ID: 736208
Sample Name:
IVO2cpEukR.exe
Cookbook: default.jbs
Time: 18:28:46
Date: 02/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

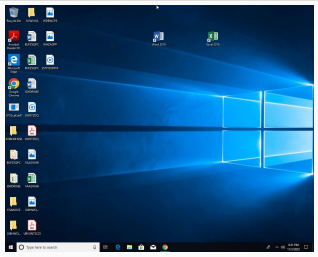
Windows Analysis Report

IVO2cpEukR.exe

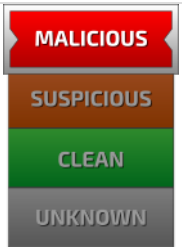
Overview

General Information

Sample Name:	IVO2cpEukR.exe
Analysis ID:	736208
MD5:	6738634d9b3bfc..
SHA1:	f08091a4b3f5c16..
SHA256:	8c77759eff69330..
Tags:	exe LaplasClipper
Infos:	



Detection



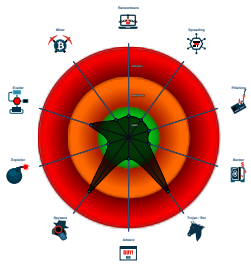
Laplas Clipper, MicroClip

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected MicroClip
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected Laplas Clipper
- Uses schtasks.exe or at.exe to add…
- Drops PE files
- PE file contains sections with non-s…
- Sample execution stops while proce…
- Creates a process in suspended mo…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- IVO2cpEukR.exe (PID: 4544 cmdline: C:\Users\user\Desktop\IVO2cpEukR.exe MD5: 6738634D9B3BFCF7EBCA8BE48C091B3E)
  - cmd.exe (PID: 5268 cmdline: cmd.exe "/C schtasks /create /tn \ipXroBUdMG /tr \ "C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe\" /st 00:00 /du 9999:59 /sc once /ri 1 /f" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 5236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 4256 cmdline: schtasks /create /tn \ipXroBUdMG /tr \"C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe\" /st 00:00 /du 9999:59 /sc once /ri 1 /f" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- svcupdater.exe (PID: 6084 cmdline: C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe MD5: 6738634D9B3BFCF7EBCA8BE48C091B3E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: IVO2cpEukR.exe PID: 4544	JoeSecurity_LaplasClipper	Yara detected Laplas Clipper	Joe Security	
Process Memory Space: svcupdater.exe PID: 6084	JoeSecurity_LaplasClipper	Yara detected Laplas Clipper	Joe Security	
Process Memory Space: svcupdater.exe PID: 6084	JoeSecurity_MicroClip	Yara detected MicroClip	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Stealing of Sensitive Information

Yara detected MicroClip

Yara detected Laplas Clipper

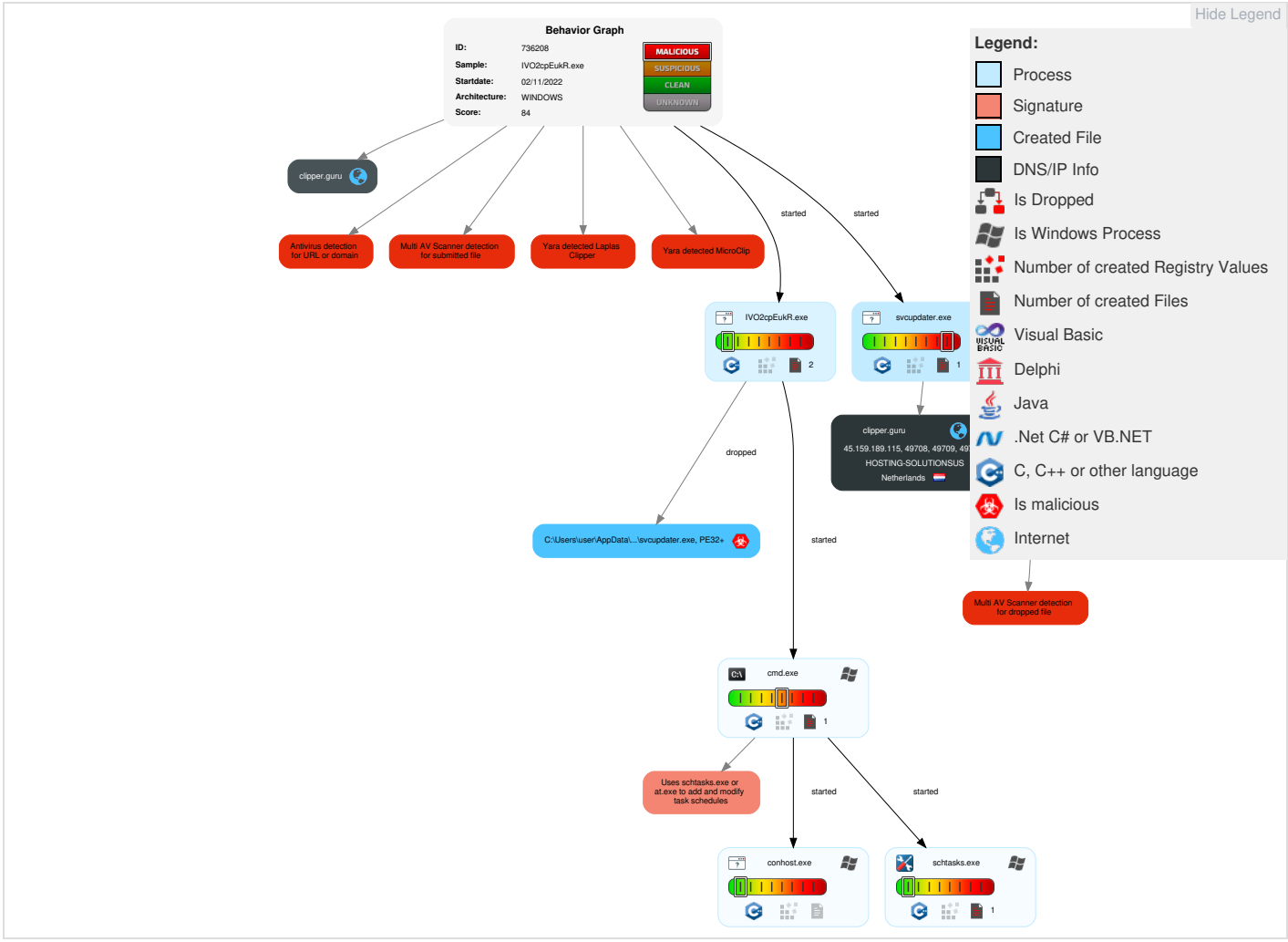
Remote Access Functionality

Yara detected MicroClip

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	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Process Injection	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 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)	Obfuscated Files or Information	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	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
IVO2cpEukR.exe	15%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe	15%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://clipper.guru/bot/online?guid=computer	100%	Avira URL Cloud	phishing	
http://clipper.guru/bot/regex?key=0f183cb4288647960d1c458ed8456bf6524ebfbc16ebc53caab66c2376fd0eef	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clipper.guru	45.159.189.115	true	false		unknown

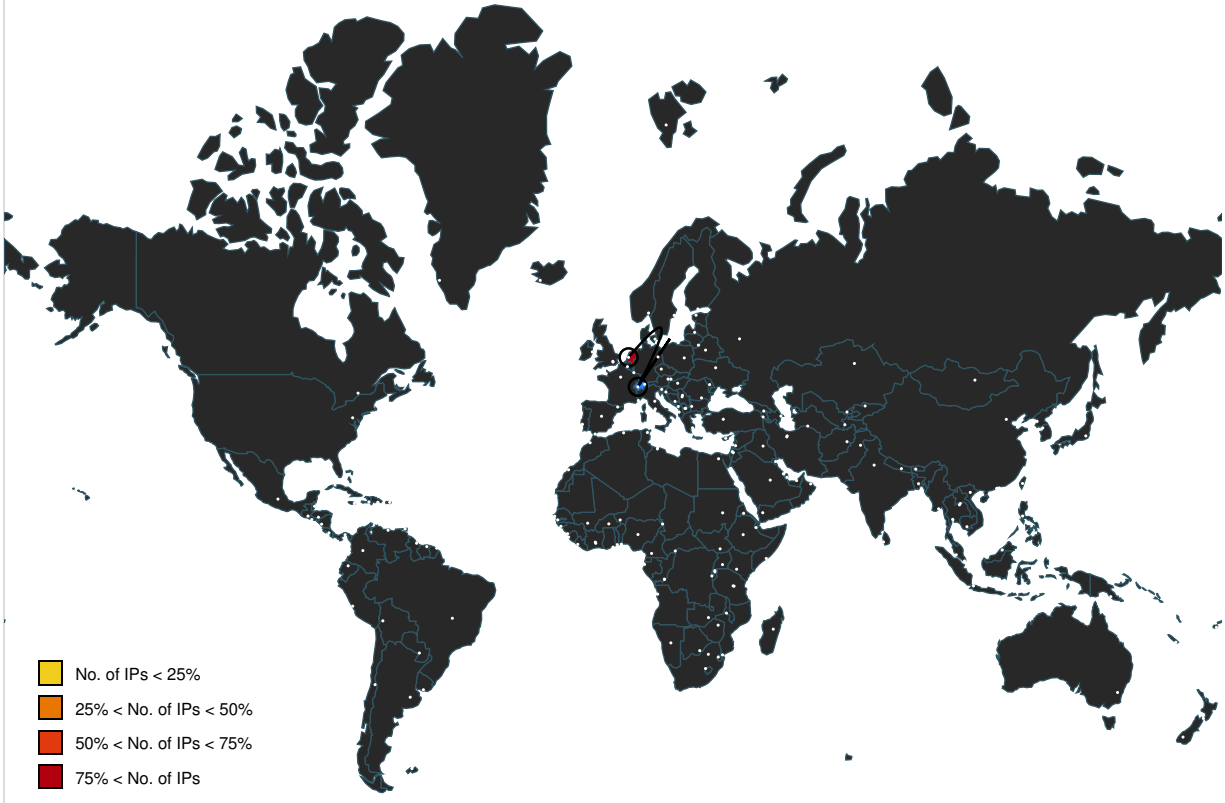
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://clipper.guru/bot/online?guid=computer\user&key=0f183cb4288647960d1c458ed8456bf6524ebfbc16ebc53caab66c2376fd0eef	false		unknown
http://clipper.guru/bot/regex?key=0f183cb4288647960d1c458ed8456bf6524ebfbc16ebc53caab66c2376fd0eef	false	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://clipper.guru/bot/online?guid=computer	svcupdater.exe, 00000004.00000002.522718471.000000C000186000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.159.189.115	clipper.guru	Netherlands		14576	HOSTING-SOLUTIONSUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736208

Start date and time:	2022-11-02 18:28:46 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IVO2cpEukR.exe
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
Number of analysed new started processes analysed:	16
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
Detection:	MAL
Classification:	mal84.troj.spyw.winEXE@7/3@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 96.9% (good quality ratio 90.6%) • Quality average: 59.3% • Quality standard deviation: 33.7%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Execution Graph export aborted for target IVO2cpEukR.exe, PID 4544 because there are no executed function
- Execution Graph export aborted for target svcupdater.exe, PID 6084 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: IVO2cpEukR.exe

Simulations

Behavior and APIs

Time	Type	Description
18:29:48	Task Scheduler	Run new task: ipXroBUdMG path: "C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe"

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\ipXroBUdMG\svcupdater.exe

Process:	C:\Users\user\Desktop\IVO2cpEukR.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	5021696
Entropy (8bit):	5.993018394677145
Encrypted:	false
SSDEEP:	49152:cAMzHHGxBRJHrcFFmJAhaShRgxuMY8qa9vjTIt0IEqYjla27/BS5g+A:bMjGxBQFFmJA3Foq+vOEdZZ+A
MD5:	6738634D9B3BFCF7EBCA8BE48C091B3E
SHA1:	F08091A4B3F5C167BCDFA565584BED8ED2A69F0C
SHA-256:	8C77759EFF69330A5C9697D05E2A0F99C6EDFF904BDD52A048DF0461D0459B27
SHA-512:	C8E6F3DD4C7DE4C9A54278A398D096AABF8391A8A92484EB2A8E74D6D288D8B066E967916645E2AAEC53FB4C8C3AC9F1CBD0FC01C1B828A1A742AF3BC57AA AF5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....L.....".....&.....@.....`P..... ..`... .....N.....N..f..... @G.H.....text.....&.....&.....`..`.rdata... ...&... ...&..... .....@..@.data.....@G.....,G.....@....idata.....N.....0K.....@....reloc...f....N..h...6K.....@..B.symtab.....PP.....L.....B..... ....

\Device\Mup\computer\PIPE\samr

Process:	C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe
File Type:	GLS_BINARY_LSB_FIRST
Category:	dropped
Size (bytes):	160
Entropy (8bit):	4.438743916256937
Encrypted:	false
SSDEEP:	3:rmHfvtH//STGlA1yqGlYUGk+ldyHGlgZty:rmHcKtGFlqty
MD5:	E467C82627F5E1524FDB4415AF19FC73
SHA1:	B86E3AA40E9FBED0494375A702EABAF1F2E56F8E
SHA-256:	116CD35961A2345CE210751D677600AADA539A66F046811FA70E1093E01F2540
SHA-512:	2A969893CC713D6388FDC768C009055BE1B35301A811A7E313D1AEEC1F75C88CCDDCD8308017A852093B1310811E90B9DA76B6330AACCF5982437D84F553183
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....xW4.4.....#Eg.....]..... .+.H`.....xW4.4.....#Eg.....3.qq..7I.....6.....xW4.4.....#Eg.....,..I..@E.....

\Device\Null

Process:	C:\Windows\System32\schtasks.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.67858562893781
Encrypted:	false
SSDEEP:	3:BgnKDOhoeK0oiH0CWKAK89AAAXb:BgnKqhxKRkd2K89o
MD5:	ABC2D94AE97A29E1FF28221D1192EA39
SHA1:	EBD96AF6D655A50FC9655FFCEEE1CAA90629BA6F
SHA-256:	AF912F9EB0344ECA3E7083E7E999E60C6430BFF221ABC04FDD51662660A12CB5

SHA-512:	F80813E55B163DCC3F6677BA92A9CB3CCB245DFAA682366A9C528B2F49B87EB78944E25717B24CA9023D9DF957147121AD68476CC7BF4ED4851EC283AB6ABA9
Malicious:	false
Preview:	SUCCESS: The scheduled task "\ipXroBUdMG" has successfully been created...

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	5.993018394677145
TrID:	• Win64 Executable (generic) (12005/4) 74.95% • Generic Win/DOS Executable (2004/3) 12.51% • DOS Executable Generic (2002/1) 12.50% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	IVO2cpEukR.exe
File size:	5021696
MD5:	6738634d9b3bfcf7ebca8be48c091b3e
SHA1:	f08091a4b3f5c167bcdfa565584bed8ed2a69f0c
SHA256:	8c77759eff69330a5c9697d05e2a0f99c6edff904bdd52a048df0461d0459b27
SHA512:	c8e6f3dd4c7de4c9a54278a398d096aabf8391a8a92484eb2a8e74d6d288d8b066e967916645e2aaec53fb4c8c3ac9f1cbd0fc01c1b828a1a742af3bc57aaaf5
SSDEEP:	49152:cAMzHHGxBRJHrcFFmJAhaShRgxuMY8qa9vjTlt0IEqYjla27/BS5g+A:bMjGxBQFFmJA3Foq+vOEdZZ+A
TLSH:	06364B17FCA214F9D5BEF13086529322BA7178A943303BD35F949A691A26FD0BB3D311
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....L....."....&.....@.....`P.....`... .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46bd80
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	93a138801d9601e4c36e6274c8b9d111

Entrypoint Preview

Instruction
jmp 00007F0FD4C47100h
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
pushfd
dec eax
sub esp, 70h
dec eax
mov dword ptr [esp+50h], edi
dec eax
mov dword ptr [esp+48h], esi
dec eax
mov dword ptr [esp+40h], ebp
dec eax
mov dword ptr [esp+38h], ebx
dec esp
mov dword ptr [esp+30h], esp
dec esp
mov dword ptr [esp+28h], ebp
dec esp
mov dword ptr [esp+20h], esi
dec esp
mov dword ptr [esp+58h], edi
dec ecx
mov edi, eax
dec eax
mov edx, dword ptr [00000028h]
dec eax
cmp edx, 00000000h
jne 00007F0FD4C4A7AEh
dec eax
mov eax, 00000000h
jmp 00007F0FD4C4A830h
dec eax
mov edx, dword ptr [edx+00000000h]
dec eax
cmp edx, 00000000h
jne 00007F0FD4C4A7A7h
call 00007F0FD4C4A8E8h
dec eax

Instruction
mov dword ptr [esp+60h], edx
dec eax
mov dword ptr [esp+68h], esp
dec eax
mov ebx, dword ptr [edx+30h]
dec eax
mov ebx, dword ptr [ebx]
dec eax
cmp edx, ebx
je 00007F0FD4C4A7CFh
dec eax
mov ebp, dword ptr [00000028h]
dec eax
mov dword ptr [ebp+00000000h], ebx
dec eax
mov edi, dword ptr [ebx+38h]
dec eax
sub edi, 08h
dec eax
lea esi, dword ptr [FFFD1DCEh]
dec eax
mov dword ptr [edi], esi
dec eax
sub edi, 78h
dec eax
mov dword ptr [edi+68h], esp
dec eax
mov esp, edi
dec eax
mov ebx, dword ptr [ecx]
dec eax
mov ecx, dword ptr [ecx+08h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4ed000	0x4a0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x4ee000	0x16684	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x474020	0x148	.data
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
.text	0x1000	0x269616	0x269800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

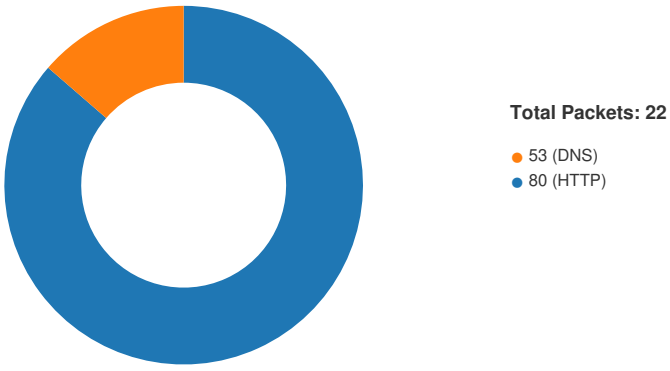
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x26b000	0x208cd8	0x208e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x474000	0x78f88	0x40400	False	0.4463954584143969	data	5.511488066172076	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x4ed000	0x4a0	0x600	False	0.3483072916666667	data	3.68798233819499	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x4ee000	0x16684	0x16800	False	0.2963324652777778	data	5.457203646831808	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.symtab	0x505000	0x4	0x200	False	0.02734375	data	0.020393135236084953	IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
kernel32.dll	WriteFile, WriteConsoleW, WaitForMultipleObjects, WaitForSingleObject, VirtualQuery, VirtualFree, VirtualAlloc, SwitchToThread, SuspendThread, SetWaitableTimer, SetUnhandledExceptionFilter, SetProcessPriorityBoost, SetEvent, SetErrorMode, SetConsoleCtrlHandler, ResumeThread, QueryFullProcessImageNameA, ProcessIdToSessionId, PostQueuedCompletionStatus, OpenProcess, LoadLibraryA, LoadLibraryW, SetThreadContext, GetThreadContext, GetSystemInfo, GetSystemDirectoryA, GetStdHandle, GetQueuedCompletionStatusEx, GetProcessAffinityMask, GetProcAddress, GetEnvironmentStringsW, GetConsoleMode, FreeEnvironmentStringsW, ExitProcess, DuplicateHandle, CreateThread, CreateIoCompletionPort, CreateEventA, CloseHandle, AddVectoredExceptionHandler

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 2, 2022 18:29:50.770592928 CET	49708	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:29:50.800642967 CET	80	49708	45.159.189.115	192.168.2.6
Nov 2, 2022 18:29:50.800806999 CET	49708	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:29:50.821186066 CET	49708	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:29:50.851111889 CET	80	49708	45.159.189.115	192.168.2.6
Nov 2, 2022 18:29:50.851912975 CET	80	49708	45.159.189.115	192.168.2.6
Nov 2, 2022 18:29:50.852407932 CET	49708	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:29:50.884027958 CET	80	49708	45.159.189.115	192.168.2.6
Nov 2, 2022 18:29:50.924983978 CET	49708	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:30:20.881997108 CET	80	49708	45.159.189.115	192.168.2.6
Nov 2, 2022 18:30:20.882083893 CET	49708	80	192.168.2.6	45.159.189.115

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 2, 2022 18:30:20.882555008 CET	49708	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:30:20.912445068 CET	80	49708	45.159.189.115	192.168.2.6
Nov 2, 2022 18:30:50.983144045 CET	49709	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:30:51.012626886 CET	80	49709	45.159.189.115	192.168.2.6
Nov 2, 2022 18:30:51.014977932 CET	49709	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:30:51.016272068 CET	49709	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:30:51.045741081 CET	80	49709	45.159.189.115	192.168.2.6
Nov 2, 2022 18:30:51.046528101 CET	80	49709	45.159.189.115	192.168.2.6
Nov 2, 2022 18:30:51.046916962 CET	49709	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:30:51.077117920 CET	80	49709	45.159.189.115	192.168.2.6
Nov 2, 2022 18:30:51.118437052 CET	49709	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:31:21.076092005 CET	80	49709	45.159.189.115	192.168.2.6
Nov 2, 2022 18:31:21.076174021 CET	49709	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:31:21.083151102 CET	49709	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:31:21.112533092 CET	80	49709	45.159.189.115	192.168.2.6
Nov 2, 2022 18:31:51.933299065 CET	49710	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:31:51.962971926 CET	80	49710	45.159.189.115	192.168.2.6
Nov 2, 2022 18:31:51.963299036 CET	49710	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:31:51.963864088 CET	49710	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:31:51.994096041 CET	80	49710	45.159.189.115	192.168.2.6
Nov 2, 2022 18:31:51.995026112 CET	80	49710	45.159.189.115	192.168.2.6
Nov 2, 2022 18:31:51.995821953 CET	49710	80	192.168.2.6	45.159.189.115
Nov 2, 2022 18:31:52.027110100 CET	80	49710	45.159.189.115	192.168.2.6
Nov 2, 2022 18:31:52.068528891 CET	49710	80	192.168.2.6	45.159.189.115

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 2, 2022 18:29:50.733129025 CET	49448	53	192.168.2.6	8.8.8.8
Nov 2, 2022 18:29:50.750500917 CET	53	49448	8.8.8.8	192.168.2.6
Nov 2, 2022 18:30:50.961983919 CET	59082	53	192.168.2.6	8.8.8.8
Nov 2, 2022 18:30:50.981436014 CET	53	59082	8.8.8.8	192.168.2.6
Nov 2, 2022 18:31:51.913724899 CET	59504	53	192.168.2.6	8.8.8.8
Nov 2, 2022 18:31:51.932436943 CET	53	59504	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 2, 2022 18:29:50.733129025 CET	192.168.2.6	8.8.8.8	0x315d	Standard query (0)	clipper.guru	A (IP address)	IN (0x0001)	false
Nov 2, 2022 18:30:50.961983919 CET	192.168.2.6	8.8.8.8	0xeef8	Standard query (0)	clipper.guru	A (IP address)	IN (0x0001)	false
Nov 2, 2022 18:31:51.913724899 CET	192.168.2.6	8.8.8.8	0x97c2	Standard query (0)	clipper.guru	A (IP address)	IN (0x0001)	false

DNS Answers

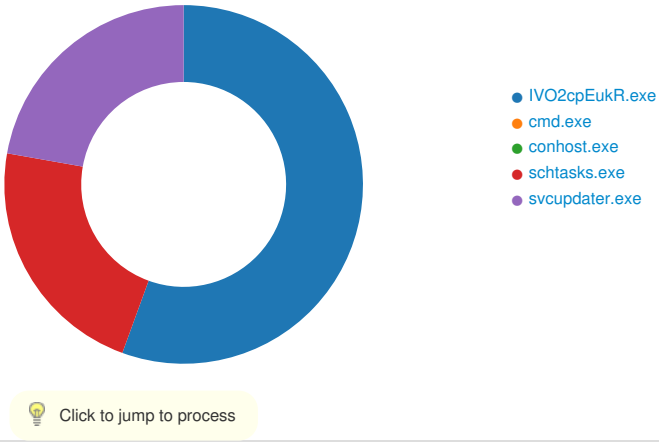
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 2, 2022 18:29:50.750500917 CET	8.8.8.8	192.168.2.6	0x315d	No error (0)	clipper.guru		45.159.189.115	A (IP address)	IN (0x0001)	false
Nov 2, 2022 18:30:50.981436014 CET	8.8.8.8	192.168.2.6	0xeef8	No error (0)	clipper.guru		45.159.189.115	A (IP address)	IN (0x0001)	false
Nov 2, 2022 18:31:51.932436943 CET	8.8.8.8	192.168.2.6	0x97c2	No error (0)	clipper.guru		45.159.189.115	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clipper.guru

Statistics

Behavior



System Behavior

Analysis Process: IVO2cpEukR.exe PID: **4544**, Parent PID: **3452**

General

Target ID:	0
Start time:	18:29:45
Start date:	02/11/2022
Path:	C:\Users\user\Desktop\IVO2cpEukR.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\IVO2cpEukR.exe
Imagebase:	0x320000
File size:	5021696 bytes
MD5 hash:	6738634D9B3BFCF7EBCA8BE48C091B3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: **5268**, Parent PID: **4544**

General

Target ID:	1
Start time:	18:29:46
Start date:	02/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe "/C schtasks /create /tn \ipXroBUdMG /tr \"C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe\" /st 00:00 /du 9999:59 /sc once /ri 1 /f"

Imagebase:	0x7ff7cb270000
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: conhost.exe PID: 5236, Parent PID: 5268

General

Target ID:	2
Start time:	18:29:46
Start date:	02/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: schtasks.exe PID: 4256, Parent PID: 5268

General

Target ID:	3
Start time:	18:29:46
Start date:	02/11/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /create /tn \ipXroBUdMG /tr \"C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe\" /st 00:00 /du 9999:59 /sc once /ri 1 /f"
Imagebase:	0x7ff7a7a50000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	69	69	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF7A7A6E023	fprintf
\Device\Null	74	74	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF7A7A6E023	fprintf

Analysis Process: svcupdater.exe PID: **6084**, Parent PID: **1064**

General

Target ID:	4
Start time:	18:29:48
Start date:	02/11/2022
Path:	C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\ipXroBUdMG\svcupdater.exe
Imagebase:	0x290000
File size:	5021696 bytes
MD5 hash:	6738634D9B3BFCF7EBCA8BE48C091B3E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 15%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ipXroBUdMG\IYyoEpMmze.pid	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2FBF1E	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	2FBF1E	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly