x30	7E24	0000	8013	0000	8701	0000	8F04	0000	~\$.€...‡... ..
0x40	9601	0000	B30B	0000	BF02	0000	CF06	0000	-...°...¿...İ...
0x50	E70B	0000	738D	2208	EC1A	5C04	D001	8F0E	ç...s ".ì.\.Đ. .
0x60	0100	5CFF	FF01	0000	00FF	FF06	8000	00FF	.. \ÿÿ...ÿÿ.€..ÿ
0x70	FF0B	0001	00FF	FF10	8001	00FF	FF15	0002	ÿ...ÿÿ.€..ÿÿ...
0x80	00FF	FF1A	8002	00B7	B01F	0003	0001	00EA	.ÿÿ.€...°.....ê
0x90	91C9	DD30	0300	0400	34E6	3CF7	0280	9F65	'ÉÝ0....4æ<+.€ÿe
0xA0	C102	0600	0120	4AD3	C093	FFFF	6C7A	0300	Á.... JÓÀ"ÿÿlz..
0xB0	FFFF	71FA	0300	FFFF	767A	0400	FFFF	7BFA	ÿÿquí..ÿÿvz..ÿÿ{ú
0xC0	0400	FFFF	807A	0500	2DD8	85FA	0500	0100	..ÿÿ€z...-ø...ú....
0xD0	4653	80B9	5206	0030	942C	5306	0016	00CF	F\$€¹R..0",s....ï
0xE0	EB04	2401	D41A	2A89	2FCD	173C	A708	0001	ë.\$.Ô.*%/Í.<\$...
0xF0	2058	3886	6F16	AD5E	6706	0016	0085	5F78	X8to.-^g....._x



# Signature Structure

# Signature Structure

```
bitfield SignatureHeader {  
    Type: 8;  
    Size: 24;  
};
```

```
struct Signature {  
    SignatureHeader header;  
    u8 Data[header.Size];  
};
```

# Signature Types

1: "SIGNATURE_TYPE_RESERVED",	100: "SIGNATURE_TYPE_HOSTSENTRY",	153: "SIGNATURE_TYPE_TUNNEL_X86",	190: "SIGNATURE_TYPE_DEXHSTR_EXT",
2: "SIGNATURE_TYPE_VOLATILE_THREAT_INFO",	103: "SIGNATURE_TYPE_STATIC",	154: "SIGNATURE_TYPE_TUNNEL_X64",	191: "SIGNATURE_TYPE_JAVAHSTR_EXT",
3: "SIGNATURE_TYPE_VOLATILE_THREAT_ID",	105: "SIGNATURE_TYPE_LATENT_THREAT",	155: "SIGNATURE_TYPE_TUNNEL_IA64",	192: "SIGNATURE_TYPE_MAGICCODE",
17: "SIGNATURE_TYPE_CKOLDREC",	106: "SIGNATURE_TYPE_REMOVAL_POLICY",	156: "SIGNATURE_TYPE_VDLL_ARM",	193: "SIGNATURE_TYPE_CLEANSOURCE_RULE",
32: "SIGNATURE_TYPE_KVIR32",	107: "SIGNATURE_TYPE_WVT_EXCEPTION",	157: "SIGNATURE_TYPE_THREAD_X86",	194: "SIGNATURE_TYPE_VDLL_CHECKSUM",
33: "SIGNATURE_TYPE_POLYVIR32",	108: "SIGNATURE_TYPE_REVOKED_CERTIFICATE",	158: "SIGNATURE_TYPE_THREAD_X64",	195: "SIGNATURE_TYPE_THREAT_UPDATE_STATUS",
39: "SIGNATURE_TYPE_NSSCRIPT_NORMAL",	112: "SIGNATURE_TYPE_TRUSTED_PUBLISHER",	159: "SIGNATURE_TYPE_THREAD_IA64",	196: "SIGNATURE_TYPE_VDLL_MSIL",
40: "SIGNATURE_TYPE_NSSCRIPT_SP",	113: "SIGNATURE_TYPE_ASEP_FILEPATH",	160: "SIGNATURE_TYPE_FRIENDLYFILE_SHA256",	197: "SIGNATURE_TYPE_ARHSTR_EXT",
41: "SIGNATURE_TYPE_NSSCRIPT_BRUTE",	115: "SIGNATURE_TYPE_DELTA_BLOB",	161: "SIGNATURE_TYPE_FRIENDLYFILE_SHA512",	198: "SIGNATURE_TYPE_MSILFOPEX",
44: "SIGNATURE_TYPE_NSSCRIPT_CURE",	116: "SIGNATURE_TYPE_DELTA_BLOB_RECINFO",	162: "SIGNATURE_TYPE_SHARED_THREAT",	199: "SIGNATURE_TYPE_VBFOPEX",
48: "SIGNATURE_TYPE_TITANFLT",	117: "SIGNATURE_TYPE_ASEP_FOLDERNAME",	163: "SIGNATURE_TYPE_VDM_METADATA",	200: "SIGNATURE_TYPE_FOP64",
61: "SIGNATURE_TYPE_PEFILE_CURE",	119: "SIGNATURE_TYPE_PATTMATCH_V2",	164: "SIGNATURE_TYPE_VSTORE",	201: "SIGNATURE_TYPE_FOPEX64",
62: "SIGNATURE_TYPE_MAC_CURE",	120: "SIGNATURE_TYPE_PEHSTR_EXT",	165: "SIGNATURE_TYPE_VDLL_SYMINFO",	202: "SIGNATURE_TYPE_JSINIT",
64: "SIGNATURE_TYPE_SIGTREE",	121: "SIGNATURE_TYPE_VDLL_X86",	166: "SIGNATURE_TYPE_TL2_PATTERN",	203: "SIGNATURE_TYPE_PESTATICEX",
65: "SIGNATURE_TYPE_SIGTREE_EXT",	122: "SIGNATURE_TYPE_VERSIONCHECK",	167: "SIGNATURE_TYPE_BM_STATIC",	204: "SIGNATURE_TYPE_KCRCX",
66: "SIGNATURE_TYPE_MACRO_PCODE",	123: "SIGNATURE_TYPE_SAMPLE_REQUEST",	168: "SIGNATURE_TYPE_BM_INFO",	205: "SIGNATURE_TYPE_FTRE_POS",
67: "SIGNATURE_TYPE_MACRO_SOURCE",	124: "SIGNATURE_TYPE_VDLL_X64",	169: "SIGNATURE_TYPE_NDAT",	206: "SIGNATURE_TYPE_NID64",
68: "SIGNATURE_TYPE_BOOT",	126: "SIGNATURE_TYPE_SNID",	170: "SIGNATURE_TYPE_FASTPATH_DATA",	207: "SIGNATURE_TYPE_MACRO_PCODE64",
73: "SIGNATURE_TYPE_CLEANSSCRIPT",	127: "SIGNATURE_TYPE_FOP",	171: "SIGNATURE_TYPE_FASTPATH_SDN",	208: "SIGNATURE_TYPE_BRUTE",
74: "SIGNATURE_TYPE_TARGET_SCRIPT",	128: "SIGNATURE_TYPE_KCRCX",	172: "SIGNATURE_TYPE_DATABASE_CERT",	209: "SIGNATURE_TYPE_SWFHSTR_EXT",
80: "SIGNATURE_TYPE_CKSIMPLEREC",	131: "SIGNATURE_TYPE_VFILE",	173: "SIGNATURE_TYPE_SOURCE_INFO",	210: "SIGNATURE_TYPE_REWSIGS",
81: "SIGNATURE_TYPE_PATTMATCH",	132: "SIGNATURE_TYPE_SIGFLAGS",	174: "SIGNATURE_TYPE_HIDDEN_FILE",	211: "SIGNATURE_TYPE_AUTOIOTHSTR_EXT",
83: "SIGNATURE_TYPE_RPFROUTINE",	133: "SIGNATURE_TYPE_PEHSTR_EXT2",	175: "SIGNATURE_TYPE_COMMON_CODE",	212: "SIGNATURE_TYPE_INNOHSTR_EXT",
85: "SIGNATURE_TYPE_NID",	134: "SIGNATURE_TYPE_PEMAIN_LOCATOR",	176: "SIGNATURE_TYPE_VREG",	213: "SIGNATURE_TYPE_ROOTCERTSTORE",
86: "SIGNATURE_TYPE_GENFSFX",	135: "SIGNATURE_TYPE_PESTATIC",	177: "SIGNATURE_TYPE_NISBLOB",	214: "SIGNATURE_TYPE_EXPLICITRESOURCE",
87: "SIGNATURE_TYPE_UNPLIB",	136: "SIGNATURE_TYPE_UFSP_DISABLE",	178: "SIGNATURE_TYPE_VFILEEX",	215: "SIGNATURE_TYPE_CMDHSTR_EXT",
88: "SIGNATURE_TYPE_DEFAULTS",	137: "SIGNATURE_TYPE_FOPEX",	179: "SIGNATURE_TYPE_SIGTREE_BM",	216: "SIGNATURE_TYPE_FASTPATH_TDN",
91: "SIGNATURE_TYPE_DBVAR",	138: "SIGNATURE_TYPE_PEPICODE",	180: "SIGNATURE_TYPE_VBFOP",	217: "SIGNATURE_TYPE_EXPLICITRESOURCENAME",
0x5C: "SIGNATURE_TYPE_THREAT_BEGIN",	139: "SIGNATURE_TYPE_IL_PATTERN",	181: "SIGNATURE_TYPE_VDLL_META",	218: "SIGNATURE_TYPE_FASTPATH_SDN_EX",
0x5D: "SIGNATURE_TYPE_THREAT_END",	140: "SIGNATURE_TYPE_ELFHSTR_EXT",	182: "SIGNATURE_TYPE_TUNNEL_ARM",	219: "SIGNATURE_TYPE_BLOOM_FILTER",
94: "SIGNATURE_TYPE_FILENAME",	141: "SIGNATURE_TYPE_MACHOHSTR_EXT",	183: "SIGNATURE_TYPE_THREAD_ARM",	220: "SIGNATURE_TYPE_RESEARCH_TAG",
95: "SIGNATURE_TYPE_FILEPATH",	142: "SIGNATURE_TYPE_DOSHSTR_EXT",	184: "SIGNATURE_TYPE_PCODEVALIDATOR",	222: "SIGNATURE_TYPE_ENVELOPE",
96: "SIGNATURE_TYPE_FOLDERNAME",	143: "SIGNATURE_TYPE_MACROHSTR_EXT",	186: "SIGNATURE_TYPE_MSILFOP",	223: "SIGNATURE_TYPE_REMOVAL_POLICY64",
97: "SIGNATURE_TYPE_PEHSTR",	144: "SIGNATURE_TYPE_TARGET_SCRIPT_PCODE",	187: "SIGNATURE_TYPE_KPAT",	224: "SIGNATURE_TYPE_REMOVAL_POLICY64_BY_NAME",
98: "SIGNATURE_TYPE_LOCALHASH",	145: "SIGNATURE_TYPE_VDLL_IA64",	188: "SIGNATURE_TYPE_KPATEX",	225: "SIGNATURE_TYPE_VDLL_META_X64",
99: "SIGNATURE_TYPE_REGKEY",	149: "SIGNATURE_TYPE_PEBMPAT",	189: "SIGNATURE_TYPE_LUASTANDALONE",	226: "SIGNATURE_TYPE_VDLL_META_ARM",
	150: "SIGNATURE_TYPE_AGGREGATOR",	190: "SIGNATURE_TYPE_DEXHSTR_EXT",	227: "SIGNATURE_TYPE_VDLL_META_MSIL",
	151: "SIGNATURE_TYPE_SAMPLE_REQUEST_BY_NAME",		228: "SIGNATURE_TYPE_MDBHSTR_EXT",
	152: "SIGNATURE_TYPE_REMOVAL_POLICY_BY_NAME",		229: "SIGNATURE_TYPE_SNIDEX",
			230: "SIGNATURE_TYPE_SNINDEX2",
			231: "SIGNATURE_TYPE_AGGREGATOR",
			232: "SIGNATURE_TYPE_PUA_APPMAP",
			233: "SIGNATURE_TYPE_PROPERTY_BAG",
			234: "SIGNATURE_TYPE_DMGHSTR_EXT",
			235: "SIGNATURE_TYPE_DATABASE_CATALOG",

# Threat Begin & Threat End

Begin

0x5C: "SIGNATURE\_TYPE\_THREAT\_BEGIN"  
0x5D: "SIGNATURE\_TYPE\_THREAT\_END",

Name	Size	Type
▼ threat	0x01D1	struct Threat
▶ begin	0x0022	struct ThreatBegin
▶ signatures	0x01A7	Signature[5]
▶ end	0x0008	struct ThreatEnd

End

5C	1E	00	00	45	06	00	00	00	00	01	00	0B	00	08	00	...	E
F4	21	41	63	6F	6E	74	69	00	00	05	40	05	82	24	00	...	!Aconti...@ \$
04	00	40	45	00	00	04	00	01	03	00	00	00	00	00	2A	...	@E.....*
30	00	00	00	00	00	00	00	00	00	02	00	00	00	00	08	...	0.....
30	00	0D	DA	FA	83	72	00	00	00	00	00	00	00	00	27	...	0.....r.....
30	06	0B	34	6B	A2	92	4F	EB	36	0D	00	00	00	00	45	...	0...4k.0.6....E
30	00	08	C1	59	D2	FE	00	00	00	00	61	0C	01	00	08	...	0...Y.....a...
00	08	00	0B	00	00	01	00	22	61	00	63	00	6F	00	6E	...	....."a con
00	74	00	69	00	20	00	4E	00	65	00	74	00	53	00	65	...	t.i. Net.Se
00	72	00	76	00	69	00	63	00	65	00	01	00	16	70	6F	...	r.v.i.c.e...po
72	74	2E	61	63	6F	6E	74	69	2E	6E	65	74	2F	64	69	...	rt.aconti.net/di
61	6C	65	72	01	00	11	41	4C	69	66	65	73	74	79	6C	...	aler...ALifestyl
65	2E	61	63	6F	6E	74	69	01	00	0B	41	4C	69	66	65	...	e.aconti...ALife
44	69	61	6C	65	72	01	00	0C	53	65	63	75	72	65	44	...	Dialer...SecureD
69	61	6C	65	72	01	00	0A	67	6F	6F	64	74	68	69	6E	...	dialer...goodthin
78	78	01	00	0F	64	69	61	6C	65	72	2F	73	74	75	62	...	xx...dialer/stub
2E	65	78	65	01	00	26	64	69	61	6C	65	72	68	61	73	...	,exe.&dialerhas
68	77	65	72	74	3D	25	73	26	64	69	61	6C	65	72	76	...	hwert=%s&dialerv
65	72	73	69	6F	6E	3D	25	75	25	73	25	73	01	00	14	...	ersion=%u%s%...
53	6F	66	74	77	61	72	65	5C	41	4C	69	66	65	73	74	...	Software\ALifest
79	6C	65	5C	01	00	0A	53	68	6F	77	45	72	6F	74	69	...	yle\... ShowEroti
63	01	00	25	25	73	3F	55	49	44	3D	25	75	26	4E	72	...	c.%%s?UID=%u&Nr
3D	25	73	26	43	6F	75	6E	74	72	79	3D	25	73	26	69	...	=%s&Country=%s&i
6E	64	63	6F	64	65	3D	25	75	00	00	67	16	00	00	F0	...	ndcode=%u.g...
1B	B5	6E	59	05	AA	8C	EC	AF	C0	BD	00	42	00	00	00	...	...nY...B...
20	EC	AF	C0	BD	67	16	00	00	80	B8	83	BE	93	97	88	...	...g...
9D	CE	23	3D	29	8B	74	01	00	00	20	4D	16	56	EF	67	...	(#)=).t...M.V.g
16	00	00	80	B8	83	BE	96	86	AF	6B	CE	23	3D	29	69	...	...k.#=)i
3D	01	00	01	20	6E	BD	EB	5D	04	00	00	45	06	00	00	...	=...n...]...E
00	5C	3A	00	00	56	06	00	00	00	01	00	0C	00	24	00	...	\:..V.....\$



# Evaluation

```
try:
    while True:
        Signature.read_one(base_data)
        counter += 1
except Exception:
    print(f'Total Signatures: {counter}')
```

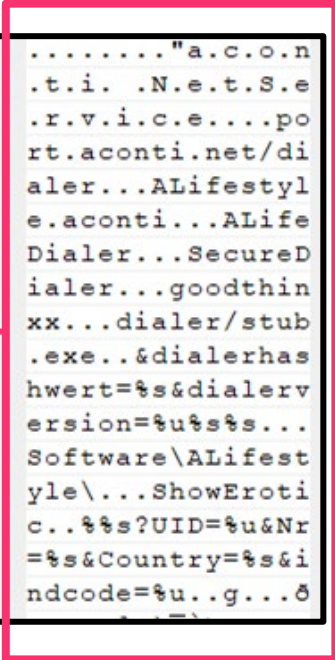
```
$ python .\CountSignatures.py
Total Signatures: 2643614
```



# Smart modification on Conti Signature

```
1  #include <stdlib.h>
2
3  wchar_t* a1 = L"aconti NetService";
4  char* a2 = "port.aconti.net/dialer";
5  char* a3 = "ALifestyle.aconti";
6  char* a4 = "ALifeDialer";
7  char* a5 = "SecureDialer";
8  char* a6 = "goodthinxx";
9  char* a7 = "dialer/stub.exe";
10 char* a8 = "dialerhashwert=%s&dialerverversion=%u%s%s";
11 char* a9 = "Software\\ALifestyle\\";
12 char* a10 = "ShowErotic";
13 char* a11 = "%s?UID=%u&Nr=%s&Country=%s&indcode=%u";
14
15
16 int main()
17 {
18
19     return 0;
20 }
```

```
0063 006F 006E ..... "a.c.o.n
0074 0053 0065 .t.i. .N.e.t.S.e
0001 0016 706F .r.v.i.c.e....po
6E65 742F 6469 rt.aconti.net/di
6665 7374 796C aler...ALifestyl
0B41 4C69 6665 e.aconti...ALife
6563 7572 6544 Dialer...SecureD
6F64 7468 696E ialer...goodthin
722F 7374 7562 xx...dialer/stub
6C65 7268 6173 .exe...&dialerhas
6961 6C65 7276 hwert=%s&dialerv
7325 7301 0014 ersion=%u%s%s...
4C69 6665 7374 Software\\ALifest
7745 726F 7469 yle\\...ShowEroti
3D25 7526 4E72 c...%s?UID=%u&Nr
793D 2573 2669 =%s&Country=%s&i
0067 1600 00F0 ndcode=%u..g...ø
```



# Smart modification on Conti Signature



Dialer:Win32/Aconti

Alert level: Severe

Status: Active

Date: 5/9/2023 5:01 AM

Category: Dialer

Details: This program dials toll numbers to gain access to adult content.

[Learn more](#)

Affected items:

file: C:\Users\potatohead\Desktop\aconti.exe

OK

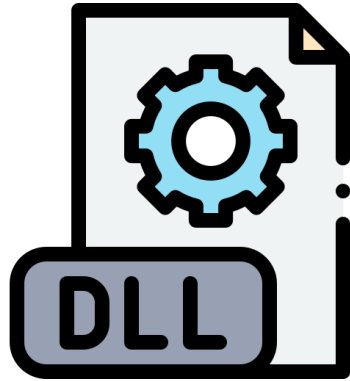
# Modify Conti Threat Name – Update failed

```
===== Upd
Product name: Microsoft Windows Defender
Package files:
  Directory: C:\Defs
mpasbase.vdm: b96f6f2cea8b43df4a154dda7d3b3997010b9b01d21af7524db677d07440816e 1.383.0.0
mpasdlt.vdm: 8bc31ebf7357bdb5a057924eb826c5fd212d968f561ac6717cd47eb6c2a0bb70 1.383.1801.0
mpavbase.vdm: 66a7af38e7cbc10faafbbfc22e4e829b663e6a407ddf93e490dae0c952226182 1.383.0.0
mpavdlt.vdm: 8d15055ae3335aa4addf7b7b06fa35edc509fd3e63ec87cfb39a710134b082cc 1.383.1801.0
MpSigStub.exe: fa42b9b84754e2e8368e8929fa045be86dbd72678176ee75814d2a16d23e5c26 1.1.18500.10
ERROR 0x8050a004 : MpUpdateEngine(C:\Defs)
ERROR 0x8050a004 : MpUpdateEngine(C:\Defs)
ERROR 0x8050a004 : Failed to update signatures from C:\Defs
```

```
0001 0203 0405 0607 0809 0A0B 0C0D 0E0F 0123456789ABCDEF
0x00 5C1E 0000 4506 0000 0000 0100 0B00 0800 \...E.....
0x10 F421 4163 6F6E 7469 0000 0540 0582 2400 !Aconti...@.,$.
0x20 0400 4045 0000 0400 0103 0000 0000 002A ..E.....*
0x30 3000 0000 0000 0000 0000 0002 0000 0008 0.....
0x40 3000 0DDA FA83 7200 0000 0000 0000 0027 0..Úúfr.....'
0x50 3006 0B34 6BA2 924F EB36 0D00 0000 0045 0..4kç'Oè6.....E
0x60 3000 08C1 59D2 FE00 0000 0061 0C01 0008 0..ÁYòp....a....
0x70 0008 000B 0000 0100 2261 0063 006F 006E ..... "a.c.o.n
0x80 0074 0069 0020 004E 0065 0074 0053 0065 .t.i. .N.e.t.S.e
0x90 0072 0076 0069 0063 0065 0001 0016 706F .r.v.i.c.e....po
0xA0 7274 2E61 636F 6E74 692E 6E65 742F 6469 rt.aconti.net/di
```

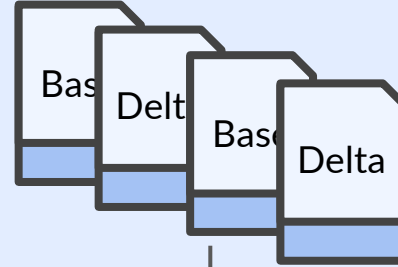
# The Validation

# Quick Reminder



mpengine.dll

For Each VDM:



*LoadDatabase*

*ConsumeInputCompress*

# RMDX & Zlib Headers

## RMDX Header

```
struct RMDX_Header {  
    u32 Signature;  
    u32 Timestamp;  
    u32 Unknown1;  
    u32 Options;  
    u32 Unknown2;  
    u32 Unknown3;  
    u32 DataOffset;  
    u32 DecompressedDataSize;  
};
```

52	4D	44	58	16	AE	7F	64	FF	FF	FF	FF	00				
00	00	00	00	00	00	00	00	BC	00	00	00	00				
00	00	00	00	00	00	00	00	00	00	00	00	00				
FF	FF	FF	FF	00	00	00	00	00	00	00	00	00				
28	01	00	00	29	C6	02	00	40	18	00	00	40				
55	E7	03	00	5B	02	00	00	5C	08	00	00	50				
61	05	00	00	67	6E	00	00	6C	16	00	00	70				
73	01	00	00	74	01	00	00	78	4B	00	00	70				
7E	67	3C	00	80	B5	0D	00	8C	0C	00	00	8D	01	00	00	~g<.....
8F	02	00	00	96	03	00	00	A0	9B	2F	00	A9	0C	00	00	...../.....
B3	02	00	00	BD	22	01	00	BE	02	00	00	CE	14	00	00	....."
CF	1F	00	00	D0	02	00	00	F7	30	13	00	4C	A4	35	00	.....0..L.5.
78	9D	D6	C6	B4	7D	07	78	54	65	D6	FF	9B	7B	EF	CC	x....}.xTe...{..
64	66	D2	67	52	81	48	15	63	0F	51	A2	94	84	00	82	df.gR.H.c.Q....
46	40	9A	14	49	03	4B	14	D7	82	09	A2	D8	0E	60	01	F@..I.K.....`
45	A3	62	23	AE	AE	8A	8A	25	D1	5D	1B	CA	46	D1	A0	E.b#....%.]..F..



# RMDX & Zlib Headers

```
52 4D 44 58 16 AE 7F 64 FF FF FF FF 02 00 20 00 RMDX... d...  
00 00 00 00 00 00 00 00 00 00 00 00 00 8A 61 56 00 ... aV.  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Zlib Data Header

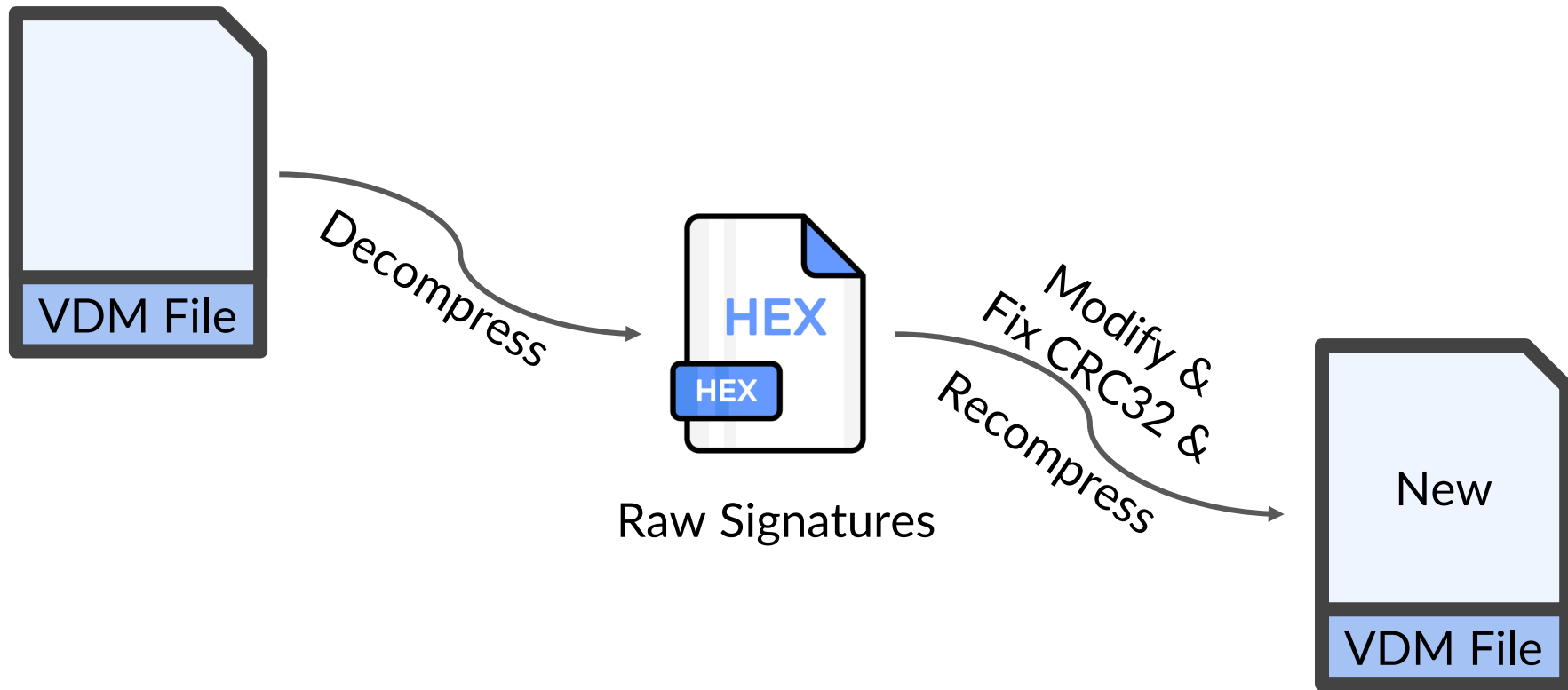
```
struct CDATA_Header {  
    u32 CompressedDataLength;  
    u32 CRC32;  
    u8 CompressedData[CompressedDataLength];  
};
```

```
01 02 00 00 90 03 00 00 70 9D 21 00 79 0C 00 00 ... / ...  
B3 02 00 00 BD 22 01 00 BE 02 00 00 CE 14 00 00 ... "  
CF 1F 00 00 D0 02 00 00 F7 30 13 00 4C A4 35 00 ... 0.. L. 5.  
78 9D D6 C6 B4 7D 07 78 54 65 D6 FF 9B 7B EF CC x... }.. xTe... {..  
64 66 D2 67 52 81 48 15 63 0F 51 A2 94 84 00 82 df.. gR.. H.. c.. Q...  
46 40 9A 14 49 03 4B 14 D7 82 09 A2 D8 0E 60 01 F@.. I.. K...  
45 A3 62 23 AE AE 8A 8A 25 D1 5D 1B CA 46 D1 A0 E.. b#... %.. ].. F..
```

# CRC32 Algorithm

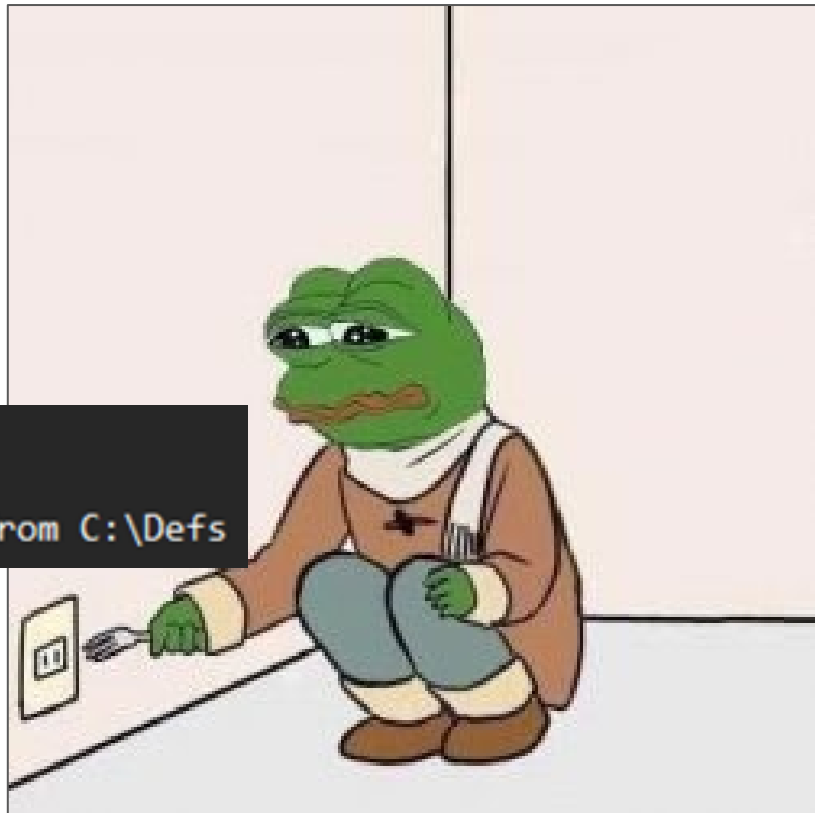
Algorithm	Result	Check	Poly	Init
<a href="#">CRC-32</a>	0xE5B92BDF	0xCBF43926	0x04C11DB7	0xFFFFFFFF
<a href="#">CRC-32/BZIP2</a>	0xB4E3A0A8	0xFC891918	0x04C11DB7	0xFFFFFFFF
<a href="#">CRC-32/JAMCRC</a>	0x1A46D420	0x340BC6D9	0x04C11DB7	0xFFFFFFFF
<a href="#">CRC-32/MPEG-2</a>	0x4B1C5F57	0x0376E6E7	0x04C11DB7	0xFFFFFFFF
<a href="#">CRC-32/POSIX</a>	0x9B769BC0	0x765E7680	0x04C11DB7	0x00000000
<a href="#">CRC-32/SATA</a>	0x4C98BB08	0xCF72AFE8	0x04C11DB7	0x52325032

# Trying One More Update Attempt

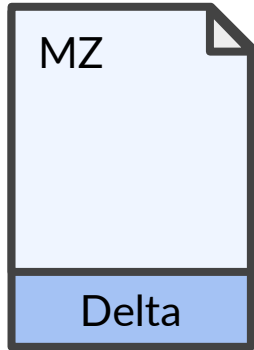


# Trying One More Update Attempt

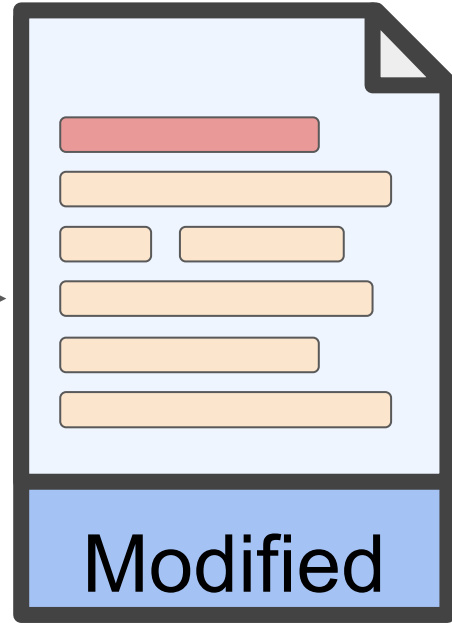
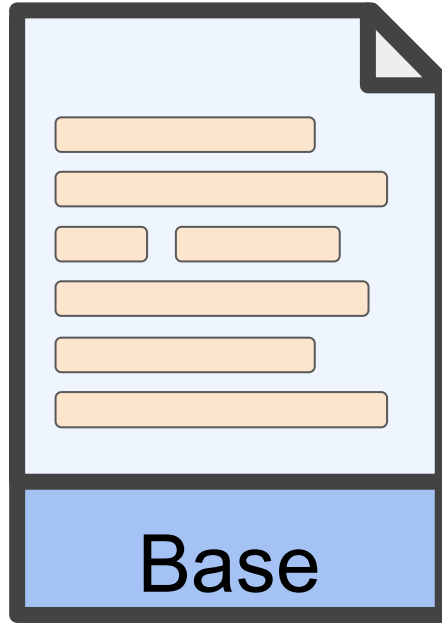
```
ERROR 0x8050a004 : MpUpdateEngine(C:\Defs)  
ERROR 0x8050a004 : MpUpdateEngine(C:\Defs)  
ERROR 0x8050a004 : Failed to update signatures from C:\Defs
```



# How Do We Modify?



**IGNORED**



# Two Pairs Of VDM Files



AntiVirus

mpavdlta

VDM

mpavbase

VDM

AntiSpyware

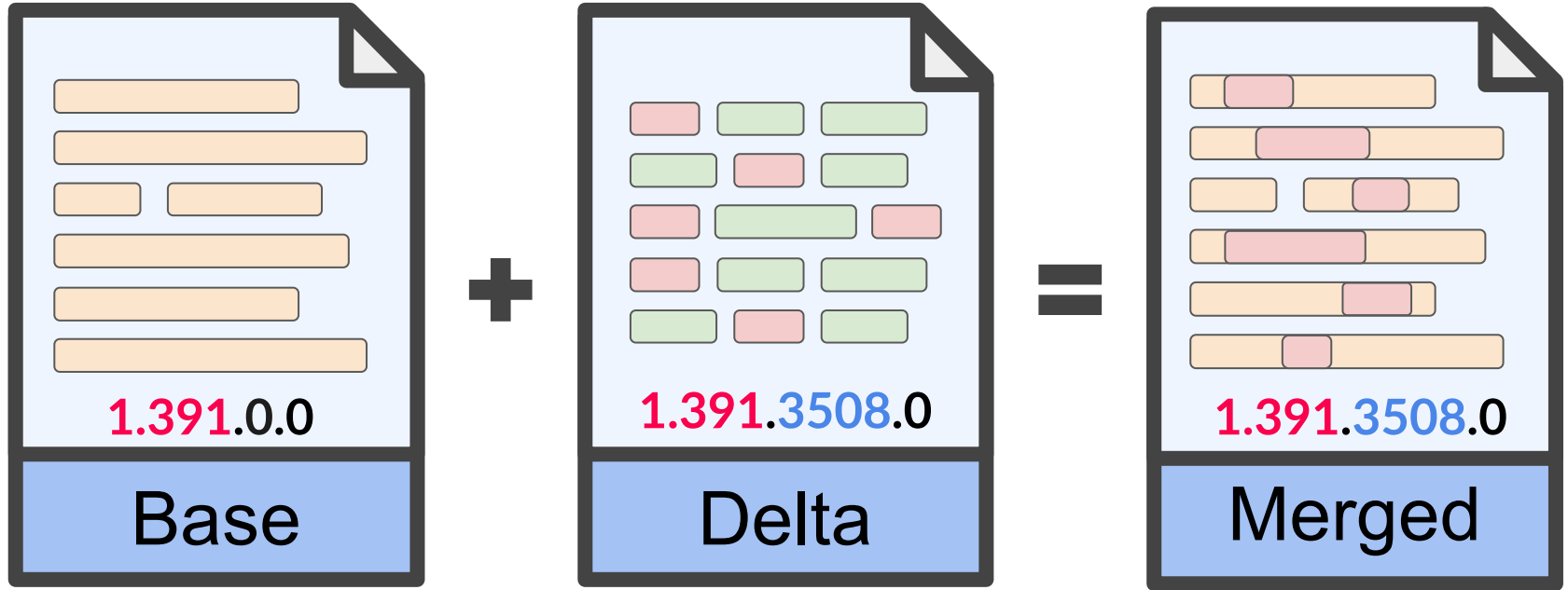
mpasdlt

VDM

mpasbase

VDM

# What The Purpose Of Delta Files?



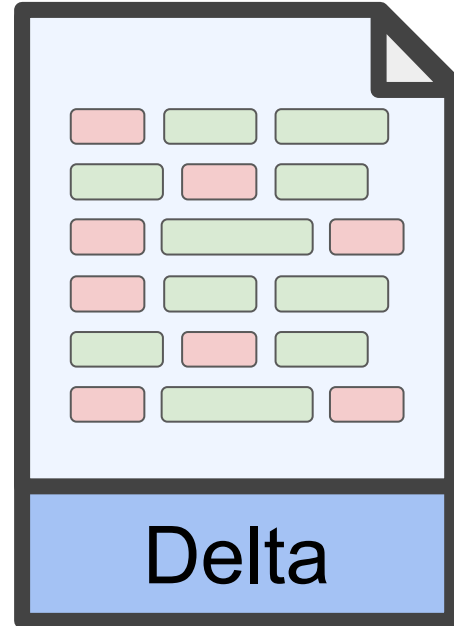
# The Merge

Internals



# What's The Delta Format?

```
bitfield SignatureHeader {  
    Type: 8;  
    Size: 24;  
};  
  
struct Signature {  
    SignatureHeader header;  
    u8 Data[header.Size];  
};
```



# BLOB\_RECINFO & BLOB

## BLOB\_RECINFO

74	64	00	00	18	00	00	00	28	AA	00	00	29	10	00	00
40	4B	00	00	41	13	00	00	5C	DC	01	00	5D	DC	01	00
61	14	00	00	78	1A	03	00	7A	C2	00	00	7E	C7	00	00
80	4E	00	00	87	12	00	00	8C	0B	00	00	8D	06	00	00
8F	14	00	00	A8	04	00	00	B3	20	00	00	BD	01	00	00
BE	40	00	00	CE	05	00	00	CF	05	00	00	D3	05	00	00
D7	08	00	00	E7	B4	00	00	73	84	69	23	45	F9	D4	03
D9	42	9F	EC	01	00	5C	FF	FF	01	00	00	00	FF	FF	06
80	00	00	FF	FF	0B	00	01	00	FF	FF	10	80	01	00	FF
FF	15	00	02	00	FF	FF	1A	80	02	00	97	B5	1F	00	03
00	01	00	05	13	BE	BD	35	03	00	FF	FF	F0	73	03	00
FF	FF	F5	F3	03	00	07	F9	FA	73	04	00	01	00	5A	66
8C	08	ED	04	00	15	00	11	09	A8	58	1F	70	11	5D	2B
C9	09	D1	F2	44	08	00	01	20	A6	38	95	CF	80	6F	F9

## BLOB

```
bitfield SignatureHeader {
    Type: 8;
    Size: 24;
};

struct Signature {
    SignatureHeader header;
    u8 Data[header.Size];
};

Signature blob_recinfo @0;
Signature blob @$;
```

# BLOB Structure

```
struct Blob {  
    SignatureHeader header;  
    u32 Unknown1;  
    u32 Unknown2;  
    u8 Data[header.Size - 8],  
};
```

AA	00	00	29	10	00	00
DC	01	00	5D	DC	01	00
C2	00	00	7E	C7	00	00
0B	00	00	8D	06	00	00
20	00	00	BD	01	00	00
05	00	00	D3	05	00	00

D7	08	00	00	E7	B4	00	00	73	84	69	23	45	F9	D4	03
D9	42	9F	EC	01	00	5C	FF	FF	01	00	00	00	FF	FF	06
80	00	00	FF	FF	0B	00	01	00	FF	FF	10	80	01	00	FF
FF	15	00	02	00	FF	FF	1A	80	02	00	97	B5	1F	00	03
00	01	00	05	13	BE	BD	35	03	00	FF	FF	F0	73	03	00
FF	FF	F5	F3	03	00	07	F9	FA	73	04	00	01	00	5A	66
8C	08	ED	04	00	15	00	11	09	A8	58	1F	70	11	5D	2B
C9	09	D1	F2	44	08	00	01	20	A6	38	95	CF	80	6F	F9

# Actions

```
struct Blob {  
    SignatureHeader header;  
    u32 Unknown1;  
    u32 Unknown2;  
    u8 Data[header.Size - 8];  
};
```

AA	00	00	29	10	00	00
DC	01	00	5D	DC	01	00
C2	00	00	7E	C7	00	00
0B	00	00	8D	06	00	00
20	00	00	BD	01	00	00
05	00	00	D3	05	00	00

D7	08	00	00	E7	B4	00	00	73	84	69	23	45	F9	D4	03
D9	42	9F	EC	01	00	5C	FF	FF	01	00	00	00	FF	FF	06
80	00	00	FF	FF	0B	00	01	00	FF	FF	10	80	01	00	FF
FF	15	00	02	00	FF	FF	1A	80	02	00	97	B5	1F	00	03
00	01	00	05	13	BE	BD	35	03	00	FF	FF	F0	73	03	00
FF	FF	F5	F3	03	00	07	F9	FA	73	04	00	01	00	5A	66
8C	08	ED	04	00	15	00	11	09	A8	58	1F	70	11	5D	2B
C9	09	D1	F2	44	08	00	01	20	A6	38	95	CF	80	6F	F9

# Reverse ConsumeInputCompress

```
.text:00007FF8D9224B66 mov     rcx, [rbp+110h+var_DecompressedDeltaData]
.text:00007FF8D9224B6A movzx   r9d, word ptr [rcx+r8] ; Move with Zero-Extend
.text:00007FF8D9224B6F mov     word ptr [rsp+210h+var_DeltaSigHeader_2Bytes], r9w
.text:00007FF8D9224B75 add     r8, 2 ; Add
.text:00007FF8D9224B79 mov     [rsp+210h+var_IndexOnDecompressData?], r8
.text:00007FF8D9224B7E test    r9w, r9w ; Logical Compare
.text:00007FF8D9224B82 jns     loc_7FF8D9224EFD ; Jump if Not Sign (SF=0)
```

MSB Check

# Action Types

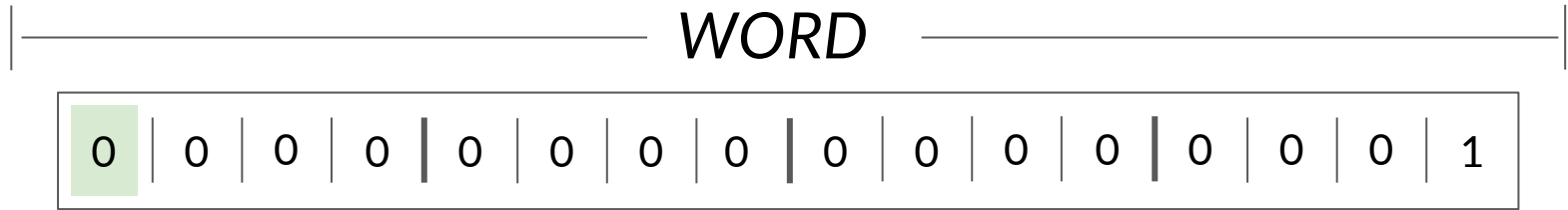
## Copy From Delta

Copy <size> bytes from the current position of delta file to the merge file

## Copy From Base

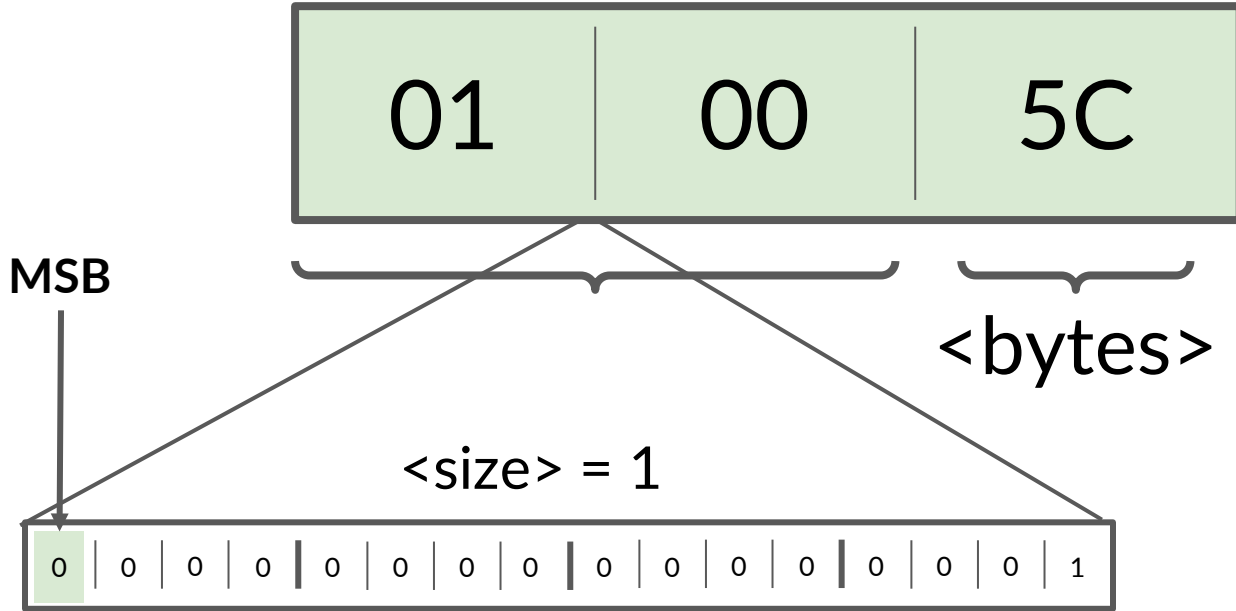
Copy <size> bytes from <offset> within the base file to the merge file

# Action Header



Action Type

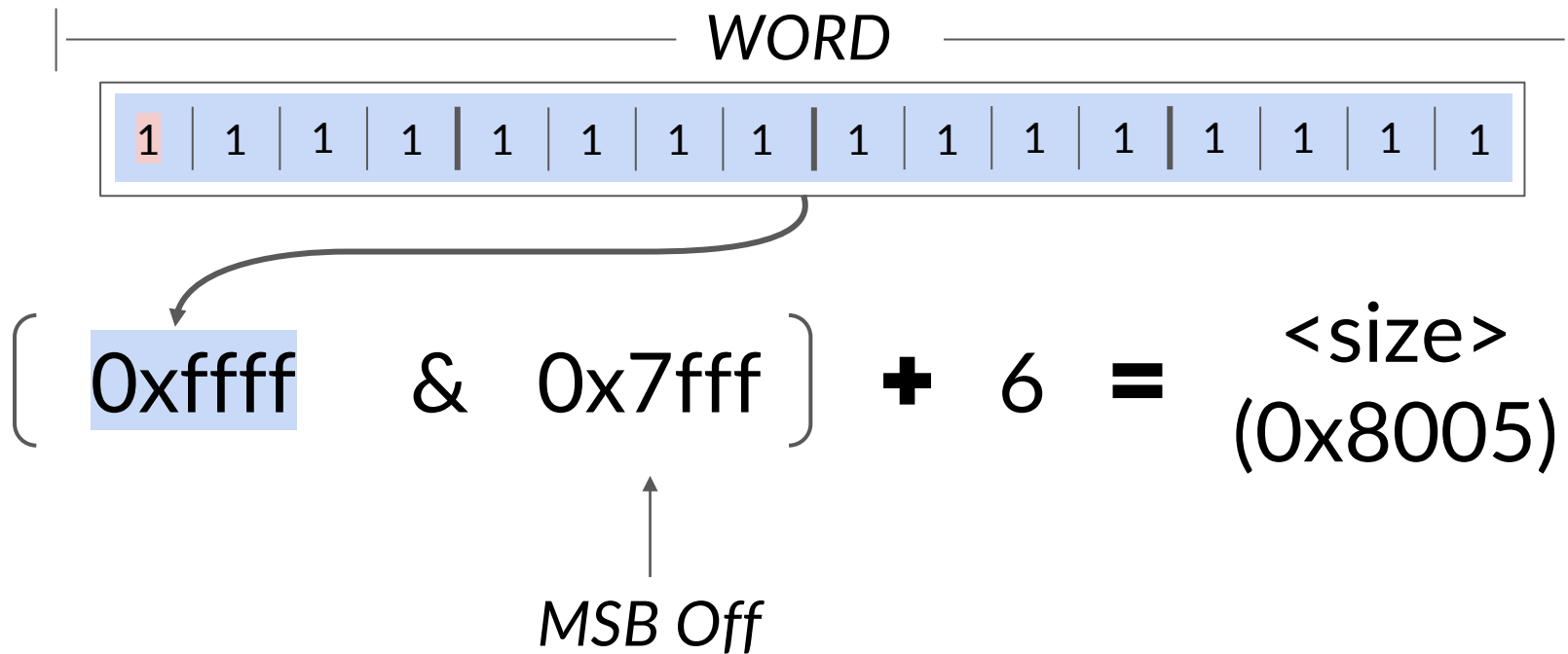
# CopyFromDelta - Example



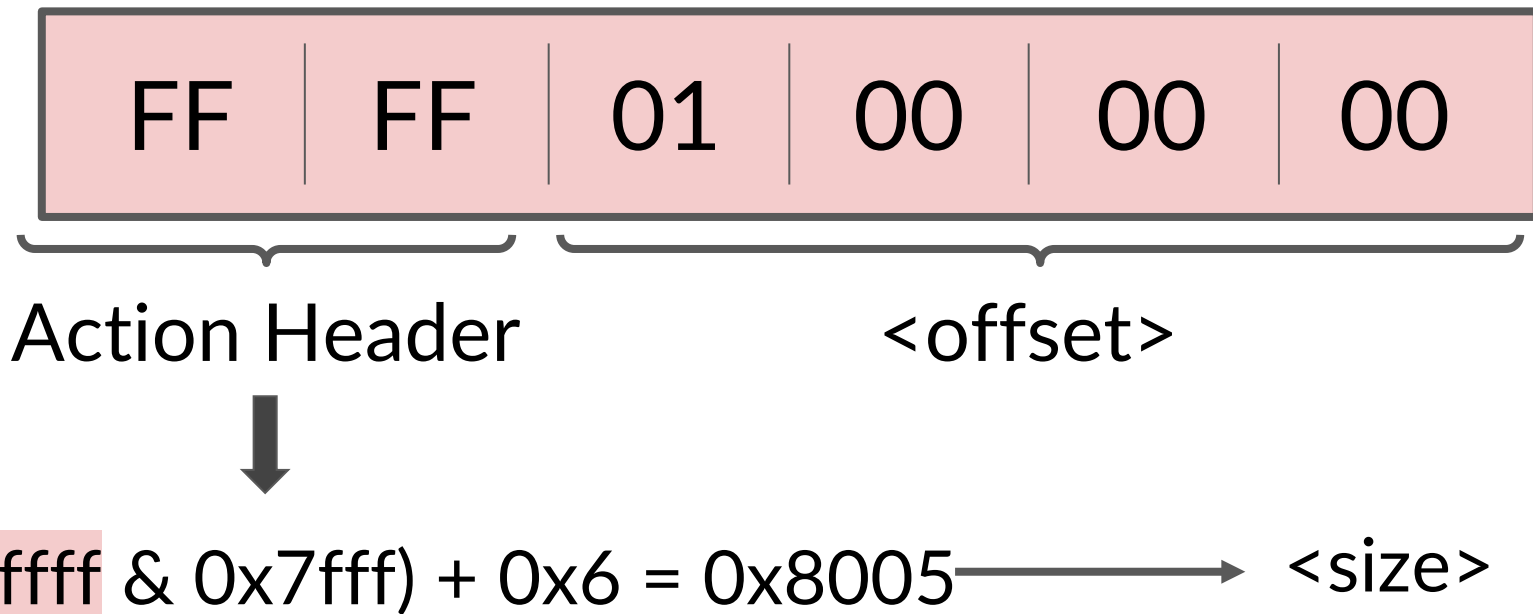




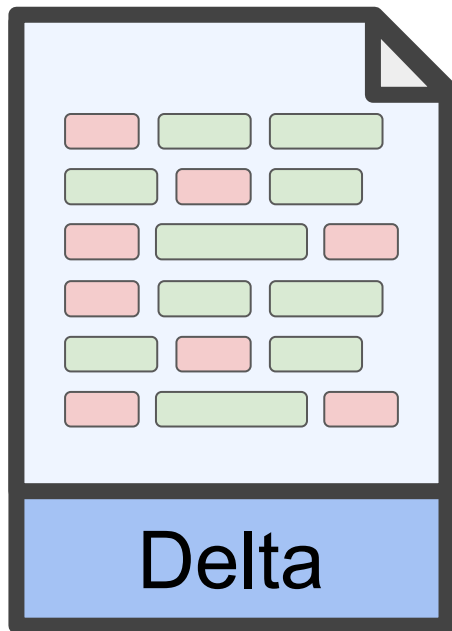
# Action Header - CopyFromBase



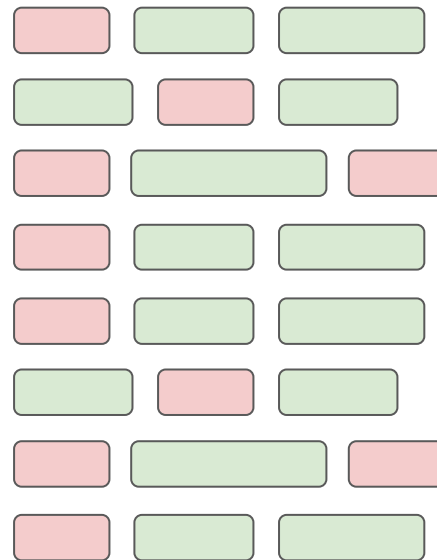
## CopyFromBase - Example



# Sum Up



## Actions



# Merge Algorithm

```
def merge(actions: list, base: io.BytesIO):
    merge_stream = io.BytesIO()

    for action in actions:
        if action.type == CopyFromBase:
            """
            CopyFromBase: <size><offset>
            """
            base.seek(action.offset)
            bytes = base.read(action.size)
        else:
            """
            CopyFromDelta: <size><bytes>
            """
            bytes = actions.bytes

        merge_stream.write(bytes)

    return merge_stream
```

# Diffing Base and Merge

## Base

```
FA 1F 5F FB 00 70 04 00 00 20 AE CE E1 AD 67 16 ... _ p ... g
00 00 F5 7E BD B2 8C 1F E9 EC 05 F9 AA 2B 00 E0 ... ~ ... +
01 00 00 20 3F 5B D6 35 67 16 00 00 E0 EF BF B2 ... ? [ 5g ...
51 C9 E5 BC A7 43 5B 33 82 10 03 00 00 20 BD 23 Q ... C[3 ... #
B8 B4 67 16 00 00 05 E3 D9 B2 59 C7 B4 C0 DF 48 ... z ... Y ... H
00 C5 7A 20 03 00 00 20 C9 B4 39 5E 67 16 00 00 ... z ... 9^g
F9 94 5D B3 1E B7 06 A7 C7 2A 5E 73 00 70 05 00 ... ] ... *^s p
00 20 7F A7 BC D5 67 16 00 00 0D 53 55 B4 B7 33 ... g ... SU 3
22 37 E3 33 44 DF 3C B0 01 00 00 20 54 73 A3 DF "7.3D < ... Ts
67 16 00 00 55 0D 26 B6 42 93 E6 63 1D 14 6B 19 g ... U 8 B c k
89 30 13 00 01 20 84 94 4F 0B 67 16 00 00 B3 30 0 ... O g ... 0
4F B6 EE FF E3 38 D9 81 12 87 03 F1 16 00 00 20 0 ... 8
63 6C C0 5B 67 16 00 00 C8 9A 72 B6 55 A3 23 3B cl [g ... r U #;
AE DF 88 B5 18 87 02 00 01 20 7F EA 74 72 67 16 ... trg
00 00 B1 1C A5 B6 F9 9F B4 7E 69 7D F4 3B 3B 90 ... i} ; ;
01 00 00 20 2F A8 DD D1 67 16 00 00 47 1A 59 B7 ... / g ... G Y i w a4r 4
69 80 77 1A 61 34 72 F9 34 B0 06 00 00 20 36 4D i w a4r 4 ... 6M
A3 96 67 16 00 00 A5 DF 5A B9 B5 3F C3 F6 69 41 g ... Z ? iA
93 49 47 20 09 00 00 20 15 CF 01 F5 67 16 00 00 IG ... g
AD 84 52 BA 31 B5 E9 1D F9 76 66 2D 37 60 01 00 R 1 ... vf-7
00 20 00 E7 54 58 67 16 00 00 2C CE FE BA 1B B8 ... TXg
93 33 6C 25 0A B6 58 58 1C 00 00 20 CB F0 04 74 31% XX ... t
67 16 00 00 45 1C 2D BB 79 6F 31 D7 30 5A 51 ED g ... E - yo1 0ZQ
00 90 04 00 00 20 20 21 B8 DE 67 16 00 00 45 1C ... pl g ... E
2D BB CD F6 F8 77 30 5A 51 ED 00 90 04 00 00 20 ... w0ZQ
C4 B8 71 7E 67 16 00 00 A7 3F 52 BB 0A 4E 39 75 q-g ... ?R N9u
```

Region: 0x00000000 - 0x0ACEE711 (0 - 181331729)

Data Size: 0x0ACEE711 (0xACEE711 | 172.93 MiB)

## After Merge

```
FA 1F 5F FB 00 70 04 00 00 20 AE CE E1 AD 67 16 ... _ p ... g
00 00 F5 7E BD B2 8C 1F E9 EC 05 F9 AA 2B 00 E0 ... ~ ... +
01 00 00 20 3F 5B D6 35 67 16 00 00 E0 EF BF B2 ... ? [ 5g ...
51 C9 E5 BC A7 43 5B 33 82 10 03 00 00 20 BD 23 Q ... C[3 ... #
B8 B4 67 16 00 00 05 E3 D9 B2 59 C7 B4 C0 DF 48 ... z ... Y ... H
00 C5 7A 20 03 00 00 20 C9 B4 39 5E 67 16 00 00 ... z ... 9^g
F9 94 5D B3 1E B7 06 A7 C7 2A 5E 73 00 70 05 00 ... ] ... *^s p
00 20 7F A7 BC D5 67 16 00 00 0D 53 55 B4 B7 33 ... g ... SU 3
22 37 E3 33 44 DF 3C B0 01 00 00 20 54 73 A3 DF "7.3D < ... Ts
67 16 00 00 B3 30 4F B6 EE FF E3 38 D9 81 12 87 g ... 0 8
03 F1 16 00 00 20 63 6C C0 5B 67 16 00 00 C8 9A ... cl [g
72 B6 55 A3 23 3B AE DF 88 B5 18 87 02 00 01 20 r U #;
7F EA 74 72 67 16 00 00 B1 1C A5 B6 F9 9F B4 7E ... trg
69 7D F4 3B 3B 90 01 00 00 20 2F A8 DD D1 67 16 i} ; ; / g
00 00 47 1A 59 B7 69 80 77 1A 61 34 72 F9 34 B0 ... G Y i w a4r 4
06 00 00 20 36 4D A3 96 67 16 00 00 A5 DF 5A B9 ... 6M g ... Z
B5 3F C3 F6 69 41 93 49 47 20 09 00 00 20 15 CF ? iA IG
01 F5 67 16 00 00 AD 84 52 BA 31 B5 E9 1D F9 76 g ... R 1 ... v
66 2D 37 60 01 00 00 20 00 E7 54 58 67 16 00 00 f-7 ... TXg
2C CE FE BA 1B 8B 93 33 6C 25 0A B6 58 58 1C 00 ... 31% XX
00 20 CB F0 04 74 67 16 00 00 00 45 1C 2D BB 79 6F ... tg ... E - yo
31 D7 30 5A 51 ED 00 90 04 00 00 20 70 21 B8 DE 1 0ZQ ... pl
67 16 00 00 45 1C 2D BB CD F6 F8 77 30 5A 51 ED g ... E - w0ZQ
00 90 04 00 00 20 C4 B8 71 7E 67 16 00 00 A7 3F ... q-g ... ?
52 BB 0A 4E 39 75 23 6F 6D 35 3B 10 07 00 00 20 R N9u#om5;
D0 F9 29 B1 67 16 00 00 A0 0E 16 BC 83 07 A6 E9 ) g
```

Region: 0x00000000 - 0x0AF6CE1C (0 - 183946780)

Data Size: 0x0AF6CE1C (0xAF6CE1C | 175.43 MiB)

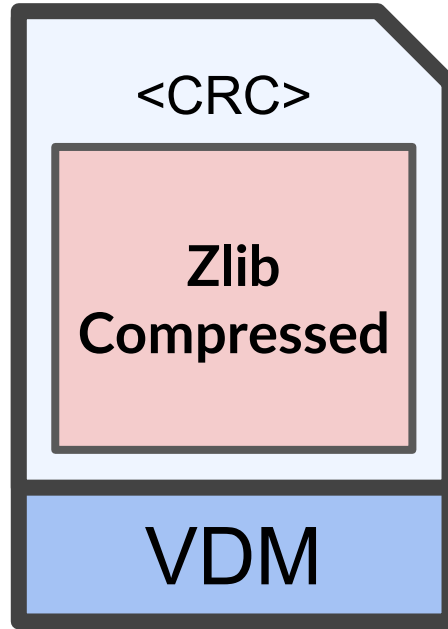
# Eureka - Unknown Numbers

```
struct Blob {  
    SignatureHeader header;  
    u32 Unknown1;  
    u32 Unknown2;  
    u8 Data[header.Size - 8];  
};
```

```
struct Blob {  
    SignatureHeader header;  
    u32 MergeSize;  
    u32 MergeCRC32;  
    u8 Data[header.Size - 8];  
};
```



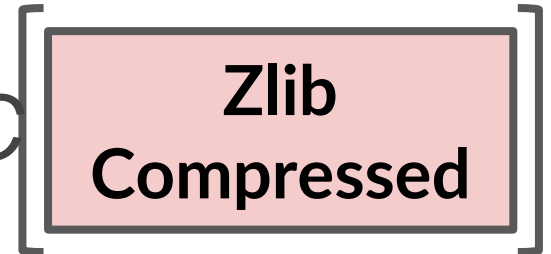
# Validations Recap - Zlib Data Validation



<CRC  
>

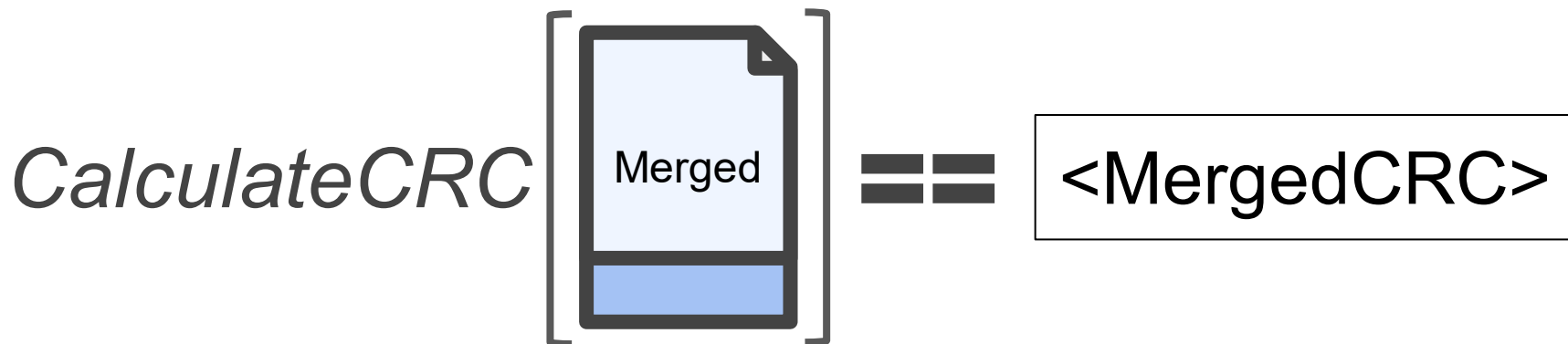
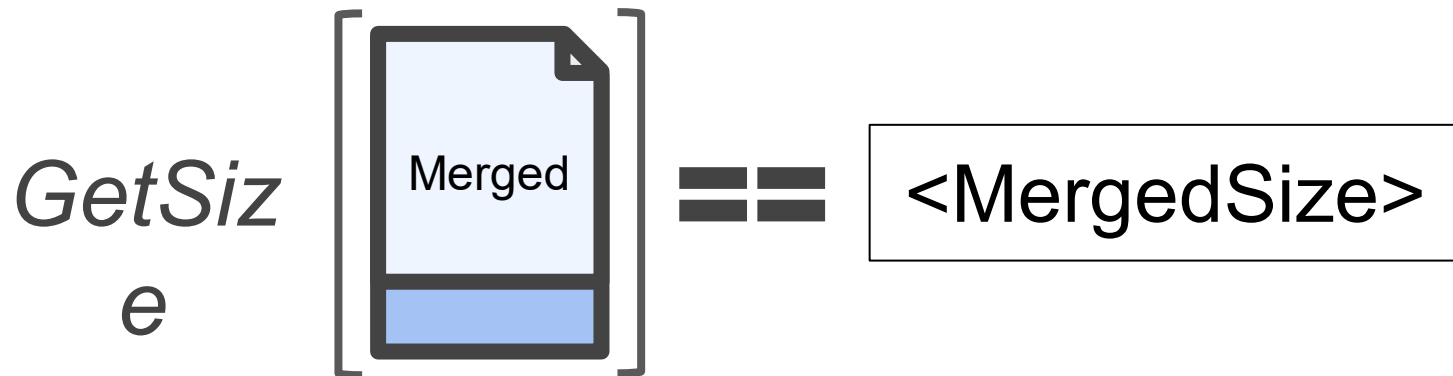
==

*CalculateCRC*





# Validations Recap - Merge Validations



# Can We Fake an Update?



# We Did It !!!



```
----- ValidateUpdate -----
```

```
MpSigStub successfully updated Microsoft Windows Defender (RS1+) using the AM Bases and Delta package.
```

	Original:	Updated to:
AS base VDM:	1.383.0.0	1.383.0.0
AV base VDM:	1.383.0.0	1.383.0.0
AS delta VDM:	1.383.1799.0	1.383.1800.0
AV delta VDM:	1.383.1799.0	1.383.1800.0

Updated to: 1.383.1800

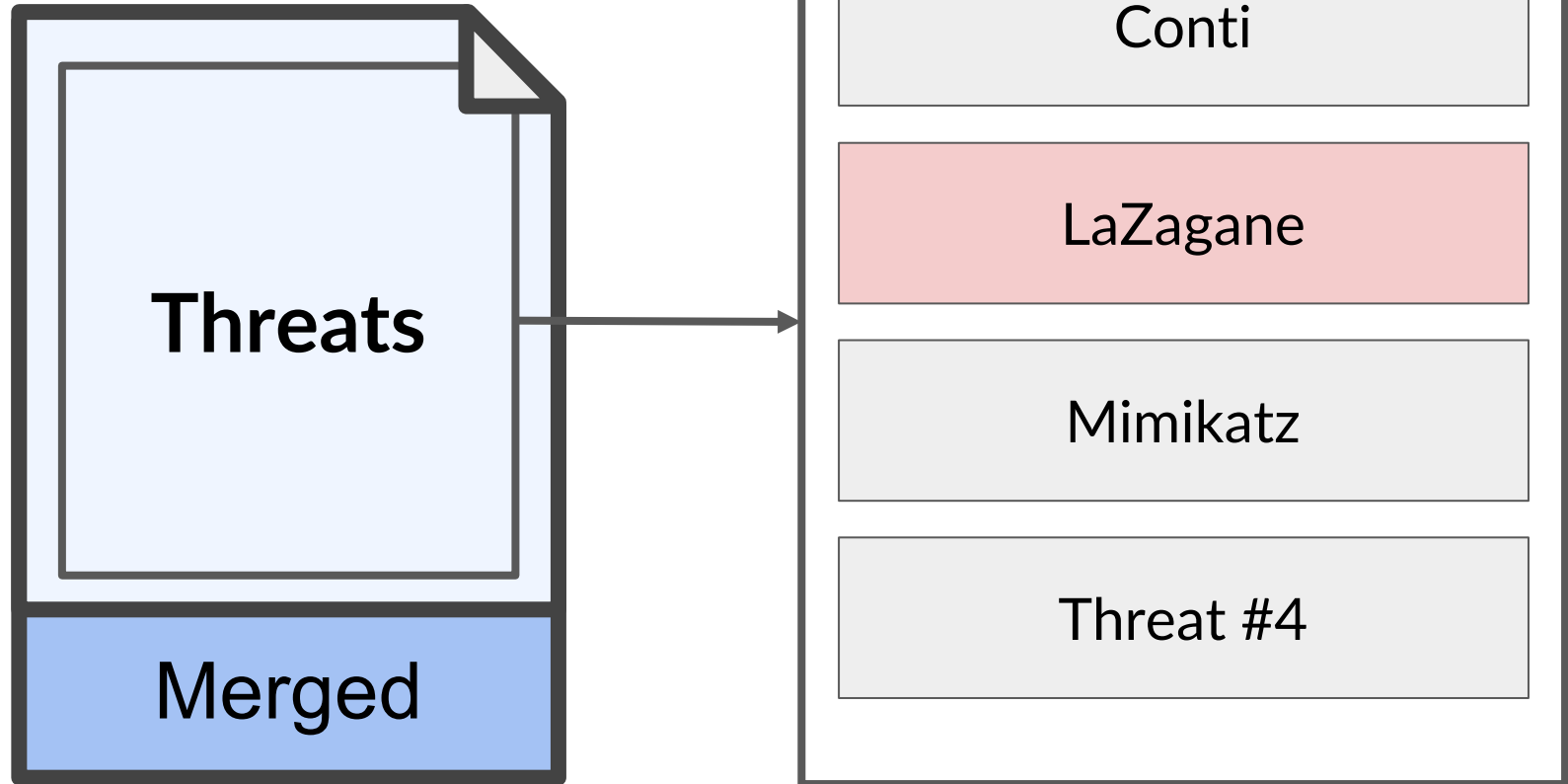
# Attack Vectors

(CVE-2023-24934)

wd-pretender



# Delete LaZagane Threats



PS C:\Users\weak\work>

New | Cut | Copy | Paste | Delete | Sort | View | ...

Users > weak > work > Defs

Name	Date modified	Type	Size
MpSigStub	1/1/2023 6:17 AM	Application	785 KB

1 item

Activate Windows  
Go to Settings to activate Windows.

# Friendly Files

## 30,000 friendly hashes

```
156: "SIGNATURE_TYPE_VDLL_ARM",
157: "SIGNATURE_TYPE_THREAD_X86",
158: "SIGNATURE_TYPE_THREAD_X64",
159: "SIGNATURE_TYPE_THREAD_IA64",
160: "SIGNATURE_TYPE_FRIENDLYFILE_SHA256",
161: "SIGNATURE_TYPE_FRIENDLYFILE_SHA512",
162: "SIGNATURE_TYPE_SHARED_THREAT",
163: "SIGNATURE_TYPE_VDM_METADATA",
164: "SIGNATURE_TYPE_VSTORE",
165: "SIGNATURE_TYPE_VDLL_SYMINFO",
166: "SIGNATURE_TYPE_IL2_PATTERN",
167: "SIGNATURE_TYPE_BM_STATIC",
168: "SIGNATURE_TYPE_BM_INFO",
```

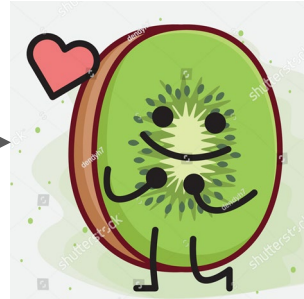
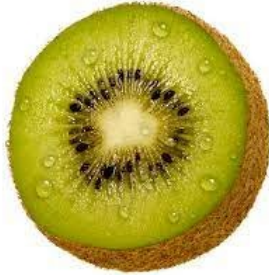
```
895 0209a3e590d5cc6c7cb69b012a59e7fd29c857e0782fcd208a90cc9baa283441
896 0209cffc2df2d39dfa9106fa00fb6d221dbd450dc6161cc2a7138c46a293add7
897 0209f490cbfe60c61b651023e1df9327e5350cd0a8be126907cdbaa6b564ceeb
898 020a4cbaebdb1bbdbdfdf141cfbb16f165457535b5a4612ffdbb33bc64743bbe3
899 020b7b54f1704c10dc5ac9b91bf037486f7b88cc21ce55b766a89ee505a5cde7
900 020c4b29f3771bac476b4ed836c0761fdda30adfaf5d59dbd1f667193cd77d9b
901 020cefa6c036894f912c69eef981efef7d3fffb6a89000efac4888ddd00c255a8
902 020dc950741800877ab9ddb69e566897ed3077c4bc181cf607cdd49dbf23419d
903 020e5eb54040628846c4bfd816b71d8c0694b2b6c94883001a2da3dcfc251346
904 02102bf3d33f117a295093e4af72bae1b6a6be35e3e4255b65ef24f1108c017d
905 02106197ff396ba5c03d528bc6e245d0de25c745237ab37bc5d6a9a913c57e52
906 0210bd8d5d5a63e1b8fa975abaf2e33486f8bc6c8c23d6e1f5c7f2b9460b023b
907 02110f602638980ea83de49f575bcaa4e94508043664676c8090f0a7e230c277
908 021129a2a3446af44a296c2a50fd5023db6e16b489719992bc7c7ce078cebde2
909 02119a7d84b692650607cd256a52d02de8016e972c22d86f6703c4ee240c142d
910 0212a89972e6e11d056323fcf7664a226dd26bce575eaa02c0b17dc5d4dc2cb3
911 0213705992cd08a07c57690ce28e6c7ee930d6a76ddc45d841df4326b04fbc33
912 02141b072b5ebe37f18be2a3658610f353fd3c63b9214472b4fc65588b464c80
913 02142531a7ae99a5509c79e1c639e34d052fb39e77e0c9dbae65c8ff61ef7e19
```





# Friendly Files: First Generic Bypass

What will happen if we will replace existing friendly file hash with mimikatz hash?



Friendly Mimikatz :)

```
Administrator: Windows PowerS
PS C:\Users\woody\work>
```

work

New | Cut | Copy | Paste | Delete | Sort | View

← → ↑ ↓ This PC > Local Disk (C:) > Users > woody > work

Search work

Name	Date modified	Type	Size
Defx	6/22/2023 3:30 AM	File folder	
wd-pretender	6/20/2023 2:42 AM	Application	6,601 KB

Documents | Pictures | Music | Videos | OneDrive | This PC | DVD Drive (D:) | Network

2 items

Windows Security

←

- Home
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control
- Device security
- Device performance & health
- Family options
- Protection history
- Settings

## Virus & threat protection

Protection for your device against threats.

Windows Community videos  
[Learn more about Virus & threat protection](#)

Have a question?  
[Get help](#)

Who's protecting me?  
[Manage providers](#)

Help improve Windows Security  
[Give us feedback](#)

Change your privacy settings  
View and change privacy settings for your Windows 11 device.

### Current threats

No current threats.  
Last scan: Not available

[Quick scan](#)

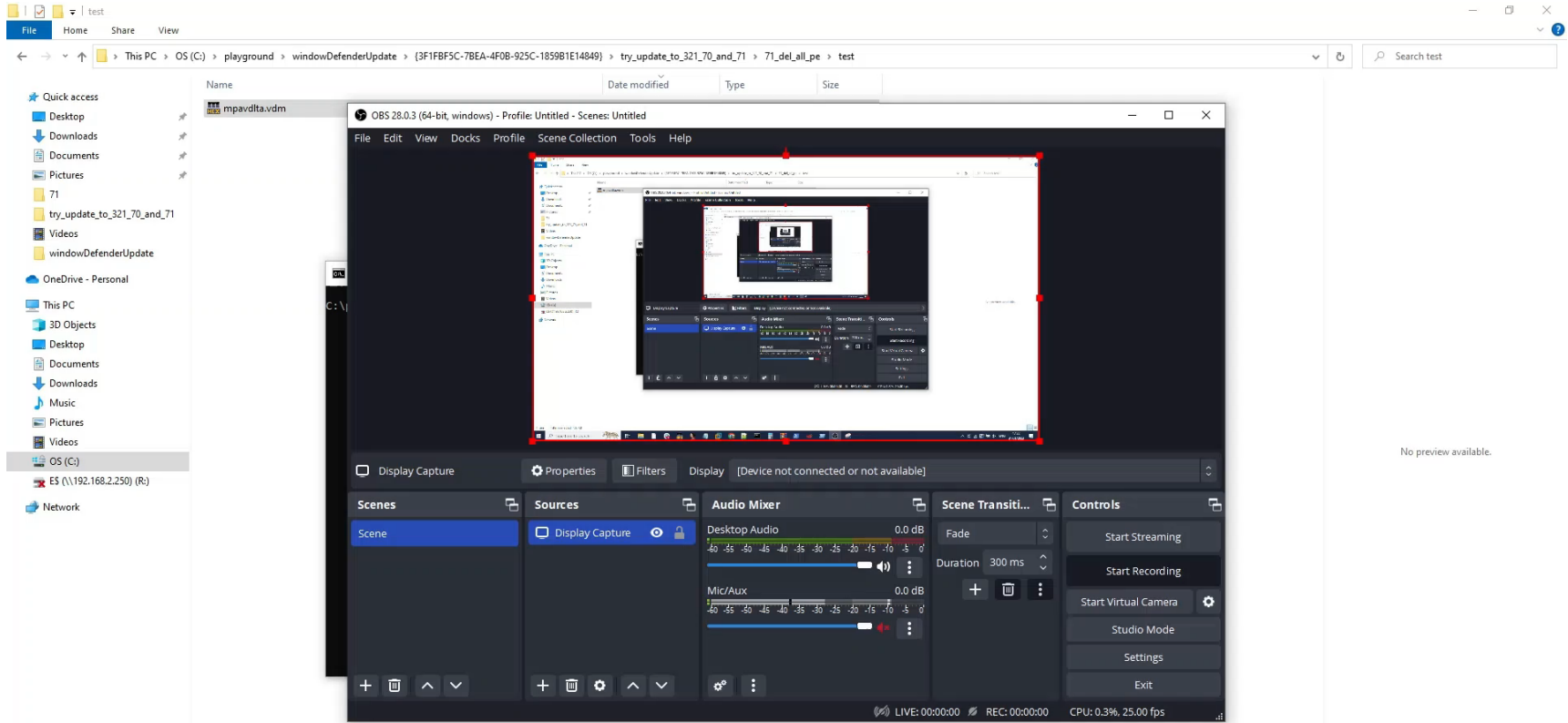
[Scan options](#)  
[Allowed threats](#)  
[Protection history](#)

### Virus & threat protection settings

No action needed.

[Manage settings](#)

# Final Attack Vector: DOS *“!This program cannot be run in DOS Mode”*
























No preview available.

# Final Attack Vector: DOS

- The demo was recorded on an older version of Defender
- The latest version implements few additional checks:  
The "SIGNATURE\_TYPE\_TRUSTED\_PUBLISHER" (112)  
To make Defender delete benign drivers and OS executables.

# Future Work - Possible Local Privilege Escalation

Name
 SIGNATURE_TYPE_LUASTANDALONE_!#_AutoitExecFile.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-AttachmentContainerExt.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-ContextFromSharepoint.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-ContextFromWebmail.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-ContextFromWordPress.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-ContextualDropFileByEmailClient.Includes.GetEmail...
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-ContextualDropFileByEmailClientTag.Includes.GetE...
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-FileInBasePathAttributes.A.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-FromSkypeTransfer.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-InnoSetupClassifier.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-ISOExt.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-LnkExt.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-NSIS_Installer.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-SuspiciousStringinURL.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_OLEHasJar.ObMpAttributes.çÚ¼iöã"üĐ.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_SuspiciousKEYGENfilename.ObMpAttributes.çÚ¼iü,üü...
 SIGNATURE_TYPE_LUASTANDALONE_!#_SuspiciousNFOfilename.ObMpAttributes.j.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-Win32_Prifoulvbs.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#_Lua-Worm-JS_Bondat.A!lnk.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#000000_First_OfficeFrame.txt
 SIGNATURE_TYPE_LUASTANDALONE_!#000010_First_FrameNumeralParam.txt

# Future Work - Possible Local Privilege Escalation

- Rule: Filename Similar To Windows File.A
- Checks if a file has the Same name of OS Executable but not in The legit path.
- Only 6 extension are Checked, what about “.SCR”
- Only in system32,syswow64

```
if l_0_3 ~= "exe" and l_0_3 ~= "dll" and l_0_3 ~= "ocx"  
and l_0_3 ~= "cpl" and l_0_3 ~= "com" then  
    return mp.CLEAN  
end  
local l_0_4 = l_0_2 .. "\\\" .. l_0_1  
if mp.IsKnownFriendlyFile(l_0_4, false, false) == true then  
    return mp.CLEAN  
end  
if mp.get_mpattribute("BM_HAS_DIGITALSIGNATURE")  
and mp.IsTrustedFile(false) == true then  
    return mp.CLEAN  
end  
local l_0_5 = MpCommon.ExpandEnvironmentVariables("%windir%")  
if l_0_5 == nil or #l_0_5 < 1.976262583365e-323 then  
    return mp.CLEAN  
end  
local l_0_6 = l_0_5 .. "\\system32\\" .. l_0_1  
if sysio.IsFileExists(l_0_6) then  
    local l_0_7 = "Lua:FilenameExistInSystemFolder.A"  
    mp.set_mpattribute(l_0_7)  
    mp.set_mpattribute(l_0_7 .. "!" .. l_0_3)  
    mp.set_mpattribute(l_0_7 .. "!" .. l_0_1)  
    return mp.INFECTED  
end
```

# Takeaways

- Trust no one
- Using **digitally signed files**  $\neq$  **totally secure**
- **Signature update process** of security controls is a **new possible attack vector**

# Vendor Response



Microsoft

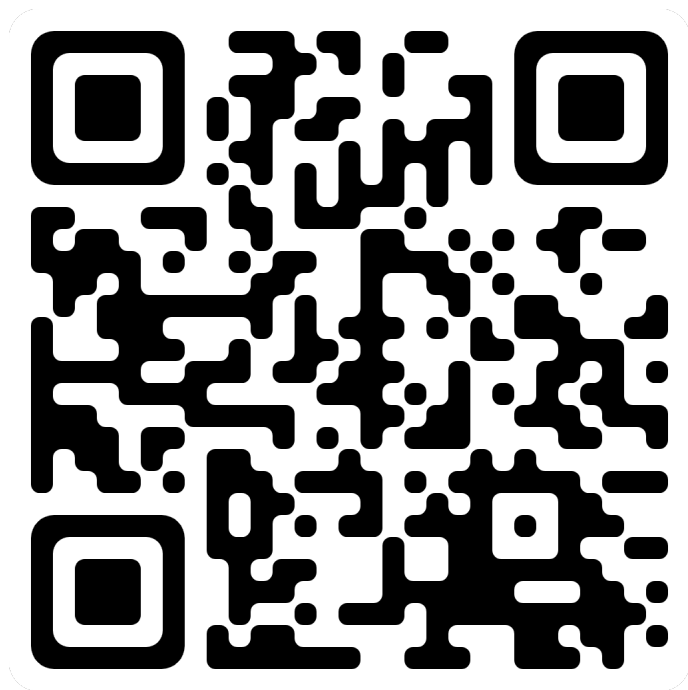
Microsoft released a fix on April - **CVE-2023-24934**  
The fix validates the digital signature of all VDM files

**The fixed version is:**

Microsoft Malware Protection Platform version **4.18.2303.8**



**wd-pretender**



<https://github.com/SafeBreach-Labs/wd-pretender>

# References

- <https://github.com/commial/experiments/tree/master/windows-defender/VDM>
- <https://github.com/sztupy/luadec51/>
- <https://www.crowdstrike.com/blog/evolution-protected-processes-part-1-pass-hash-mitigations-windows-81/>

 SafeBreachLABS

# Thank you!

Tomer Bar

Omer Attias

