Recorded Future® Triage

Submit Reports

Overview overview 7	Static static 3	WX.pdf.lnk windows7-x64 3	WX.pdf.lnk windows10-2004-x64 7	i1v/zN/JI/...qd.pdf windows7-x64 1	i1v/zN/JI/...qd.pdf windows10-2004-x64

Report Analysis Logs

Download Sample

Download PCAP

Download PCAPNG

Feedback

Print to PDF

Analysis

max time kernel
146s

max time network
147s

platform
windows10-2004_x64

resource
win10v2004-20230915-en

resource tags

ARCH:X64

ARCH:X86

IMAGE:WIN10V2004-20230915-EN

LOCALE:EN-US

OS:WINDOWS10-2004-X64

SYSTEM

submitted
04-10-2023 16:15

Sharing

Copy URL

Twitter

E-mail

General

Target
WX.pdf.lnk

Size
1KB

MD5
4081b99306478e563fcb8737ea368029

SHA1
49a54cbbd519c1a10835542f704ba174e65d078f

SHA256
77dc2c45251101c6967d9368de8750fff2c5981e5452c8539e85dfae2373703b

SHA512
6b0e0a44d8cd13af1788c961090a4b6d895f233158917f6c06521081d74cca9509882ff0fe1cc4a1dd64d5c491bced52e5f45eacef0943e993d85b1b8936eefb

Score
7/10

Malware Config

Signatures

Execution Defense Evasion Discovery

Checks computer location settings • 2 TTPs 1 IoCs
Looks up country code configured in the registry, likely geofence.

Suspicious use of SetThreadContext • 1 IoCs

Enumerates physical storage devices • 1 TTPs
Attempts to interact with connected storage/optical drive(s).

Checks processor information in registry • 2 TTPs 2 IoCs
Processor information is often read in order to detect sandboxing environments.

Gathers network information • 2 TTPs 2 IoCs
Uses commandline utility to view network configuration.

Modifies Internet Explorer settings • 1 TTPs 1 IoCs
ADWARE SPYWARE

Modifies registry class • 1 IoCs

Suspicious behavior: EnumeratesProcesses • 24 IoCs

Suspicious behavior: GetForegroundWindowSpam • 1 IoCs

Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary • 1 IoCs

Suspicious use of AdjustPrivilegeToken • 28 IoCs

Suspicious use of FindShellTrayWindow • 1 IoCs

Suspicious use of SetWindowsHookEx • 6 IoCs

Suspicious use of WriteProcessMemory • 64 IoCs

Processes

C:\Windows\system32\cmd.exe PID:3556

```
cmd /c C:\Users\Admin\AppData\Local\Temp\WX.pdf.lnk
```

C:\Windows\System32\regsvr32.exe PID:4280

```
"C:\Windows\System32\regsvr32.exe" /s /u /i:i1v\zN\JI\eWJM\MVst\qI\1Q52\uURq\QIPJ\J4Xw\J6V\CO\bOs8\GMV\N53B\bow.sct scrobj.dll
```

C:\Windows\System32\rundll32.exe PID:3028

```
"C:\Windows\System32\rundll32.exe" i1v\zN\JI\eWJM\MVst\qI\1Q52\uURq\QIPJ\J4Xw\J6V\CO\bOs8\GMV\N53B\xSa.log, HUF_inc_var
```

C:\Windows\SysWOW64\rundll32.exe PID:3692

```
"C:\Windows\System32\rundll32.exe" i1v\zN\JI\eWJM\MVst\qI\1Q52\uURq\QIPJ\J4Xw\J6V\CO\bOs8\GMV\N53B\xSa.log, HUF_inc_var
```

C:\Windows\SysWOW64\SearchProtocolHost.exe PID:1740

```
"C:\Windows\System32\SearchProtocolHost.exe"
```

C:\Windows\SysWOW64\whoami.exe PID:4168

PID:2260

PID:4720

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy.

Accept

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

PID:1268

```
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe"
"C:\Users\Admin\AppData\Local\Temp\i1v\zN\JI\eWJM\MVst\qI\1Q52\uURq\QIPJ
\J4Xw\J6V\CO\bOs8\GMV\N53B\Abqd.pdf"
```

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

PID:4696

```
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCE
F.exe" --backgroundcolor=16514043
```

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

PID:2840

```
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrC
EF.exe" --type=gpu-process --disable-pack-loading --lang=en-US --lo
g-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroC
EF\debug.log" --log-severity=disable --product-version="ReaderServi
ces/19.10.20064 Chrome/64.0.3282.119" --gpu-preferences=GAAAAAAAAA
AB4AAAQAAAAAAAAAAAGAA --use-gl=swiftshader-webgl --gpu-vendor-id=0x
1234 --gpu-device-id=0x1111 --gpu-driver-vendor="Google Inc." --gpu
-driver-version=3.3.0.2 --gpu-driver-date=2017/04/07 --disable-pack
-loading --lang=en-US --log-file="C:\Program Files (x86)\Adobe\Acro
bat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --pr
oduct-version="ReaderServices/19.10.20064 Chrome/64.0.3282.119" --s
ervice-request-channel-token=F701B6C083BEB4F0D4BB864581D2F8D3 --moj
o-platform-channel-handle=1736 --allow-no-sandbox-job --ignored=" -
-type=renderer " /prefetch:2
```

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

PID:4912

```
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrC
EF.exe" --type=renderer --disable-browser-side-navigation --disable
-gpu-compositing --service-pipe-token=632A56E7975808FD337C1F3B80CF4
A2A --lang=en-US --disable-pack-loading --lang=en-US --log-file
="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\deb
ug.log" --log-severity=disable --product-version="ReaderServices/1
9.10.20064 Chrome/64.0.3282.119" --enable-pinch --device-scale-fact
or=1 --num-raster-threads=4 --enable-main-frame-before-activation -
-enable-gpu-async-worker-context --content-image-texture-target=0,
0,3553;0,1,3553;0,2,3553;0,3,3553;0,4,3553;0,5,3553;0,6,3553;0,7,35
53;0,8,3553;0,9,3553;0,10,3553;0,11,3553;0,12,3553;0,13,3553;0,14,3
553;0,15,3553;0,16,3553;0,17,3553;0,18,3553;1,0,3553;1,1,3553;1,2,3
553;1,3,3553;1,4,3553;1,5,3553;1,6,3553;1,7,3553;1,8,3553;1,9,3553;
1,10,3553;1,11,3553;1,12,3553;1,13,3553;1,14,3553;1,15,3553;1,16,35
53;1,17,3553;1,18,3553;2,0,3553;2,1,3553;2,2,3553;2,3,3553;2,4,355
3;2,5,3553;2,6,3553;2,7,3553;2,8,3553;2,9,3553;2,10,3553;2,11,3553;
2,12,3553;2,13,3553;2,14,3553;2,15,3553;2,16,3553;2,17,3553;2,18,35
53;3,0,3553;3,1,3553;3,2,3553;3,3,3553;3,4,3553;3,5,3553;3,6,3553;
3,7,3553;3,8,3553;3,9,3553;3,10,3553;3,11,3553;3,12,3553;3,13,3553;
3,14,3553;3,15,3553;3,16,3553;3,17,3553;3,18,3553;4,0,3553;4,1,355
3;4,2,3553;4,3,3553;4,4,3553;4,5,3553;4,6,3553;4,7,3553;4,8,3553;4,
9,3553;4,10,3553;4,11,3553;4,12,3553;4,13,3553;4,14,3553;4,15,3553;
4,16,3553;4,17,3553;4,18,3553;5,0,3553;5,1,3553;5,2,3553;5,3,3553;
5,4,3553;5,5,3553;5,6,3553;5,7,3553;5,8,3553;5,9,3553;5,10,3553;5,1
1,3553;5,12,3553;5,13,3553;5,14,3553;5,15,3553;5,16,3553;5,17,3553;
5,18,3553;6,0,3553;6,1,3553;6,2,3553;6,3,3553;6,4,3553;6,5,3553;6,
6,3553;6,7,3553;6,8,3553;6,9,3553;6,10,3553;6,11,3553;6,12,3553;6,1
3,3553;6,14,3553;6,15,3553;6,16,3553;6,17,3553;6,18,3553 --disable-
accelerated-video-decode --service-request-channel-token=632A56E797
5808FD337C1F3B80CF4A2A --renderer-client-id=2 --mojo-platform-chann
el-handle=1836 --allow-no-sandbox-job /prefetch:1
```

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

PID:1680

```
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrC
EF.exe" --type=gpu-process --disable-pack-loading --lang=en-US --lo
g-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroC
EF\debug.log" --log-severity=disable --product-version="ReaderServi
ces/19.10.20064 Chrome/64.0.3282.119" --gpu-preferences=GAAAAAAAAA
AB4AAAQAAAAAAAAAAAGAA --use-gl=swiftshader-webgl --gpu-vendor-id=0x
1234 --gpu-device-id=0x1111 --gpu-driver-vendor="Google Inc." --gpu
-driver-version=3.3.0.2 --gpu-driver-date=2017/04/07 --disable-pack
-loading --lang=en-US --log-file="C:\Program Files (x86)\Adobe\Acro
bat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --pr
oduct-version="ReaderServices/19.10.20064 Chrome/64.0.3282.119" --s
ervice-request-channel-token=894A914DCDDDE9ACB7FCB75FC8BF2012 --moj
o-platform-channel-handle=2296 --allow-no-sandbox-job --ignored=" -
-type=renderer " /prefetch:2
```

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

PID:1944

```
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrC
EF.exe" --type=renderer --disable-browser-side-navigation --disable
-gpu-compositing --service-pipe-token=330FD45D3B11128C416F8F8254611
6CD --lang=en-US --disable-pack-loading --lang=en-US --log-file
="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\deb
ug.log" --log-severity=disable --product-version="ReaderServices/1
9.10.20064 Chrome/64.0.3282.119" --enable-pinch --device-scale-fact
or=1 --num-raster-threads=4 --enable-main-frame-before-activation -
-enable-gpu-async-worker-context --content-image-texture-target=0,
0,3553;0,1,3553;0,2,3553;0,3,3553;0,4,3553;0,5,3553;0,6,3553;0,7,35
53;0,8,3553;0,9,3553;0,10,3553;0,11,3553;0,12,3553;0,13,3553;0,14,3
553;0,15,3553;0,16,3553;0,17,3553;0,18,3553;1,0,3553;1,1,3553;1,2,3
553;1,3,3553;1,4,3553;1,5,3553;1,6,3553;1,7,3553;1,8,3553;1,9,3553;
1,10,3553;1,11,3553;1,12,3553;1,13,3553;1,14,3553;1,15,3553;1,16,35
53;1,17,3553;1,18,3553;2,0,3553;2,1,3553;2,2,3553;2,3,3553;2,4,355
3;2,5,3553;2,6,3553;2,7,3553;2,8,3553;2,9,3553;2,10,3553;2,11,3553;
2,12,3553;2,13,3553;2,14,3553;2,15,3553;2,16,3553;2,17,3553;2,18,35
53;3,0,3553;3,1,3553;3,2,3553;3,3,3553;3,4,3553;3,5,3553;3,6,3553;
3,7,3553;3,8,3553;3,9,3553;3,10,3553;3,11,3553;3,12,3553;3,13,3553;
3,14,3553;3,15,3553;3,16,3553;3,17,3553;3,18,3553;4,0,3553;4,1,355
3;4,2,3553;4,3,3553;4,4,3553;4,5,3553;4,6,3553;4,7,3553;4,8,3553;4,
9,3553;4,10,3553;4,11,3553;4,12,3553;4,13,3553;4,14,3553;4,15,3553;
4,16,3553;4,17,3553;4,18,3553;5,0,3553;5,1,3553;5,2,3553;5,3,3553;
5,4,3553;5,5,3553;5,6,3553;5,7,3553;5,8,3553;5,9,3553;5,10,3553;5,1
1,3553;5,12,3553;5,13,3553;5,14,3553;5,15,3553;5,16,3553;5,17,3553;
5,18,3553;6,0,3553;6,1,3553;6,2,3553;6,3,3553;6,4,3553;6,5,3553;6,
6,3553;6,7,3553;6,8,3553;6,9,3553;6,10,3553;6,11,3553;6,12,3553;6,1
3,3553;6,14,3553;6,15,3553;6,16,3553;6,17,3553;6,18,3553 --disable-
accelerated-video-decode --service-request-channel-token=330FD45D3B
11128C416F8F82546116CD --renderer-client-id=5 --mojo-platform-chann
```

PID:2184

```
AB4AAAQAAAAAAAAAAAGAA --use-gl=swiftshader-webgl --gpu-vendor-id=0x
```

```
1234 --gpu-device-id=0x1111 --gpu-driver-vendor="Google Inc." --gpu
-driver-version=3.3.0.2 --gpu-driver-date=2017/04/07 --disable-pack
-loading --lang=en-US --log-file="C:\Program Files (x86)\Adobe\Acro
bat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --pr
oduct-version="ReaderServices/19.10.20064 Chrome/64.0.3282.119" --s
ervice-request-channel-token=806AFEAC8B00C8FBF5136A5A2BFA186E --moj
o-platform-channel-handle=2664 --allow-no-sandbox-job --ignored=" -
-type=renderer " /prefetch:2
```

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe PID:1384

```
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrC
EF.exe" --type=gpu-process --disable-pack-loading --lang=en-US --lo
g-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroC
EF\debug.log" --log-severity=disable --product-version="ReaderServi
ces/19.10.20064 Chrome/64.0.3282.119" --gpu-preferences=GAAAAAAAAA
AB4AAAQAAAAAAAAAAAGAA --use-gl=swiftshader-webgl --gpu-vendor-id=0x
1234 --gpu-device-id=0x1111 --gpu-driver-vendor="Google Inc." --gpu
-driver-version=3.3.0.2 --gpu-driver-date=2017/04/07 --disable-pack
-loading --lang=en-US --log-file="C:\Program Files (x86)\Adobe\Acro
bat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --pr
oduct-version="ReaderServices/19.10.20064 Chrome/64.0.3282.119" --s
ervice-request-channel-token=42A434A6D17947E90B37C044408D33AB --moj
o-platform-channel-handle=2408 --allow-no-sandbox-job --ignored=" -
-type=renderer " /prefetch:2
```

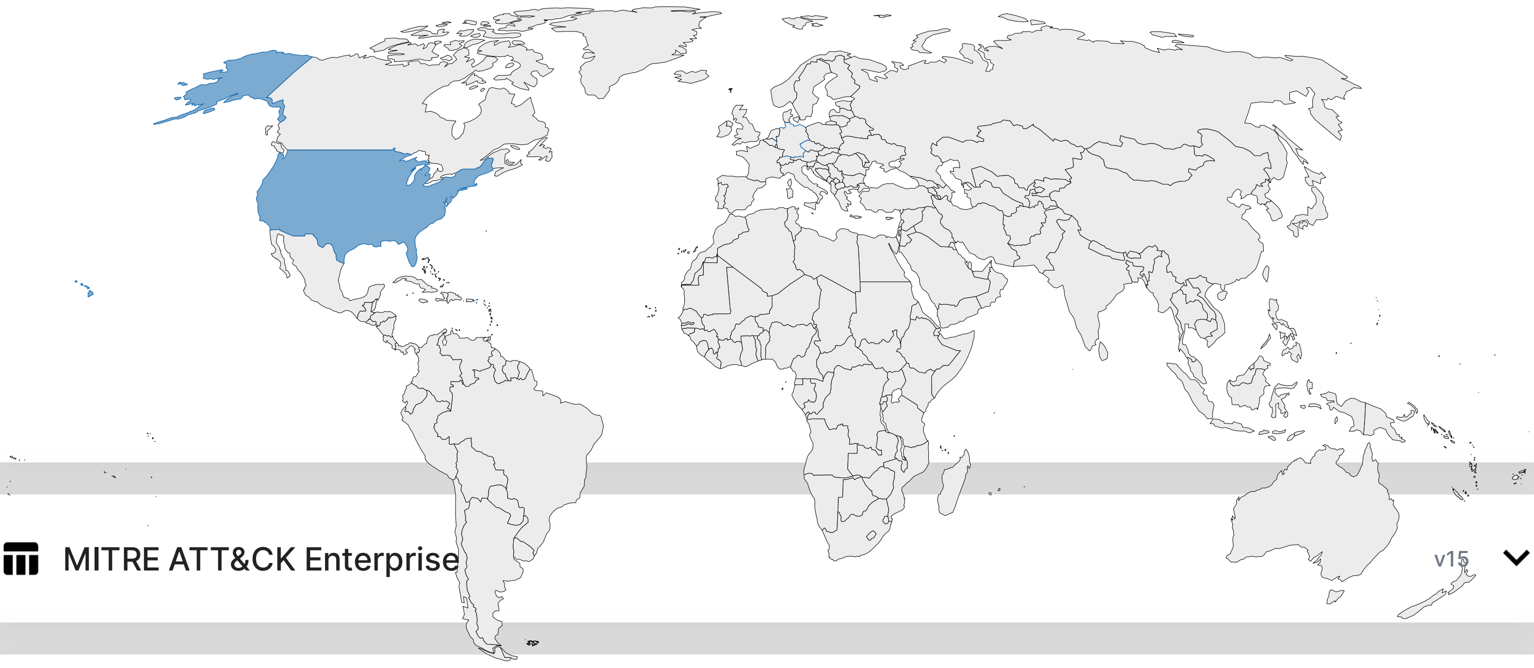
C:\Windows\System32\CompPkgSrv.exe PID:3224

```
C:\Windows\System32\CompPkgSrv.exe -Embedding
```

Network

Requests TCP UDP

🇺🇸	DNS	146.78.124.51.in-addr.arpa	
🇺🇸	DNS	75.159.190.20.in-addr.arpa	
🇺🇸	DNS	95.221.229.192.in-addr.arpa	
🇺🇸	DNS	241.154.82.20.in-addr.arpa	
🇺🇸	DNS	41.110.16.96.in-addr.arpa	
🇺🇸	DNS	57.169.31.20.in-addr.arpa	
🇺🇸	DNS	59.128.231.4.in-addr.arpa	
🇺🇸	DNS	137.0.85.104.in-addr.arpa	
🇺🇸	DNS	139.121.18.2.in-addr.arpa	
🇺🇸	DNS	157.123.68.40.in-addr.arpa	
🇺🇸	DNS	15.164.165.52.in-addr.arpa	
🇩🇪	POST	https://45.131.108.250:1194/Cookbooks/HXvRxx93G6edC?Papilionaceous=dourines	SEARCHPROTOC...
🇺🇸	DNS	254.109.26.67.in-addr.arpa	
🇺🇸	DNS	250.108.131.45.in-addr.arpa	
🇺🇸	DNS	14.227.111.52.in-addr.arpa	
🇺🇸	DNS	tse1.mm.bing.net	
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.10239317301145_1Y8CXK45BT2OHNQQQ&pid=21.2&w=1920&h=1080&c=4	
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.10239317301111_1DKW3SIPELFG6R5I0&pid=21.2&w=1920&h=1080&c=4	
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.10239317301544_150BJDG31FJ0ZNF34&pid=21.2&w=1080&h=1920&c=4	
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.10239317301554_133DWC45UAH2W18HX&pid=21.2&w=1080&h=1920&c=4	
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.10239317300927_1MHQY2TQNUIH7ZQRL&pid=21.2&w=1920&h=1080&c=4	
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.10239317301360_1Q2LDLW388L48JF4Q&pid=21.2&w=1080&h=1920&c=4	
🇺🇸	DNS	26.35.223.20.in-addr.arpa	
🇺🇸	DNS	123.10.44.20.in-addr.arpa	



MITRE ATT&CK Enterprise

v15

Replay Monitor

Downloads

C:\Users\Admin\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages

Filesize	64KB
MD5	17e64be8adeda4467b8ffc7e9e602c0b
SHA1	7dc1ffc21f27e46aeb39cc162f66580f445af891
SHA256	d943b61fdb3ea5e2c1fec7747b2dadb96a650d482cd27686b2064dce40bf0a00
SHA512	982d928ab8f272681a4f0dd0717d6371d916b36a5c24677de0c0f78bd7b52622726b815d1e65add40ea790...

Download

Submit

C:\Users\Admin\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages

Filesize	36KB
MD5	b30d3becc8731792523d599d949e63f5
SHA1	19350257e42d7aee17fb3bf139a9d3adb330fad4
SHA256	b1b77e96279ead2b460de3de70e2ea4f5ad1b853598a4e27a5caf3f1a32cc4f3
SHA512	523f54895fb07f62b9a5f72c8b62e83d4d9506bda57b183818615f6eb7286e3b9c5a50409bc5c5164867c3...

Download

Submit

C:\Users\Admin\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages

Filesize	56KB
MD5	752a1f26b18748311b691c7d8fc20633
SHA1	c1f8e83eebc1cc1e9b88c773338eb09ff82ab862
SHA256	111dac2948e4cecb10b0d2e10d8afaa663d78d643826b592d6414a1fd77cc131
SHA512	a2f5f262faf2c3e9756da94b2c47787ce3a9391b5bd53581578aa9a764449e114836704d6dec4aadc097fed...

Download

Submit

memory/1268-35-0×000000000A5F0000-0×000000000A611000-memory.dmp

Filesize	132KB

Download

memory/1268-171-0×000000000B8B0000-0×000000000BB5B000-memory.dmp

Filesize	2.7MB

Download

memory/1740-5-0×0000000000C20000-0×0000000000C6B000-memory.dmp

Filesize	300KB

Download

memory/1740-40-0×0000000000C20000-0×0000000000C6B000-memory.dmp

Filesize	300KB

Download

memory/1740-4-0×0000000000C20000-0×0000000000C6B000-memory.dmp

Filesize	300KB

Download

memory/1740-2-0×0000000000C20000-0×0000000000C6B000-memory.dmp

Filesize	300KB

Download

memory/1740-138-0×0000000000C20000-0×0000000000C6B000-memory.dmp

Filesize	300KB

Download

memory/1740-146-0×0000000000C20000-0×0000000000C6B000-memory.dmp

Filesize	300KB

Download

memory/1740-153-0×0000000000C20000-0×0000000000C6B000-memory.dmp

Filesize	300KB

Download

memory/3692-6-0×0000000002E00000-0×0000000002ED1000-memory.dmp

Filesize	836KB

Download

memory/3692-0-0×0000000002C50000-0×0000000002D13000-memory.dmp

Filesize	780KB

Download

memory/3692-1-0×0000000002E00000-0×0000000002ED1000-memory.dmp

Filesize	836KB

Download

Recorded Future®

Terms | Privacy