ID: 800792
Sample Name: VGPINVPA.dll
Cookbook: default.jbs
Time: 19:57:57
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

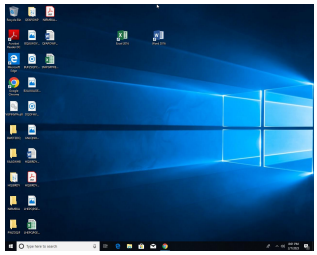
Windows Analysis Report

VGPINVPA.dll

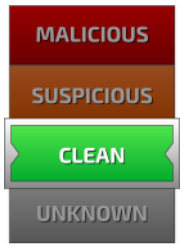
Overview

General Information

Sample Name:	VGPINVPA.dll
Analysis ID:	800792
MD5:	20993d0e3f4ce..
SHA1:	e1ad60184a03...
SHA256:	be9f858306daf...
Infos:	



Detection

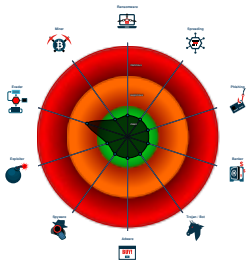


Score:	3
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sample execution stops while proce...
- PE file does not import any functions
- Sample file is different than original ...
- May sleep (evasive loops) to hinder...
- Program does not show much activi...
- Creates a process in suspended mo...

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 2104 cmdline: loaddll64.exe "C:\Users\user\Desktop\VGPINVPA.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 1552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 3508 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5128 cmdline: rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - conhost.exe (PID: 5164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 3732 cmdline: rundll32.exe C:\Users\user\Desktop\VGPINVPA.dll,AllocConsole MD5: 73C519F050C20580F8A62C849D49215A)
    - conhost.exe (PID: 5152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 5236 cmdline: rundll32.exe C:\Users\user\Desktop\VGPINVPA.dll,GetConsoleCP MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5252 cmdline: rundll32.exe C:\Users\user\Desktop\VGPINVPA.dll,GetConsoleMode MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5272 cmdline: rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",AllocConsole MD5: 73C519F050C20580F8A62C849D49215A)
    - conhost.exe (PID: 5300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 5280 cmdline: rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",GetConsoleCP MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5308 cmdline: rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",GetConsoleMode MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5336 cmdline: rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",GetConsoleOutputCP MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5360 cmdline: rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",GetNumberOfConsoleInputEvents MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

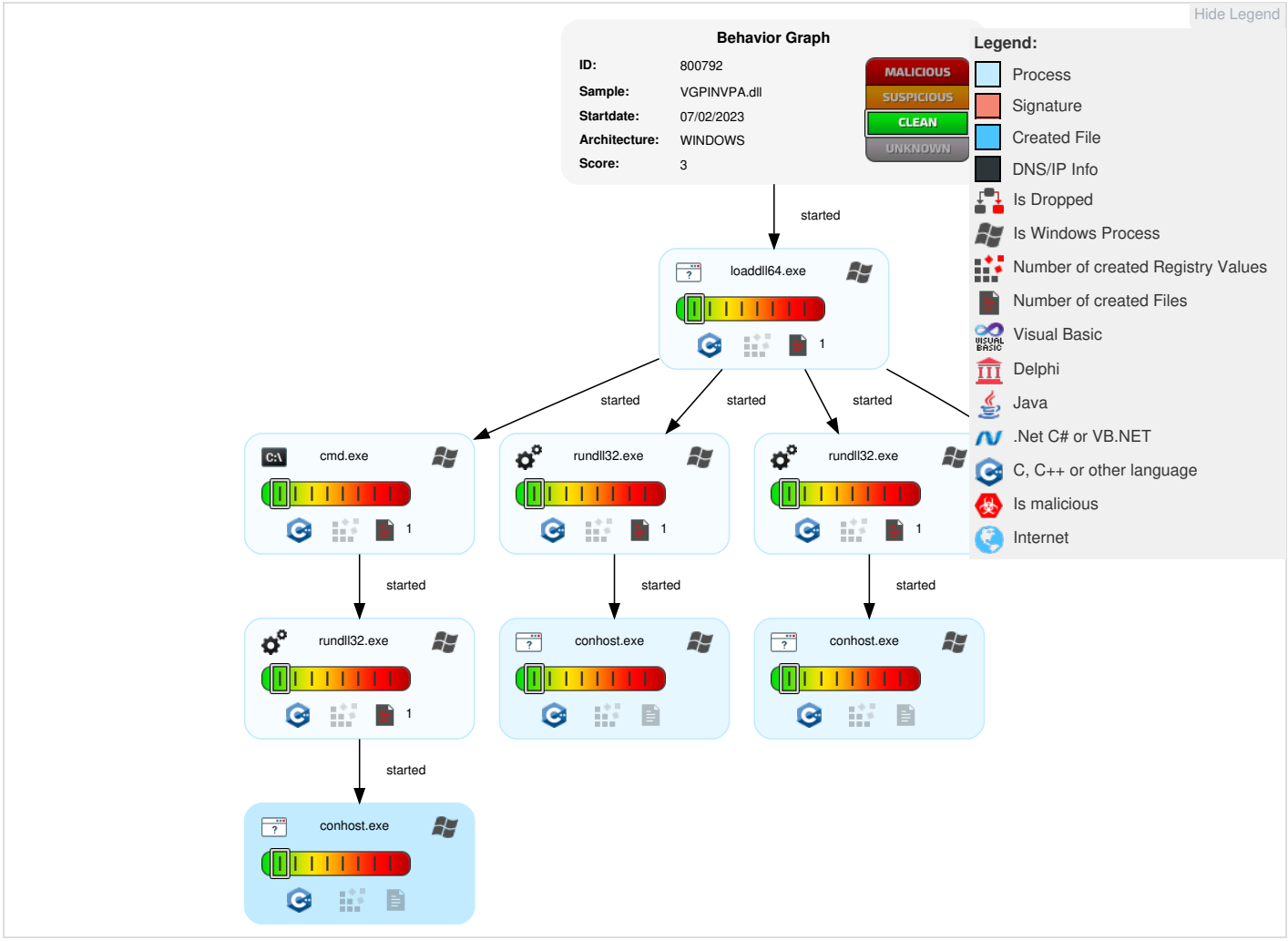
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Rundll32	OS Credential Dumping	1 1 Virtualization/Sandbox Evasion	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

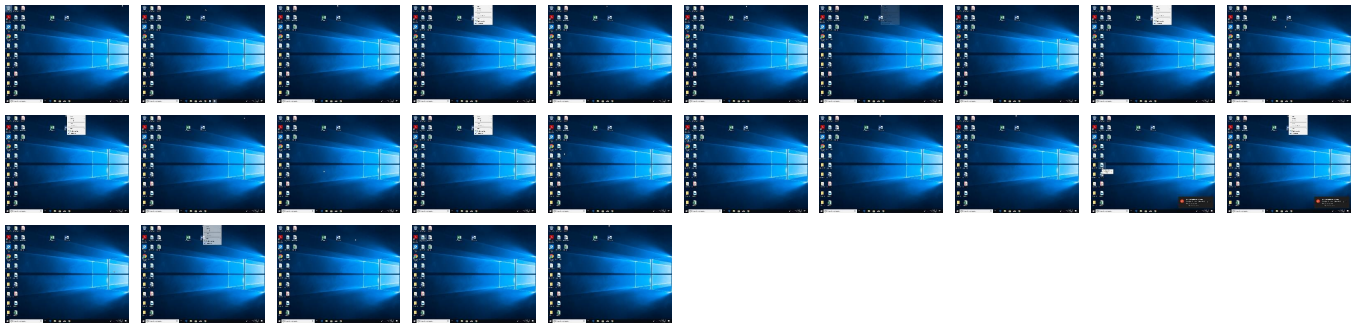
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
VGPINVPA.dll	0%	ReversingLabs		
VGPINVPA.dll	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800792
Start date and time:	2023-02-07 19:57:57 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	VGPINVPA.dll
Detection:	CLEAN
Classification:	clean3.winDLL@25/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	6.889593778286631
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	VGPINVPA.dll
File size:	12800
MD5:	20993d0e3f4ce09f39cd119624f3541d
SHA1:	e1ad60184a03f48217ab48742b1e2e141272d829
SHA256:	be9f858306daf9c886fbe579db2f788a21a5531c7d0028b6d663fac43ffaeb0c
SHA512:	1997c07f0cec3df29a849c1a950ffe80b9c3259d73a43b8a90cc99341fbdfb123f7d6825a5ed1020607261aa5ddd8c089ec3a2ba4bed8c4904fb8e95d445dd33
SSDEEP:	192:PZWVghWcRlYiYF8r7S4maIYiYF8r7SvOjuFW:RW2hWoIYiE4maIYiE22W
TLSH:	12422BA74DE84C20ECA78E30BCE0D03ABA75BD5155A0C2C9327D822997D63406F6D3BD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....](S....A.+S....^.(S....C. (S..Rich)S.....PE..d...48.U....." .....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180000000

Entrypoint Section:	
Digitally signed:	true
Imagebase:	0x180000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x559F3834 [Fri Jul 10 03:12:52 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	10
OS Version Minor:	0
File Version Major:	10
File Version Minor:	0
Subsystem Version Major:	10
Subsystem Version Minor:	0
Import Hash:	

Authenticode Signature	
Signature Valid:	**true**
Signature Issuer:	CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 1/31/2022 4:00:00 PM 2/1/2023 3:59:59 PM
Subject Chain	• CN="Private Internet Access, Inc.", O="Private Internet Access, Inc.", L=Greenwood Village, S=Colorado, C=US
Version:	3
Thumbprint MD5:	C5A421483E5E755C987295DBBBBAC713
Thumbprint SHA-1:	25743ED6B96AD266058E0252ED0E0775A35F382B
Thumbprint SHA-256:	5853D76E78D6A621C3FAABCB26587E1EC1DDACBBC4F38A8F7AEBDE55A2B3BA7E
Serial:	07F18D9C7FE1F1BAA5F95C745C110598

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1060	0x32b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2000	0x3e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xe00	0x2400	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1000	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x1000	0x440	0x600	False	0.2923177083333333	Matlab v4 mat-file (little endian) \214\023, numeric, rows 1436497972, columns 0, imaginary	3.8377787933674052	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2000	0x3e8	0x400	False	0.4404296875	data	3.2940915718481807	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2060	0x384	data	English	United States

Exports

Name	Ordinal	Address
AllocConsole	1	0x180001144
GetConsoleCP	2	0x180001167
GetConsoleMode	3	0x18000118c
GetConsoleOutputCP	4	0x1800011b7
GetNumberOfConsoleInputEvents	5	0x1800011f1
PeekConsoleInputA	6	0x18000122a
ReadConsoleA	7	0x180001252
ReadConsoleInputA	8	0x18000127a
ReadConsoleInputW	9	0x1800012a7
ReadConsoleW	10	0x1800012cf
SetConsoleCtrlHandler	11	0x1800012fb
SetConsoleMode	12	0x180001329
WriteConsoleA	13	0x18000134f
WriteConsoleW	14	0x180001374

Possible Origin

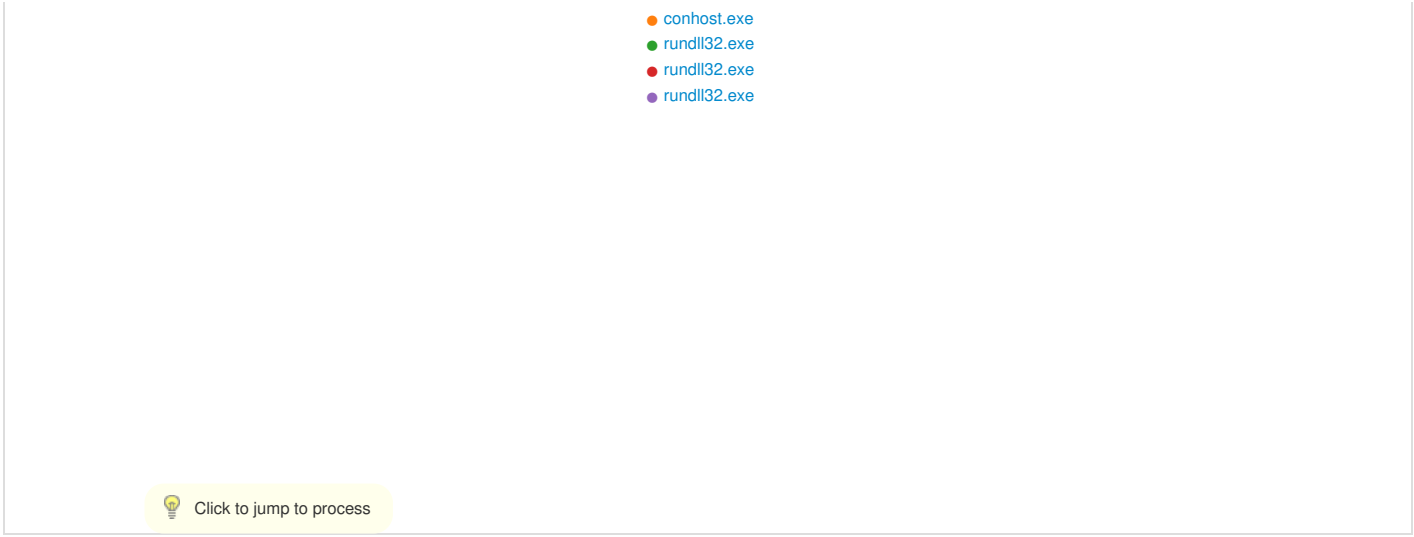
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 2104, Parent PID: 3452

General

Target ID:	0
Start time:	19:58:57
Start date:	07/02/2023
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\VGPINVPA.dll"
Imagebase:	0x7ff6ccf30000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1552, Parent PID: 2104

General

Target ID:	1
Start time:	19:58:57
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: cmd.exe PID: 3508, Parent PID: 2104

General

Target ID:	2
Start time:	19:58:58
Start date:	07/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",#1
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3732, Parent PID: 2104

General

Target ID:	3
Start time:	19:58:58
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\VGPINVPA.dll,AllocConsole
Imagebase:	0x7ff758ae0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5128, Parent PID: 3508

General

Target ID:	4
Start time:	19:58:58
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",#1
Imagebase:	0x7ff758ae0000

File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5152, Parent PID: 3732

General

Target ID:	5
Start time:	19:58:58
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5164, Parent PID: 5128

General

Target ID:	6
Start time:	19:58:58
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5236, Parent PID: 2104

General

Target ID:	7
Start time:	19:59:01
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\VGPINVPA.dll,GetConsoleCP
Imagebase:	0x7ff758ae0000
File size:	69632 bytes

MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **5252**, Parent PID: **2104**

General

Target ID:	8
Start time:	19:59:04
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\VGPINVPA.dll,GetConsoleMode
Imagebase:	0x7ff758ae0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **5272**, Parent PID: **2104**

General

Target ID:	9
Start time:	19:59:07
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",AllocConsole
Imagebase:	0x7ff758ae0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5280**, Parent PID: **2104**

General

Target ID:	10
Start time:	19:59:07
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",GetConsoleCP
Imagebase:	0x7ff758ae0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5300**, Parent PID: **5272**

General	
Target ID:	11
Start time:	19:59:07
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **5308**, Parent PID: **2104**

General	
Target ID:	12
Start time:	19:59:07
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",GetConsoleMode
Imagebase:	0x7ff758ae0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **5336**, Parent PID: **2104**

General	
Target ID:	13
Start time:	19:59:07
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",GetConsoleOutputCP
Imagebase:	0x7ff758ae0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **5360**, Parent PID: **2104**

General	
Target ID:	14

Start time:	19:59:08
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\VGPINVPA.dll",GetNumberOfConsoleInputEvents
Imagebase:	0x7ff758ae0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly