ID: 652394
Sample Name:
p3jNeWT0GE.exe
Cookbook: default.jbs
Time: 09:43:28
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

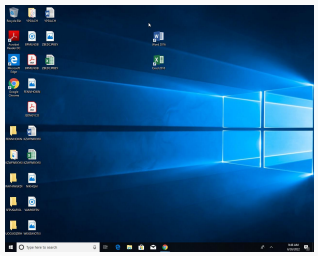
Windows Analysis Report

p3jNeWT0GE.exe

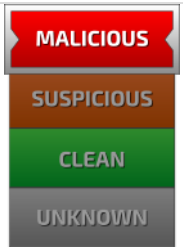
Overview

General Information

Sample Name:	p3jNeWT0GE.exe
Analysis ID:	652394
MD5:	25b54f50600604..
SHA1:	be28d831c51833..
SHA256:	9904784c707abb..
Tags:	Dofoil exe SmokeLoader
Infos:	



Detection



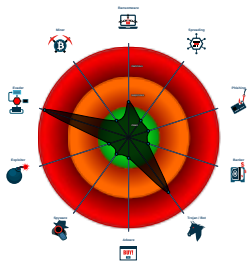
SmokeLoader

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

Signatures

- Benign windows process drops PE f…
- Yara detected SmokeLoader
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Checks for kernel code integrity (NtQ…
- Contains functionality to inject code…
- Deletes itself after installation
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- p3jNeWT0GE.exe (PID: 6516 cmdline: "C:\Users\user\Desktop\p3jNeWT0GE.exe" MD5: 25B54F50600604A53E80163B9049421E)
  - p3jNeWT0GE.exe (PID: 6648 cmdline: "C:\Users\user\Desktop\p3jNeWT0GE.exe" MD5: 25B54F50600604A53E80163B9049421E)
    - explorer.exe (PID: 3808 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- hdgaecu (PID: 7136 cmdline: C:\Users\user\AppData\Roaming\hdgaecu MD5: 25B54F50600604A53E80163B9049421E)
  - hdgaecu (PID: 5244 cmdline: C:\Users\user\AppData\Roaming\hdgaecu MD5: 25B54F50600604A53E80163B9049421E)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader

```
{
  "C2 list": [
    "http://host-file-host6.com/",
    "http://host-host-file8.com/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.415791287.0000000002681000.00000020.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000D.00000002.501978878.0000000002051000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.442558438.0000000001E51000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000D.00000002.501732921.00000000004B0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.442516398.0000000001E30000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.p3jNeWT0GE.exe.c215a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
12.2.hdgaecu.c215a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.2.p3jNeWT0GE.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
13.2.hdgaecu.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- System process connects to network (likely due to code injection or exploit)
- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Yara detected SmokeLoader

Hooking and other Techniques for Hiding and Protection

- Deletes itself after installation
- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected SmokeLoader

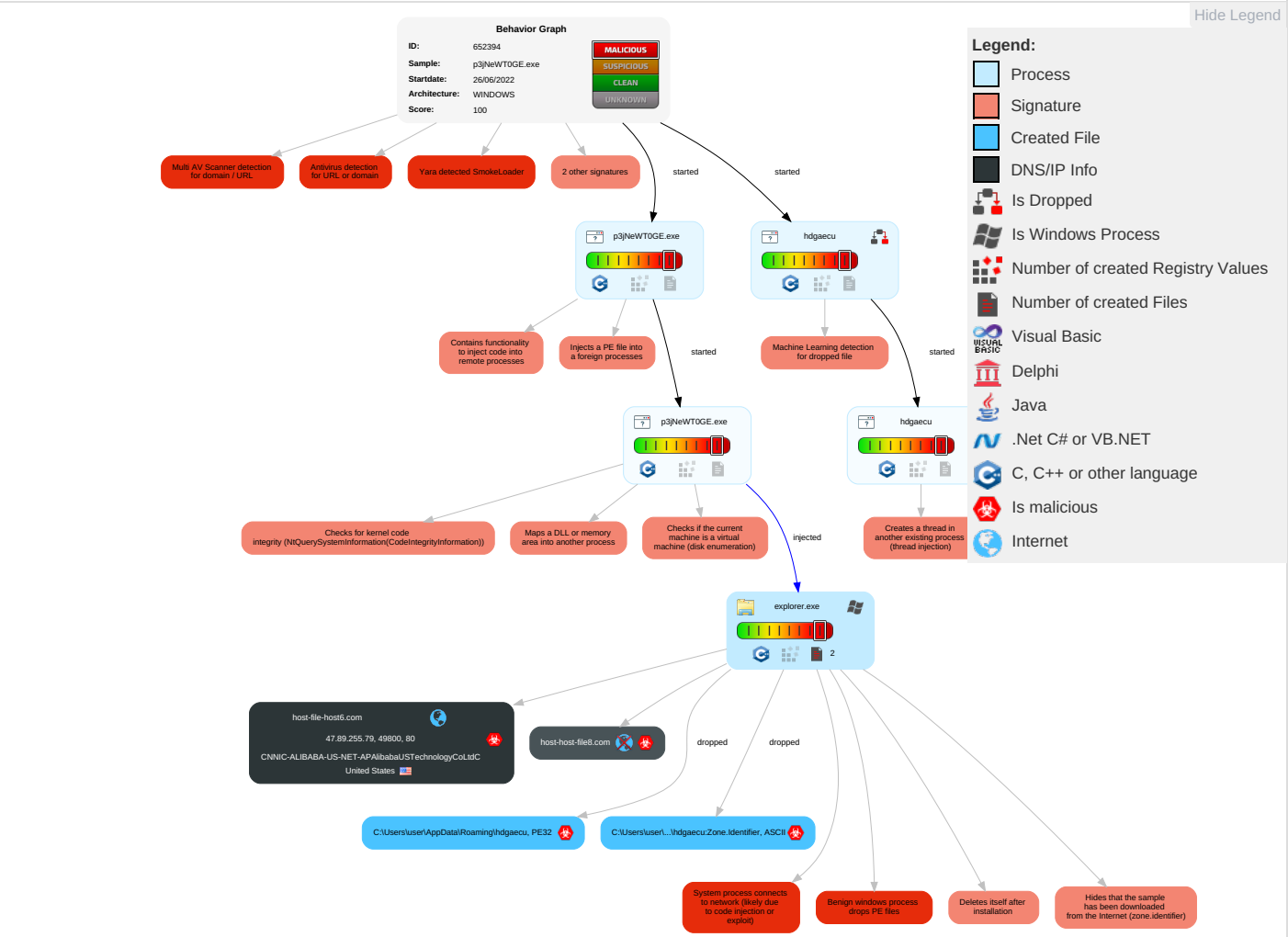
Remote Access Functionality

Yara detected SmokeLoader

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	2 Native API	1 DLL Side-Loading	5 1 2 Process Injection	1 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 2 Virtualization/Sandbox Evasion	LSASS Memory	2 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	5 1 2 Process Injection	Security Account Manager	1 2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Hidden Files and Directories	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 File Deletion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
p3jNeWT0GE.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\hdgaecu	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.p3jNeWT0GE.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.p3jNeWT0GE.exe.c215a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.hdgaecu.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.hdgaecu.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.hdgaecu.c215a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.p3jNeWT0GE.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.p3jNeWT0GE.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.hdgaecu.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.p3jNeWT0GE.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.hdgaecu.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
host-file-host6.com	18%	Virustotal		Browse
host-host-file8.com	13%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ns.adobY	0%	URL Reputation	safe	
http://host-file-host6.com/	0%	URL Reputation	safe	
http://host-host-file8.com/	100%	URL Reputation	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host-file-host6.com	47.89.255.79	true	true	• 18%, Virustotal, Browse	unknown
host-host-file8.com	unknown	unknown	true	• 13%, Virustotal, Browse	unknown

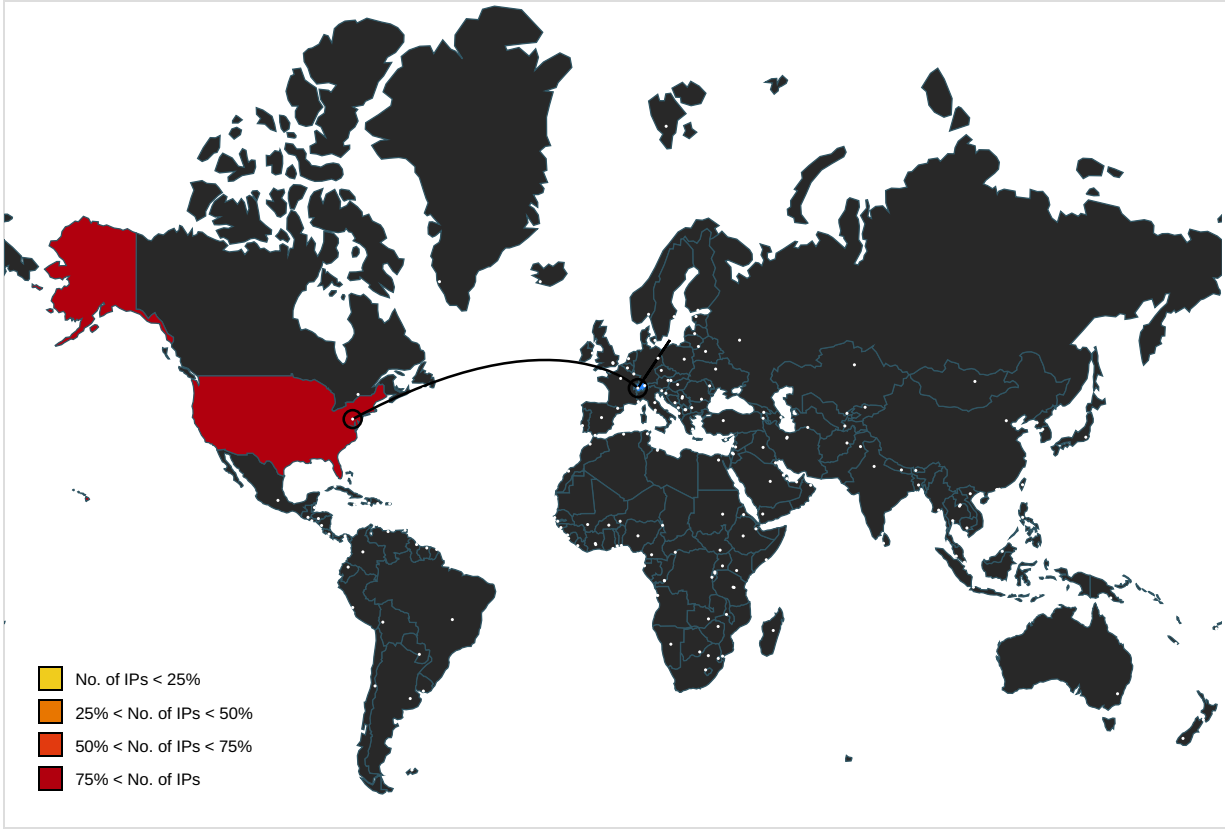
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://host-file-host6.com/	true	• URL Reputation: safe	unknown
http://host-host-file8.com/	true	• URL Reputation: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobY	explorer.exe, 00000004.00000000.39711442 5.00000000026D0000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000000.374277431.00000000026D0000. 00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.89.255.79	host-file-host6.com	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	652394
Start date and time: 26/06/202209:43:28	2022-06-26 09:43:28 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	p3jNeWT0GE.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/2@5/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 78.9% (good quality ratio 69.7%) • Quality average: 57.7% • Quality standard deviation: 32.1%

HCA Information:	• Successful, ratio: 70% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
09:45:40	Task Scheduler	Run new task: Firefox Default Browser Agent 48F1ADA0A38E1F04 path: C:\Users\user\AppData\Roaming\hdgaecu

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\hdgaecu

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	293376
Entropy (8bit):	6.884791106060294
Encrypted:	false
SSDEEP:	6144:HShclg/jkSrmFybCvqYNOpd5I165kcpe1+JAtGI8E2lxiz:yCllImFO4qYNGI45kM2+JAtdyni
MD5:	25B54F50600604A53E80163B9049421E

SHA1:	BE28D831C5183368F057F8BEC104A2B0BABB406C
SHA-256:	9904784C707ABB24585E3E61FA5CC094380206385CBB7D087C968D7DC5EE0991
SHA-512:	3CBE8FAB28D77F7E7477C31DD3FC69E930FD3BE72B20411CC077592440E6EA487D3EDA66EBACE44C0C58FD35A9FC1AE5F1C3FB563FFAE33658930525DCB69027
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-\..i=..i=..i=...r..h=..wo..v=..wo...=..N...j=..i=...=..wo..V=..wo..h=..wo..h=..Richi=.....PE..L.....`.....p.....0....@.....s.....(@.....(....`s..?.....P..... ...@.....text..... ..`.data.....p..0.....@....zineha.K....@s.....6.....@....cixu...J....Ps.....8.....@....rsrc....?...`s..@...:. .....@..@..... .....

C:\Users\user\AppData\Roaming\hdgaecu:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.884791106060294
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	p3jNeWT0GE.exe
File size:	293376
MD5:	25b54f50600604a53e80163b9049421e
SHA1:	be28d831c5183368f057f8bec104a2b0babb406c
SHA256:	9904784c707abb24585e3e61fa5cc094380206385cbb7d087c968d7dc5ee0991
SHA512:	3cbe8fab28d77f7e7477c31dd3fc69e930fd3be72b20411cc077592440e6ea487d3eda66ebace44c0c58fd35a9fc1ae5f1c3fb563ffae33658930525dcb69027
SSDEEP:	6144:HShclg/jkSrmFybCvqYNOpd5I165kcpe1+JAtGI8E2lxiz:yCIlmFO4qYNGI45kM2+JAtdyni
TLSH:	32549E10B650C434F5F712F44ABA926CB63E7AA19B3491CF62D56AEE5B346E0EC31307
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....- \..i=..i=..i=...r..h=..wo..v=..wo...=..N...j=..i=...=..wo..V=..wo..h=..wo..h=..Richi=.....PE..L.....`...

File Icon

Icon Hash:	aecaae9ecea62ea2

Static PE Info

General

Entrypoint:	0x40eec0

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x608DF612 [Sun May 2 00:45:06 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	9708e7dbb84fb2e34dfb5e05eada89dd

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007F93ECC81C1Bh
call 00007F93ECC74586h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 00430CA0h
push 00412510h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h
push ebx
push esi
push edi
mov eax, dword ptr [0044387Ch]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp

Instruction
mov dword ptr [ebp-70h], 00000000h
mov dword ptr [ebp-04h], 00000000h
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [004010DCh]
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007F93ECC74598h
mov eax, 00000001h
ret
mov esp, dword ptr [ebp-18h]
mov dword ptr [ebp-78h], 000000FFh
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, dword ptr [ebp-78h]
jmp 00007F93ECC746C8h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007F93ECC74704h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007F93ECC82CDAh
add esp, 04h
test eax, eax
jne 00007F93ECC7457Ch
push 0000001Ch
call 00007F93ECC746BCh
add esp, 04h
call 00007F93ECC7C304h
test eax, eax
jne 00007F93ECC7457Ch
push 00000010h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x313bc	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x736000	0x3f98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1350	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xb2f0	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x2fc	.text
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x315ac	0x31600	False	0.45167128164556963	data	6.39681715338854	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x33000	0x700da8	0x11c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.zineha	0x734000	0x4b	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.cixu	0x735000	0x4a	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x736000	0x3f98	0x4000	False	0.73095703125	data	6.341519681079148	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7361f0	0x25a8	data	Korean	North Korea
RT_ICON	0x7361f0	0x25a8	data	Korean	South Korea
RT_ICON	0x738798	0x10a8	data	Korean	North Korea
RT_ICON	0x738798	0x10a8	data	Korean	South Korea
RT_STRING	0x739918	0x42	data	Korean	North Korea
RT_STRING	0x739918	0x42	data	Korean	South Korea
RT_STRING	0x739960	0x4ae	data	Korean	North Korea
RT_STRING	0x739960	0x4ae	data	Korean	South Korea
RT_STRING	0x739e10	0x188	data	Korean	North Korea
RT_STRING	0x739e10	0x188	data	Korean	South Korea
RT_ACCELERATOR	0x7398a8	0x70	data	Korean	North Korea
RT_ACCELERATOR	0x7398a8	0x70	data	Korean	South Korea
RT_ACCELERATOR	0x739868	0x40	data	Korean	North Korea
RT_ACCELERATOR	0x739868	0x40	data	Korean	South Korea
RT_GROUP_ICON	0x739840	0x22	data	Korean	North Korea
RT_GROUP_ICON	0x739840	0x22	data	Korean	South Korea

Imports

DLL	Import

DLL	Import
KERNEL32.dll	DebugBreakProcess, FindFirstChangeNotificationW, GetNamedPipeHandleStateW, CreateIoCompletionPort, FillConsoleOutputCharacterW, DisableThreadLibraryCalls, TerminateProcess, GetProcessId, VerifyVersionInfoW, EnumDateFormatsW, FindNextFileW, CopyFileExA, BuildCommDCBAndTimeoutsA, VirtualUnlock, WriteProfileStringW, VerifyVersionInfoA, SetProcessPriorityBoost, GetDriveTypeW, FindFirstChangeNotificationA, GetFileType, DeleteFileA, FindNextVolumeMountPointA, OutputDebugStringA, ResetWriteWatch, WriteConsoleInputA, WriteConsoleInputW, GetConsoleTitleW, SetComputerNameExW, SetTimeZoneInformation, LoadLibraryA, GetSystemDirectoryA, GetDriveTypeA, GetShortPathNameW, ActivateActCtx, GetProfileSectionA, DeleteFileW, GetCommandLineW, InterlockedIncrement, AddRefActCtx, FindResourceA, FormatMessageA, GetModuleFileNameW, CreateJobObjectW, InitializeCriticalSection, SetFirmwareEnvironmentVariableW, GetDllDirectoryW, GetExitCodeThread, WritePrivateProfileStringW, GetConsoleAliasesLengthW, WriteProfileSectionW, AddAtomA, InterlockedDecrement, GetVersionExA, HeapSize, _hwrite, GetStartupInfoA, DisconnectNamedPipe, GetCPInfoExW, GetSystemWow64DirectoryW, GetPrivateProfileIntA, GetConsoleAliasExesW, DebugBreak, EndUpdateResourceW, SetLastError, InterlockedExchangeAdd, GetStringTypeExW, DeleteVolumeMountPointW, OpenFileMappingA, SetDefaultCommConfigW, lstrcpyA, TerminateThread, GetACP, _lwrite, GetQueuedCompletionStatus, GetNamedPipeHandleStateA, GetDiskFreeSpaceExW, RemoveVectoredExceptionHandler, WriteConsoleW, VirtualProtect, ReadConsoleOutputW, SetThreadContext, BuildCommDCBA, ReleaseActCtx, GetHandleInformation, WritePrivateProfileSectionW, DeleteCriticalSection, GetFileAttributesA, OpenWaitableTimerW, GetVolumePathNameW, SetConsoleMode, HeapSetInformation, SetComputerNameA, FindNextFileA, SetEvent, UnlockFile, GetProcAddress, DeleteTimerQueueTimer, CopyFileW, MoveFileA, GlobalAlloc, GetCommMask, SetFileShortNameA, GetFileAttributesW, FreeEnvironmentStringsW, GetProfileStringA, GetConsoleTitleA, SetComputerNameW, GetConsoleAliasesW, CreateMailslotA, EnumDateFormatsA, GetTimeZoneInformation, SetConsoleOutputCP, GetFileInformationByHandle, SetLocalTime, CallNamedPipeA, GetConsoleAliasExesLengthW, GetCurrentActCtx, OpenSemaphoreW, GetModuleHandleExA, LoadLibraryW, FoldStringW, GetTickCount, GetConsoleAliasesLengthA, GetLastError, LocalUnlock, GetFileTime, EnumResourceNamesW, OpenFileMappingW, UnhandledExceptionFilter, GetCompressedFileSizeW, GetThreadPriority, ReadConsoleA, AssignProcessToJobObject, Sleep, EnterCriticalSection, LeaveCriticalSection, RaiseException, RtlUnwind, GetCurrentProcess, SetUnhandledExceptionFilter, IsDebuggerPresent, WideCharToMultiByte, GetCommandLineA, HeapValidate, IsBadReadPtr, GetModuleHandleA, TlsGetValue, GetModuleHandleW, TlsAlloc, TlsSetValue, GetCurrentThreadId, TlsFree, GetStdHandle, WriteFile, OutputDebugStringW, ExitProcess, GetOEMCP, GetCPInfo, IsValidCodePage, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, HeapDestroy, HeapCreate, HeapFree, VirtualFree, FlushFileBuffers, GetConsoleCP, GetConsoleMode, HeapAlloc, HeapReAlloc, VirtualAlloc, InitializeCriticalSectionAndSpinCount, MultiByteToWideChar, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, LCMapStringA, LCMapStringW, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, SetFilePointer, CloseHandle, CreateFileA

Possible Origin

Language of compilation system	Country where language is spoken	Map
Korean	North Korea	
Korean	South Korea	

Network Behavior

Network Port Distribution

Total Packets: 11

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:45:40.786709070 CEST	49800	80	192.168.2.7	47.89.255.79
Jun 26, 2022 09:45:40.966763973 CEST	80	49800	47.89.255.79	192.168.2.7
Jun 26, 2022 09:45:40.966864109 CEST	49800	80	192.168.2.7	47.89.255.79
Jun 26, 2022 09:45:40.966998100 CEST	49800	80	192.168.2.7	47.89.255.79
Jun 26, 2022 09:45:40.967025042 CEST	49800	80	192.168.2.7	47.89.255.79
Jun 26, 2022 09:45:41.150403023 CEST	80	49800	47.89.255.79	192.168.2.7
Jun 26, 2022 09:45:41.516522884 CEST	80	49800	47.89.255.79	192.168.2.7
Jun 26, 2022 09:45:41.516628981 CEST	49800	80	192.168.2.7	47.89.255.79
Jun 26, 2022 09:45:41.526240110 CEST	49800	80	192.168.2.7	47.89.255.79
Jun 26, 2022 09:45:41.707974911 CEST	80	49800	47.89.255.79	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:45:40.467047930 CEST	51824	53	192.168.2.7	8.8.8.8
Jun 26, 2022 09:45:40.779170990 CEST	53	51824	8.8.8.8	192.168.2.7
Jun 26, 2022 09:45:41.537991047 CEST	65214	53	192.168.2.7	8.8.8.8
Jun 26, 2022 09:45:42.543178082 CEST	65214	53	192.168.2.7	8.8.8.8
Jun 26, 2022 09:45:43.574409962 CEST	65214	53	192.168.2.7	8.8.8.8
Jun 26, 2022 09:45:45.621850967 CEST	65214	53	192.168.2.7	8.8.8.8
Jun 26, 2022 09:45:45.624289036 CEST	53	65214	8.8.8.8	192.168.2.7
Jun 26, 2022 09:45:46.609745979 CEST	53	65214	8.8.8.8	192.168.2.7
Jun 26, 2022 09:45:47.613452911 CEST	53	65214	8.8.8.8	192.168.2.7
Jun 26, 2022 09:45:49.680742979 CEST	53	65214	8.8.8.8	192.168.2.7

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jun 26, 2022 09:45:46.609853983 CEST	192.168.2.7	8.8.8.8	cffa	(Port unreachable)	Destination Unreachable
Jun 26, 2022 09:45:47.613527060 CEST	192.168.2.7	8.8.8.8	cffa	(Port unreachable)	Destination Unreachable
Jun 26, 2022 09:45:49.680871010 CEST	192.168.2.7	8.8.8.8	cffa	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:45:40.467047930 CEST	192.168.2.7	8.8.8.8	0x7150	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:41.537991047 CEST	192.168.2.7	8.8.8.8	0xae74	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:42.543178082 CEST	192.168.2.7	8.8.8.8	0xae74	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:43.574409962 CEST	192.168.2.7	8.8.8.8	0xae74	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:45.621850967 CEST	192.168.2.7	8.8.8.8	0xae74	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:45:40.779170990 CEST	8.8.8.8	192.168.2.7	0x7150	No error (0)	host-file-host6.com		47.89.255.79	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:45.624289036 CEST	8.8.8.8	192.168.2.7	0xae74	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:46.609745979 CEST	8.8.8.8	192.168.2.7	0xae74	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:47.613452911 CEST	8.8.8.8	192.168.2.7	0xae74	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:49.680742979 CEST	8.8.8.8	192.168.2.7	0xae74	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- xcxakxdec.net
  - host-file-host6.com

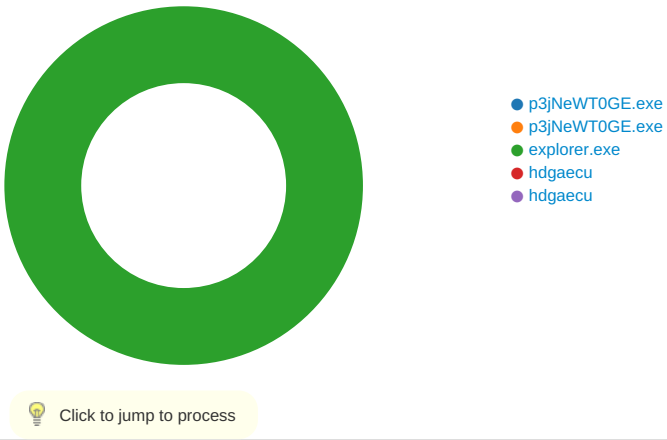
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49800	47.89.255.79	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 26, 2022 09:45:40.966998100 CEST	1413	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xcxakxdec.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 282 Host: host-file-host6.com
Jun 26, 2022 09:45:41.516522884 CEST	3953	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 26 Jun 2022 07:45:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Data Raw: 66 0d 0a 59 6f 75 72 20 49 50 20 62 6c 6f 63 6b 65 64 0d 0a 30 0d 0a 0d 0a Data Ascii: fYour IP blocked0

Statistics

Behavior



System Behavior

Analysis Process: p3jNeWT0GE.exe PID: **6516**, Parent PID: **5656**

General

Target ID:	0
Start time:	09:44:39
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\p3jNeWT0GE.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\p3jNeWT0GE.exe"
Imagebase:	0x400000
File size:	293376 bytes
MD5 hash:	25B54F50600604A53E80163B9049421E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: p3jNeWT0GE.exe PID: **6648**, Parent PID: **6516**

General

Target ID:	1
Start time:	09:44:44
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\p3jNeWT0GE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\p3jNeWT0GE.exe"
Imagebase:	0x400000
File size:	293376 bytes
MD5 hash:	25B54F50600604A53E80163B9049421E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.442558438.0000000001E51000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.442516398.0000000001E30000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: **3808**, Parent PID: **6648**

General

Target ID:	4
Start time:	09:44:52
Start date:	26/06/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff631f70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000000.415791287.0000000002681000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hdgaecu	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	2681F42	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hdgaecu\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2681F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\p3jNeWT0GE.exe	success or wait	1	2681F53	DeleteFileW
C:\Users\user\AppData\Roaming\hdgaecu:Zone.Identifier	success or wait	1	2681F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hdgaecu	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 2d 5c fd fd 69 3d fd fd 69 3d fd fd 69 3d fd fd fd 72 12 fd 68 3d fd fd 77 6f 11 fd 76 3d fd fd 77 6f 07 fd fd 3d fd fd 4e fd fd fd 6a 3d fd fd 69 3d fd fd fd 3d fd fd 77 6f 00 fd 56 3d fd fd 77 6f 10 fd 68 3d fd fd 77 6f 15 fd 68 3d fd fd 52 69 63 68 69 3d fd fd 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 50 45 00 00 4c 01 05 00 12 fd fd 60 00 00 00	MZ@!L!This program cannot be run in DOS mode.$-\i=i=i=rh=wov =wo=Nj=i==woV=woh=w oh=Richi=PEL`	success or wait	3	2681F42	CopyFileW
C:\Users\user\AppData\Roaming\hdgaecu:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	2681F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: hdgaecu

PID: **7136**, Parent PID: **1108**

General

Target ID:	12
Start time:	09:45:40
Start date:	26/06/2022
Path:	C:\Users\user\AppData\Roaming\hdgaecu
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hdgaecu
Imagebase:	0x400000
File size:	293376 bytes
MD5 hash:	25B54F50600604A53E80163B9049421E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: hdgaecu PID: **5244**, Parent PID: **7136**

General	
Target ID:	13
Start time:	09:45:43
Start date:	26/06/2022
Path:	C:\Users\user\AppData\Roaming\hdgaecu
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hdgaecu
Imagebase:	0x400000
File size:	293376 bytes
MD5 hash:	25B54F50600604A53E80163B9049421E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.501978878.0000000002051000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.501732921.00000000004B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly