ID: 652392
Sample Name:
bh4BVURVUr.exe
Cookbook: default.jbs
Time: 09:43:25
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report bh4BVURVUr.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 10
World Map of Contacted IPs 11
Public IPs 11
Private 11
General Information 12
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bh4BVURVUr.exe.log 13
Static File Info 13
General 13
File Icon 14
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 17
TCP Packets 17
UDP Packets 17
DNS Queries 17
DNS Answers 17
HTTP Request Dependency Graph 18
HTTP Packets 18
Statistics 18
Behavior 18

Copyright Joe Security LLC 2022

System Behavior 19
Analysis Process: bh4BVURVUr.exePID: 6944, Parent PID: 4632 19
General 19
File Activities 19
File Created 19
File Written 20
File Read 20
Analysis Process: bh4BVURVUr.exePID: 6364, Parent PID: 6944 20
General 20
File Activities 21
File Created 21
File Read 21
Registry Activities 22
Disassembly 22

Copyright Joe Security LLC 2022

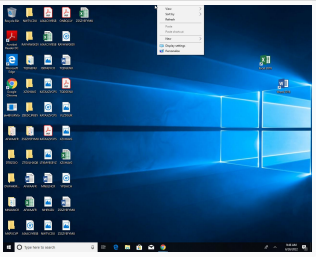
Windows Analysis Report

bh4BVURVUr.exe

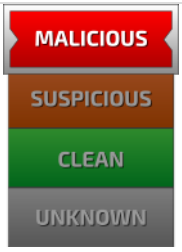
Overview

General Information

Sample Name:	bh4BVURVUr.exe
Analysis ID:	652392
MD5:	146c170d7ad83e..
SHA1:	c5849331066878..
SHA256:	fe8f94b75b067df..
Tags:	exe SnakeKeylogger
Infos:	



Detection



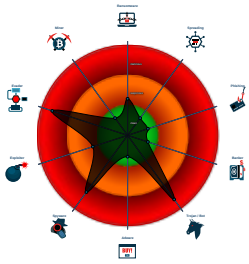
Snake Keylogger

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**
- bh4BVURVUr.exe (PID: 6944 cmdline: "C:\Users\user\Desktop\bh4BVURVUr.exe" MD5: 146C170D7AD83ED8302A01081326BCDD)
  - bh4BVURVUr.exe (PID: 6364 cmdline: C:\Users\user\Desktop\bh4BVURVUr.exe MD5: 146C170D7AD83ED8302A01081326BCDD)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger


```
{
  "Exfil Mode": "SMTP",
  "Username": "yugolog@gthltd.buzz",
  "Password": "7213575aceACE@#$",
  "Host": "cp5ua.hyperhost.ua",
  "Port": "yugo@gthltd.buzz"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	• 0x173ac:$x1: $%SMTPDV$ • 0x173c2:$x2: $#TheHashHere%& • 0x1874c:$x3: %FTPDV$ • 0x18814:$x4: $%TelegramDv$ • 0x14d0b:$x5: KeyLoggerEventArgs • 0x150a1:$x5: KeyLoggerEventArgs • 0x187bc:$m1: \| Snake Keylogger • 0x18874:$m1: | Snake Keylogger • 0x189c8:$m1: \| Snake Keylogger • 0x18aee:$m1: | Snake Keylogger • 0x18c48:$m1: \| Snake Keylogger • 0x18770:$m2: Clipboard Logs ID • 0x1897e:$m2: Screenshot Logs ID • 0x18a92:$m2: keystroke Logs ID • 0x18c7e:$m3: SnakePW • 0x18956:$m4: \SnakeKeylogger\
00000006.00000002.712878525.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.bh4BVURVUr.exe.400000.4.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x1b2d2:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x1a4bb:$a3: \Google\Chrome\User Data\Default\Login Data • 0x1a902:$a4: \Orbitum\User Data\Default\Login Data • 0x1ba83:$a5: \Kometa\User Data\Default\Login Data
6.0.bh4BVURVUr.exe.400000.4.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
6.0.bh4BVURVUr.exe.400000.4.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
6.0.bh4BVURVUr.exe.400000.4.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
6.0.bh4BVURVUr.exe.400000.4.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 70 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.2.5 - Destination IP: 132.226.8.169

Timestamp:	192.168.2.5132.226.8.16949772802842536 06/26/22-09:45:10.882218
SID:	2842536
Source Port:	49772
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

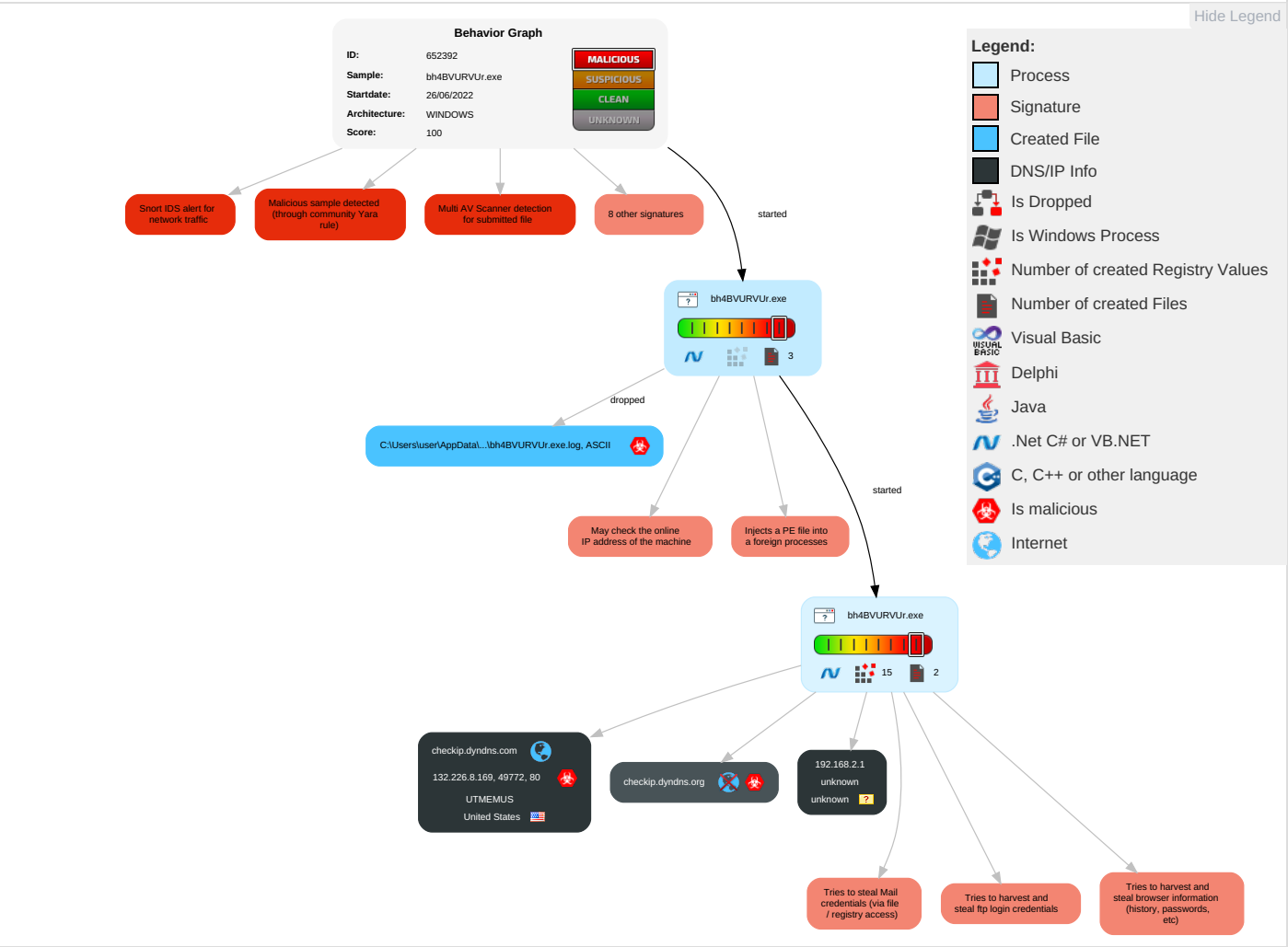
Yara detected Telegram RAT

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	2 Command and Scripting Interpreter	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	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 Input Capture	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)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 System Network Configuration 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	2 Obfuscated Files or Information	Cached Domain Credentials	1 3 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 3 Software Packing	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.

Copyright Joe Security LLC 2022

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bh4BVURVUr.exe	34%	Virustotal		Browse
bh4BVURVUr.exe	28%	ReversingLabs	ByteCode-MSIL.Spyware.SnakeLogger	
bh4BVURVUr.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Copyright Joe Security LLC 2022

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.bh4BVURVUr.exe.400000.12.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
6.0.bh4BVURVUr.exe.400000.6.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
6.0.bh4BVURVUr.exe.400000.10.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
6.0.bh4BVURVUr.exe.400000.4.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
6.2.bh4BVURVUr.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
6.0.bh4BVURVUr.exe.400000.8.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

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	132.226.8.169	true	true	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

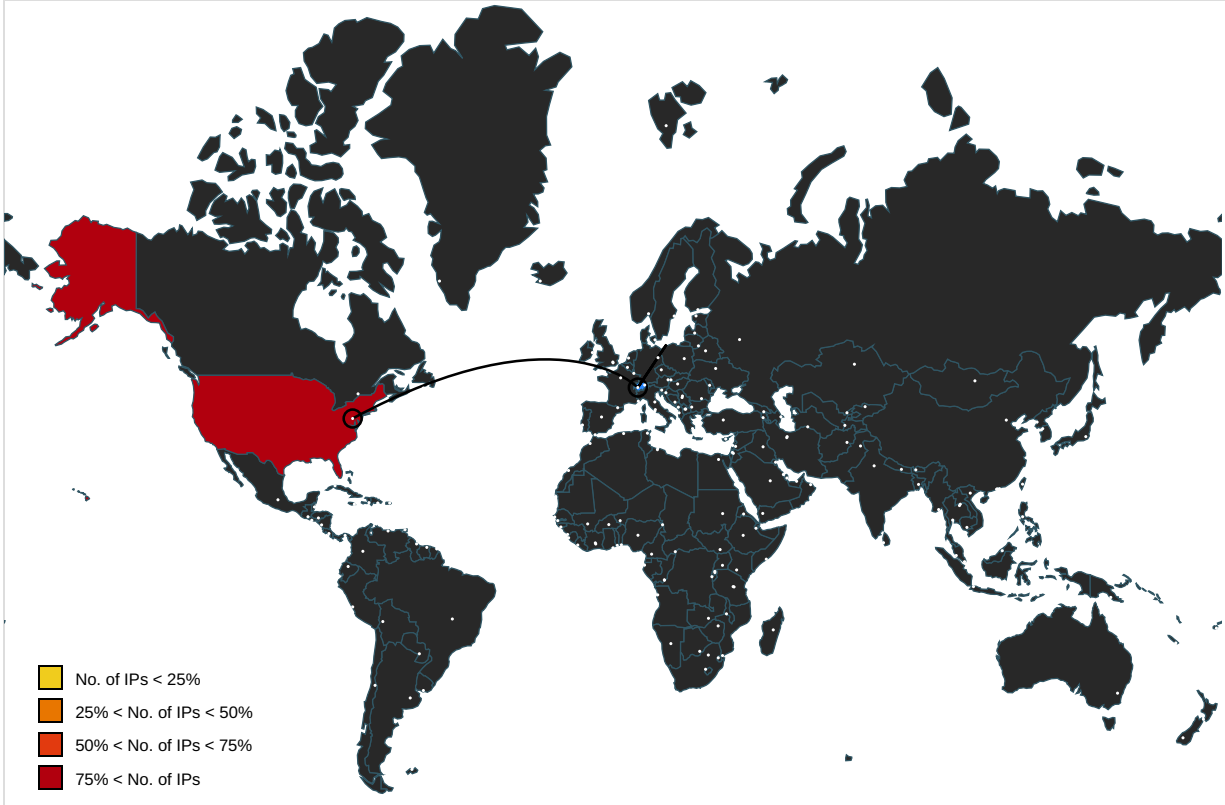
Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	bh4BVURVUr.exe, 00000000.00000002.493615011.000000000457A000.00000004.00000800.00020000.00000000.sdmp, bh4BVURVUr.exe, 00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org	bh4BVURVUr.exe, 00000006.00000002.714415764.00000000030E7000.00000004.00000800.00020000.00000000.sdmp, bh4BVURVUr.exe, 00000006.00000002.714240616.0000000003041000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org4	bh4BVURVUr.exe, 00000006.00000002.714240616.0000000003041000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://checkip.dyndns.org/q	bh4BVURVUr.exe, 00000000.00000002.493615011.000000000457A000.00000004.00000800.00020000.00000000.sdmp, bh4BVURVUr.exe, 00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.com	bh4BVURVUr.exe, 00000006.00000002.714415764.00000000030E7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	bh4BVURVUr.exe, 00000006.00000002.714240616.0000000003041000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	bh4BVURVUr.exe, 00000000.00000002.494970792.0000000007282000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
132.226.8.169	checkip.dyndns.com	United States		16989	UTMEMUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	652392
Start date and time: 26/06/202209:43:25	2022-06-26 09:43:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bh4BVURVUr.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:	19
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@2/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 3.7% (good quality ratio 1.8%) • Quality average: 30.2% • Quality standard deviation: 38.2%
HCA Information:	• Successful, ratio: 99% • 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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, licensing.mp.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target bh4BVURVUr.exe, PID 6944 because it is empty
- 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
09:45:01	API Interceptor	1x Sleep call for process: bh4BVURVUr.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\bh4BVURVUr.exe.log

Process:	C:\Users\user\Desktop\bh4BVURVUr.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:	FED34146BF2F2FA59DCF8702FCC8232E
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\f1d8480152e0da9a60ad49c6d16a3b6d\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):	7.9268931202438395
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:	bh4BVURVUr.exe
File size:	784384
MD5:	146c170d7ad83ed8302a01081326bcdd
SHA1:	c5849331066878e36bbab16b9117b5abe043f1de
SHA256:	fe8f94b75b067dfa0fb373ea8c05c4c18dbaec41cf83b2de27a02740ad6f43c2
SHA512:	bee1aff05e0023060f96e7be988a717060af6c81bb301f8b58271855fd7fca60dd80e7a86a9c93fd67a422319dc0cbe48991cc651c99683266e4f7f2a57f8dcc
SSDEEP:	12288:PEH2iN1kPRxliW1hzMCuQaW9pXajhYQXzlRWtw7prlmUaO1wtqrU+iEp9esIUTat:o13kPRrhhzNVaGNajhTXRmgr5wtq/XzF

TLSH:	FAF412C5E3A45EDAC58383F51CACD5042666F38E45BCC21178BA759FD4723E291A3E0B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...:..b.....0..... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c0ede
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:	0x62B71B3A [Sat Jun 25 14:27:06 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

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
dec eax
push edx
dec eax
inc ecx
xor eax, 45373434h
cmp byte ptr [3534564Eh], dh
xor eax, 4F373751h
push esp
inc ecx
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

Copyright Joe Security LLC 2022

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

Copyright Joe Security LLC 2022

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
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	0xc0e8c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc2000	0x3a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc4000	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	0xbeefc	0xbf000	False	0.9247612279123036	data	7.932077624932354	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc2000	0x3a8	0x400	False	0.3759765625	data	2.9336148862162847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	0xc	0x200	False	0.041015625	data	0.07763316234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc2058	0x34c	data		

Imports

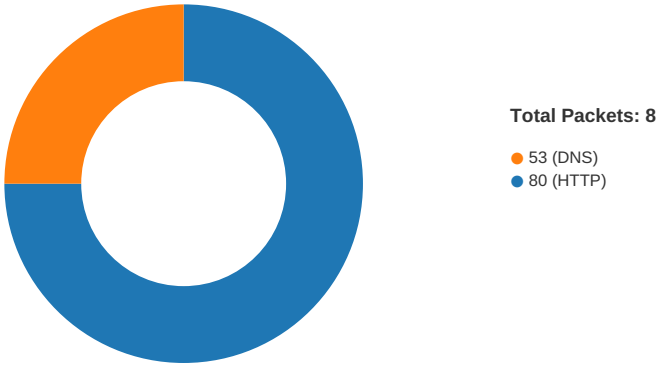
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5132.226.8.169 49772802842536 06/26/22-09:45:10.882218	TCP	2842536	ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49772	80	192.168.2.5	132.226.8.169

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:45:10.612282991 CEST	49772	80	192.168.2.5	132.226.8.169
Jun 26, 2022 09:45:10.881300926 CEST	80	49772	132.226.8.169	192.168.2.5
Jun 26, 2022 09:45:10.881459951 CEST	49772	80	192.168.2.5	132.226.8.169
Jun 26, 2022 09:45:10.882217884 CEST	49772	80	192.168.2.5	132.226.8.169
Jun 26, 2022 09:45:11.146639109 CEST	80	49772	132.226.8.169	192.168.2.5
Jun 26, 2022 09:45:12.152662039 CEST	80	49772	132.226.8.169	192.168.2.5
Jun 26, 2022 09:45:12.286751032 CEST	49772	80	192.168.2.5	132.226.8.169
Jun 26, 2022 09:46:17.151365995 CEST	80	49772	132.226.8.169	192.168.2.5
Jun 26, 2022 09:46:17.151546001 CEST	49772	80	192.168.2.5	132.226.8.169
Jun 26, 2022 09:46:52.177752018 CEST	49772	80	192.168.2.5	132.226.8.169
Jun 26, 2022 09:46:52.442231894 CEST	80	49772	132.226.8.169	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:45:10.522610903 CEST	53934	53	192.168.2.5	8.8.8.8
Jun 26, 2022 09:45:10.541312933 CEST	53	53934	8.8.8.8	192.168.2.5
Jun 26, 2022 09:45:10.566931963 CEST	63712	53	192.168.2.5	8.8.8.8
Jun 26, 2022 09:45:10.583794117 CEST	53	63712	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:45:10.522610903 CEST	192.168.2.5	8.8.8.8	0xac43	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:10.566931963 CEST	192.168.2.5	8.8.8.8	0x6219	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 09:45:10.541312933 CEST	8.8.8.8	192.168.2.5	0xac43	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jun 26, 2022 09:45:10.541312933 CEST	8.8.8.8	192.168.2.5	0xac43	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:45:10.541312933 CEST	8.8.8.8	192.168.2.5	0xac43	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:10.541312933 CEST	8.8.8.8	192.168.2.5	0xac43	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:10.541312933 CEST	8.8.8.8	192.168.2.5	0xac43	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:10.541312933 CEST	8.8.8.8	192.168.2.5	0xac43	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:10.583794117 CEST	8.8.8.8	192.168.2.5	0x6219	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jun 26, 2022 09:45:10.583794117 CEST	8.8.8.8	192.168.2.5	0x6219	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:10.583794117 CEST	8.8.8.8	192.168.2.5	0x6219	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:10.583794117 CEST	8.8.8.8	192.168.2.5	0x6219	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:10.583794117 CEST	8.8.8.8	192.168.2.5	0x6219	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
Jun 26, 2022 09:45:10.583794117 CEST	8.8.8.8	192.168.2.5	0x6219	No error (0)	checkip.dyndns.com		193.122.130.0	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	192.168.2.5	49772	132.226.8.169	80	C:\Users\user\Desktop\bh4BVURVUr.exe

Timestamp	kBytes transferred	Direction	Data
Jun 26, 2022 09:45:10.882217884 CEST	1166	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 09:45:12.152662039 CEST	1167	IN	HTTP/1.1 200 OK Date: Sun, 26 Jun 2022 07:45:11 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

Click to jump to process

System Behavior

Analysis Process: bh4BVURVUr.exe PID: **6944**, Parent PID: **4632**

General

Target ID:	0
Start time:	09:44:42
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\bh4BVURVUr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\bh4BVURVUr.exe"
Imagebase:	0xd30000
File size:	784384 bytes
MD5 hash:	146C170D7AD83ED8302A01081326BCDD
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: 00000000.00000002.490396689.0000000003121000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.493615011.000000000457A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.493615011.000000000457A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.493615011.000000000457A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.493615011.000000000457A000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.491801402.0000000004129000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.491801402.0000000004129000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.491801402.0000000004129000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.491801402.0000000004129000.00000004.00000800.00020000.00000000.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	6E46CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6E46CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bh4BVURVUr.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E77C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bh4BVURVUr.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 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	6E77C907	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	6E445705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E445705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E44CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E445705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E445705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2B1B4F	ReadFile

Analysis Process: bh4BVURVUr.exe PID: **6364**, Parent PID: **6944**

General

Target ID:	6
Start time:	09:45:02
Start date:	26/06/2022

Path:	C:\Users\user\Desktop\bh4BVURVUr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\bh4BVURVUr.exe
Imagebase:	0xc30000
File size:	784384 bytes
MD5 hash:	146C170D7AD83ED8302A01081326BCDD
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: 00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000006.00000000.485021040.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000006.00000002.712878525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000002.712878525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.712878525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000006.00000002.712878525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000006.00000000.486276914.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000000.486276914.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000000.486276914.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000006.00000000.486276914.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000006.00000000.487003315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000000.487003315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000000.487003315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000006.00000000.487003315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000006.00000000.487687196.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000000.487687196.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000000.487687196.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000006.00000000.487687196.0000000000402000.00000040.00000400.00020000.00000000.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	6E46CF06	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	6E46CF06	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	6E445705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E445705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E44CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3A03DE	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E445705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E445705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2B1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D2B1B4F	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