

JoeSandbox Cloud BASIC



ID: 652386

Sample Name:

HvAnUIF17C.exe

Cookbook: default.jbs

Time: 09:32:32

Date: 26/06/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report HvAnUIF17C.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Snake Keylogger	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	6
System Summary	6
Data Obfuscation	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	11
Public IPs	11
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASNs	12
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HvAnUIF17C.exe.log	13
Static File Info	13
General	13
File Icon	13
Static PE Info	14
General	14
Entrypoint Preview	14
Data Directories	16
Sections	16
Resources	16
Imports	16
Network Behavior	16
Snort IDS Alerts	16
Network Port Distribution	16
TCP Packets	17
UDP Packets	17
DNS Queries	17
DNS Answers	17
HTTP Request Dependency Graph	18
HTTP Packets	18
Statistics	18
Behavior	18

System Behavior

Analysis Process: HvAnUIF17C.exePID: 5684, Parent PID: 788

General

File Activities

File Created

File Written

File Read

Analysis Process: HvAnUIF17C.exePID: 3120, Parent PID: 5684

General

File Activities

File Created

File Read

Registry Activities

Disassembly

19

19

19

19

19

20

20

21

21

21

22

22

Windows Analysis Report

HvAnUIF17C.exe

Overview

General Information

Sample Name:

HvAnUIF17C.exe

Analysis ID:

652386

MD5:

515bae8e826da0.

SHA1:

b17e6b0aefc3c9...

SHA256:

1f446fcfd533aab..

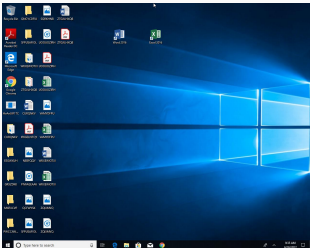
Tags:

exe

SnakeKeylogger

Infos:





Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Snake Keylogger

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Yara detected Snake Keylogger

Malicious sample detected (through...

Yara detected Telegram RAT

Yara detected AntiVM3

Snort IDS alert for network traffic

Tries to steal Mail credentials (via fi...

Tries to harvest and steal ftp login c...

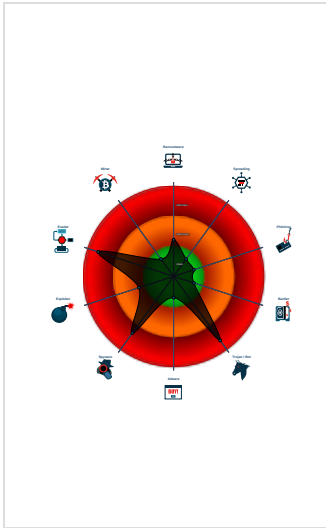
.NET source code references suspic...

Tries to detect sandboxes and other...

Machine Learning detection for sam...

May check the online IP address of...

Classification



Process Tree

System is w10x64

HvAnUIF17C.exe (PID: 5684 cmdline: "C:\Users\user\Desktop\HvAnUIF17C.exe" MD5: 515BAE8E826DA0259AEA4C4F3F05A654)

HvAnUIF17C.exe (PID: 3120 cmdline: C:\Users\user\Desktop\HvAnUIF17C.exe MD5: 515BAE8E826DA0259AEA4C4F3F05A654)

cleanup

Malware Configuration

Threatname: Snake Keylogger

```
{
  "Exfil Mode": "Telegram",
  "Telegram Token": "5125489588:AAG9rJipU-Qp9bVmgyzvinlz5gpATRgg5qo",
  "Telegram ID": "5149913163"
}
```

Yara Signatures

Memory Dumps				
Source	Rule	Description	Author	Strings
00000004.00000000.266393482.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000004.00000000.266393482.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000004.00000000.266393482.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.266393482.0000000000402000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	0x18570:\$x1: \$%SMTPDV\$ 0x17232:\$x2: \$#TheHashHere%& 0x18518:\$x3: %FTPDV\$ 0x17214:\$x4: \$%TelegramDv\$ 0x14b95:\$x5: KeyLoggerEventArgs 0x14f2b:\$x5: KeyLoggerEventArgs 0x1859c:\$m1: Snake Keylogger 0x18642:\$m1: Snake Keylogger 0x18796:\$m1: Snake Keylogger 0x188bc:\$m1: Snake Keylogger 0x18a16:\$m1: Snake Keylogger 0x1853c:\$m2: Clipboard Logs ID 0x1874c:\$m2: Screenshot Logs ID 0x18860:\$m2: keystroke Logs ID 0x18a4c:\$m3: SnakePW 0x18724:\$m4: \SnakeKeylogger\
00000004.00000002.509304253.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
Click to see the 28 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
4.0.HvAnUIF17C.exe.400000.4.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	0x1b070:\$a2: \Comodo\Dragon\User Data\Default\Login Data 0x1a259:\$a3: \Google\Chrome\User Data\Default\Login Data 0x1a6a0:\$a4: \Orbitum\User Data\Default\Login Data 0x1b821:\$a5: \Kometa\User Data\Default\Login Data
4.0.HvAnUIF17C.exe.400000.4.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
4.0.HvAnUIF17C.exe.400000.4.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
4.0.HvAnUIF17C.exe.400000.4.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
4.0.HvAnUIF17C.exe.400000.4.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 62 entries				

Sigma Signatures	
No Sigma rule has matched	

Snort Signatures	
ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.2.4 - Destination IP: 193.122.130.0	
Timestamp:	192.168.2.4193.122.130.049760802842536 06/26/22-09:34:00.732371
SID:	2842536
Source Port:	49760
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample



Networking



Snort IDS alert for network traffic
May check the online IP address of the machine
Yara detected Generic Downloader

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



.NET source code contains potential unpacker
--

Malware Analysis System Evasion



Yara detected AntiVM3
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion



.NET source code references suspicious native API functions
Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected Snake Keylogger
Yara detected Telegram RAT
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal ftp login credentials
Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality



Yara detected Snake Keylogger
Yara detected Telegram RAT

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 Native API	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Email Collection	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 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 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)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data



Antivirus, Machine Learning and Genetic Malware Detection				
Initial Sample				
Source	Detection	Scanner	Label	Link
HvAnUIF17C.exe	36%	Virustotal		Browse
HvAnUIF17C.exe	9%	Metadefender		Browse
HvAnUIF17C.exe	50%	ReversingLabs	ByteCode-MSIL.Spyware.Sna keLogger	
HvAnUIF17C.exe	100%	Joe Sandbox ML		
Dropped Files				
No Antivirus matches				

Unpacked PE Files					
Source	Detection	Scanner	Label	Link	Download
4.2.HvAnUIF17C.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Ge n		Download File
4.0.HvAnUIF17C.exe.400000.6.unpack	100%	Avira	TR/ATRAPS.Ge n		Download File
4.0.HvAnUIF17C.exe.400000.8.unpack	100%	Avira	TR/ATRAPS.Ge n		Download File
4.0.HvAnUIF17C.exe.400000.4.unpack	100%	Avira	TR/ATRAPS.Ge n		Download File
4.0.HvAnUIF17C.exe.400000.10.unpack	100%	Avira	TR/ATRAPS.Ge n		Download File
4.0.HvAnUIF17C.exe.400000.12.unpack	100%	Avira	TR/ATRAPS.Ge n		Download File

Domains
 No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs					
Contacted Domains					
Name	IP	Active	Malicious	Antivirus Detection	Reputation
checkip.dyndns.com	193.122.130.0	true	true		unknown
checkip.dyndns.org	unknown	unknown	true		unknown

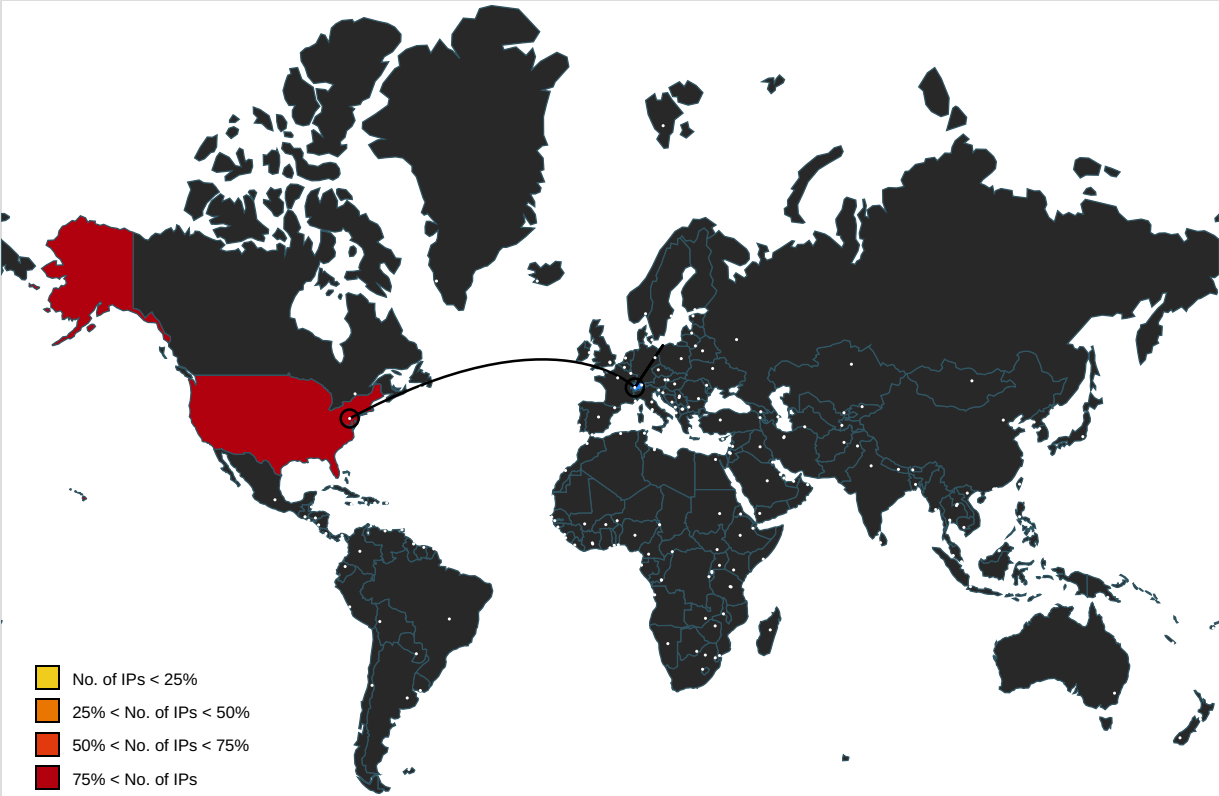
Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	true	URL Reputation: safe	unknown

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.telegram.org/bot	HvAnUIF17C.exe, 00000000.00000002.279912469.00000000044DF000.00000004.00000800.00020000.00000000.sdmp, HvAnUIF17C.exe, 00000004.00000000.266393482.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://checkip.dyndns.org	HvAnUIF17C.exe, 00000004.00000002.511395073.0000000003549000.00000004.00000800.00020000.00000000.sdmp, HvAnUIF17C.exe, 00000004.00000002.511505410.0000000003556000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.carterandcone.coml	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.sajatypeworks.com	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://checkip.dyndns.org4	HvAnUIF17C.exe, 00000004.00000002.511395073.0000000003549000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.typography.netD	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://fontfabrik.com	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cn	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://checkip.dyndns.org/q	HvAnUIF17C.exe, 00000000.00000002.279912469.00000000044DF000.00000004.00000800.00020000.00000000.sdmp, HvAnUIF17C.exe, 00000004.00000000.266393482.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://checkip.dyndns.com	HvAnUIF17C.exe, 00000004.00000002.511505410.0000000003556000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.urwpp.deDPlease	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	HvAnUIF17C.exe, 00000004.00000002.511172584.00000000034B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	HvAnUIF17C.exe, 00000000.00000002.282080429.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.122.130.0	checkip.dyndns.com	United States		31898	ORACLE-BMC-31898US	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	652386

Start date and time: 26/06/202209:32:32	2022-06-26 09:32:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HvAnUIF17C.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:	25
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:	mal100.troj.spyw.evad.winEXE@3/1@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 2.6% (good quality ratio 0.5%) • Quality average: 9.6% • Quality standard deviation: 24.8%
HCA Information:	• Successful, ratio: 85% • 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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:33:48	API Interceptor	1x Sleep call for process: HvAnUIF17C.exe modified

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\HvAnUIF17C.exe.log

Process:	C:\Users\user\Desktop\HvAnUIF17C.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DC8F8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	true
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.916901106793155
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.83% - Win32 Executable (generic) a (10002005/4) 49.78% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Generic Win/DOS Executable (2004/3) 0.01% - DOS Executable Generic (2002/1) 0.01%
File name:	HvAnUIF17C.exe
File size:	720384
MD5:	515bae8e826da0259aea4c4f3f05a654
SHA1:	b17e6b0aecf3c98bf27c6d3c03411007c964a35b
SHA256:	1f446fcfd533aab46514bc919c327c75e9dae84d6086777beeed532cdb787c85
SHA512:	3d4459645525b07d06a346af096b47d499cef495013eb0f8b8df2f750c74892b64cd74ee7c59f30796e0f8fa7f153bc3b174bdbbce83d7d27677350db2960545
SSDEEP:	12288:/xgH2iN1kPRxliW12/vxmScPANxmy674XKsQBV8rnBFi7Lie+LNU3NayyfRo:K13kPRrh2/5CPAnxMMXRQ/0b0vxU3NaH
TLSH:	79E41299E3A41EAAC08353F91C6CE5442A1BF70E82BCC60AB4F6355AE5723D59063F17
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....\$.....PE..L...Z..b.....0.....@..

File Icon



Icon Hash:	00828e8e8686b000
------------	------------------

General	
---------	--

Entrypoint:	0x4b1496
-------------	----------

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62B71C5A [Sat Jun 25 14:31:54 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Instruction

```
jmp dword ptr [00402000h]
```

push edx

inc ecx

```
xor eax, 45373434h
```

cmp byte ptr [3534564Eh], dh

xor eax, 4F373751h

push esp

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

add byte ptr [eax], al	
add byte ptr [eax], al	

add byte ptr [eax], al	
add byte ptr [eax], al	

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```


Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb1444	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb2000	0x3e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb4000	0xc	.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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xaf4b4	0xaf600	False	0.9178977525837491	data	7.922642417266635	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xb2000	0x3e0	0x400	False	0.3896484375	data	3.1085984086504888	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb4000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources						
Name	RVA	Size	Type	Language	Country	
RT_VERSION	0xb2058	0x384	data			

Imports	
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior								
Snort IDS Alerts								
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP	
192.168.2.4193.122.130.0 49760802842536 06/26/22-09:34:00.732371	TCP	2842536	ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49760	80	192.168.2.4	193.122.130.0	

Network Port Distribution

Total Packets: 8

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:34:00.624166965 CEST	49760	80	192.168.2.4	193.122.130.0
Jun 26, 2022 09:34:00.731515884 CEST	80	49760	193.122.130.0	192.168.2.4
Jun 26, 2022 09:34:00.731792927 CEST	49760	80	192.168.2.4	193.122.130.0
Jun 26, 2022 09:34:00.732371092 CEST	49760	80	192.168.2.4	193.122.130.0
Jun 26, 2022 09:34:00.839612961 CEST	80	49760	193.122.130.0	192.168.2.4
Jun 26, 2022 09:34:00.840661049 CEST	80	49760	193.122.130.0	192.168.2.4
Jun 26, 2022 09:34:00.920098066 CEST	49760	80	192.168.2.4	193.122.130.0
Jun 26, 2022 09:35:05.842036963 CEST	80	49760	193.122.130.0	192.168.2.4
Jun 26, 2022 09:35:05.843590975 CEST	49760	80	192.168.2.4	193.122.130.0
Jun 26, 2022 09:35:40.855221033 CEST	49760	80	192.168.2.4	193.122.130.0
Jun 26, 2022 09:35:40.966523886 CEST	80	49760	193.122.130.0	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:34:00.512381077 CEST	64454	53	192.168.2.4	8.8.8.8
Jun 26, 2022 09:34:00.530930042 CEST	53	64454	8.8.8.8	192.168.2.4
Jun 26, 2022 09:34:00.549586058 CEST	60506	53	192.168.2.4	8.8.8.8
Jun 26, 2022 09:34:00.566579103 CEST	53	60506	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:34:00.512381077 CEST	192.168.2.4	8.8.8.8	0x279	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Jun 26, 2022 09:34:00.549586058 CEST	192.168.2.4	8.8.8.8	0x6bf4	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:34:00.530930042 CEST	8.8.8.8	192.168.2.4	0x279	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jun 26, 2022 09:34:00.530930042 CEST	8.8.8.8	192.168.2.4	0x279	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Jun 26, 2022 09:34:00.530930042 CEST	8.8.8.8	192.168.2.4	0x279	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Jun 26, 2022 09:34:00.530930042 CEST	8.8.8.8	192.168.2.4	0x279	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
Jun 26, 2022 09:34:00.530930042 CEST	8.8.8.8	192.168.2.4	0x279	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Jun 26, 2022 09:34:00.530930042 CEST	8.8.8.8	192.168.2.4	0x279	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:34:00.566579103 CEST	8.8.8.8	192.168.2.4	0x6bf4	No error (0)	checkip.dy ndns.org	checkip.dyndns.co m		CNAME (Canonical name)	IN (0x0001)
Jun 26, 2022 09:34:00.566579103 CEST	8.8.8.8	192.168.2.4	0x6bf4	No error (0)	checkip.dy ndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Jun 26, 2022 09:34:00.566579103 CEST	8.8.8.8	192.168.2.4	0x6bf4	No error (0)	checkip.dy ndns.com		158.101.44.242	A (IP address)	IN (0x0001)
Jun 26, 2022 09:34:00.566579103 CEST	8.8.8.8	192.168.2.4	0x6bf4	No error (0)	checkip.dy ndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Jun 26, 2022 09:34:00.566579103 CEST	8.8.8.8	192.168.2.4	0x6bf4	No error (0)	checkip.dy ndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Jun 26, 2022 09:34:00.566579103 CEST	8.8.8.8	192.168.2.4	0x6bf4	No error (0)	checkip.dy ndns.com		193.122.6.168	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	193.122.130.0	80	C:\Users\user\Desktop\HvAnUIF17C.exe

Timestamp	kBytes transferred	Direction	Data
Jun 26, 2022 09:34:00.732371092 CEST	1139	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Jun 26, 2022 09:34:00.840661049 CEST	1139	IN	HTTP/1.1 200 OK Date: Sun, 26 Jun 2022 07:34:00 GMT Content-Type: text/html Content-Length: 106 Connection: keep-alive Cache-Control: no-cache Pragma: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 30 32 2e 31 32 39 2e 31 34 33 2e 36 31 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 102.129.143.61</body></html>

Statistics

Behavior

HvAnUIF17C.exe

HvAnUIF17C.exe

Click to jump to process

System Behavior

Analysis Process: **HvAnUIF17C.exe** PID: **5684**, Parent PID: **788**

General

Target ID:	0
Start time:	09:33:38
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\HvAnUIF17C.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\HvAnUIF17C.exe"
Imagebase:	0xf10000
File size:	720384 bytes
MD5 hash:	515BAE8E826DA0259AEA4C4F3F05A654
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.278554759.000000000333B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.279912469.00000000044DF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.279912469.00000000044DF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.279912469.00000000044DF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.279912469.00000000044DF000.00000004.00000800.00020000.00000000.sdmp, Author: ditekShen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.278443910.0000000003291000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6D96CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D96CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HvAnUIF17C.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6DC7C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HvAnUIF17C.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DC7C907	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D945705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D945705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D94CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D945705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D945705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C7B1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C7B1B4F	ReadFile	

Analysis Process: HvAnUIF17C.exe PID: 3120, Parent PID: 5684	
General	
Target ID:	4
Start time:	09:33:49
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\HvAnUIF17C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HvAnUIF17C.exe
Imagebase:	0xfe0000
File size:	720384 bytes
MD5 hash:	515BAE8E826DA0259AEA4C4F3F05A654
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000004.00000000.266393482.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000000.266393482.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.266393482.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000000.266393482.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000004.00000002.509304253.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000002.509304253.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.509304253.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000002.509304253.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000004.00000000.266790550.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000000.266790550.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.266790550.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000000.266790550.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000004.00000000.266009764.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000000.266009764.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.266009764.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000000.266009764.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000004.00000000.267402332.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000000.267402332.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.267402332.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000000.267402332.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
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	6D96CF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D96CF06	unknown	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D945705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D945705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.b1a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D94CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8A03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D945705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D945705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C7B1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C7B1B4F	ReadFile	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	40960	success or wait	1	6C7B1B4F	ReadFile

Registry Activities						
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.						
Key Path			Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Disassembly							
 No disassembly							