ID: 632543
Sample Name:
KNHLO60SC4.exe
Cookbook: default.jbs
Time: 18:58:32
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

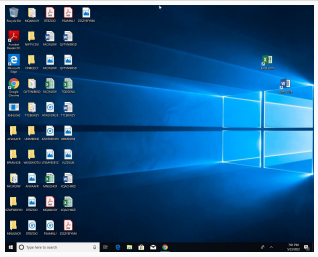
Windows Analysis Report

KNHLO60SC4.exe

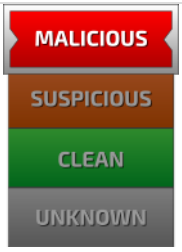
Overview

General Information

Sample Name:	KNHLO60SC4.exe
Analysis ID:	632543
MD5:	59a661dfcb4e0c…
SHA1:	ad04ceca0a6db8..
SHA256:	7e5d9c7f336e94..
Tags:	exe SnakeKeylogger
Infos:	



Detection



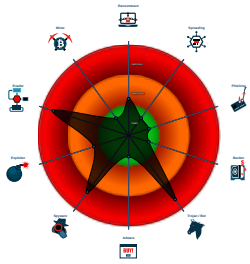
Snake Keylogger

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

Signatures

- Found malware configuration
- 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…

Classification



Process Tree

- **System is w10x64**
- KNHLO60SC4.exe (PID: 7104 cmdline: "C:\Users\user\Desktop\KNHLO60SC4.exe" MD5: 59A661DFCB4E0CFE6AAAACCD2D9B3E29)
  - KNHLO60SC4.exe (PID: 5116 cmdline: C:\Users\user\Desktop\KNHLO60SC4.exe MD5: 59A661DFCB4E0CFE6AAAACCD2D9B3E29)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger


```
{
  "Exfil Mode": "SMTP",
  "Username": "Null!",
  "Password": "greglog@samsung-tv.buzz",
  "Host": "7213575aceACE@#$",
  "Port": "samsung-tv.buzz"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	• 0x17428:$x1: $%SMTPDV$ • 0x1743e:$x2: $#TheHashHere%& • 0x1875e:$x3: %FTPDV$ • 0x18826:$x4: $%TelegramDv$ • 0x14d99:$x5: KeyLoggerEventArgs • 0x1512f:$x5: KeyLoggerEventArgs • 0x187ce:$m1: \| Snake Keylogger • 0x18886:$m1: | Snake Keylogger • 0x189da:$m1: \| Snake Keylogger • 0x18b00:$m1: | Snake Keylogger • 0x18c5a:$m1: \| Snake Keylogger • 0x18782:$m2: Clipboard Logs ID • 0x18990:$m2: Screenshot Logs ID • 0x18aa4:$m2: keystroke Logs ID • 0x18c90:$m3: SnakePW • 0x18968:$m4: \SnakeKeylogger\
00000000.00000002.479630658.0000000007180000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x514bf:$s1: file:/// • 0x513cf:$s2: {11111-22222-10009-11112} • 0x5144f:$s3: {11111-22222-50001-00000} • 0x4e8ad:$s4: get_Module • 0x4ecf3:$s5: Reverse • 0x50cfe:$s6: BlockCopy • 0x50b42:$s7: ReadByte • 0x514d1:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.KNHLO60SC4.exe.37d2ad8.8.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x194d0:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x186b9:$a3: \Google\Chrome\User Data\Default\Login Data • 0x18b00:$a4: \Orbitum\User Data\Default\Login Data • 0x19c81:$a5: \Kometa\User Data\Default\Login Data
0.2.KNHLO60SC4.exe.37d2ad8.8.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.2.KNHLO60SC4.exe.37d2ad8.8.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
0.2.KNHLO60SC4.exe.37d2ad8.8.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.KNHLO60SC4.exe.37d2ad8.8.unpack	INDICATOR_SUSPICIOUS_EXE_DotNetProcHook	Detects executables with potential process hoocking	ditekSHen	• 0x12b21:$s1: UnHook • 0x12b28:$s2: SetHook • 0x12b30:$s3: CallNextHook • 0x12b3d:$s4: _hook
Click to see the 72 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:	192.168.2.5132.226.8.16949777802842536 05/23/22-19:00:12.843188
SID:	2842536
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- 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

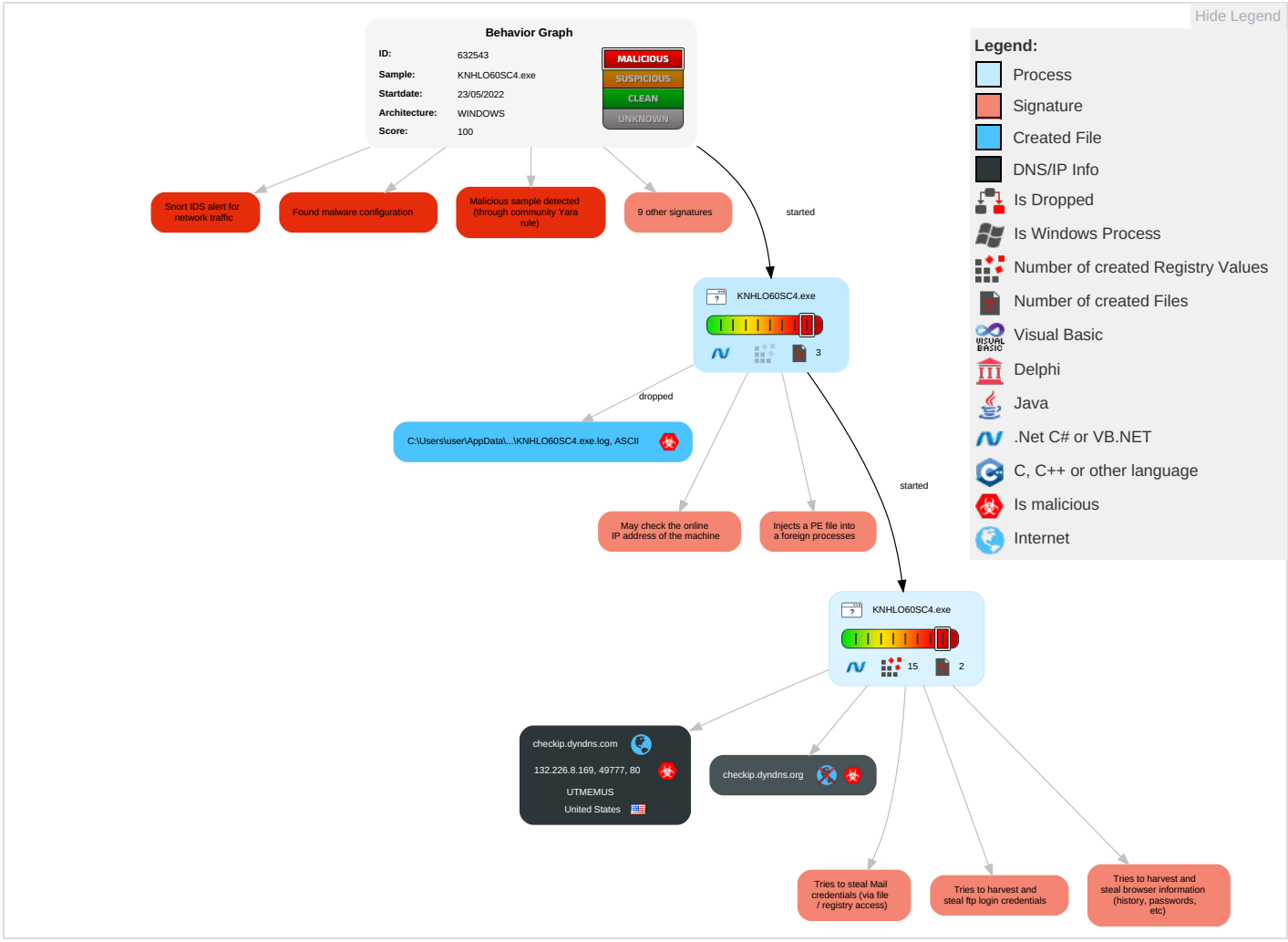
- Yara detected Snake Keylogger
- Yara detected Telegram RAT

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

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)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	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	3 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

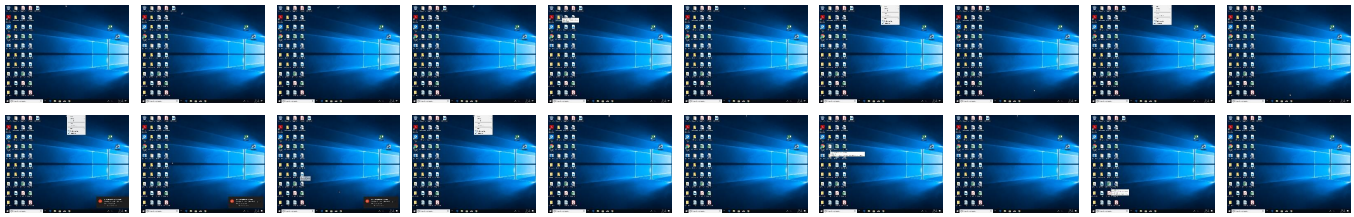
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
KNHLO60SC4.exe	35%	Virustotal		Browse
KNHLO60SC4.exe	29%	ReversingLabs	Win32.Trojan.AgentTesla	
KNHLO60SC4.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.KNHLO60SC4.exe.400000.8.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.0.KNHLO60SC4.exe.400000.10.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.0.KNHLO60SC4.exe.400000.4.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.0.KNHLO60SC4.exe.400000.6.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.0.KNHLO60SC4.exe.400000.12.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.KNHLO60SC4.exe.400000.0.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.carterandcone.comhic	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn//www.foundcci	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.comZPu	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://www.tiro.comion	0%	Avira URL Cloud	safe	
http://www.carterandcone.comPPC	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.coml1	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://www.fontbureau.comf	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://www.founder.com.cn/cny	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.carterandcone.comLPo	0%	Avira URL Cloud	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	
http://www.carterandcone.comrP	0%	Avira URL Cloud	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

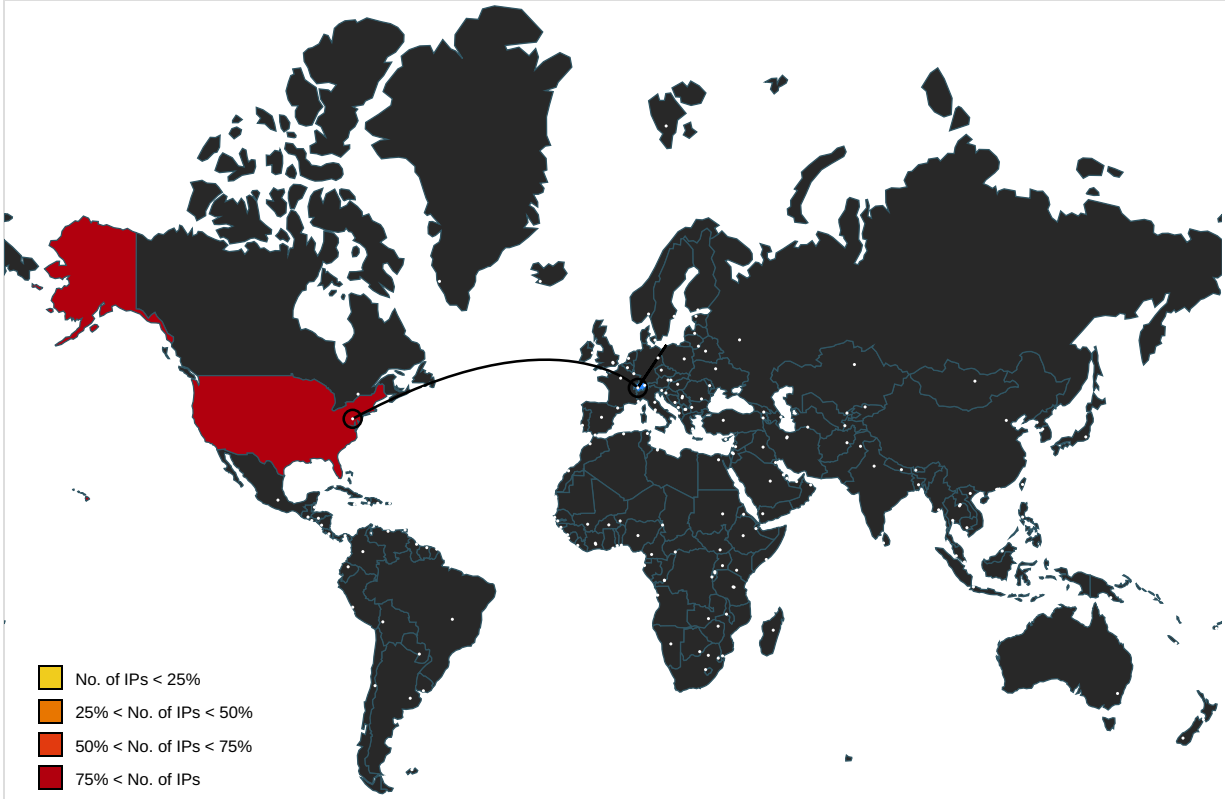
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	KNHLO60SC4.exe, 00000000.00000002.474876681.00000000037AD000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comhic	KNHLO60SC4.exe, 00000000.00000003.433800163.0000000005795000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn//www.foundcci	KNHLO60SC4.exe, 00000000.00000003.431020187.0000000005798000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.431218305.0000000005798000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comZPu	KNHLO60SC4.exe, 00000000.00000003.433800163.0000000005795000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org	KNHLO60SC4.exe, 00000004.00000002.693627091.0000000002D07000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000004.00000002.693380662.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.comion	KNHLO60SC4.exe, 00000000.00000003.431218305.0000000005798000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comPPC	KNHLO60SC4.exe, 00000000.00000003.433800163.0000000005795000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.435733496.000000000579E000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.435496176.000000000579D000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.435983488.000000000579E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	KNHLO60SC4.exe, 00000000.00000003.433800163.0000000005795000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.435733496.000000000579E000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.435496176.000000000579D000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.435983488.000000000579E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coml1	KNHLO60SC4.exe, 00000000.00000002.472339770.0000000000BF7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.427322559.00000000057AB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org4	KNHLO60SC4.exe, 00000004.00000002.693380662.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comf	KNHLO60SC4.exe, 00000000.00000002.472339770.0000000000BF7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cny	KNHLO60SC4.exe, 00000000.00000003.431020187.0000000005798000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org/q	KNHLO60SC4.exe, 00000000.00000002.474876681.00000000037AD000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comLPo	KNHLO60SC4.exe, 00000000.00000003.433800163.0000000005795000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.435733496.000000000579E000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.435496176.000000000579D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.com	KNHLO60SC4.exe, 00000004.00000002.693627091.0000000002D07000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	KNHLO60SC4.exe, 00000004.00000002.693380662.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	KNHLO60SC4.exe, 00000000.00000002.477680636.00000000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comrP	KNHLO60SC4.exe, 00000000.00000003.433800163.0000000005795000.00000004.00000800.00020000.00000000.sdmp, KNHLO60SC4.exe, 00000000.00000003.435496176.000000000579D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: 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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632543
Start date and time: 23/05/202218:58:32	2022-05-23 18:58:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KNHLO60SC4.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@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, settings-win.data.microsoft.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior 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
18:59:57	API Interceptor	1x Sleep call for process: KNHLO60SC4.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\KNHLO60SC4.exe.log

Process:	C:\Users\user\Desktop\KNHLO60SC4.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
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):	7.975444799848249
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:	KNHLO60SC4.exe
File size:	495616
MD5:	59a661dfcb4e0cfe6aaaaccd2d9b3e29
SHA1:	ad04ceca0a6db84de19919c6e4f1cd029cf80b1e
SHA256:	7e5d9c7f336e94ee88a9cee55858de158ba66862527ede87e3e7dec7ece79688
SHA512:	22816aebcc0bfddc52e7852c4e3ff2385b03de245d1b5deb09c031fc05b8d8b4f5fc1ae9abf534dc7c881899c2bb156ed7ffb225203c34ca32773c82ab5ef842
SSDEEP:	6144:NLmFuWf+hBp4akt41jCd5XSRPOn18y7czw34JOD7HCmYg1vSulyygU9og2Hj11A4:E+h/lNRBgaocFI7HCK3yygUCpVdd
TLSH:	83B4231DA765C23CC7DF4678DEB013DA42F06322F062DDE68A31A4DD1B51B96A1C43AB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...bS.b.....0.....^.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47a55e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x628B5362 [Mon May 23 09:26:58 2022 UTC]

TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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]
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7a50c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7c000	0x5ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7e000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
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	0x78564	0x78600	False	0.975303008178	data	7.98184842674	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x5ec	0x600	False	0.434895833333	data	4.21198324257	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x7c090	0x35c	data		
RT_MANIFEST	0x7c3fc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

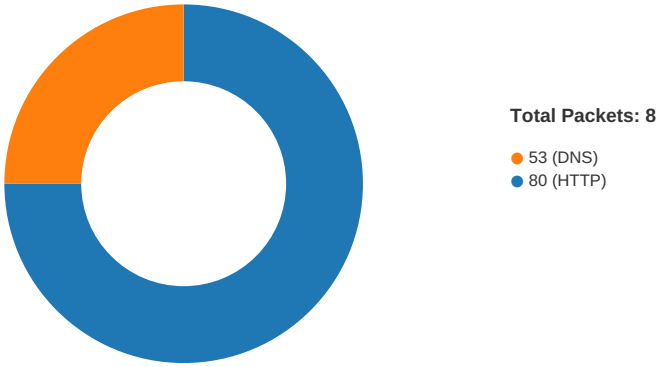
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	ReadBufferAsync.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	CIS501FinalProject
ProductVersion	1.0.0.0
FileDescription	CIS501FinalProject
OriginalFilename	ReadBufferAsync.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5132.226.8.169 49777802842536 05/23/22-19:00:12.843188	TCP	2842536	ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49777	80	192.168.2.5	132.226.8.169

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 19:00:09.159305096 CEST	49777	80	192.168.2.5	132.226.8.169
May 23, 2022 19:00:12.167556047 CEST	49777	80	192.168.2.5	132.226.8.169
May 23, 2022 19:00:12.438028097 CEST	80	49777	132.226.8.169	192.168.2.5
May 23, 2022 19:00:12.438183069 CEST	49777	80	192.168.2.5	132.226.8.169
May 23, 2022 19:00:12.843188047 CEST	49777	80	192.168.2.5	132.226.8.169
May 23, 2022 19:00:13.113843918 CEST	80	49777	132.226.8.169	192.168.2.5
May 23, 2022 19:00:14.114531040 CEST	80	49777	132.226.8.169	192.168.2.5
May 23, 2022 19:00:14.167785883 CEST	49777	80	192.168.2.5	132.226.8.169
May 23, 2022 19:01:19.114142895 CEST	80	49777	132.226.8.169	192.168.2.5
May 23, 2022 19:01:19.114289999 CEST	49777	80	192.168.2.5	132.226.8.169

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 19:00:09.064232111 CEST	54322	53	192.168.2.5	8.8.8.8
May 23, 2022 19:00:09.083138943 CEST	53	54322	8.8.8.8	192.168.2.5
May 23, 2022 19:00:09.100950956 CEST	62704	53	192.168.2.5	8.8.8.8
May 23, 2022 19:00:09.119755983 CEST	53	62704	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 19:00:09.064232111 CEST	192.168.2.5	8.8.8.8	0x319b	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.100950956 CEST	192.168.2.5	8.8.8.8	0xd5fc	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
May 23, 2022 19:00:09.083138943 CEST	8.8.8.8	192.168.2.5	0x319b	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 19:00:09.083138943 CEST	8.8.8.8	192.168.2.5	0x319b	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.083138943 CEST	8.8.8.8	192.168.2.5	0x319b	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.083138943 CEST	8.8.8.8	192.168.2.5	0x319b	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.083138943 CEST	8.8.8.8	192.168.2.5	0x319b	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.083138943 CEST	8.8.8.8	192.168.2.5	0x319b	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 19:00:09.119755983 CEST	8.8.8.8	192.168.2.5	0xd5fc	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 19:00:09.119755983 CEST	8.8.8.8	192.168.2.5	0xd5fc	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.119755983 CEST	8.8.8.8	192.168.2.5	0xd5fc	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.119755983 CEST	8.8.8.8	192.168.2.5	0xd5fc	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.119755983 CEST	8.8.8.8	192.168.2.5	0xd5fc	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.119755983 CEST	8.8.8.8	192.168.2.5	0xd5fc	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

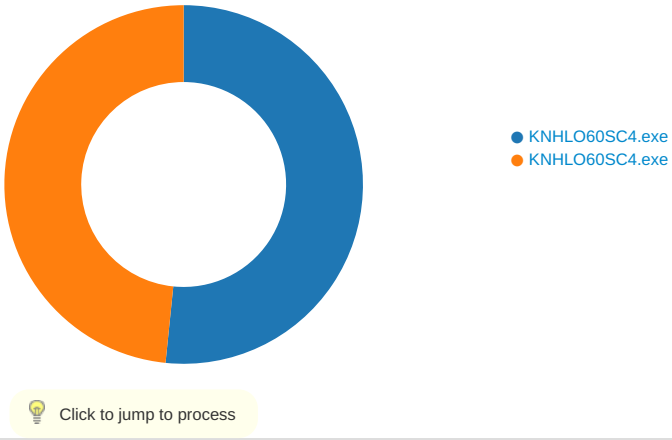
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49777	132.226.8.169	80	C:\Users\user\Desktop\KNHLO60SC4.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 19:00:12.843188047 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
May 23, 2022 19:00:14.114531040 CEST	1139	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 17:00:13 GMT Content-Type: text/html Content-Length: 103 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 38 34 2e 31 37 2e 35 32 2e 31 39 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: 84.17.52.19</body></html>

Statistics

Behavior



System Behavior

Analysis Process: KNHLO60SC4.exe PID: **7104**, Parent PID: **4844**

General

Target ID:	0
Start time:	18:59:41
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\KNHLO60SC4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\KNHLO60SC4.exe"
Imagebase:	0x3d0000
File size:	495616 bytes
MD5 hash:	59A661DFCB4E0CFE6AAAACCD2D9B3E29
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.479630658.0000000007180000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.474876681.00000000037AD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.474876681.00000000037AD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.474876681.00000000037AD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.474876681.00000000037AD000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.473028212.0000000002788000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.472920575.0000000002745000.00000004.00000800.00020000.00000000.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	6E44CF06	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	6E44CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\KNHLO60SC4.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E75C78D	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\KNHLO60SC4.exe.log	0	1308	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	6E75C907	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	6E425705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E425705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E42CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E425705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E425705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D291B4F	ReadFile

Analysis Process: KNHLO60SC4.exe PID: **5116**, Parent PID: **7104**

General

Target ID:	4
Start time:	19:00:00
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\KNHLO60SC4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\KNHLO60SC4.exe
Imagebase:	0x900000
File size:	495616 bytes
MD5 hash:	59A661DFCB4E0CFE6AAAACCD2D9B3E29
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: 00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000000.468061106.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000004.00000000.467290560.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000000.467290560.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.467290560.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000000.467290560.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000004.00000000.466200704.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000000.466200704.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.466200704.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000000.466200704.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000004.00000000.466741860.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000000.466741860.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.466741860.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000000.466741860.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000004.00000002.691544852.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000002.691544852.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.691544852.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000004.00000002.691544852.0000000000402000.00000040.00000400.00020000.00000000.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	6E44CF06	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	6E44CF06	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	6E425705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E425705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E42CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E425705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E425705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D291B4F	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	6D291B4F	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