SafeBreach LABS

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

SafeBreach LABS

https://tomerbar.net

Omer Attias

Security Researcher @ SafeBreach

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

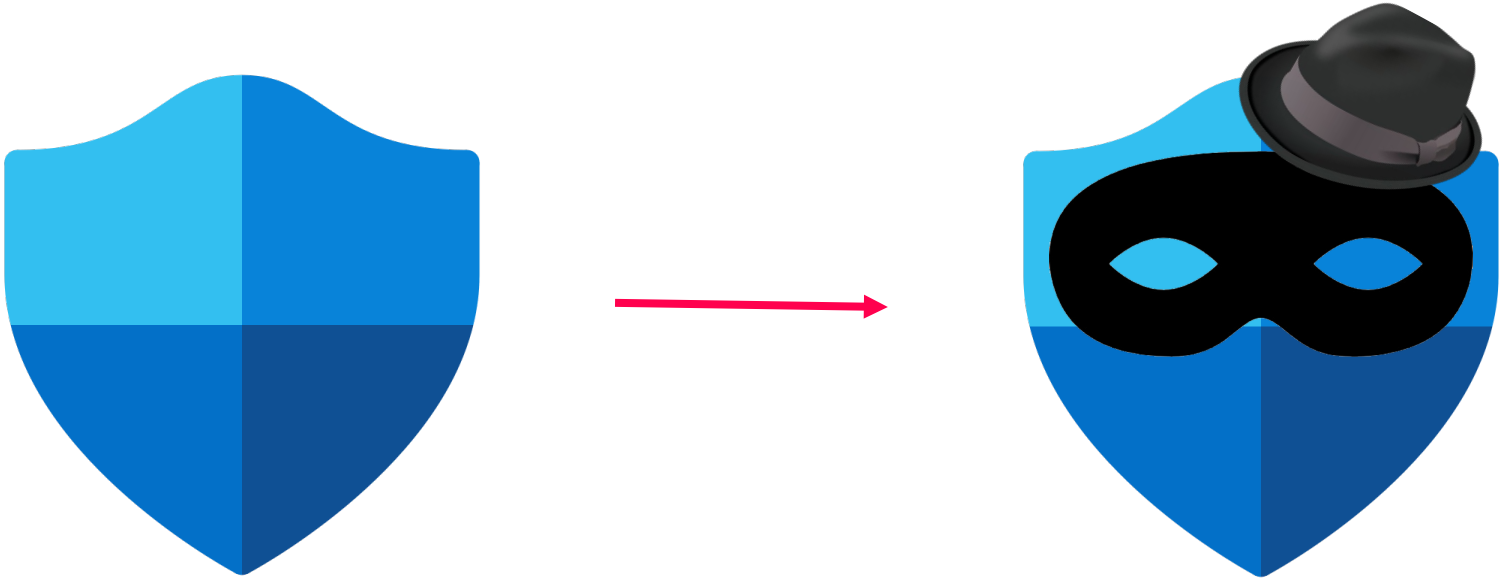
SafeBreach LABS

https://github.com/learn-more

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

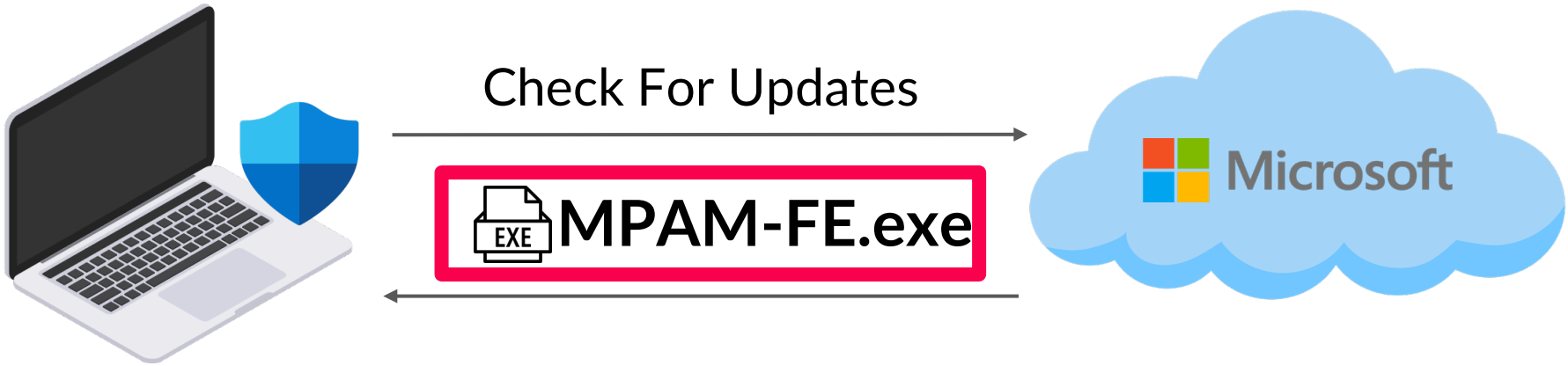
Achieve similar capabilities running as an unprivileged user without possessing a forged certificate and without using MITM.

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

Update Process

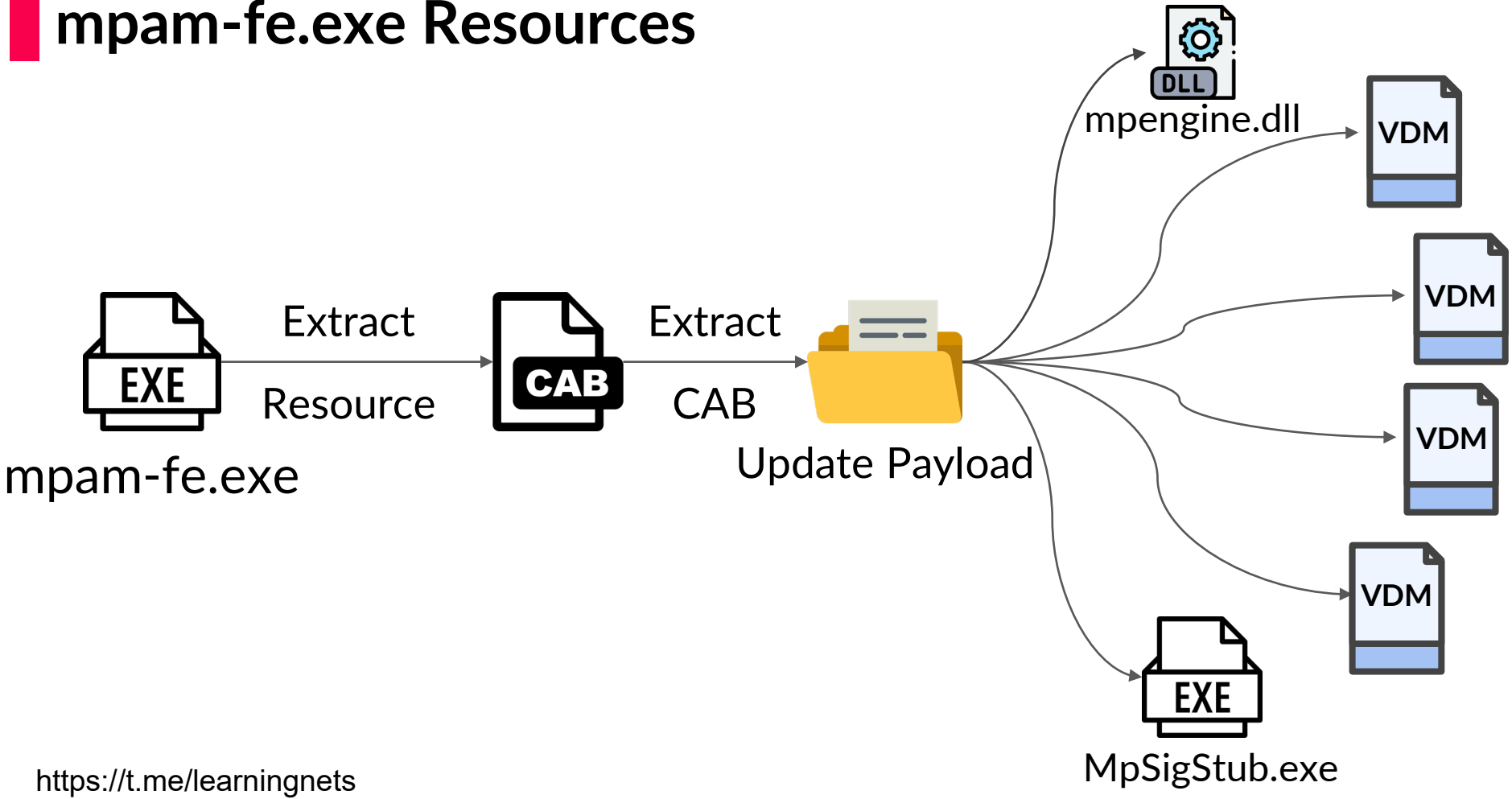
High Level Understanding

What Windows Defender Pulls?

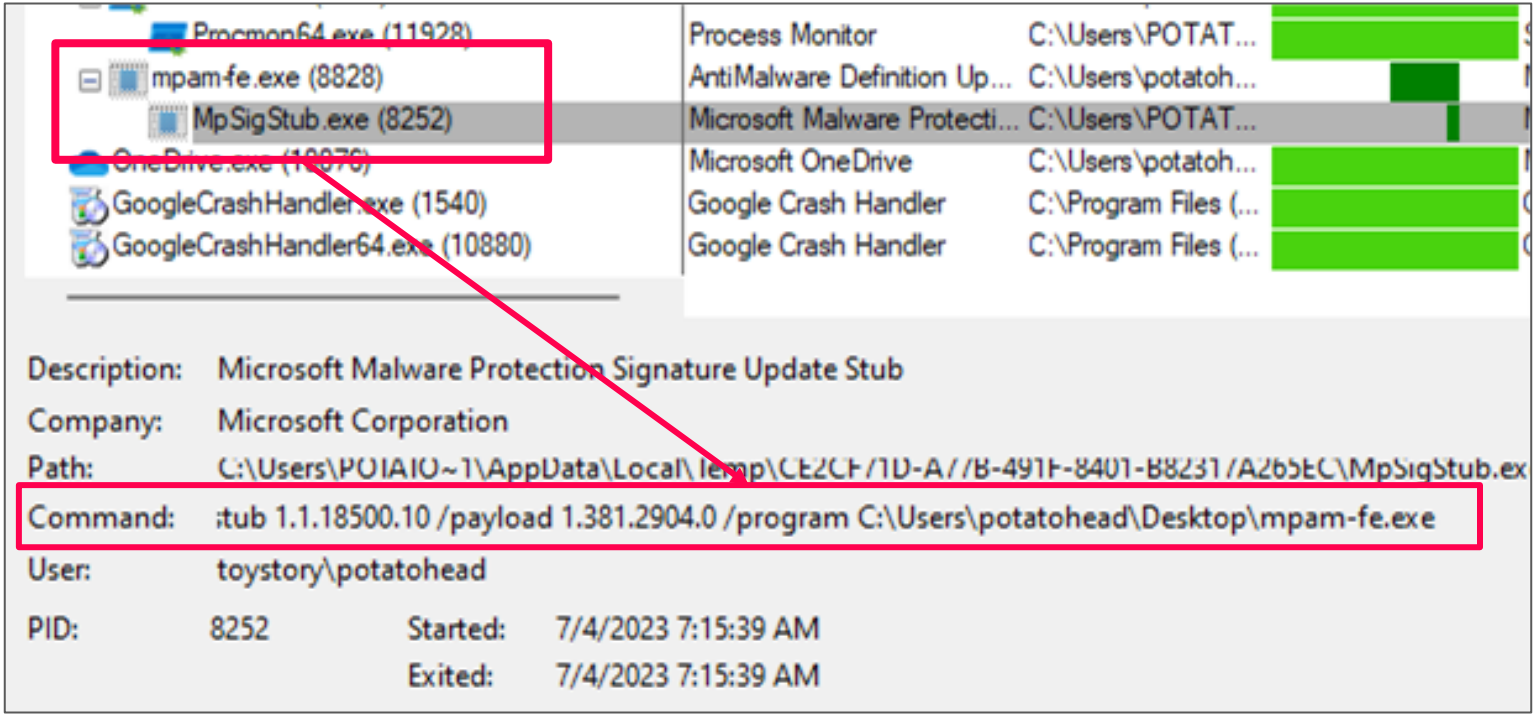


Microsoft **P**rotection **A**ntimalware **F**ront **E**nd.

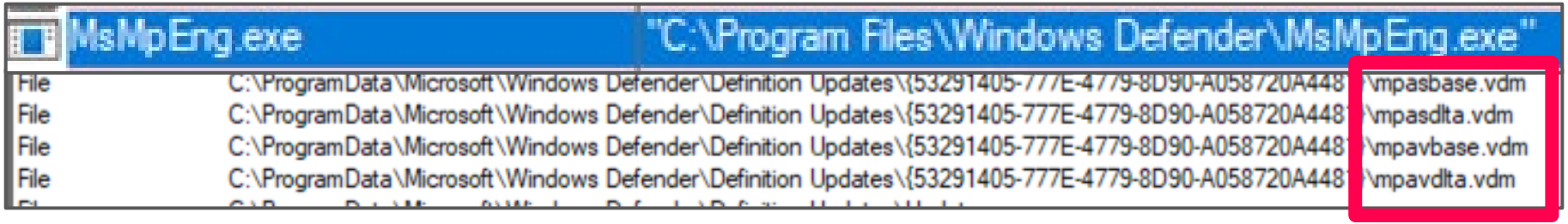
mpam-fe.exe Resources

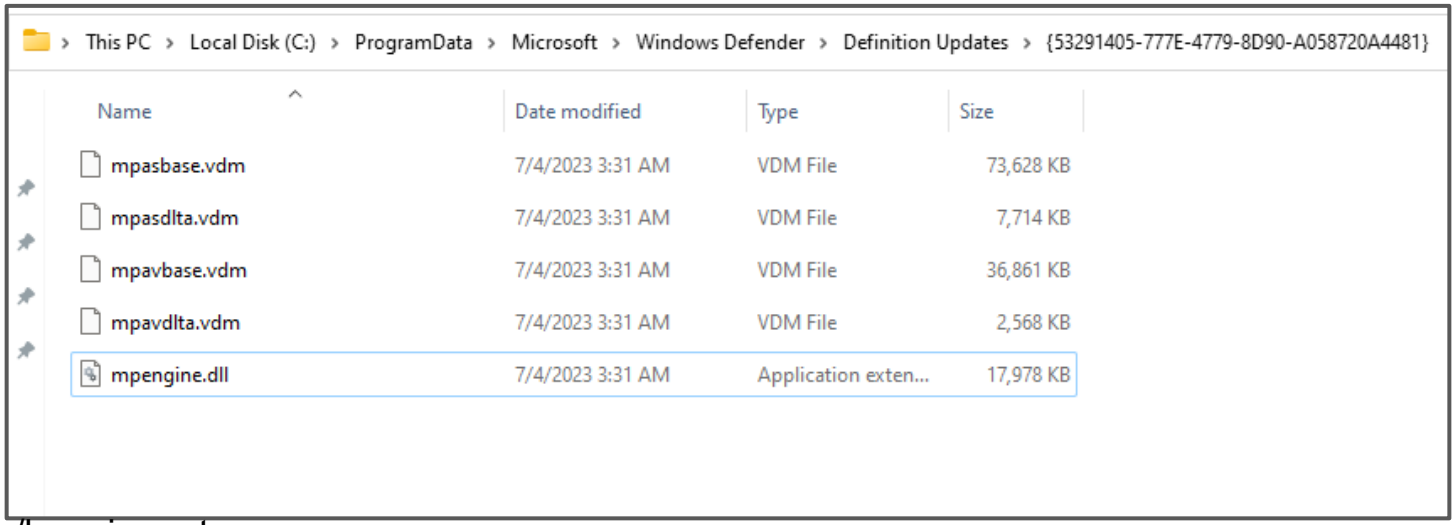


mpam-fe.exe Execution

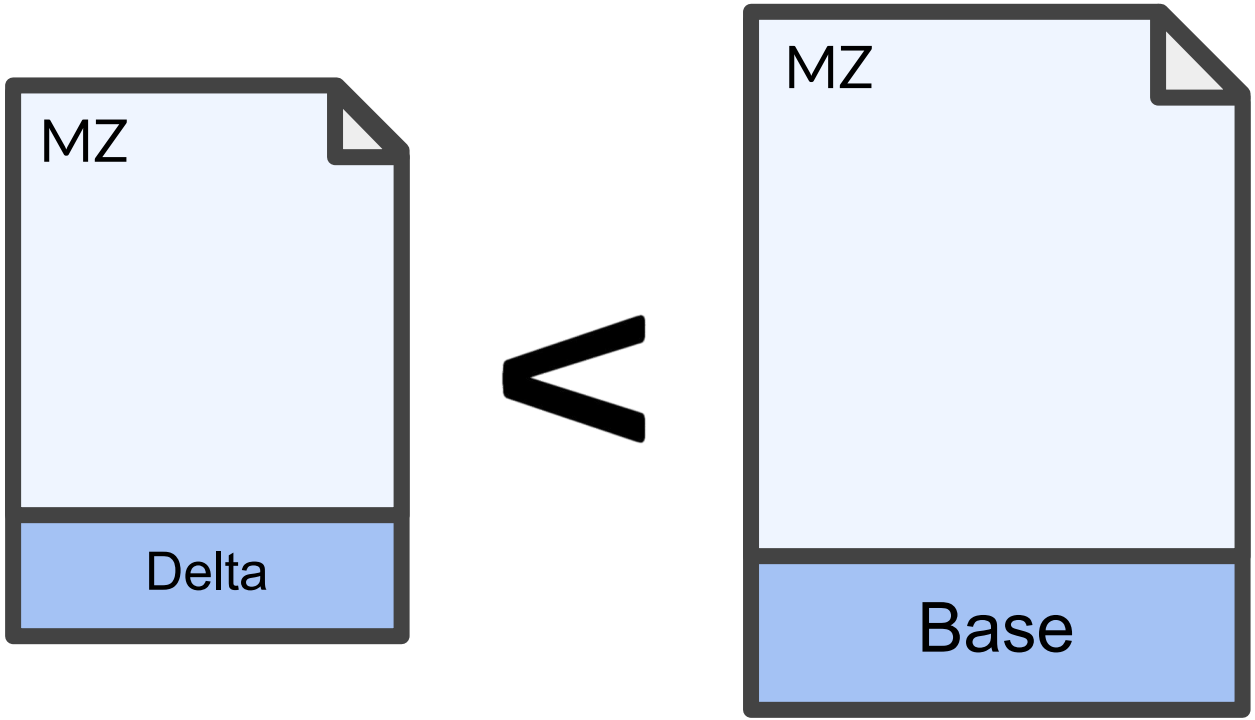


Database Files & mpengine.dll

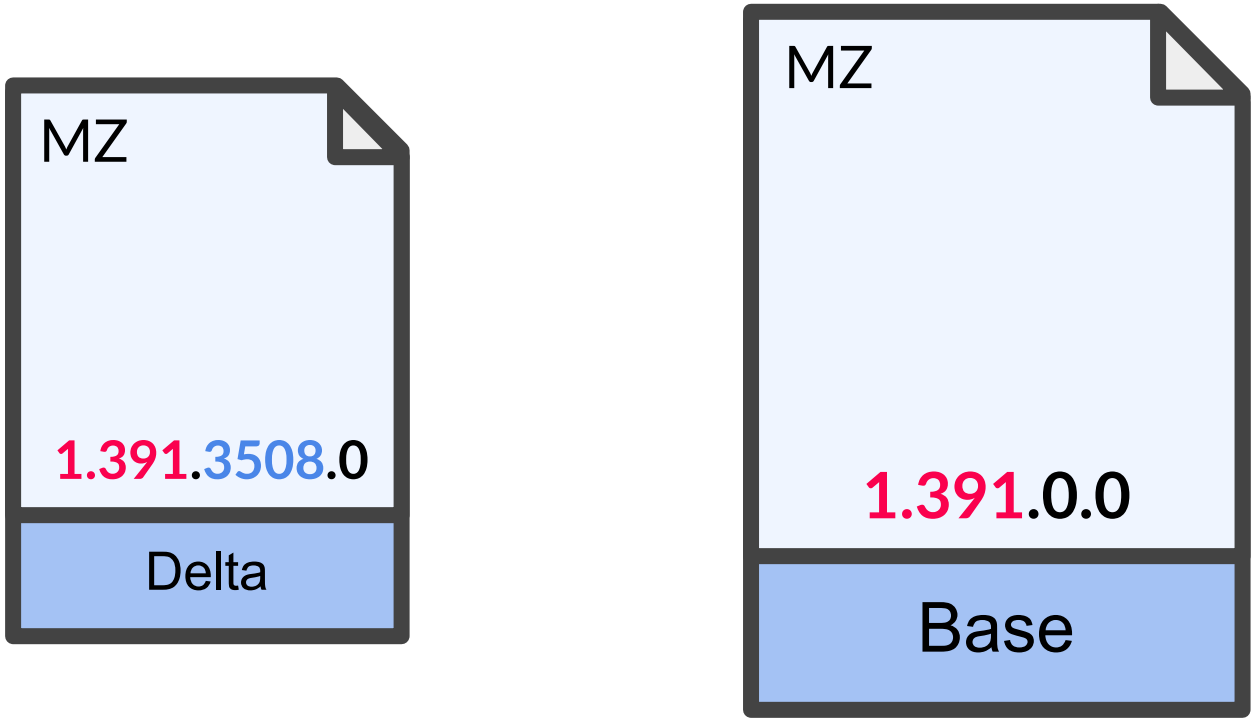




Base & Delta Files

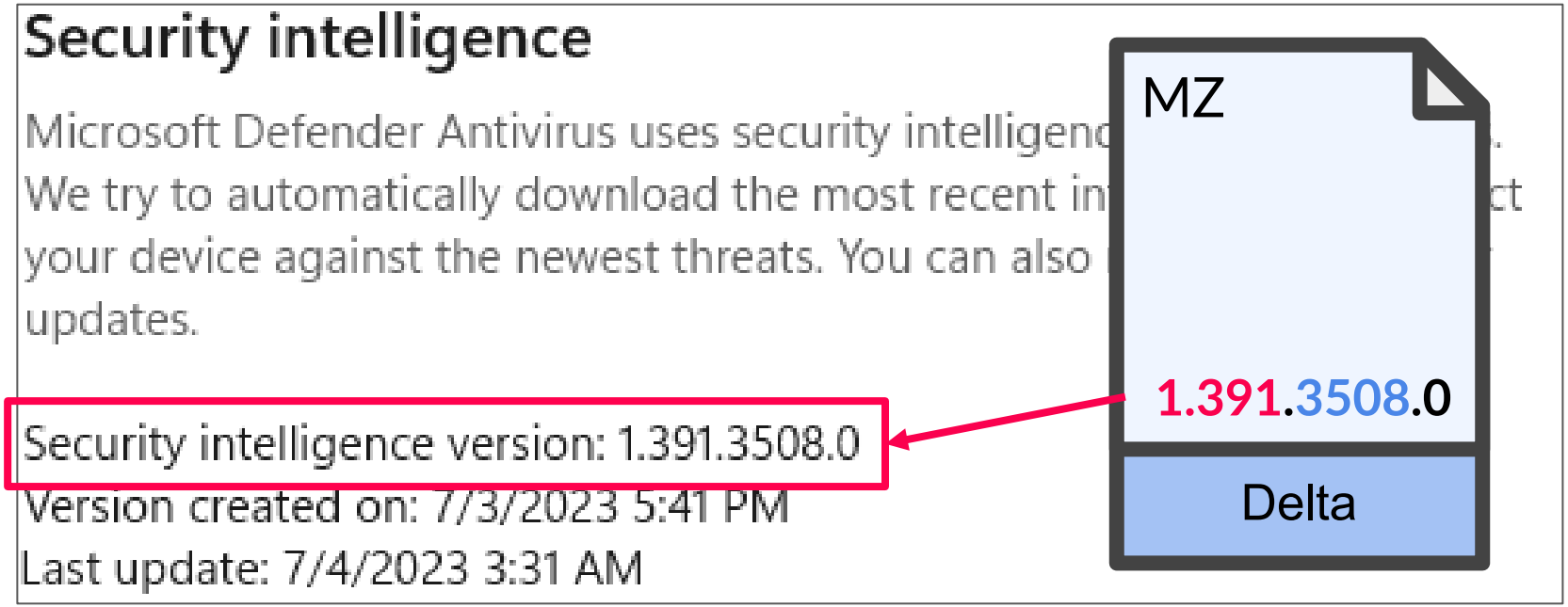


Base & Delta Versions

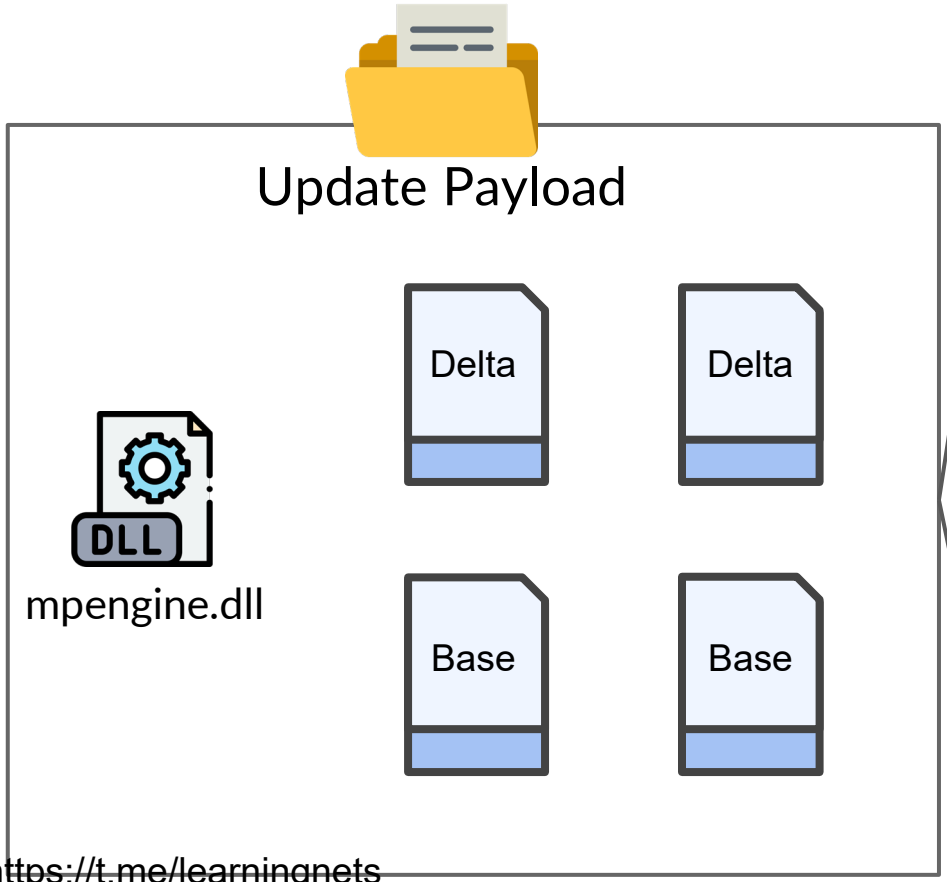


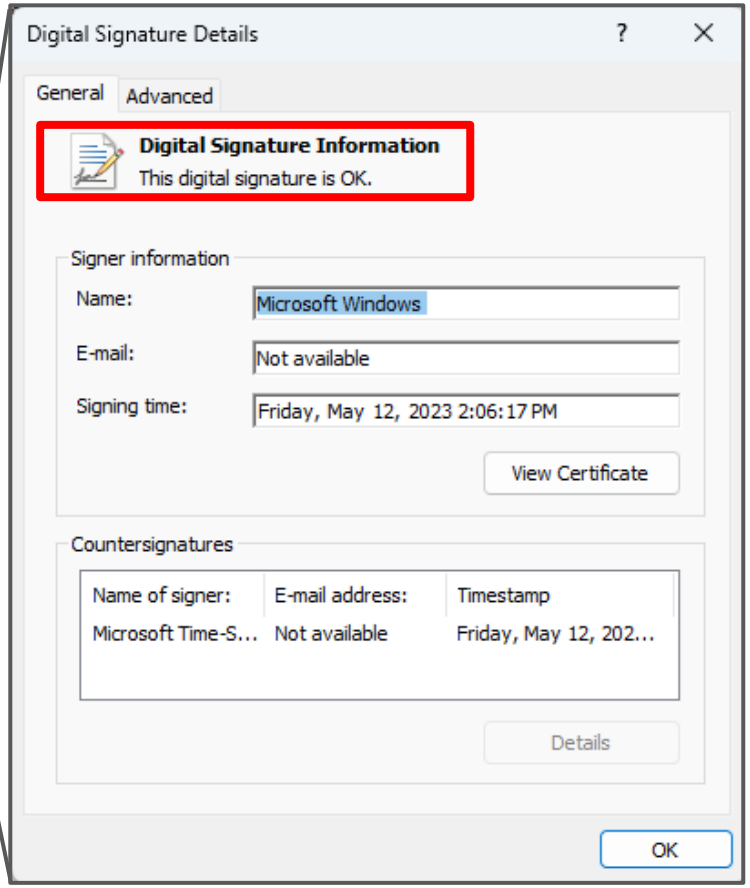
<major.minor.build.revision>

Security Intelligence Version

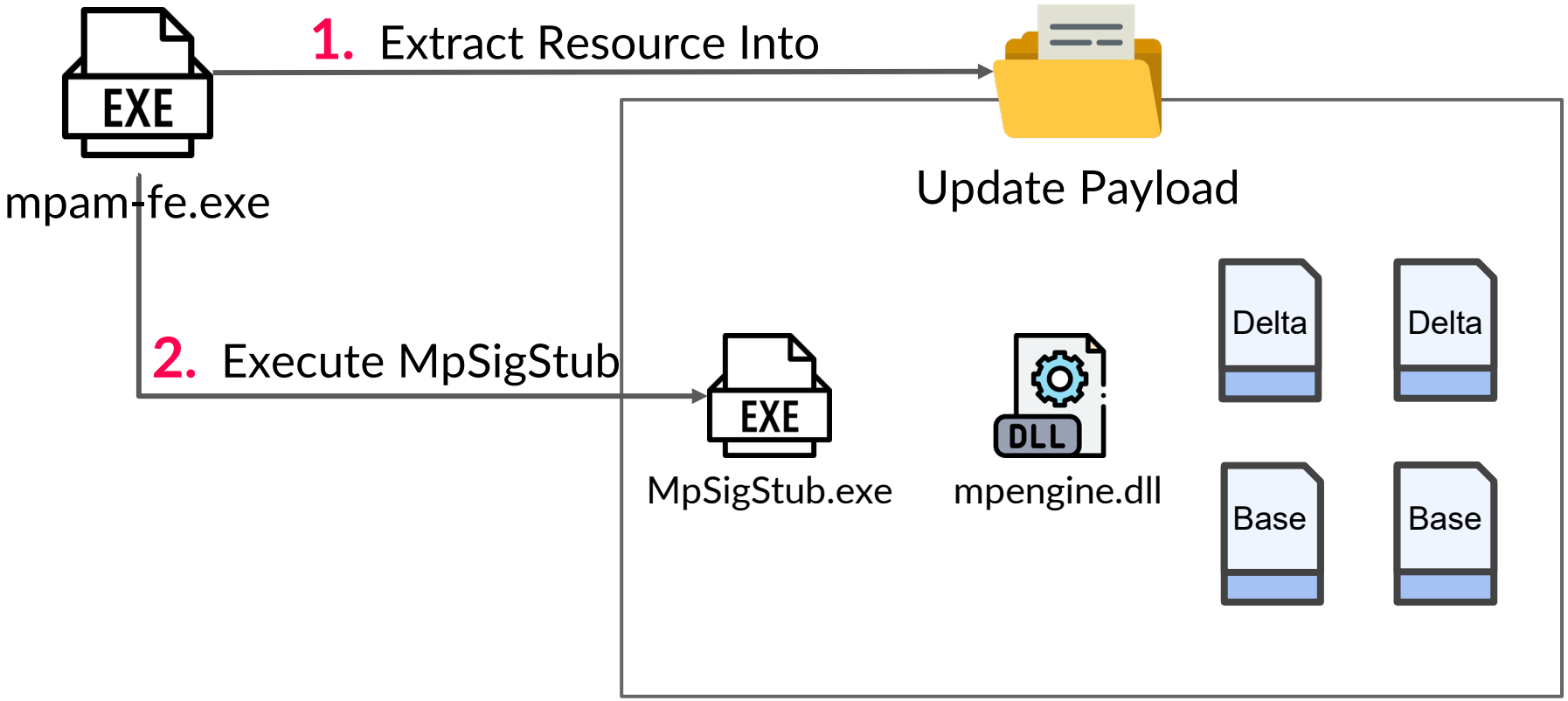


Digital Signature





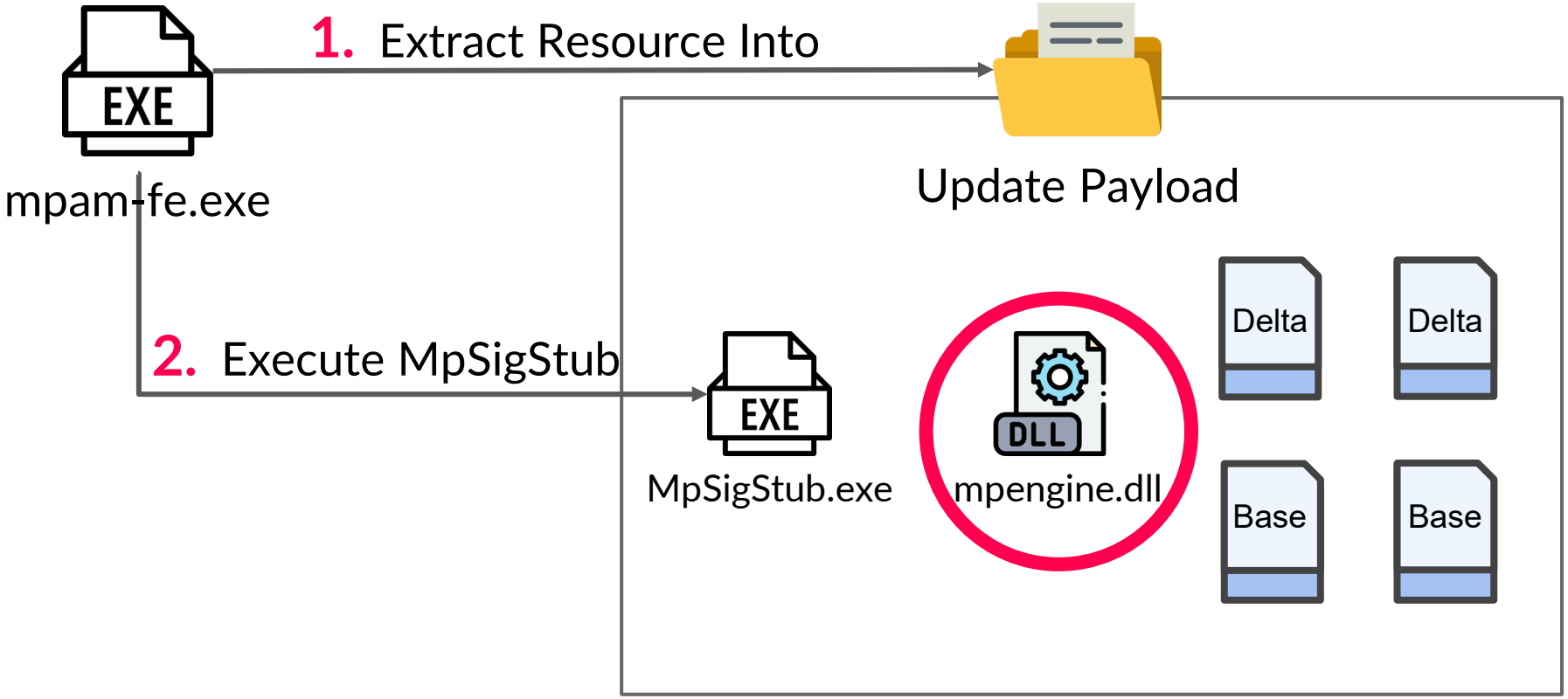
Update Process Summary



Playing Around With The Files

The First Clue That Something Is Fishy

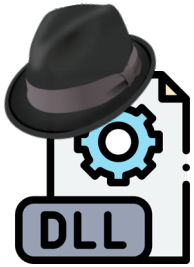
Pick a Target



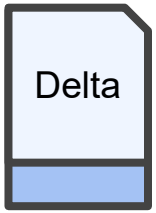
Trying To Modify MpEngine.dll

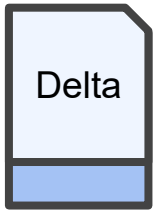
Update Payload

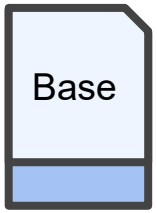
MpSigStub.exe

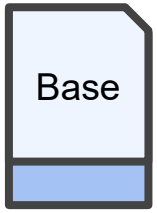


FAKE
mpengine.dll

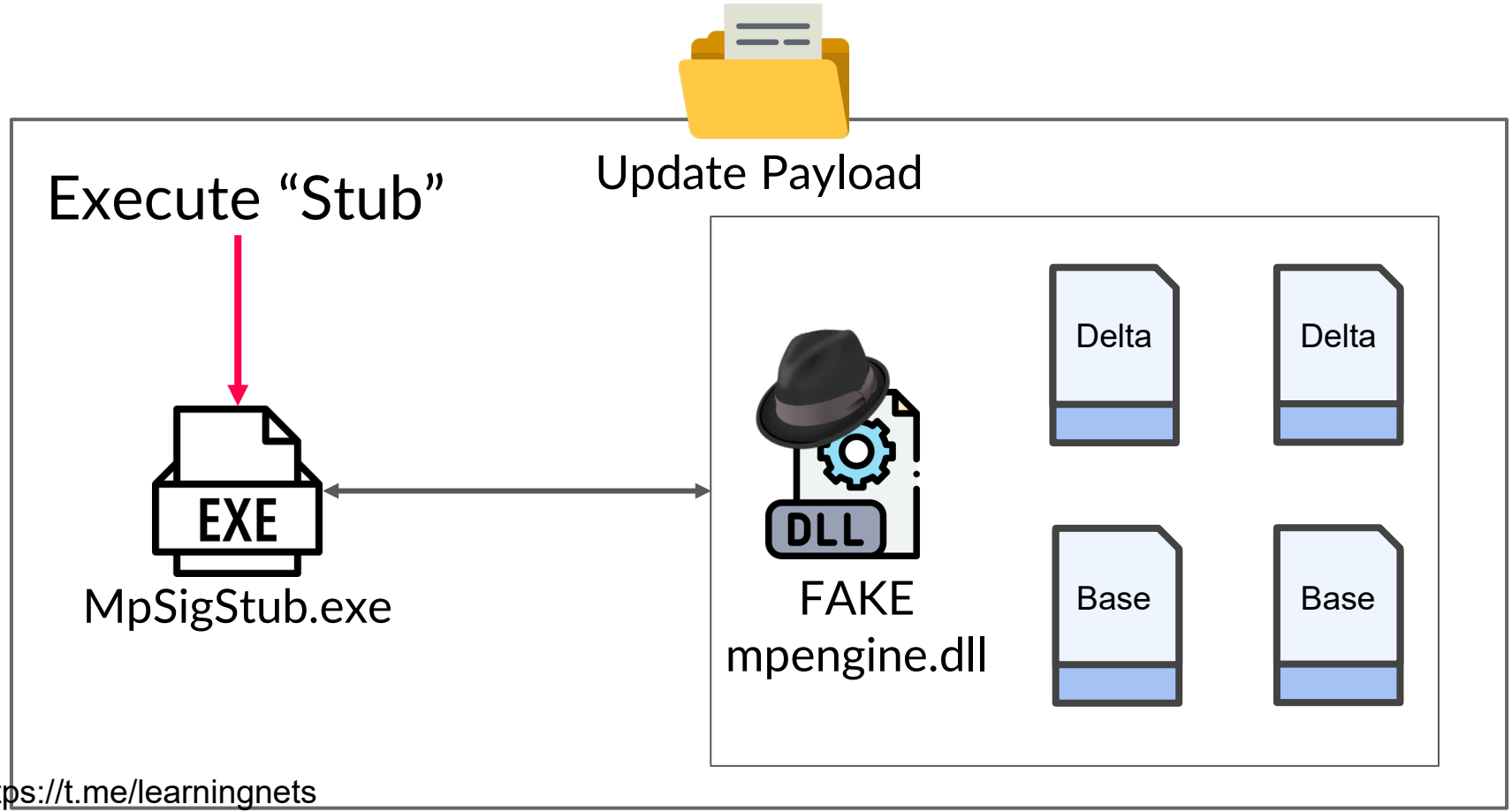






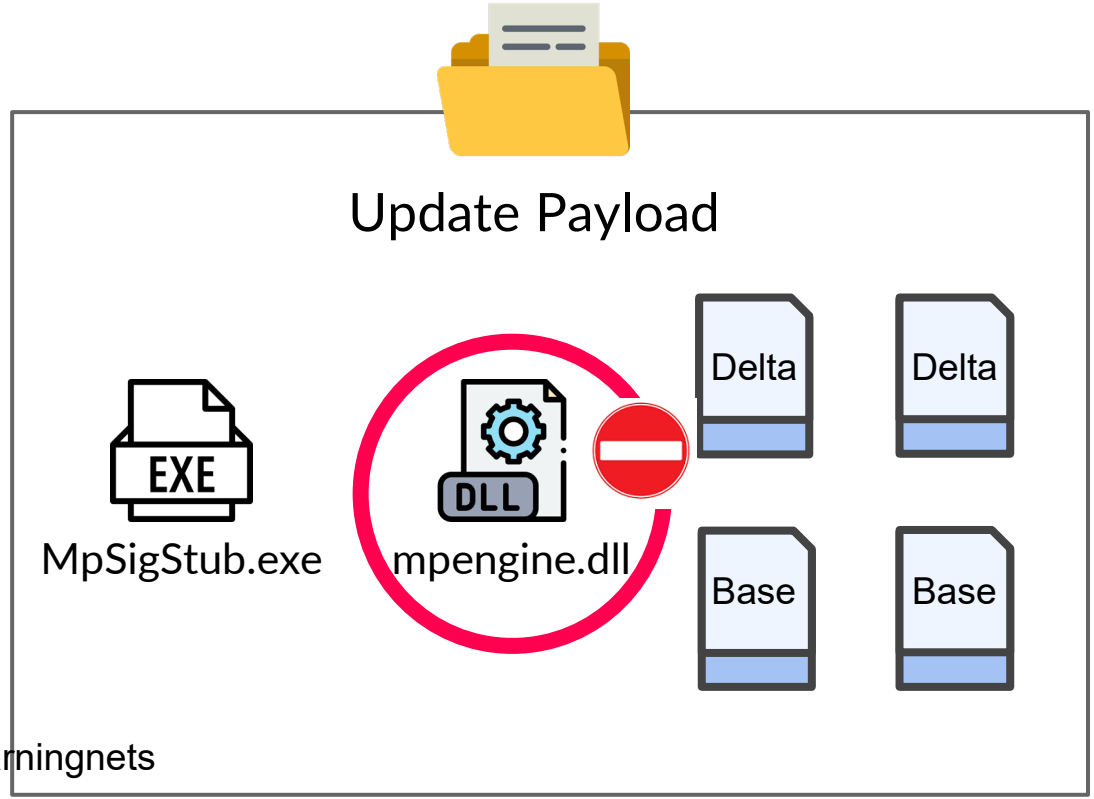


Trying To Modify MpEngine.dll

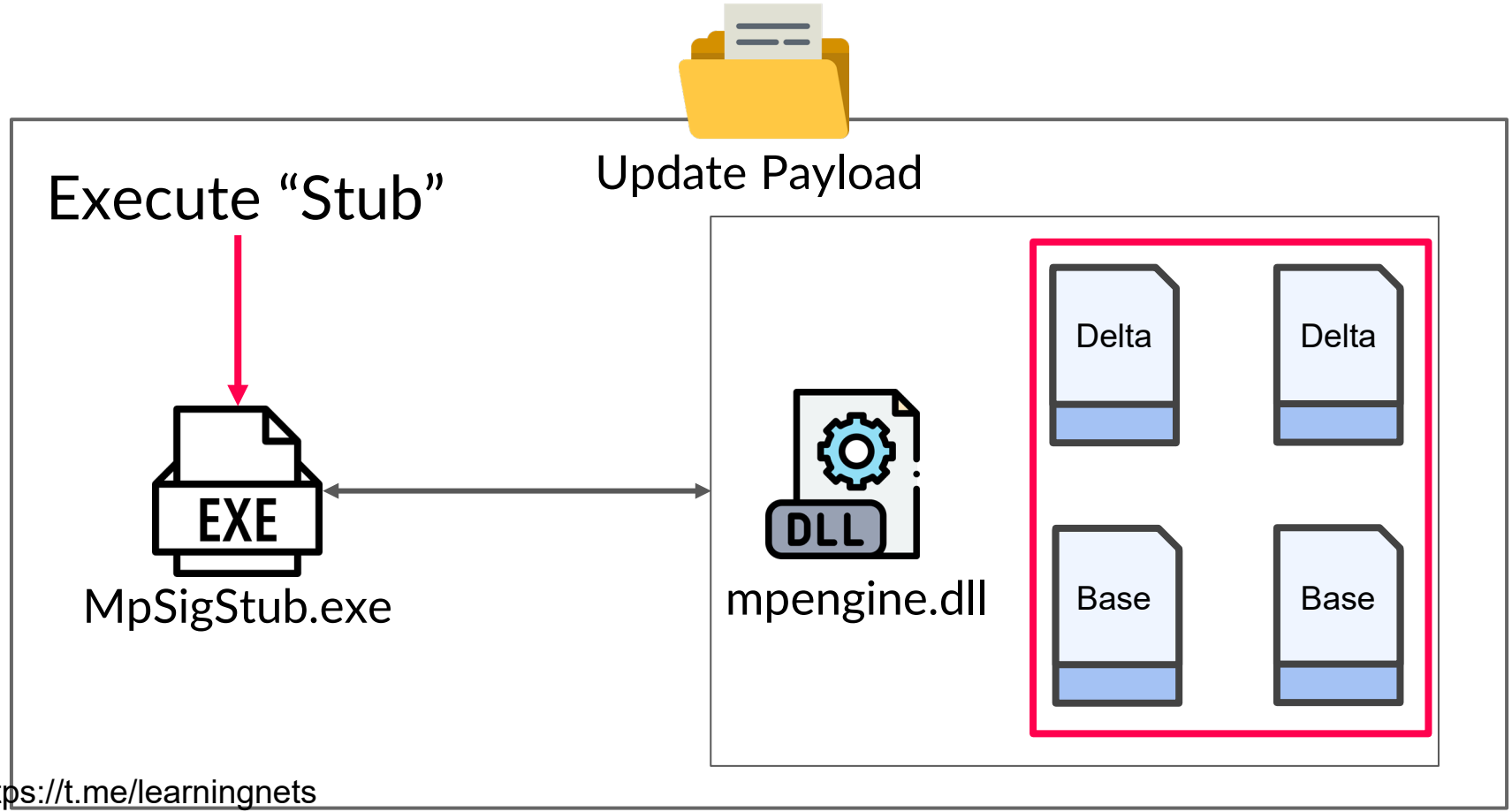


Trying To Modify MpEngine.dll

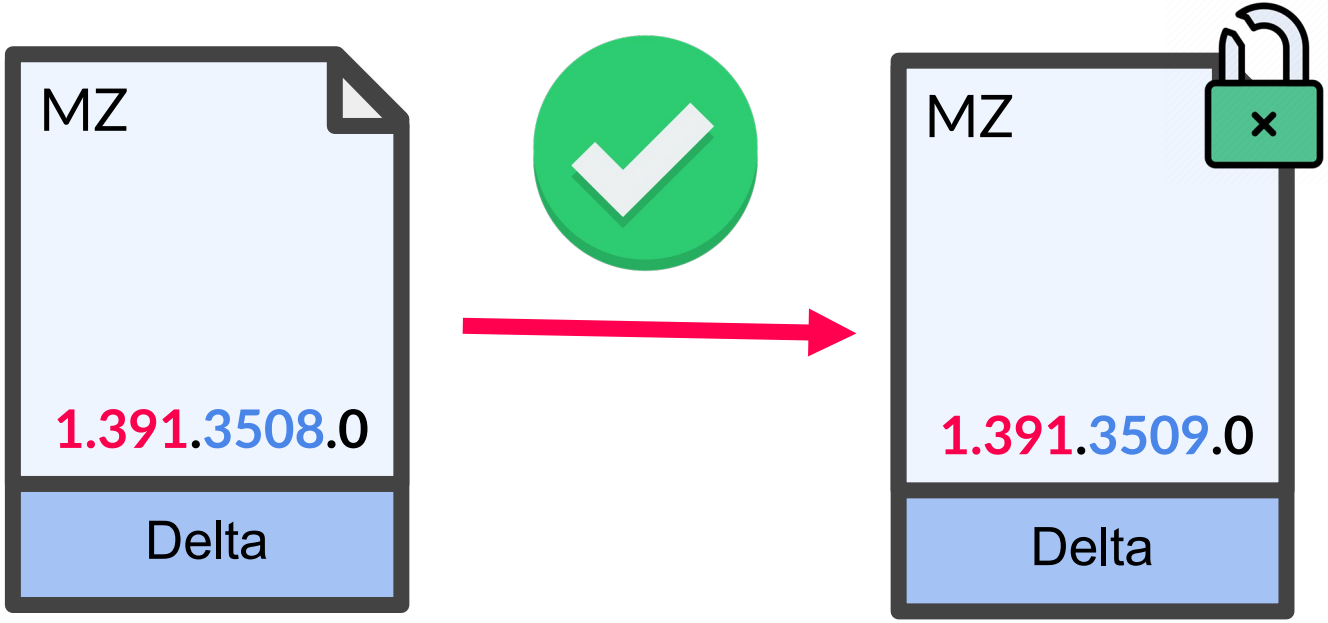
```
**********************************************************************
* This break indicates this binary is not signed correctly:
```



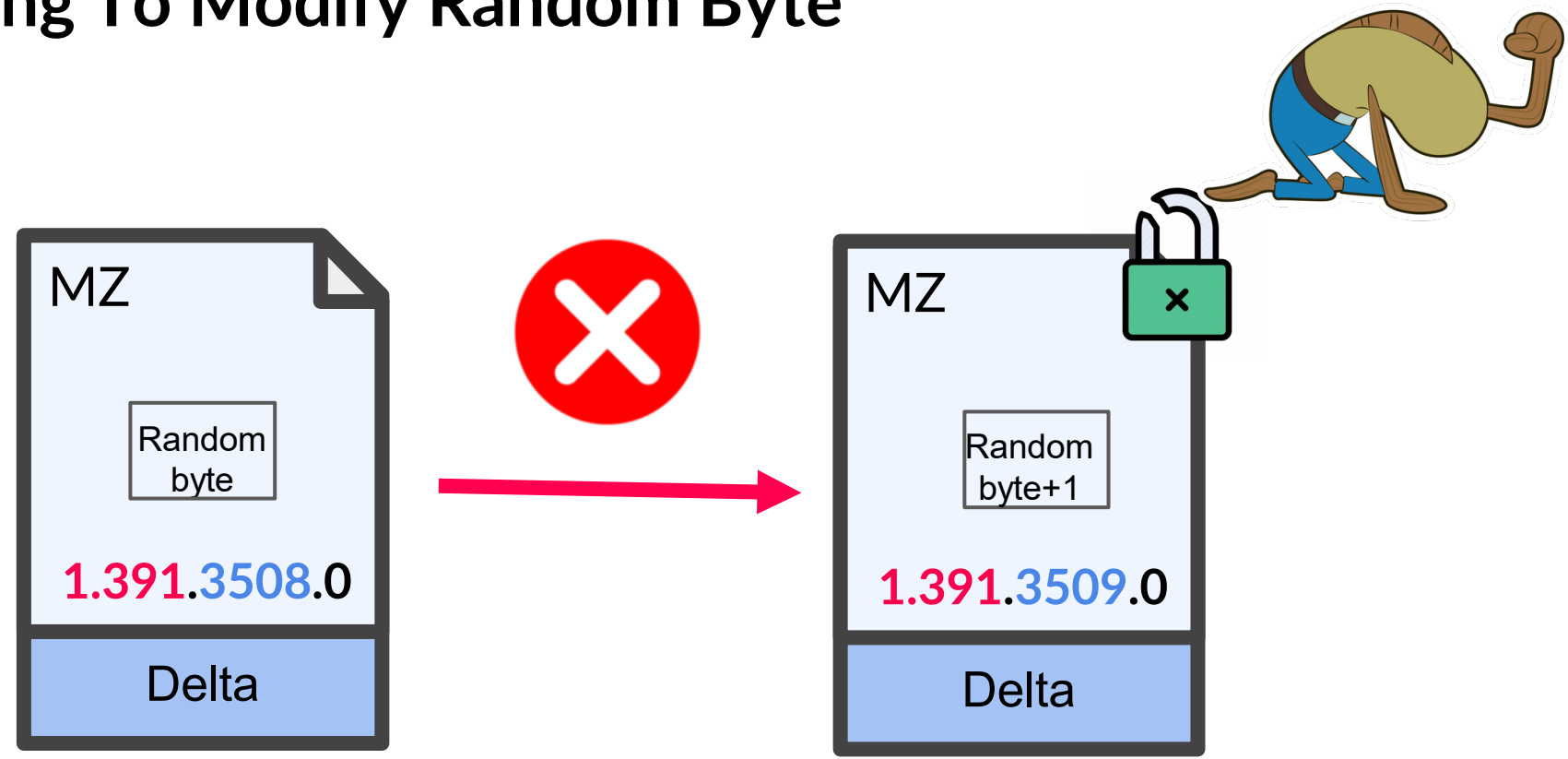
Trying To Modify the VDM files



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

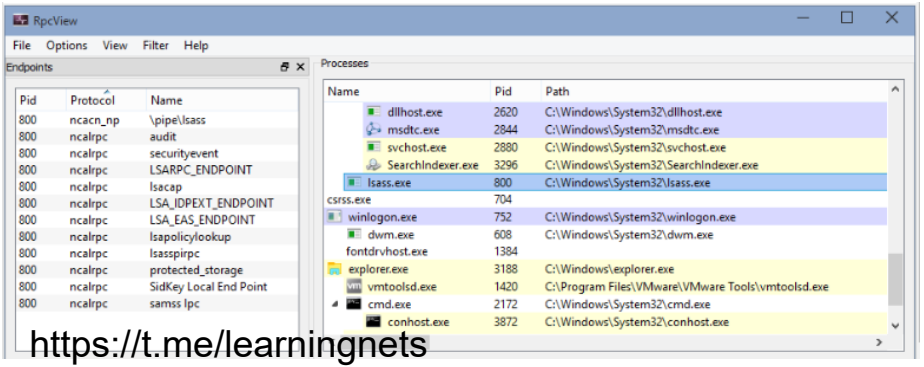
???

MsMpEng.exe

Microsoft Malware Protection Engine

Protected Process Light Process (PPL)

Black Box



MpSigStub to MsMpEng

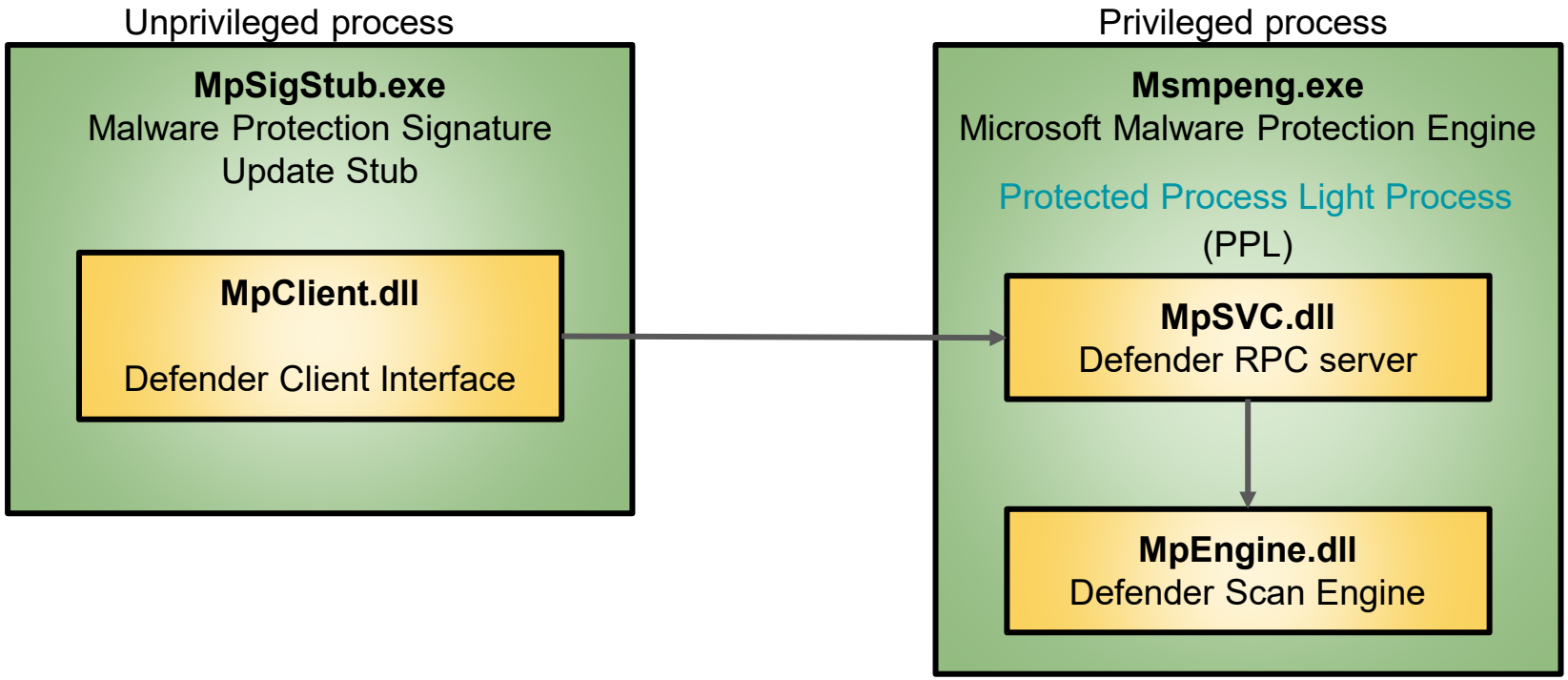
Manual reversing reveals RPC_GUID which belongs to mpsvc.dll
RPC func num:42

```
.rdata:00000075B8B8DA8          dq offset unk_75B8BA1D0
.rdata:00000075B8B8DB0 _rpc_guid db  60h ; `
.rdata:00000075B8B8DB1          db    0
.rdata:00000075B8B8DB2          db    0
.rdata:00000075B8B8DB3          db    0
.rdata:00000075B8B8DB4          dd 0C503F532h
.rdata:00000075B8B8DB8          dw 443Ah
.rdata:00000075B8B8DBA          dw 4C69h
.rdata:00000075B8B8DBC          db  83h ; ƒ
.rdata:00000075B8B8DBD          db    0
.rdata:00000075B8B8DBE          db 0CCh ; Ì
.rdata:00000075B8B8DBF          db 0D1h ; Ñ
.rdata:00000075B8B8DC0          db 0FBh ; û
.rdata:00000075B8B8DC1          db 0DBh ; Û
.rdata:00000075B8B8DC2          db  38h ; 8
.rdata:00000075B8B8DC3          db  39h ; 9
```

```
3736 RPC  c503f532-443a-4c69-8300-ccd1fbdb3839 (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



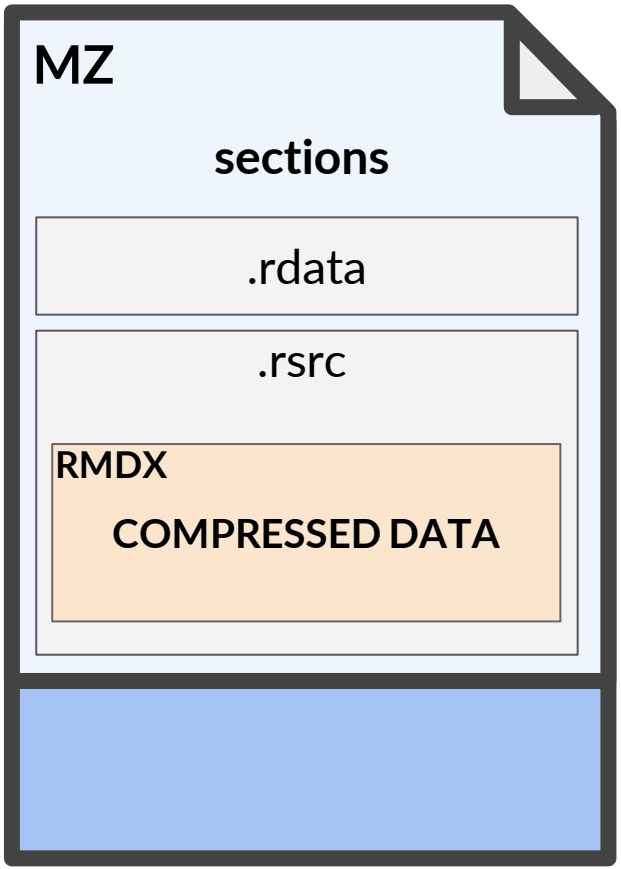
Execution Flow - mpsvc to mpengine

mpsvc::InitEngineContext
- mpengine::__rsignal
  - mpengine::StartMpEngine
    - mpengine::DispatchSignalHelper
      - mpengine::ksignalupper
        - mpengine::ModProbeInit
          - mpengine::modprobe_init_worker
            - mpengine::LoadDatabase
              - mpengine::ConsumeInputCompressed

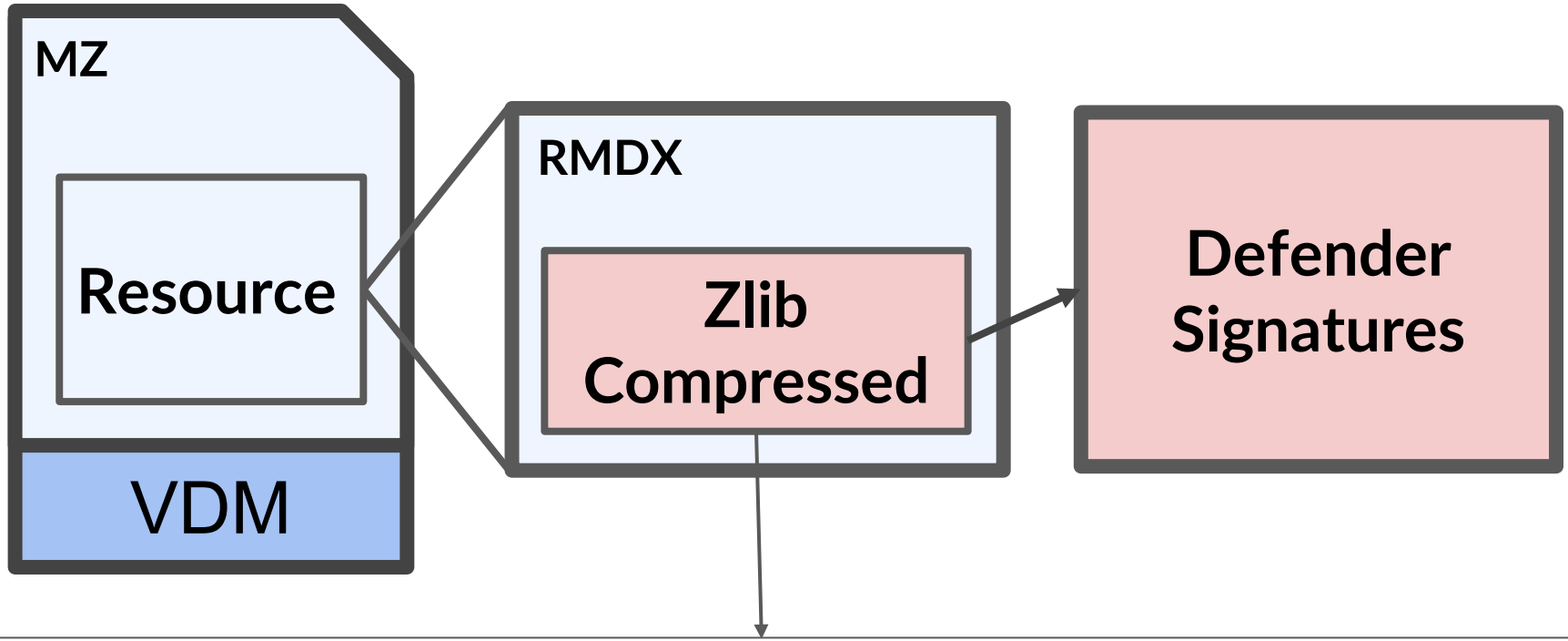
Called 4 times

VDM File Format

VDM File Format



VDM File Format




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

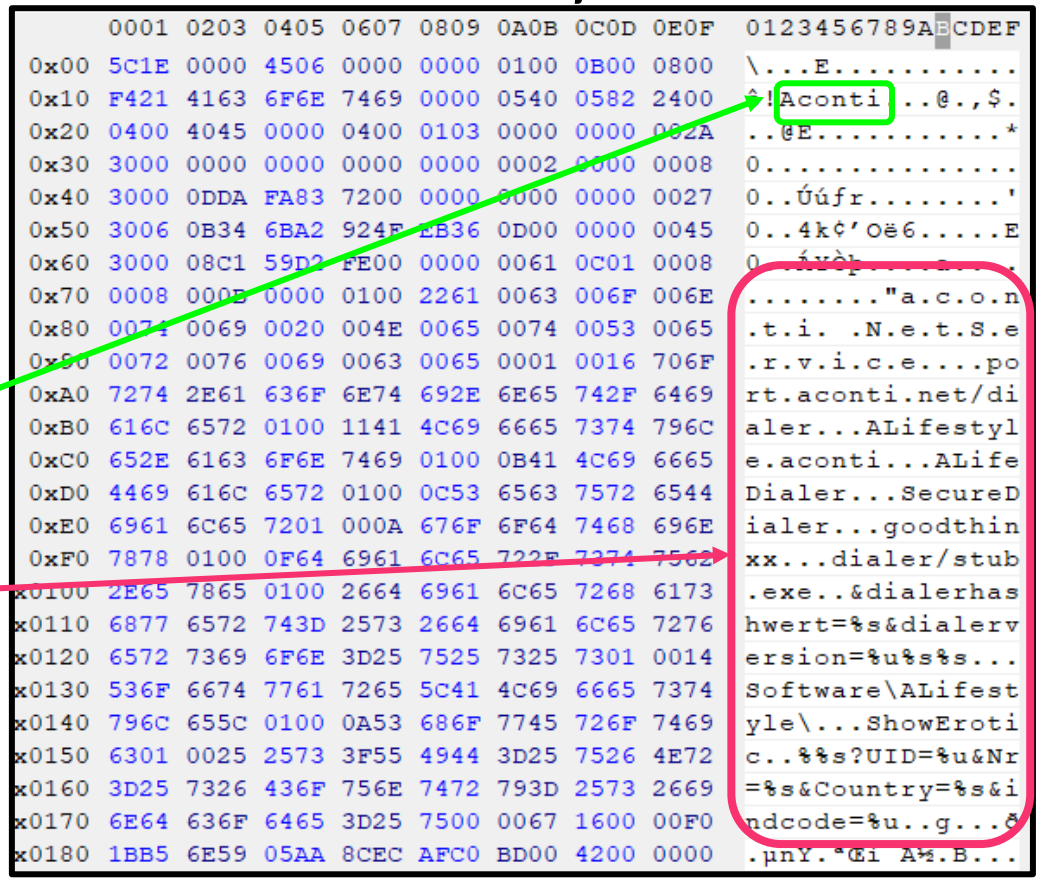
The Signatures Are Not Encrypted!

proprietary structure

Threat Name

Signature Bytes

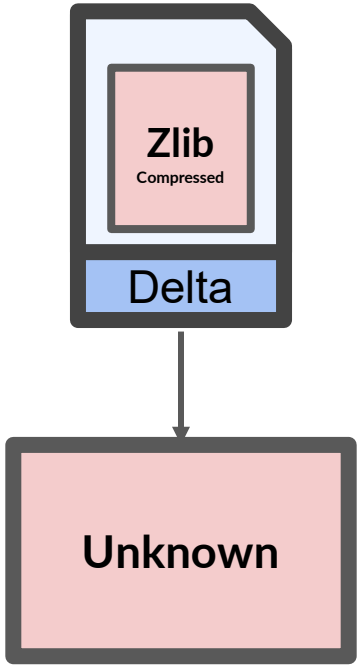
Base file

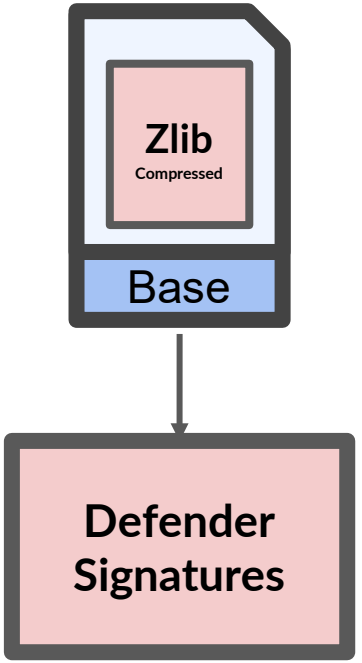


```
      0001 0203 0405 0607 0809 0A0B 0C0D 0E0F  0123456789ABCDEF
0x00  5C1E 0000 4506 0000 0000 0100 0B00 0800  \...E...........
0x10  F421 4163 6F6E 7469 0000 0540 0582 2400  ô!Aconti ..@.,$.
0x20  0400 4045 0000 0400 0103 0000 0000 002A  ..@E...........*
0x30  3000 0000 0000 0000 0000 0002 0000 0008  0...............
0x40  3000 0DDA FA83 7200 0000 0000 0000 0027  0..Úúƒr........'
0x50  3006 0B34 6BA2 924F EB36 0D00 0000 0045  0..4k¢'Oë6.....E
0x60  3000 08C1 59D2 FE00 0000 0061 0C01 0008  0..ÁYÒþ...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
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
0x100 2E65 7865 0100 2664 6961 6C65 7268 6173  .exe..&dialerhas
0x110 6877 6572 743D 2573 2664 6961 6C65 7276  hwert=%s&dialerv
0x120 6572 7369 6F6E 3D25 7525 7325 7301 0014  ersion=%u%s%s...
0x130 536F 6674 7761 7265 5C41 4C69 6665 7374  Software\ALifest
0x140 796C 655C 0100 0A53 686F 7745 726F 7469  yle\...ShowEroti
0x150 6301 0025 2573 3F55 4944 3D25 7526 4E72  c..%%s?UID=%u&Nr
0x160 3D25 7326 436F 756E 7472 793D 2573 2669  =%s&Country=%s&i
0x170 6E64 636F 6465 3D25 7500 0067 1600 00F0  ndcode=%u..g...ð
0x180 1BB5 6E59 05AA 8CEC AFC0 BD00 4200 0000  .µnY.ª Œì À½.B...
```

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	~$..€...‡... ...
0x40	9601	0000	B30B	0000	BF02	0000	CF06	0000	–...³...¿...Ï...
0x50	E70B	0000	738D	2208	EC1A	5C04	D001	8F0E	ç...s "ì.\.Ð. .
0x60	0100	5CFF	FF01	0000	00FF	FF06	8000	00FF	..\ÿÿ....ÿÿ.€..ÿ
0x70	FF0B	0001	00FF	FF10	8001	00FF	FF15	0002	ÿ....ÿÿ.€..ÿÿ...
0x80	00FF	FF1A	8002	00B7	B01F	0003	0001	00EA	.ÿÿ.€..·°......ê
0x90	91C9	DD30	0300	0400	34E6	3CF7	0280	9F65	'ÉÝ0....4æ<÷.€Ÿe
0xA0	C102	0600	0120	4AD3	C093	FFFF	6C7A	0300	Á.... JÓÀ"ÿÿlz..
0xB0	FFFF	71FA	0300	FFFF	767A	0400	FFFF	7BFA	ÿÿqú..ÿÿvz..ÿÿ{ú
0xC0	0400	FFFF	807A	0500	2DD8	85FA	0500	0100	..ÿÿ€z..-Ø…ú....
0xD0	4653	80B9	5206	0030	942C	5306	0016	00CF	FS€¹R..0”,S....Ï
0xE0	EB04	2401	D41A	2A89	2FCD	173C	A708	0001	ë.$.Ô.*‰/Í.<§...
0xF0	2058	3886	6F16	AD5E	6706	0016	0085	5F78	X8†o.-^g....…_x





Signature Structure

Signature Structure

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

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

Signature Types

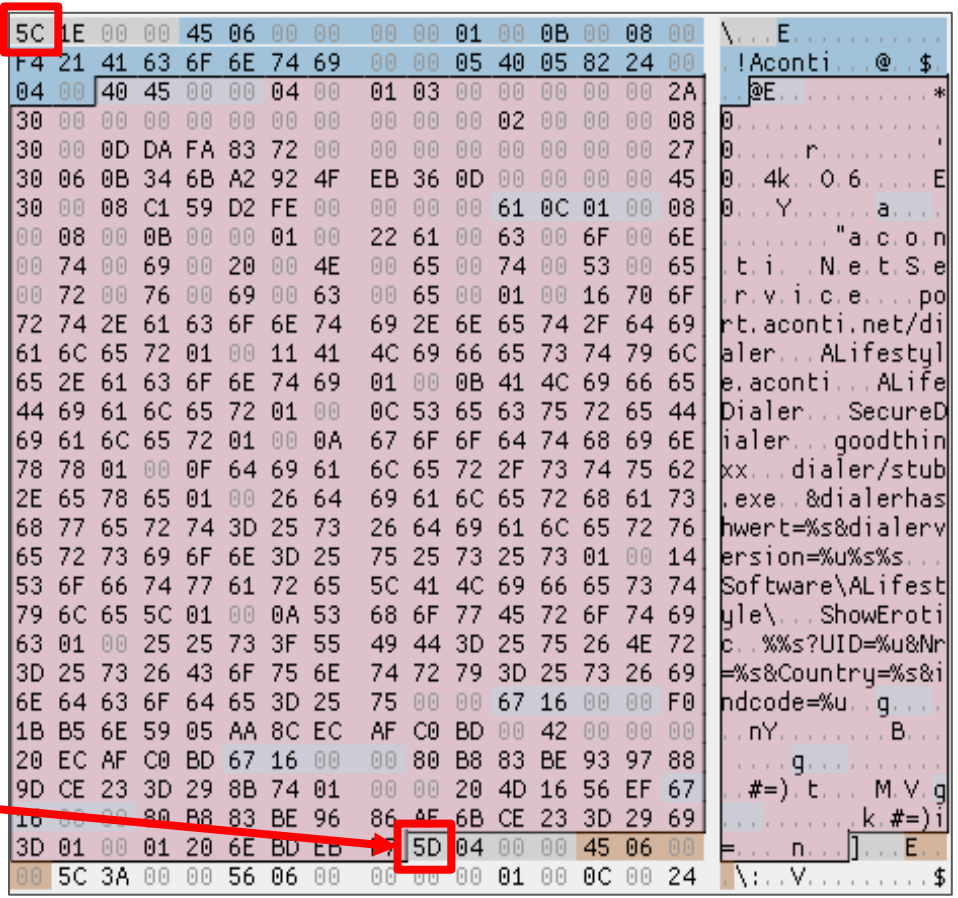
```
1: "SIGNATURE_TYPE_RESERVED",
2: "SIGNATURE_TYPE_VOLATILE_THREAT_INFO",
3: "SIGNATURE_TYPE_VOLATILE_THREAT_ID",
17: "SIGNATURE_TYPE_CKOLDREC",
32: "SIGNATURE_TYPE_KVIR32",
33: "SIGNATURE_TYPE_POLYVIR32",
39: "SIGNATURE_TYPE_NSCRIPT_NORMAL",
40: "SIGNATURE_TYPE_NSCRIPT_SP",
41: "SIGNATURE_TYPE_NSCRIPT_BRUTE",
44: "SIGNATURE_TYPE_NSCRIPT_CURE",
48: "SIGNATURE_TYPE_TITANFLT",
61: "SIGNATURE_TYPE_PEFILE_CURE",
62: "SIGNATURE_TYPE_MAC_CURE",
64: "SIGNATURE_TYPE_SIGTREE",
65: "SIGNATURE_TYPE_SIGTREE_EXT",
66: "SIGNATURE_TYPE_MACRO_PCODE",
67: "SIGNATURE_TYPE_MACRO_SOURCE",
68: "SIGNATURE_TYPE_BOOT",
73: "SIGNATURE_TYPE_CLEANSCRIPT",
74: "SIGNATURE_TYPE_TARGET_SCRIPT",
80: "SIGNATURE_TYPE_CKSIMPLEREC",
81: "SIGNATURE_TYPE_PATTMATCH",
83: "SIGNATURE_TYPE_RPFROUTINE",
85: "SIGNATURE_TYPE_NID",
86: "SIGNATURE_TYPE_GENSFX",
87: "SIGNATURE_TYPE_UNPLIB",
88: "SIGNATURE_TYPE_DEFAULTS",
91: "SIGNATURE_TYPE_DBVAR",
0x5C: "SIGNATURE_TYPE_THREAT_BEGIN",
0x5D: "SIGNATURE_TYPE_THREAT_END",
94: "SIGNATURE_TYPE_FILENAME",
95: "SIGNATURE_TYPE_FILEPATH",
96: "SIGNATURE_TYPE_FOLDERNAME",
97: "SIGNATURE_TYPE_PEHSTR",
98: "SIGNATURE_TYPE_LOCALHASH",
99: "SIGNATURE_TYPE_REGKEY",
100: "SIGNATURE_TYPE_HOSTSENTRY",
103: "SIGNATURE_TYPE_STATIC",
105: "SIGNATURE_TYPE_LATENT_THREAT",
106: "SIGNATURE_TYPE_REMOVAL_POLICY",
107: "SIGNATURE_TYPE_WVT_EXCEPTION",
108: "SIGNATURE_TYPE_REVOKED_CERTIFICATE",
112: "SIGNATURE_TYPE_TRUSTED_PUBLISHER",
113: "SIGNATURE_TYPE_ASEP_FILEPATH",
115: "SIGNATURE_TYPE_DELTA_BLOB",
116: "SIGNATURE_TYPE_DELTA_BLOB_RECINFO",
117: "SIGNATURE_TYPE_ASEP_FOLDERNAME",
119: "SIGNATURE_TYPE_PATTMATCH_V2",
120: "SIGNATURE_TYPE_PEHSTR_EXT",
121: "SIGNATURE_TYPE_VDLL_X86",
122: "SIGNATURE_TYPE_VERSIONCHECK",
123: "SIGNATURE_TYPE_SAMPLE_REQUEST",
124: "SIGNATURE_TYPE_VDLL_X64",
126: "SIGNATURE_TYPE_SNID",
127: "SIGNATURE_TYPE_FOP",
128: "SIGNATURE_TYPE_KCRCE",
131: "SIGNATURE_TYPE_VFILE",
132: "SIGNATURE_TYPE_SIGFLAGS",
133: "SIGNATURE_TYPE_PEHSTR_EXT2",
134: "SIGNATURE_TYPE_PEMAIN_LOCATOR",
135: "SIGNATURE_TYPE_PESTATIC",
136: "SIGNATURE_TYPE_UFSP_DISABLE",
137: "SIGNATURE_TYPE_FOPEX",
138: "SIGNATURE_TYPE_PEPCODE",
139: "SIGNATURE_TYPE_IL_PATTERN",
140: "SIGNATURE_TYPE_ELFHSTR_EXT",
141: "SIGNATURE_TYPE_MACHOHSTR_EXT",
142: "SIGNATURE_TYPE_DOSHSTR_EXT",
143: "SIGNATURE_TYPE_MACROHSTR_EXT",
144: "SIGNATURE_TYPE_TARGET_SCRIPT_PCODE",
145: "SIGNATURE_TYPE_VDLL_IA64",
149: "SIGNATURE_TYPE_PEBMPAT",
150: "SIGNATURE_TYPE_AAGGREGATOR",
151: "SIGNATURE_TYPE_SAMPLE_REQUEST_BY_NAME",
152: "SIGNATURE_TYPE_REMOVAL_POLICY_BY_NAME",
153: "SIGNATURE_TYPE_TUNNEL_X86",
154: "SIGNATURE_TYPE_TUNNEL_X64",
155: "SIGNATURE_TYPE_TUNNEL_IA64",
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",
169: "SIGNATURE_TYPE_NDAT",
170: "SIGNATURE_TYPE_FASTPATH_DATA",
171: "SIGNATURE_TYPE_FASTPATH_SDN",
172: "SIGNATURE_TYPE_DATABASE_CERT",
173: "SIGNATURE_TYPE_SOURCE_INFO",
174: "SIGNATURE_TYPE_HIDDEN_FILE",
175: "SIGNATURE_TYPE_COMMON_CODE",
176: "SIGNATURE_TYPE_VREG",
177: "SIGNATURE_TYPE_NISBLOB",
178: "SIGNATURE_TYPE_VFILEEX",
179: "SIGNATURE_TYPE_SIGTREE_BM",
180: "SIGNATURE_TYPE_VBFOP",
181: "SIGNATURE_TYPE_VDLL_META",
182: "SIGNATURE_TYPE_TUNNEL_ARM",
183: "SIGNATURE_TYPE_THREAD_ARM",
184: "SIGNATURE_TYPE_PCODEVALIDATOR",
186: "SIGNATURE_TYPE_MSILFOP",
187: "SIGNATURE_TYPE_KPAT",
188: "SIGNATURE_TYPE_KPATEX",
189: "SIGNATURE_TYPE_LUASTANDALONE",
190: "SIGNATURE_TYPE_DEXHSTR_EXT",
190: "SIGNATURE_TYPE_DEXHSTR_EXT",
191: "SIGNATURE_TYPE_JAVAHSTR_EXT",
192: "SIGNATURE_TYPE_MAGICCODE",
193: "SIGNATURE_TYPE_CLEANSTORE_RULE",
194: "SIGNATURE_TYPE_VDLL_CHECKSUM",
195: "SIGNATURE_TYPE_THREAT_UPDATE_STATUS",
196: "SIGNATURE_TYPE_VDLL_MSIL",
197: "SIGNATURE_TYPE_ARHSTR_EXT",
198: "SIGNATURE_TYPE_MSILFOPEX",
199: "SIGNATURE_TYPE_VBFOPEX",
200: "SIGNATURE_TYPE_FOP64",
201: "SIGNATURE_TYPE_FOPEX64",
202: "SIGNATURE_TYPE_JSINIT",
203: "SIGNATURE_TYPE_PESTATICEX",
204: "SIGNATURE_TYPE_KCRCEX",
205: "SIGNATURE_TYPE_FTRIE_POS",
206: "SIGNATURE_TYPE_NID64",
207: "SIGNATURE_TYPE_MACRO_PCODE64",
208: "SIGNATURE_TYPE_BRUTE",
209: "SIGNATURE_TYPE_SWFHSTR_EXT",
210: "SIGNATURE_TYPE_REWSIGS",
211: "SIGNATURE_TYPE_AUTOITHSTR_EXT",
212: "SIGNATURE_TYPE_INNOHSTR_EXT",
213: "SIGNATURE_TYPE_ROOTCERTSTORE",
214: "SIGNATURE_TYPE_EXPLICITRESOURCE",
215: "SIGNATURE_TYPE_CMDHSTR_EXT",
216: "SIGNATURE_TYPE_FASTPATH_TDN",
217: "SIGNATURE_TYPE_EXPLICITRESOURCEHASH",
218: "SIGNATURE_TYPE_FASTPATH_SDN_EX",
219: "SIGNATURE_TYPE_BLOOM_FILTER",
220: "SIGNATURE_TYPE_RESEARCH_TAG",
222: "SIGNATURE_TYPE_ENVELOPE",
223: "SIGNATURE_TYPE_REMOVAL_POLICY64",
224: "SIGNATURE_TYPE_REMOVAL_POLICY64_BY_NAME",
225: "SIGNATURE_TYPE_VDLL_META_X64",
226: "SIGNATURE_TYPE_VDLL_META_ARM",
227: "SIGNATURE_TYPE_VDLL_META_MSIL",
228: "SIGNATURE_TYPE_MDBHSTR_EXT",
229: "SIGNATURE_TYPE_SNIDEX",
230: "SIGNATURE_TYPE_SNIDEX2",
231: "SIGNATURE_TYPE_AAGGREGATOREX",
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

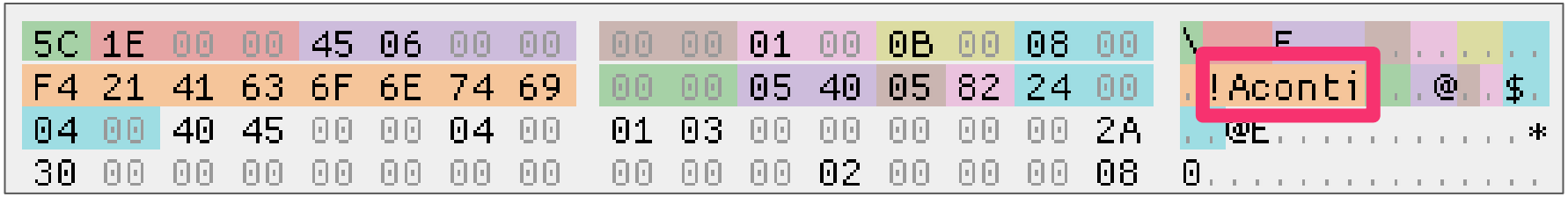
Evaluation

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

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

Threat Begin Signature

```
struct ThreatBegin {
    SignatureHeader header;
    u32 Id;
    u16 Unknown1;
    u16 Counter;
    u16 Category;
    u16 ThreatNameLength;
    u8 Name[ThreatNameLength];
    u16 Unknown2;
    u16 Resources[Counter];
    u8 Sevirity;
    u8 Action;
    u8 Unknown3[4];
};
```

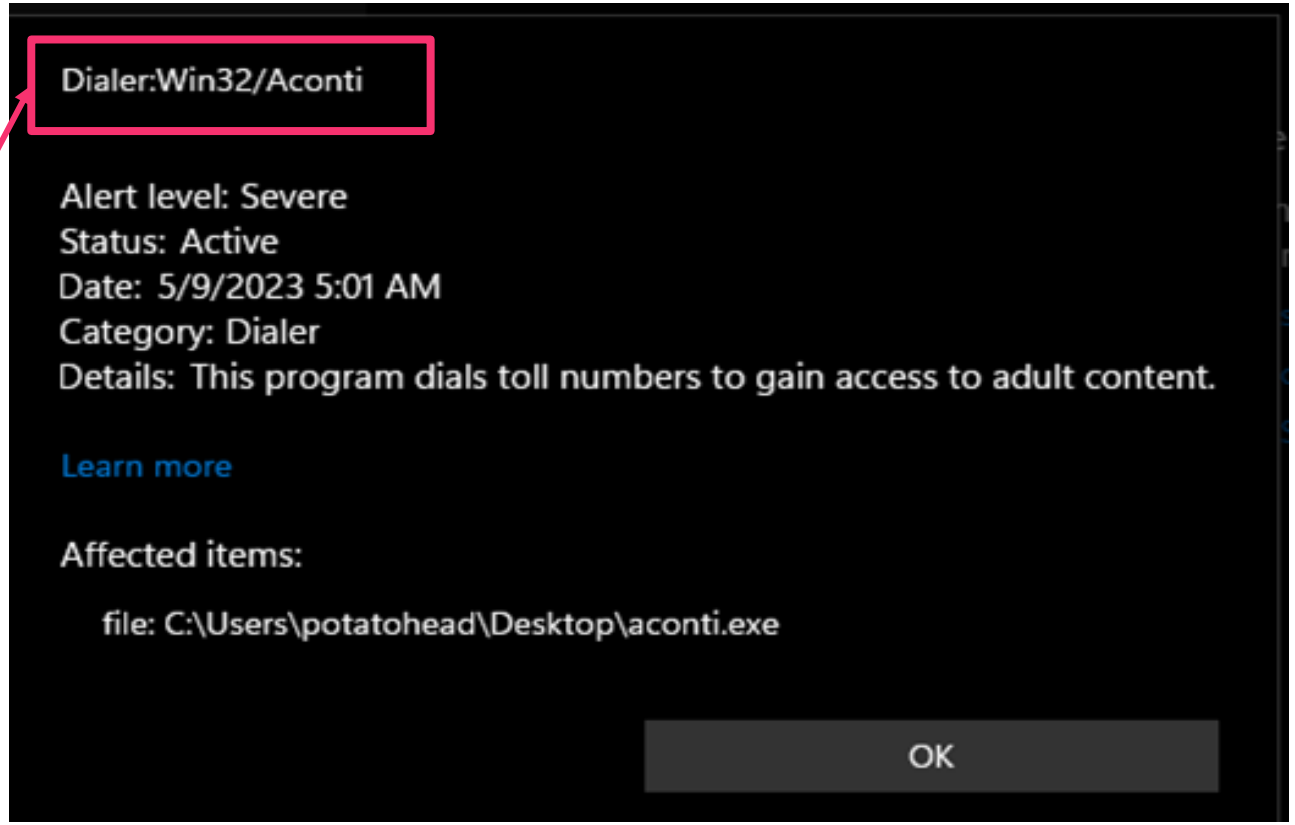


Smart modification on Conti Signature

```
#include <stdlib.h>

wchar_t* a1 = L"aconti NetService";
char* a2 = "port.aconti.net/dialer";
char* a3 = "ALifestyle.aconti";
char* a4 = "ALifeDialer";
char* a5 = "SecureDialer";
char* a6 = "goodthinxx";
char* a7 = "dialer/stub.exe";
char* a8 = "dialerhashwert=%s&dialerversion=%u%s%s";
char* a9 = "Software\\ALifestyle\\";
char* a10 = "ShowErotic";
char* a11 = "%s?UID=%u&Nr=%s&Country=%s&indcode=%u";


int main()
{

    return 0;
}
```

```
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...ð
```

Smart modification on Conti Signature



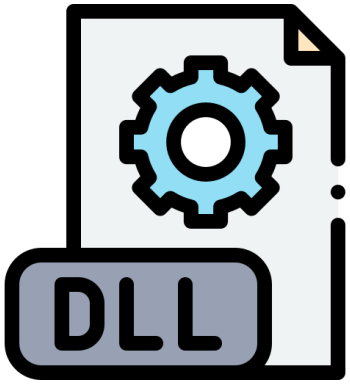
Modify Conti Threat Name – Update failed

```
      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  ô!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..4k¢'Oë6.....E
0x60  3000 08C1 59D2 FE00 0000 0061 0C01 0008  0..ÁYÒþ....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
```

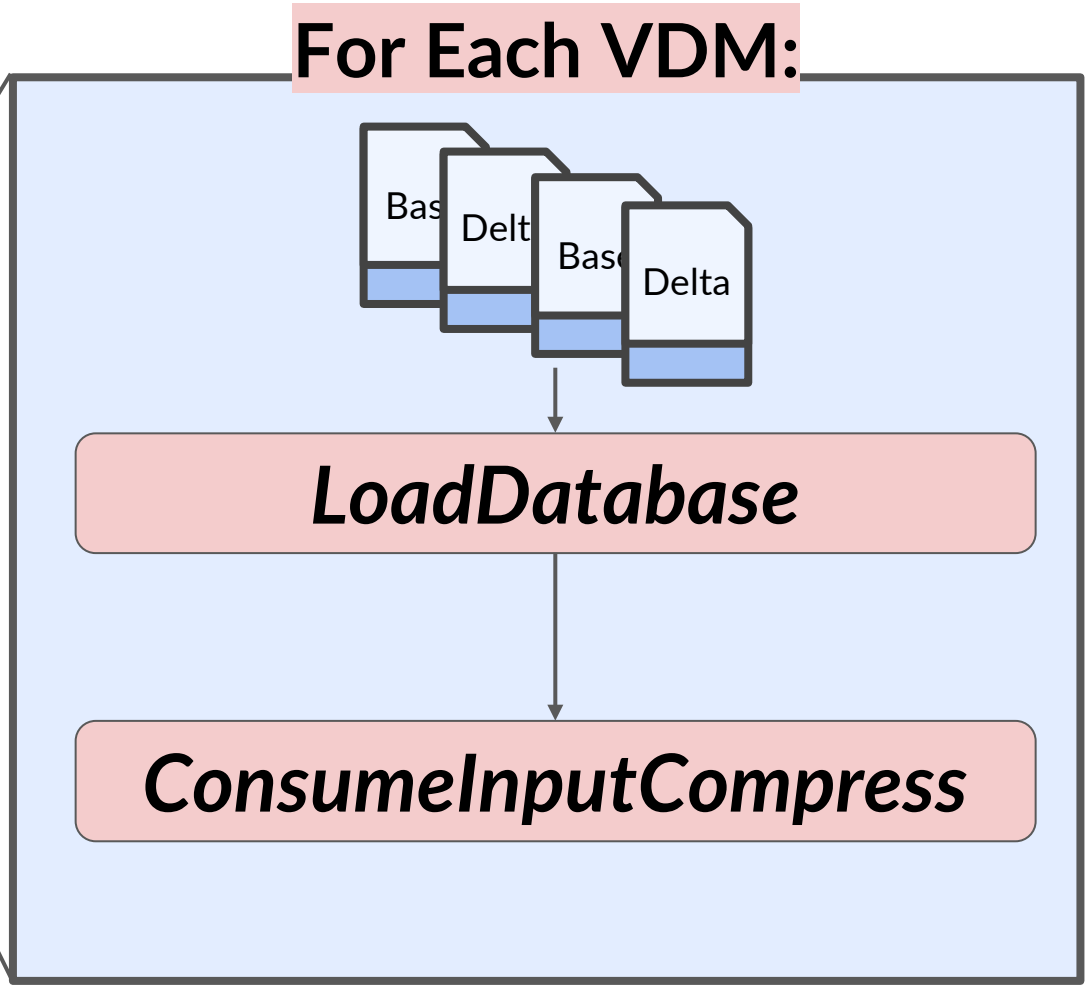
```
========================================= Upd

 Product name: Microsoft Windows Defende
 Package files:
     Directory: C:\Defs
  mpasbase.vdm: b96f6f2cea8b43df4a154dda7d3b3997010b9b01d21af7524db677d07440816e  1.383.0.0
  mpasdlta.vdm: 8bc31ebf7357bdb5a057924eb826c5fd212d968f561ac6717cd47eb6c2a0bb70  1.383.1801.0
  mpavbase.vdm: 66a7af38e7cbc10faafbbfc22e4e829b663e6a407ddf93e490dae0c952226182  1.383.0.0
  mpavdlta.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
```

The Validation

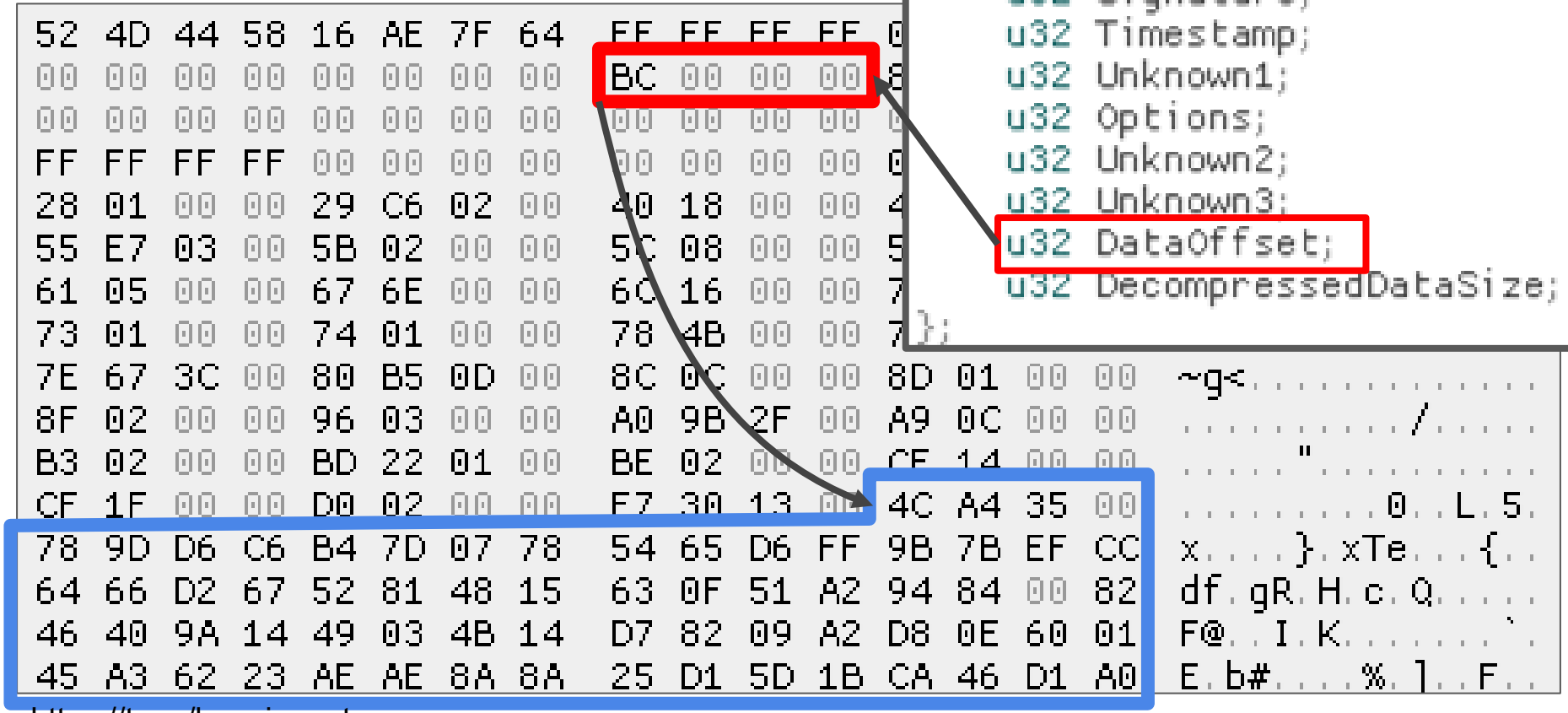
Quick Reminder



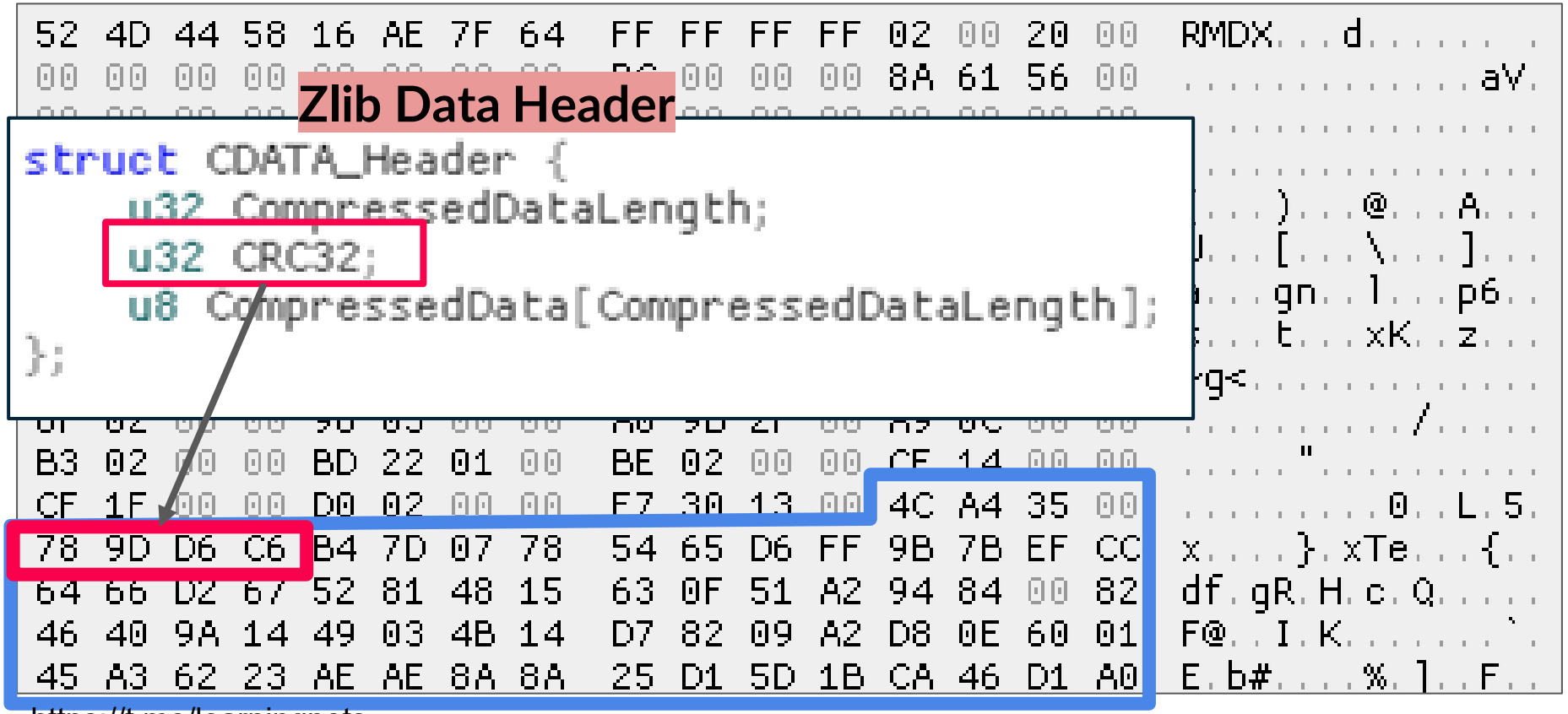
mpengine.dll



RMDX & Zlib Headers



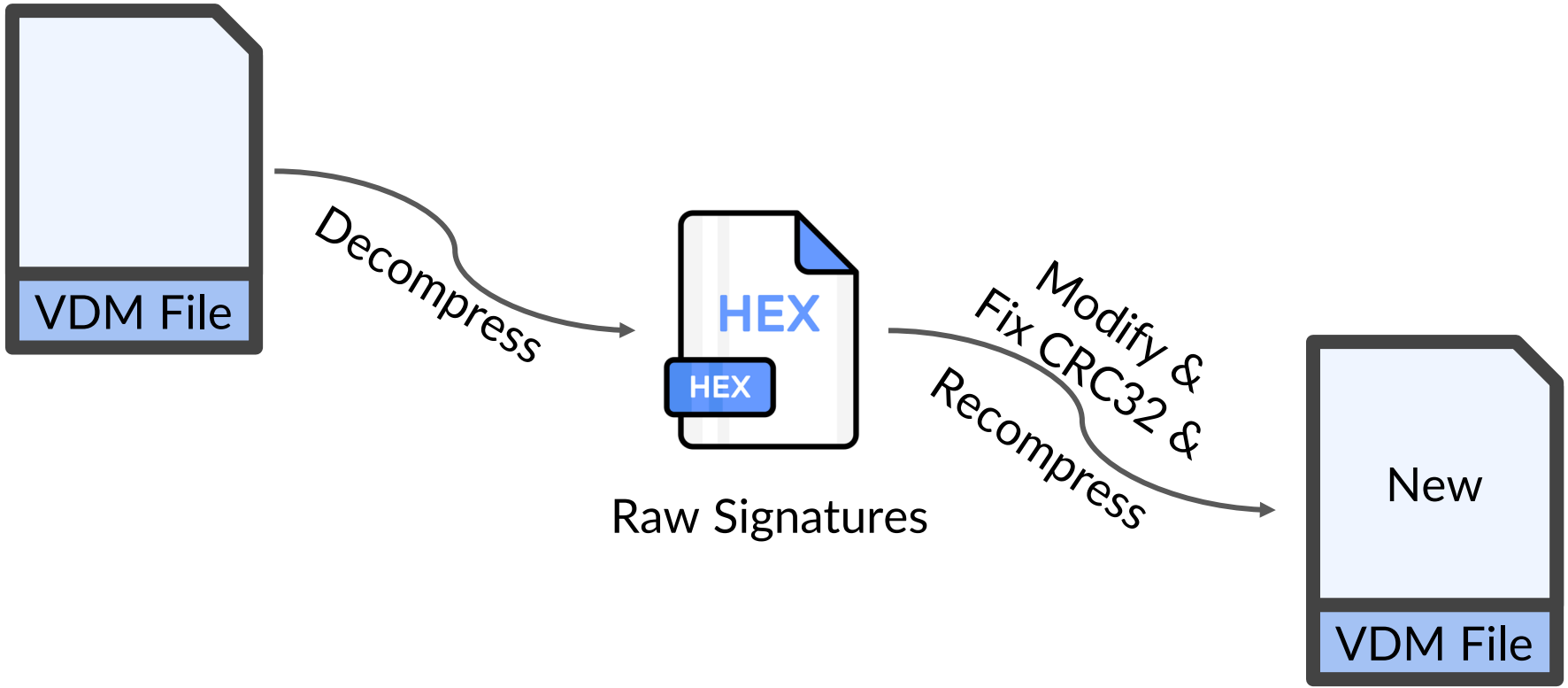
RMDX & Zlib Headers



CRC32 Algorithm

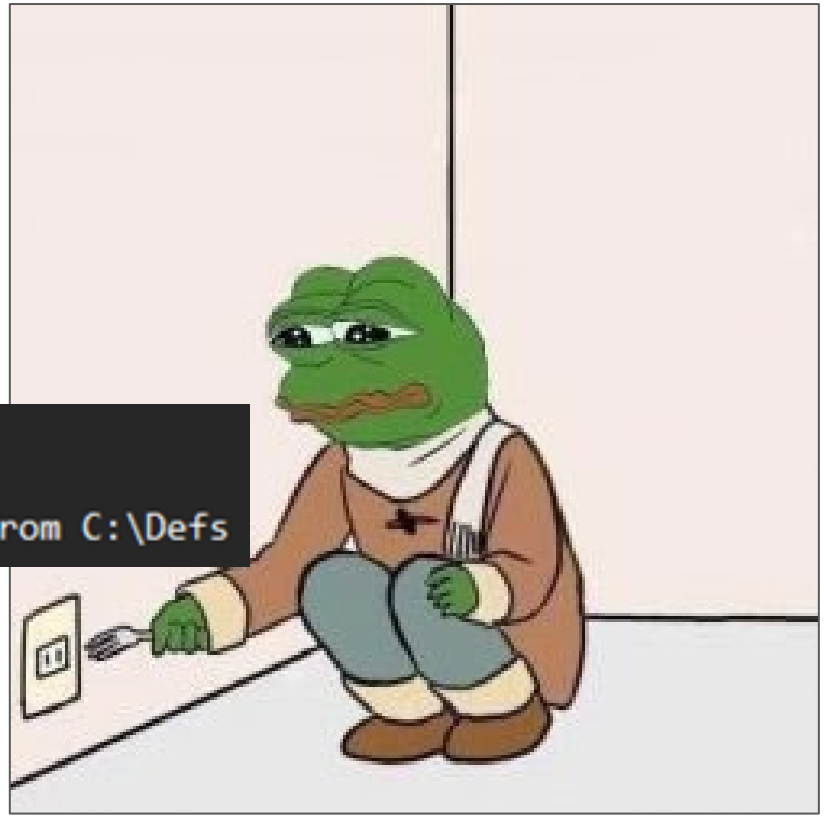
Algorithm	Result	Check	Poly	Init
CRC-32	0xE5B92BDF	0xCBF43926	0x04C11DB7	0xFFFFFFFF
CRC-32/BZIP2	0xB4E3A0A8	0xFC891918	0x04C11DB7	0xFFFFFFFF
CRC-32/JAMCRC	0x1A46D420	0x340BC6D9	0x04C11DB7	0xFFFFFFFF
CRC-32/MPEG-2	0x4B1C5F57	0x0376E6E7	0x04C11DB7	0xFFFFFFFF
CRC-32/POSIX	0x9B769BC0	0x765E7680	0x04C11DB7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

Trying One More Update Attempt

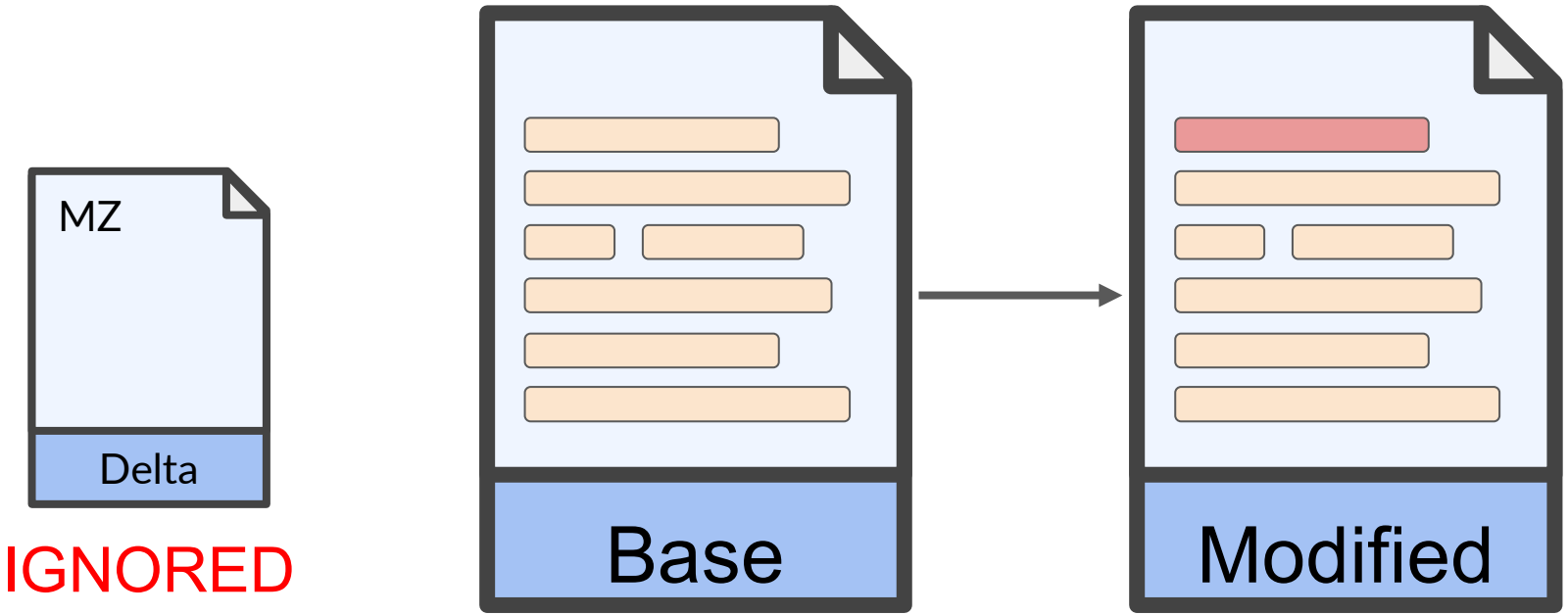


Trying One More Update Attempt

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

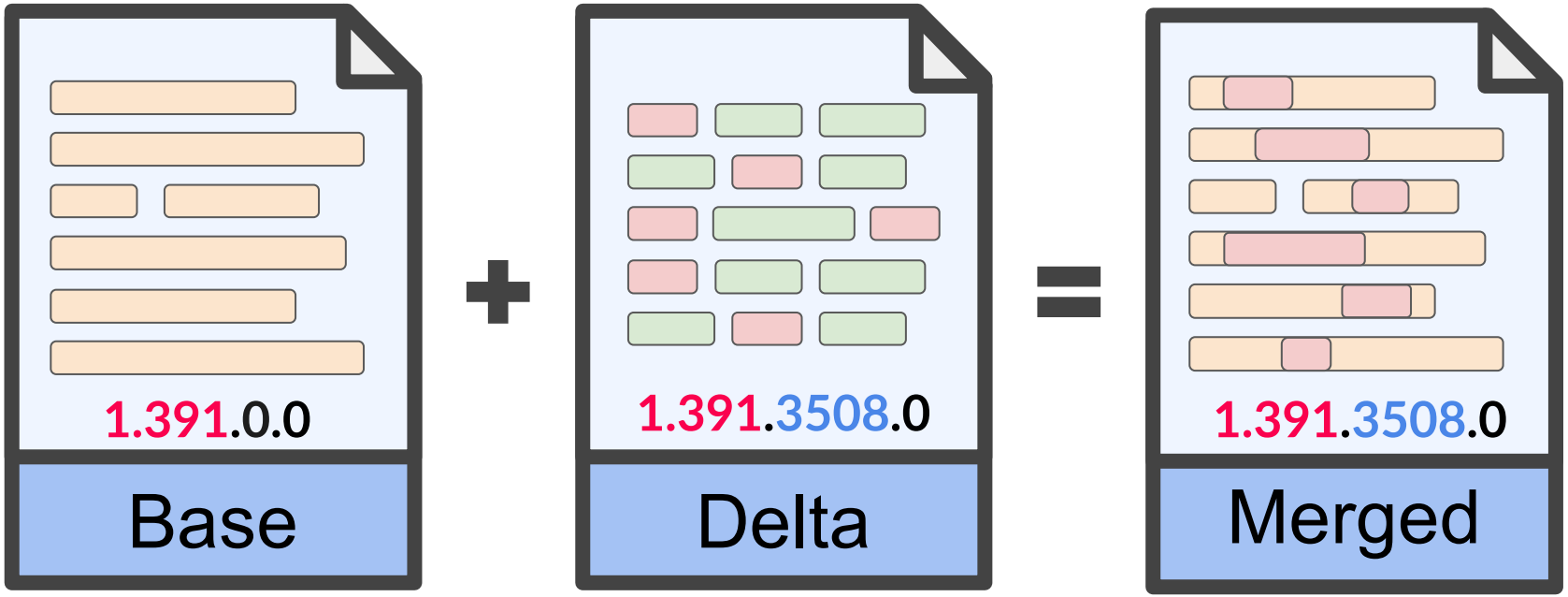


How Do We Modify?



Two Pairs Of VDM Files

What The Purpose Of Delta Files?

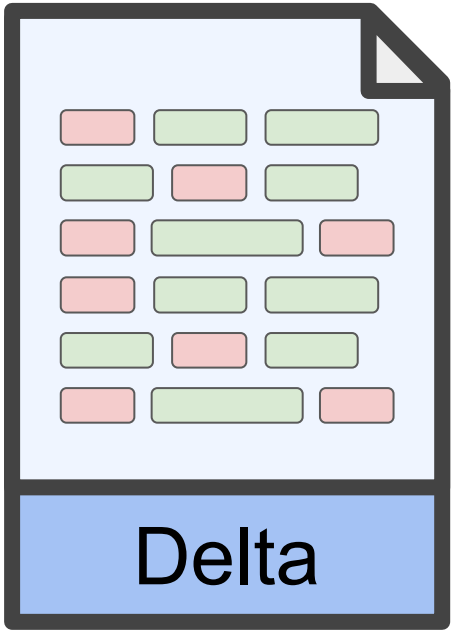


The Merge

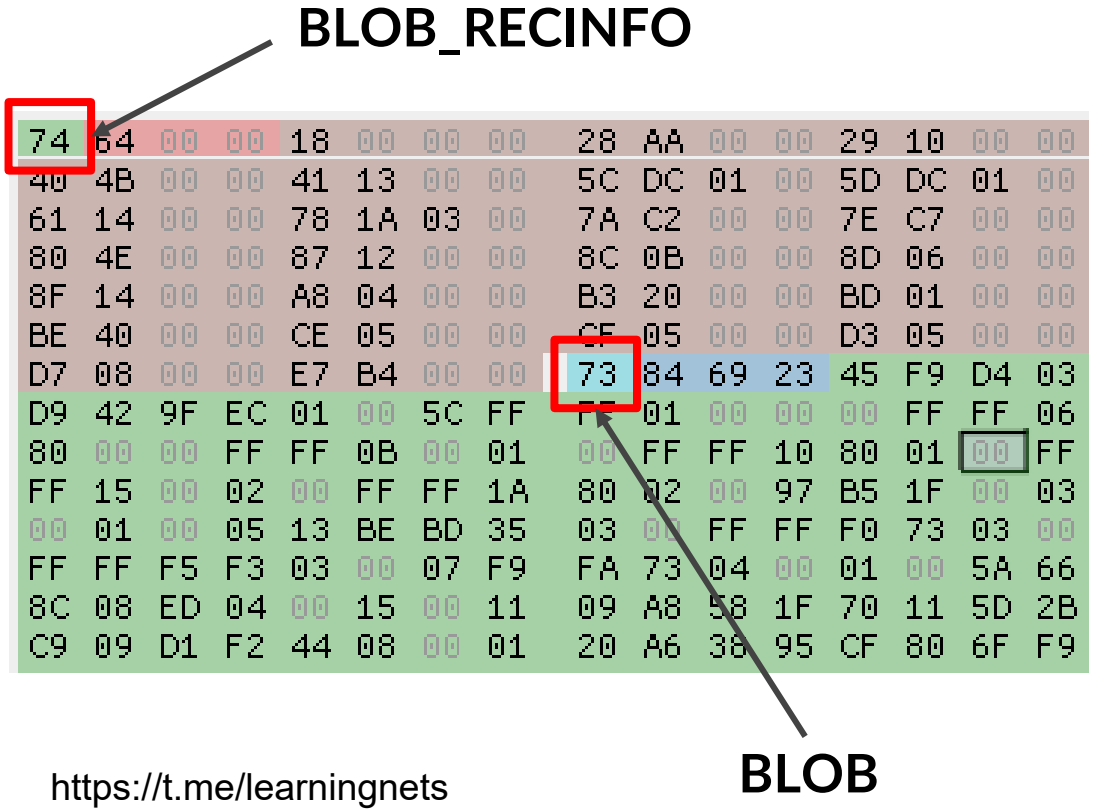
Internals

What's The Delta Format?

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

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

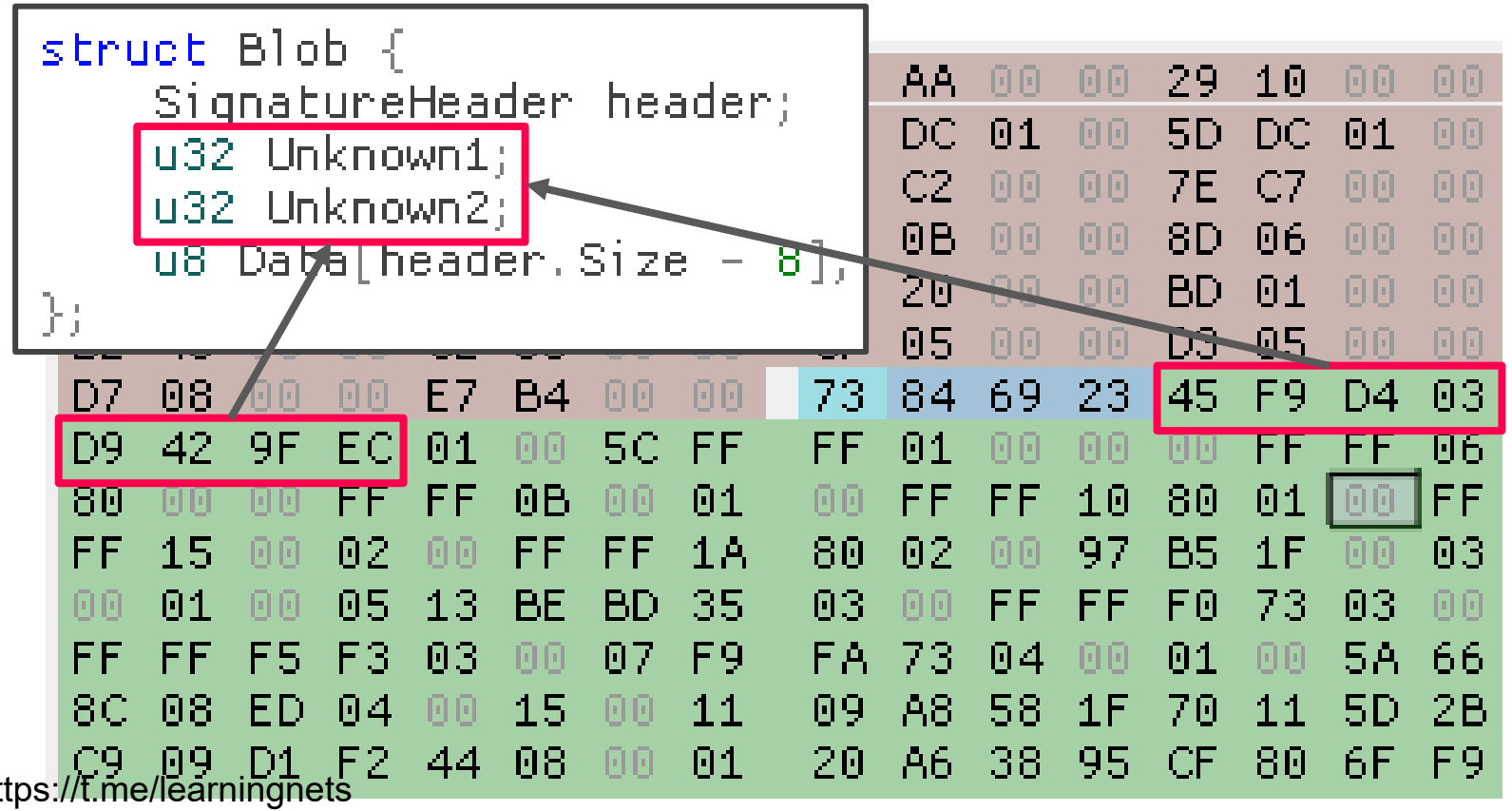


BLOB_RECINFO & BLOB

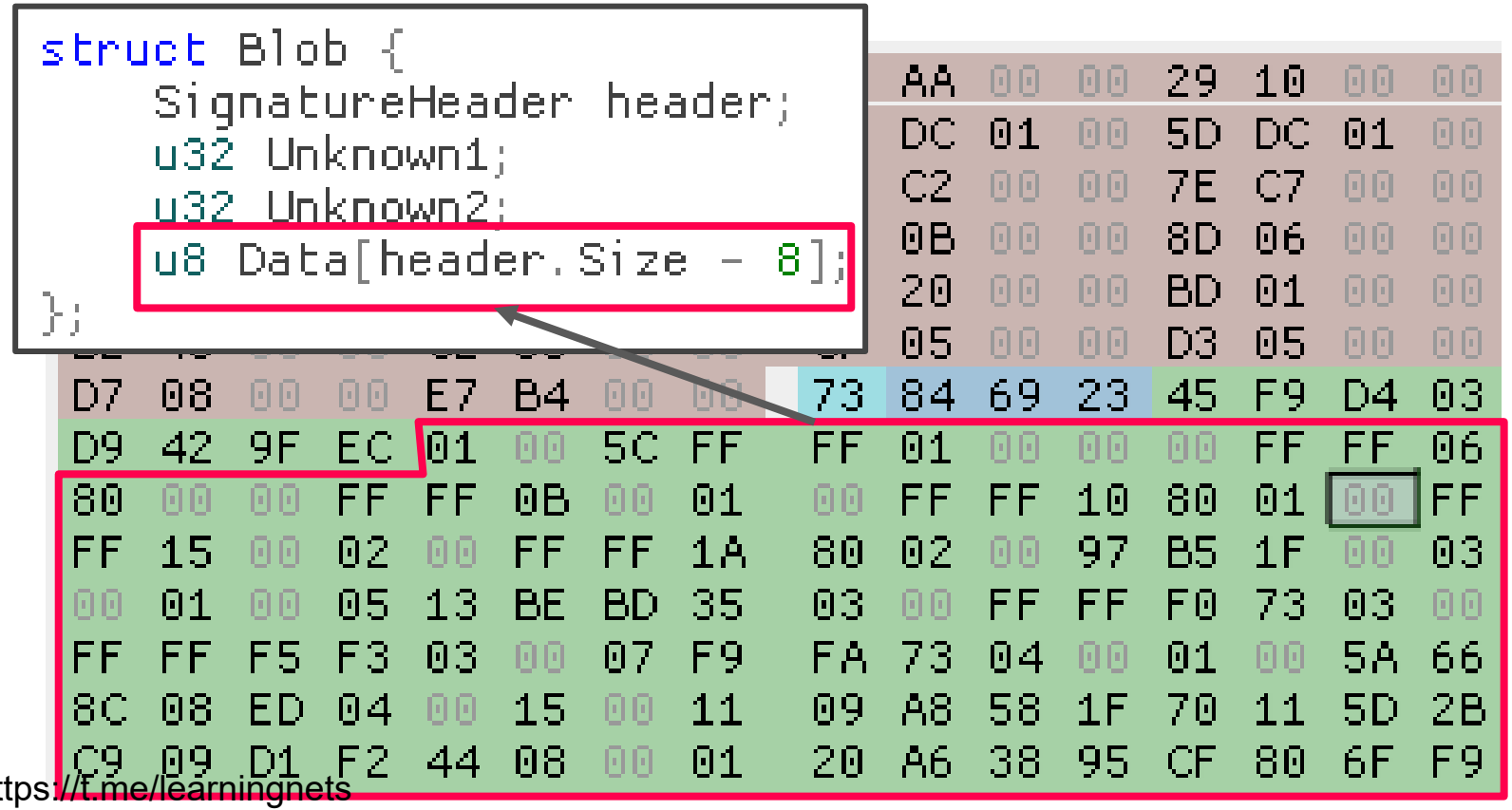



```
bitfield SignatureHeader {
    Type: 8;
    Size: 24;
};

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

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

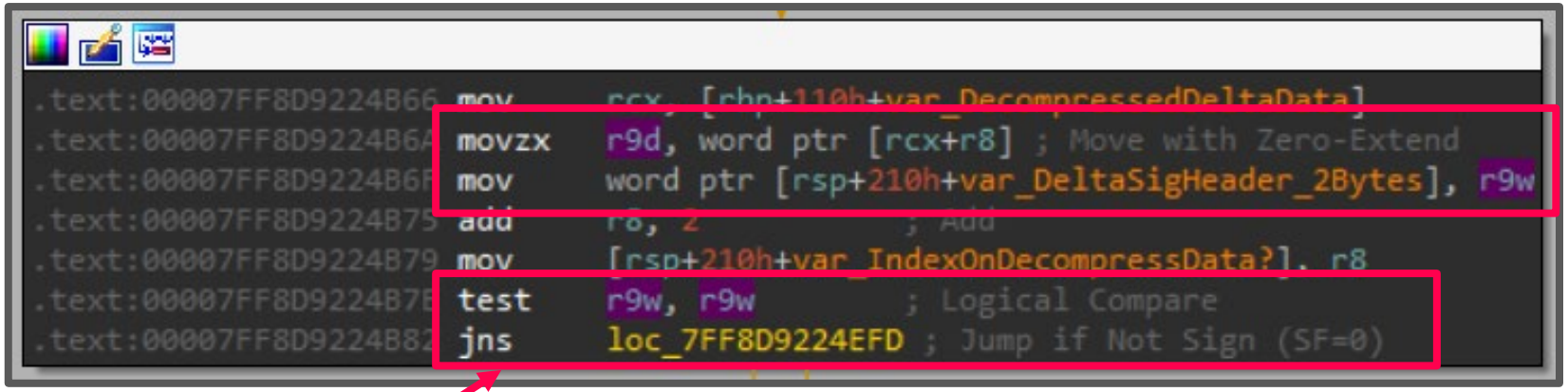
BLOB Structure



Actions



Reverse ConsumeInputCompress



MSB Check

Action Types

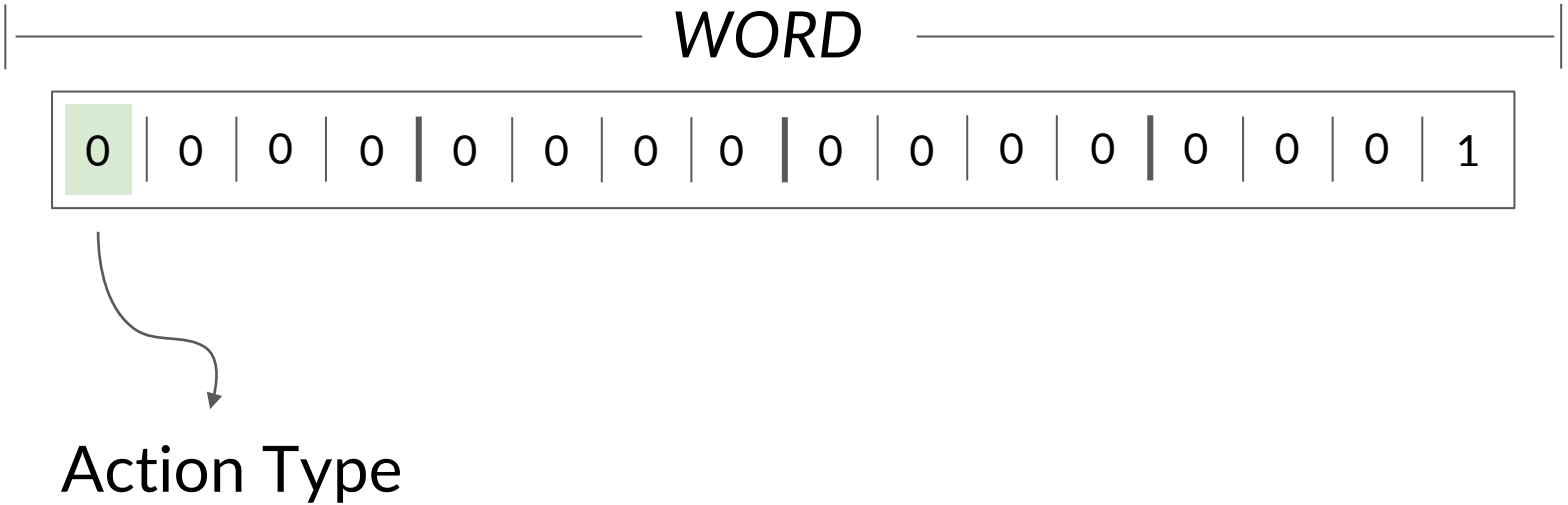
Copy From Delta

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

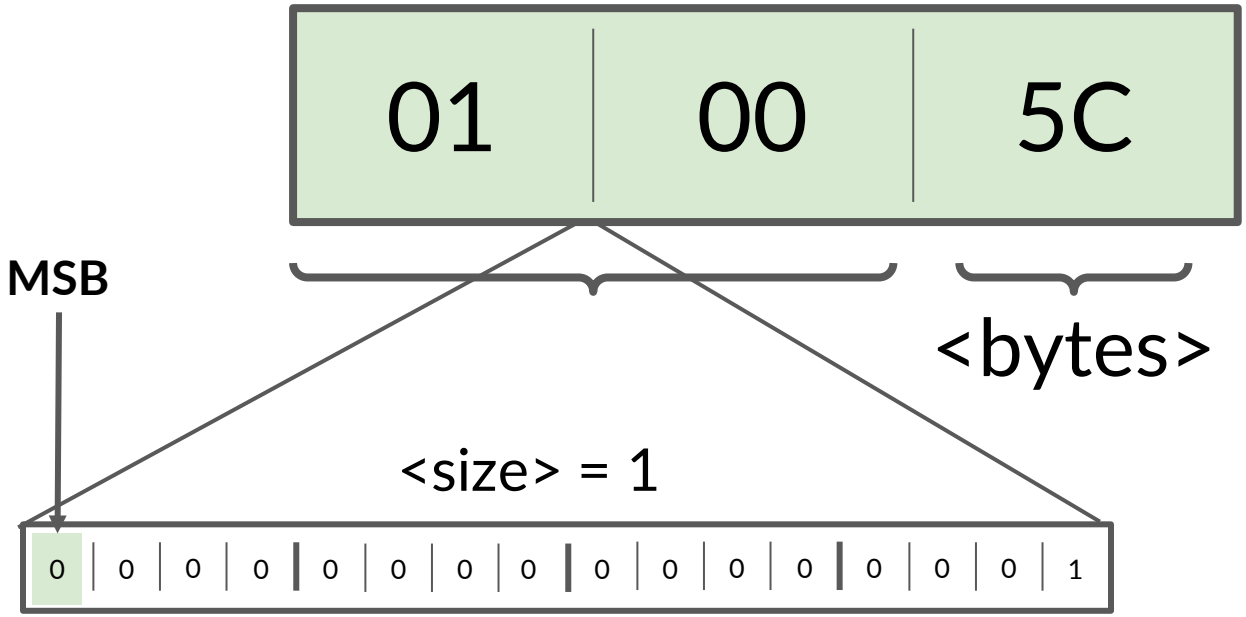
Copy From Base

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

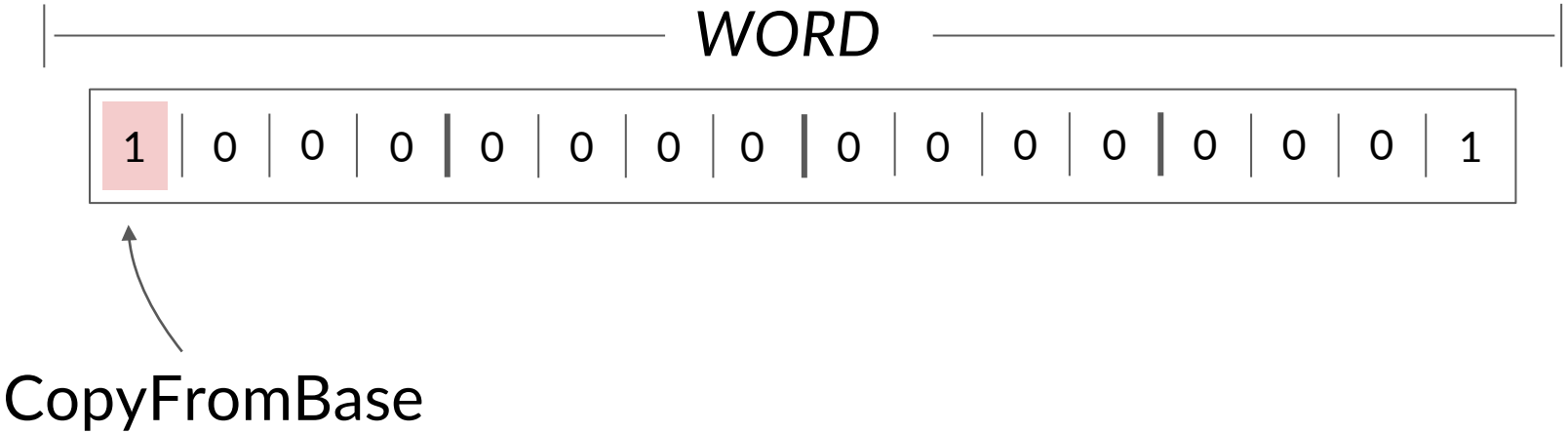
Action Header



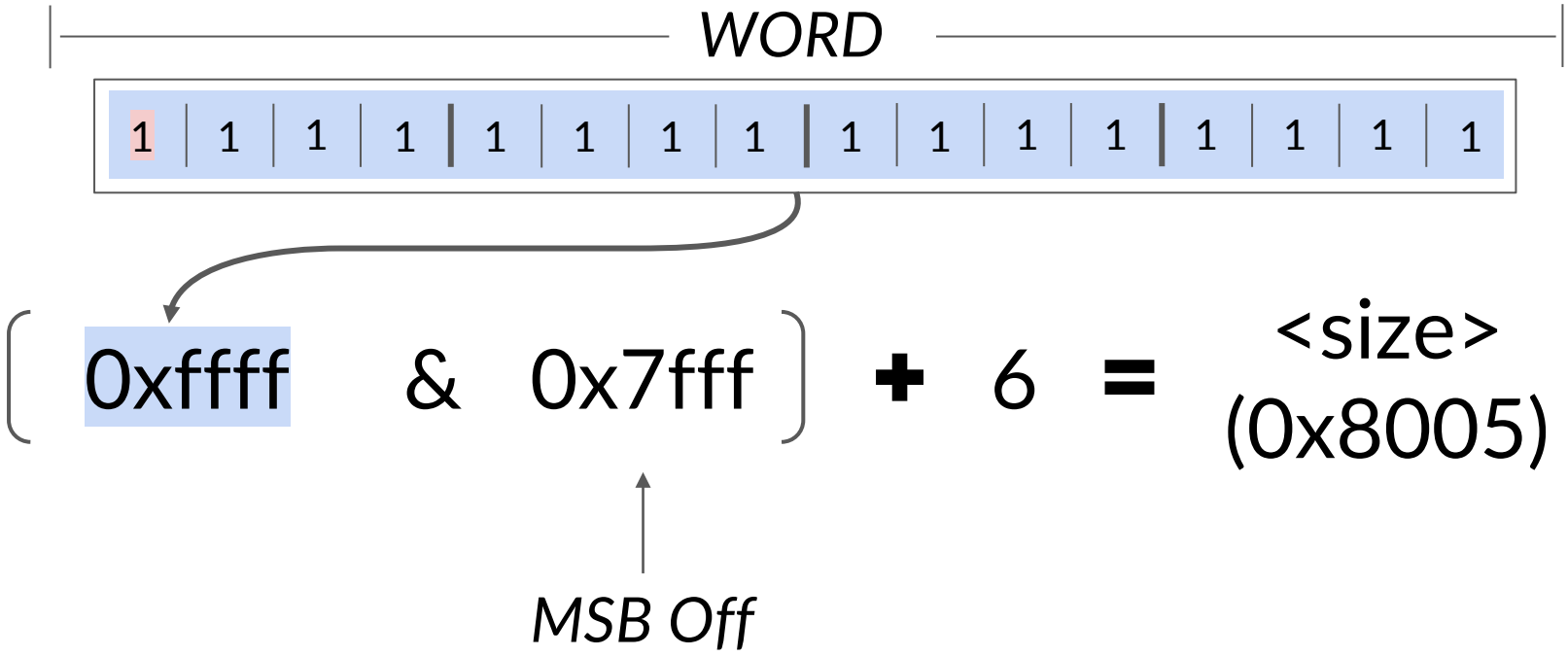
CopyFromDelta - Example



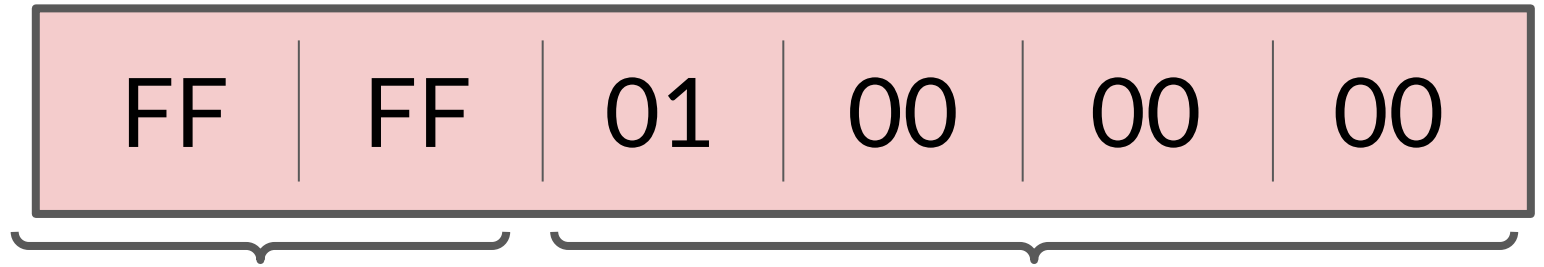
Action Header - CopyFromBase



Action Header - CopyFromBase

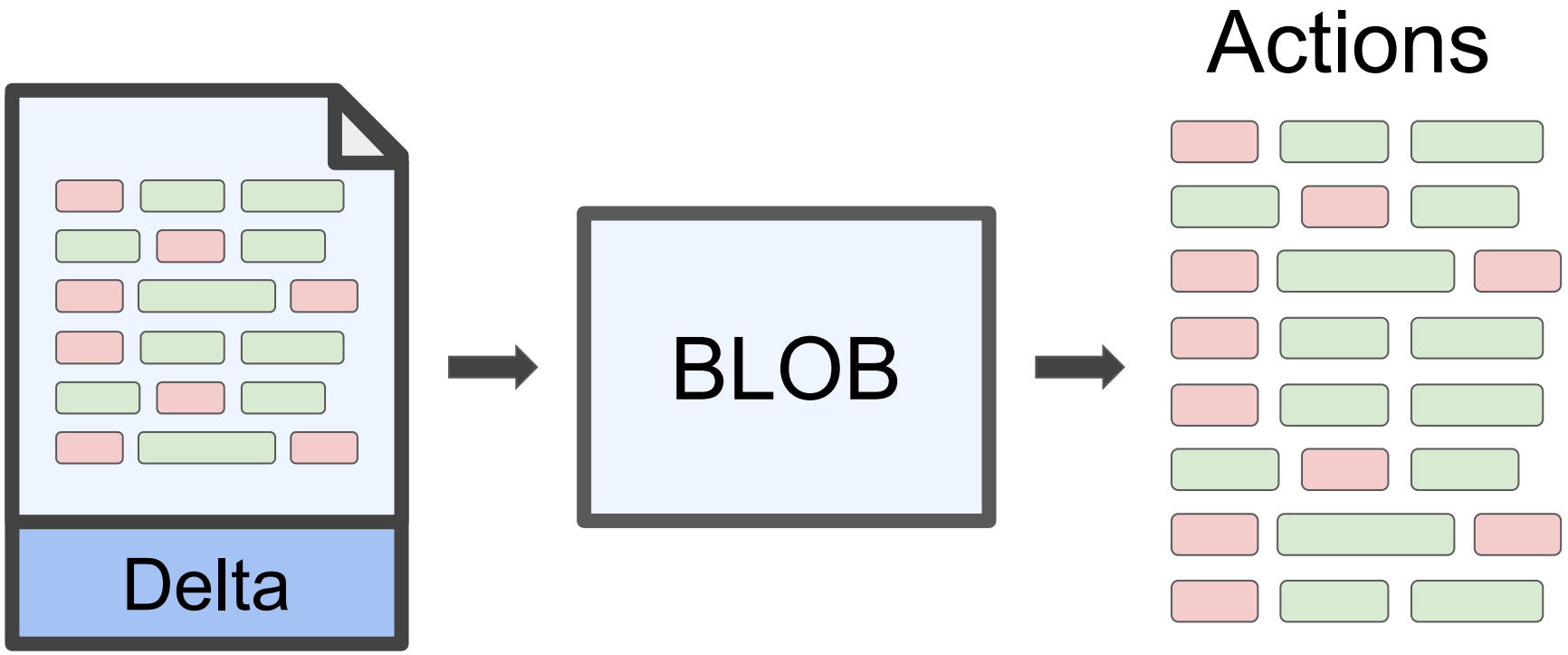


CopyFromBase - Example



(0xffff & 0x7fff) + 0x6 = 0x8005 → <size>

Sum Up

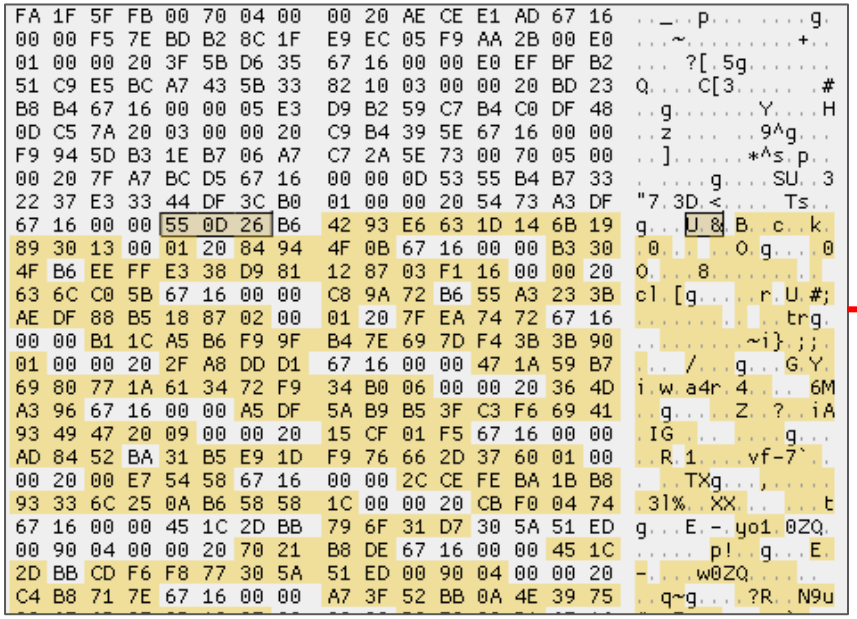


Merge Algorithm

```
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
```

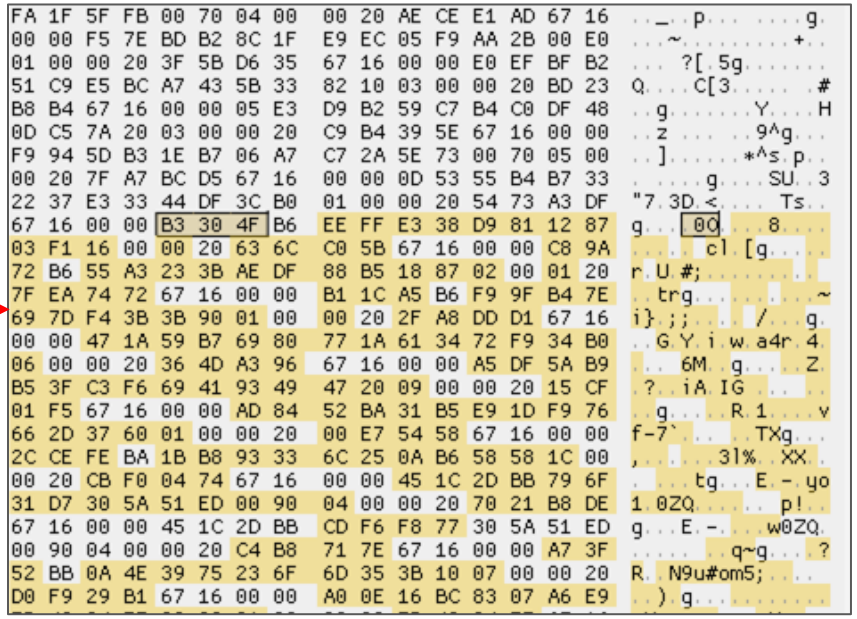
Diffing Base and Merge

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  ..g.....Y....H
0D 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.&.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  O....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.
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  .3l%..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 70 21  B8 DE 67 16 00 00 45 1C  ..... p!..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
```

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  ..g.....Y....H
0D 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....0O....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 B8 93 33  6C 25 0A B6 58 58 1C 00  ,.....3l%..XX...
00 20 CB F0 04 74 67 16  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..... ..p!..
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 - 0x0ACEE711 (0 - 181331729)
Data Size: 0x0ACEE711 (0xACEE711 | 172.93 MiB)
```

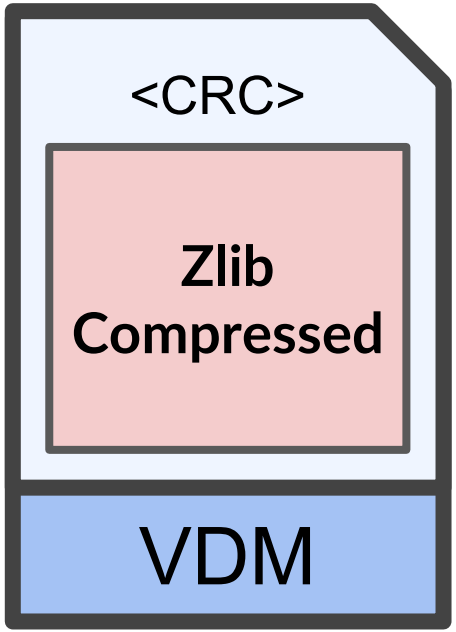
```
Region: 0x00000000 - 0x0AF6CE1C (0 - 183946780)
Data Size: 0x0AF6CE1C (0xAF6CE1C | 175.43 MiB)
```

Eureka - Unknown Numbers

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

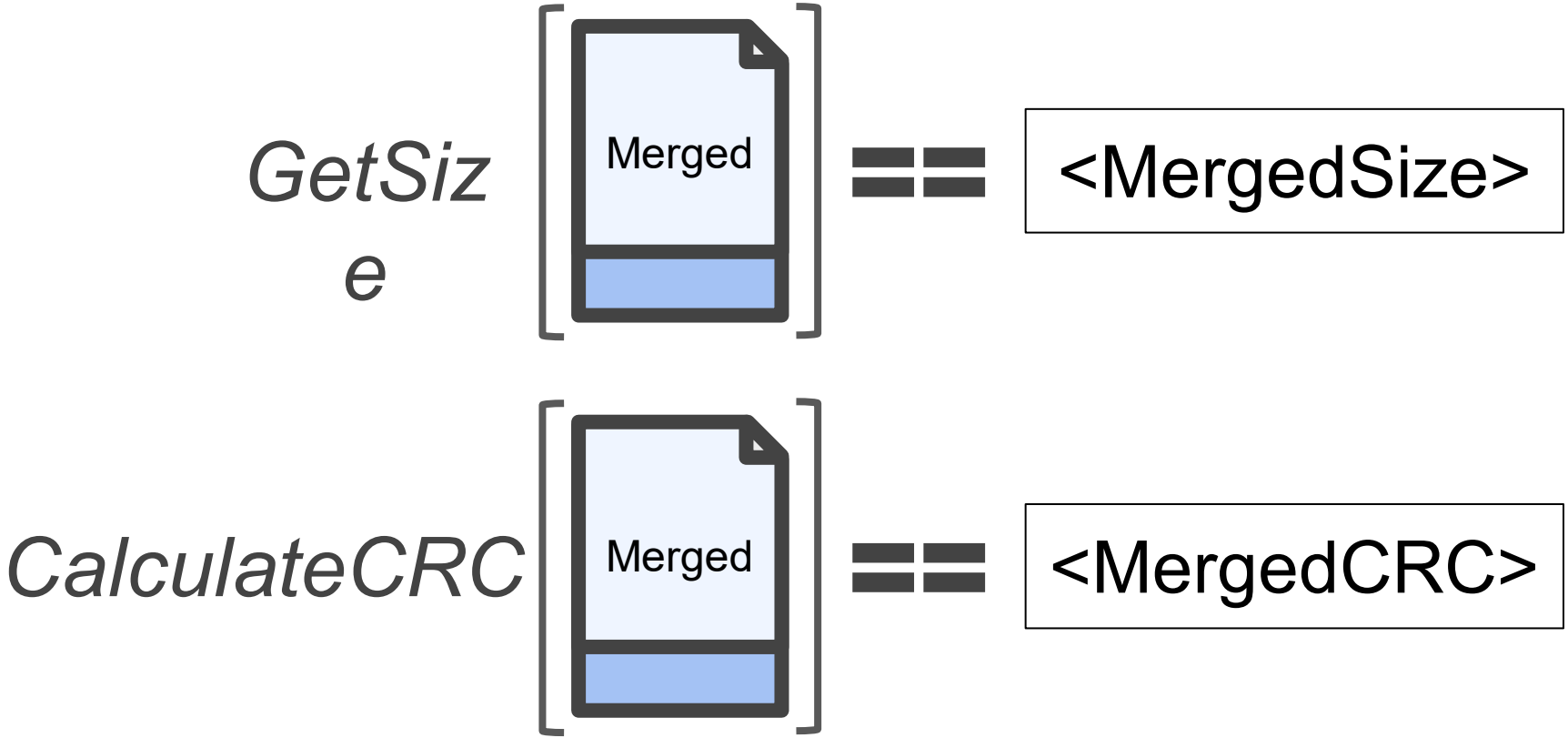
```
struct Blob {
    SignatureHeader header;
    u32 MergeSize;
    u32 MergeCRC32;
    u8 Data[header.Size - 8];
};
```

Validations Recap - Zlib Data Validation



<CRC> == *CalculateCRC* [Zlib Compressed]

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
```

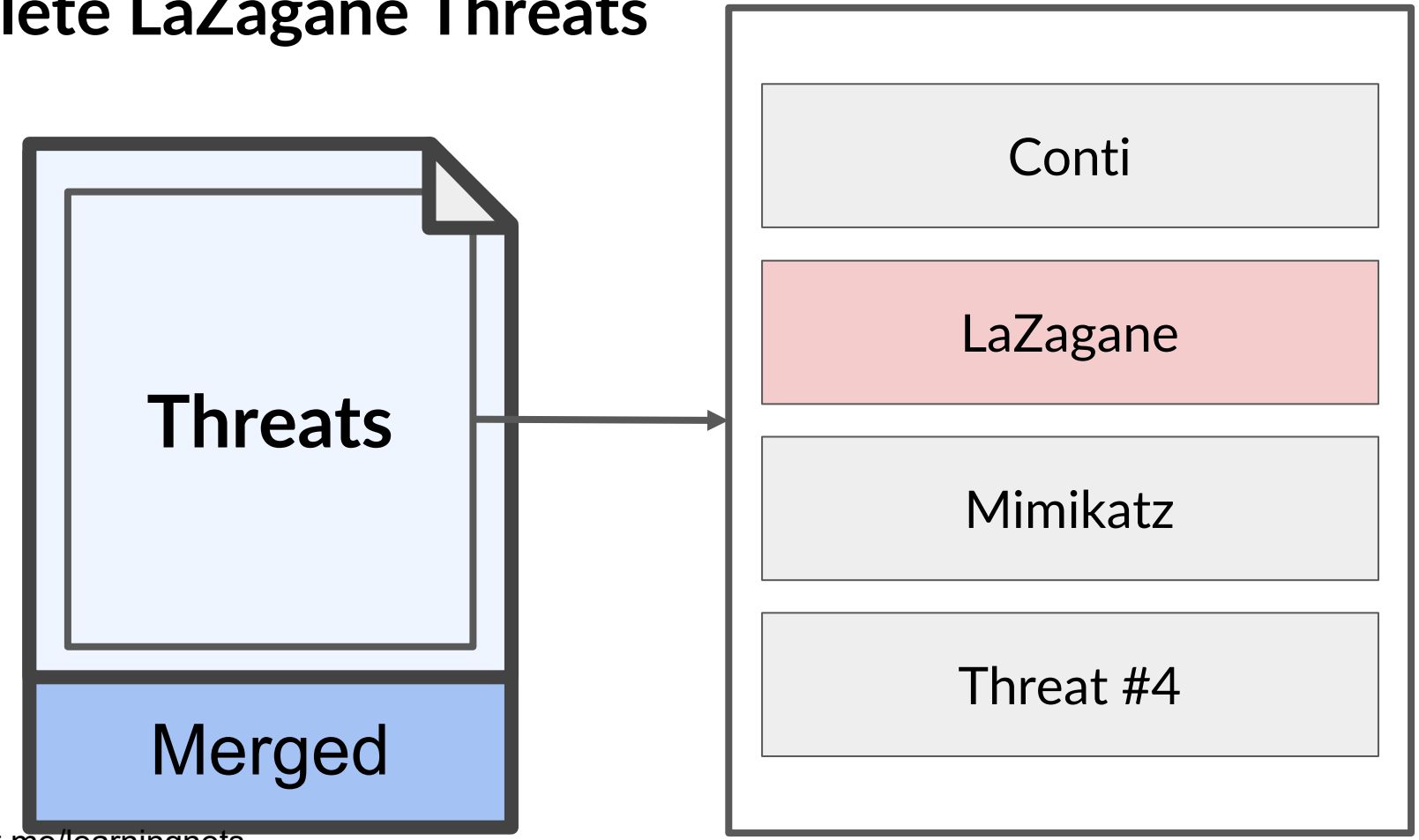
Updated to: 1.383.1800

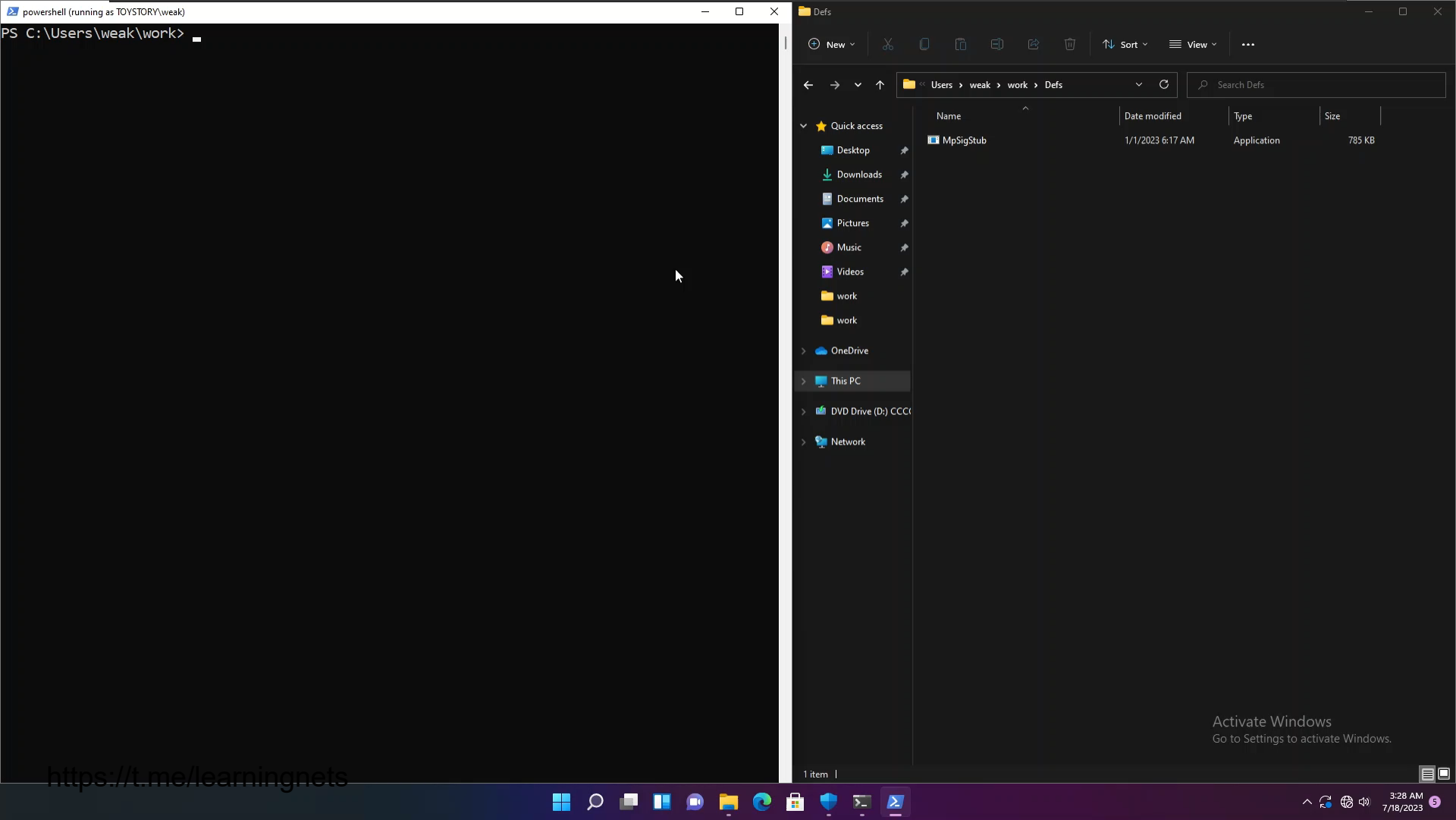
Attack Vectors

(CVE-2023-24934)

wd-pretender

Delete LaZagane Threats




powershell (running as TOYSTORY\weak)
PS C:\Users\weak\work>
Defs
New
Sort
View
Users › weak › work › Defs
Search Defs
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
work
work
OneDrive
This PC
DVD Drive (D:) CCC(
Network
Name
Date modified
Type
Size
MpSigStub
1/1/2023 6:17 AM
Application
785 KB
Activate Windows
Go to Settings to activate Windows.
1 item
https://t.me/learningnots
3:28 AM
7/18/2023

Friendly Files

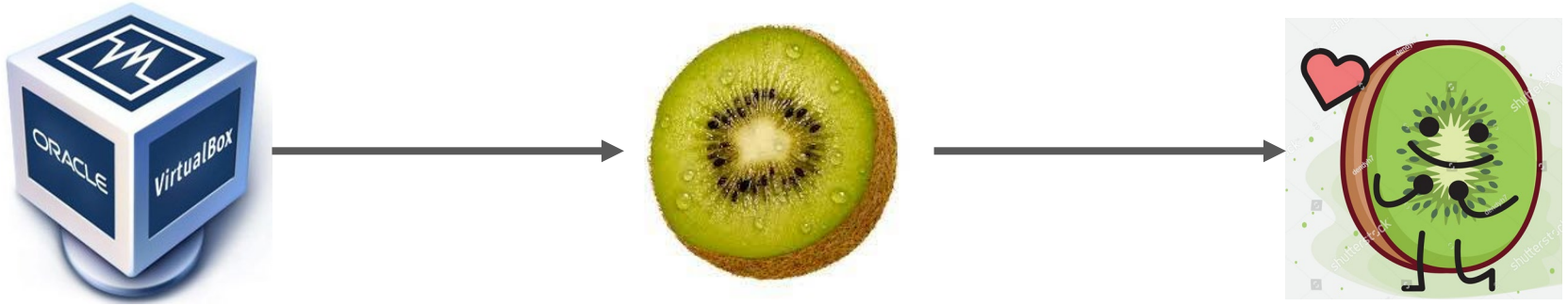
```
156: "SIGNATURE_TYPE_VDLL_ARM",
157: "SIGNATURE_TYPE_THREAD_X86",
158: "SIGNATURE_TYPE_THREAD_X64",
159: "SIGNATURE_TYPE_THREAD_IA64",
160: "SIGNATURE_TYPE_FRIENDLYFILE_SHA256",
161: "SIGNATURE_TYPE_FRIENDLYFILE_SHA512",
162: "SIGNATURE_TYPE_SHARED_THREAT",
163: "SIGNATURE_TYPE_VDM_METADATA",
164: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

30,000 friendly hashes

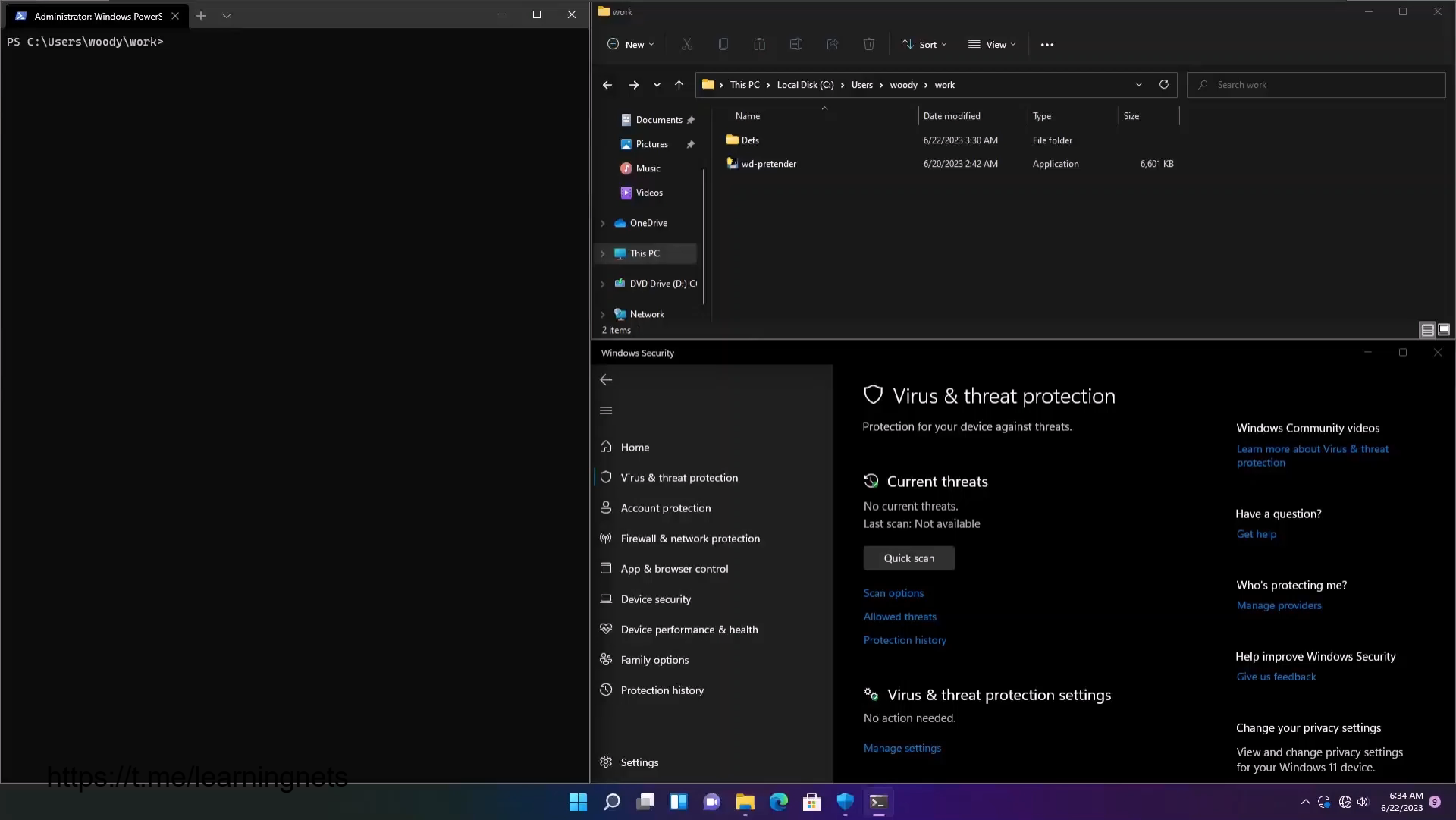
```
895 0209a3e590d5cc6c7cb69b012a59e7fd29c857e0782fcd208a90cc9baa283441
896 0209cffc2df2d39dfa9106fa00fb6d221dbd450dc6161cc2a7138c46a293add7
897 0209f490cbfe60c61b651023e1df9327e5350cd0a8be126907cdbaa6b564ceeb
898 020a4cbaebdb1bbbdfdf141cfbb16f165457535b5a4612ffdbb33bc64743bbe3
899 020b7b54f1704c10dc5ac9b91bf037486f7b88cc21ce55b766a89ee505a5cde7
900 020c4b29f3771bac476b4ed836c0761fdda30adfaf5d59dbd1f667193cd77d9b
901 020cefa6c036894f912c69eef981efef7d3ffb6a89000efac4888ddd00c255a8
902 020dc950741800877ab9ddb69e566897ed3077c4bc181cf607cdd49dbf23419d
903 020e5eb54040628846c4bfd816b71d8c0694b2b6c94883001a2da3dcfc251346
904 02102bf3d33f117a295093e4af72bae1b6a6be35e3e4255b65ef24f1108c017d
905 02106197ff396ba5c03d528bc6e245d0de25c745237ab37bc5d6a9a913c57e52
906 0210bd8d5d5a63e1b8fa975abaf2e33486f8bc6c8c23d6e1f5c7f2b9460b023b
907 02110f602638980ea83de49f575bcaa4e94508043664676c8090f0a7e230c277
908 021129a2a3446af44a296c2a50fd5023db6e16b489719992bc7c7ce078cebde2
909 02119a7d84b692650607cd256a52d02de8016e972c22d86f6703c4ee240c142d
910 0212a89972e6e11d056323fcf7664a226dd26bce575eaa02c0b17dc5d4dc2cb3
911 0213705992cd08a07c57690ce28e6c7ee930d6a76ddc45d841df4326b04fbcc3
912 02141b072b5ebe37f18be2a3658610f353fd3c63b9214472b4fc65588b464c80
913 02142531a7ae99a5509c79e1c639e34d052fb39e77e0c9dbae65c8ff61ef7e19
```

Friendly Files: First Generic Bypass

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

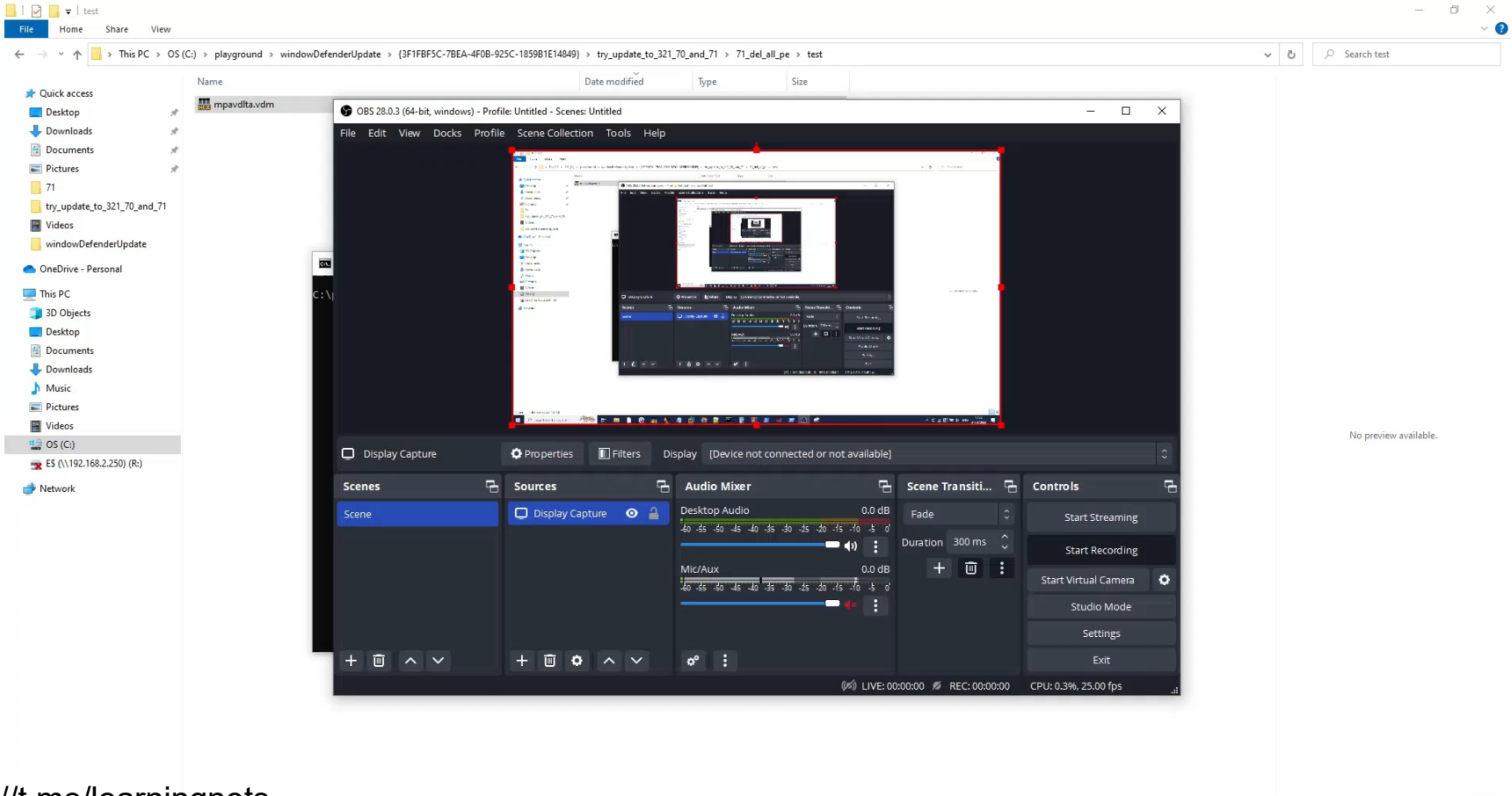


Friendly Mimikatz :)



Final Attack Vector: DOS

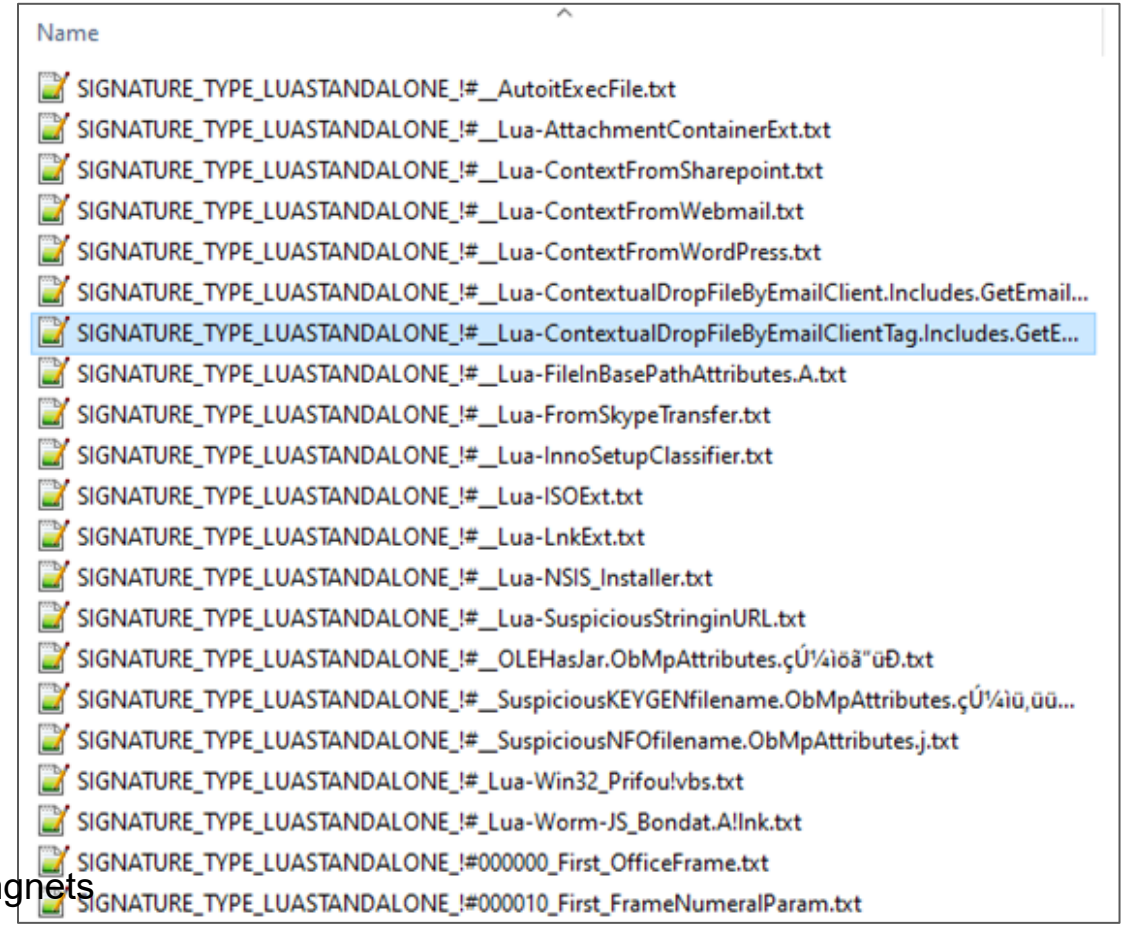
"!This program cannot be run in DOS Mode"



Final Attack Vector: DOS

- The demo was recorded on an older version of Defender
- The latetst 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



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

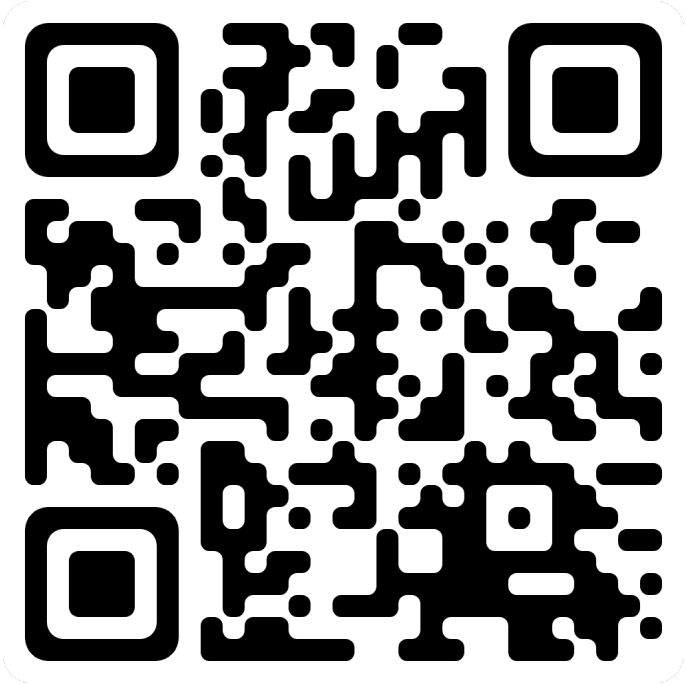
Microsoft released a fix on April - **CVE-2023-24934**

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/

SafeBreach LABS

Thank you!

Tomer Bar
Omer Attias