ID: 830325
Sample Name:
Hbi8WUpShm.exe
Cookbook: default.jbs
Time: 09:09:36
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

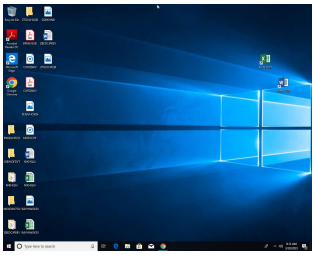
Windows Analysis Report

Hbi8WUpShm.exe

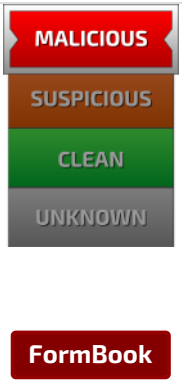
Overview

General Information

Sample Name:	Hbi8WUpShm.exe
Original Sample Name:	9739b15bd849…
Analysis ID:	830325
MD5:	00a41a480467…
SHA1:	a9ebc4956b89…
SHA256:	9739b15bd849…
Tags:	exe Formbook
Infos:	



Detection



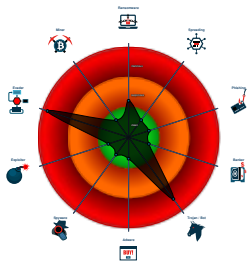
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- Hbi8WUpShm.exe (PID: 5868 cmdline: C:\Users\user\Desktop\Hbi8WUpShm.exe MD5: 00A41A4804673581F675471BFFA2BAFC)
  - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - chkdsk.exe (PID: 6012 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: 2D5A2497CB57C374B3AE3080FF9186FB)
      - cmd.exe (PID: 4208 cmdline: /c del "C:\Users\user\Desktop\Hbi8WUpShm.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 3536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	**http://** blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://asec.ahnlab.com/en/32149/https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.eltres-iot.info/nu06/"
  ],
  "decoy": [
    "cutmentor.net",
    "alexwright.xyz",
    "gymbastic.com",
    "creperie-lalios.com",
    "equipmentblock.com",
    "zwangerschapvanweektotweek.net",
    "asimulationcompany.com",
    "g9technoinnovation.com",
    "bestbirdies.xyz",
    "addhair.online",
    "get-breakfastburns.com",
    "aex-studentki.guru",
    "jhpx888.com",
    "gemologic.dev",
    "thegreencarshop.co.uk",
    "alessandromargonari.com",
    "cosmosynz.click",
    "letstalkreparation.com",
    "bka-i.com",
    "hervelegerdressshop.co.uk",
    "xn--5hqsa64xi8tdhd1xsp5oyyi.com",
    "jobstrendpk.com",
    "pavilionroofingservices.co.uk",
    "gonulserezart.com",
    "iby923.xyz",
    "languageforall.africa",
    "helloular3.com",
    "faster1.one",
    "lborient.com",
    "bzhxqm.com",
    "smartmetersystems.co.uk",
    "icfc2019.com",
    "handymantroop.com",
    "mychefacademy.com",
    "credit-cards-70626.com",
    "letmewowyou.com",
    "cityguide.africa",
    "dismissalnoise.com",
    "edu-degrees-89998.com",
    "estebanecheverry.com",
    "celsopaula.com",
    "jihuajl.com",
    "pyvob.xyz",
    "gdbdkj.com",
    "ballinc.online",
    "amadeussalem.net",
    "ievc-technologies.com",
    "arrindellnotary.com",
    "laneseempowerment.com",
    "bullreward.com",
    "evaluatemyathlete.com",
    "seu-qzs.com",
    "hexmexico.com",
    "coiffeur-kosmetik-basel1.ch",
    "1wacdu.top",
    "hoot.software",
    "goldhillmesatimes.com",
    "jobsnailikely.com",
    "cyberlavender.com",
    "ldgyb.com",
    "crunchtimemotion.com",
    "xn--74q746a2tj.net",
    "heikeshuwu.com",
    "fotel.xyz"
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Hbi8WUpShm.exe	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
Hbi8WUpShm.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Hbi8WUpShm.exe	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5651:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bfc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0x9dcf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x14cb7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
Hbi8WUpShm.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8d08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8f82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14ab5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x145a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14bb7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14d2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x999a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1381c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa693:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ad27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bd2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Hbi8WUpShm.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17c49:$sqlite3step: 68 34 1C 7B E1 • 0x17d5c:$sqlite3step: 68 34 1C 7B E1 • 0x17c78:$sqlite3text: 68 38 2A 90 C5 • 0x17d9d:$sqlite3text: 68 38 2A 90 C5 • 0x17c8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17db3:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0x99cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x148b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x959a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17849:$sqlite3step: 68 34 1C 7B E1 • 0x1795c:$sqlite3step: 68 34 1C 7B E1 • 0x17878:$sqlite3text: 68 38 2A 90 C5 • 0x1799d:$sqlite3text: 68 38 2A 90 C5 • 0x1788b:$sqlite3blob: 68 53 D8 7F 8C • 0x179b3:$sqlite3blob: 68 53 D8 7F 8C

Click to see the 49 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Hbi8WUpShm.exe.830000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
0.2.Hbi8WUpShm.exe.830000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Hbi8WUpShm.exe.830000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bdc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9bcf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x14ab7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0.2.Hbi8WUpShm.exe.830000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.Hbi8WUpShm.exe.830000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 34.102.136.180

Timestamp:	192.168.2.534.102.136.18049699802031412 03/20/23-09:11:34.950454
SID:	2031412
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 34.102.136.180

Timestamp:	192.168.2.534.102.136.18049699802031449 03/20/23-09:11:34.950454
SID:	2031449
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 34.117.168.233

Timestamp:	192.168.2.534.117.168.23349701802031412 03/20/23-09:12:16.158626
SID:	2031412
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 34.117.168.233	
Timestamp:	192.168.2.534.117.168.23349701802031453 03/20/23-09:12:16.158626
SID:	2031453
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 34.117.168.233	
Timestamp:	192.168.2.534.117.168.23349701802031449 03/20/23-09:12:16.158626
SID:	2031449
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 34.102.136.180	
Timestamp:	192.168.2.534.102.136.18049699802031453 03/20/23-09:11:34.950454
SID:	2031453
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Machine Learning detection for sample

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- 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

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

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

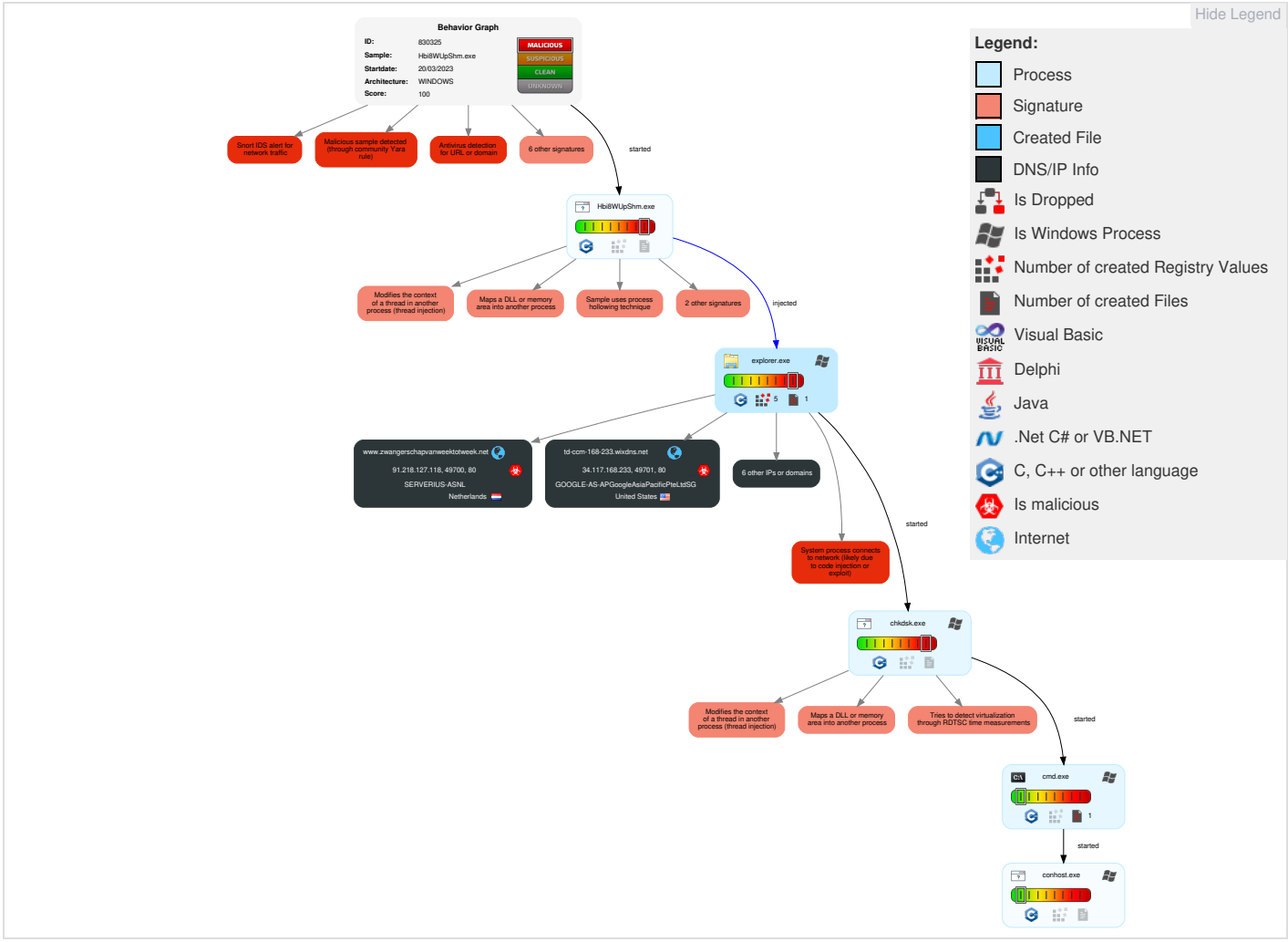
Remote Access Functionality

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
Valid Accounts	1 Shared Modules	Path Interception	5 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	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	2 Virtualization/Sandbox Evasion	LSASS Memory	2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	4 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)	5 1 2 Process Injection	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	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)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	LSA Secrets	1 Remote System 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 Software Packing	Cached Domain Credentials	1 1 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
Hbi8WUpShm.exe	85%	ReversingLabs	Win32.Trojan.FormBook	
Hbi8WUpShm.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
Hbi8WUpShm.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Hbi8WUpShm.exe.830000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Hbi8WUpShm.exe.830000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.alexwright.xyz	0%	Avira URL Cloud	safe	
http://www.zwangerschapvanweektotweek.net	0%	Avira URL Cloud	safe	
http://www.eltres-iot.info	0%	Avira URL Cloud	safe	
http://www.alessandromargonari.com/nu06/www.languageforall.africa	100%	Avira URL Cloud	malware	
http://www.alessandromargonari.com/nu06/	100%	Avira URL Cloud	malware	
http://www.arrindellnotary.com/nu06/	100%	Avira URL Cloud	malware	
http://www.edu-degrees-89998.com/nu06/www.arrindellnotary.com	100%	Avira URL Cloud	malware	
http://www.coiffeur-kosmetik-basel1.chReferer:	0%	Avira URL Cloud	safe	
http://www.eltres-iot.info/nu06/www.smartmetersystems.co.uk	100%	Avira URL Cloud	malware	
http://www.letstalkreparation.com/nu06/www.zwangerschapvanweektotweek.net	100%	Avira URL Cloud	malware	
http://www.heikeshuwu.com/nu06/www.alessandromargonari.com	100%	Avira URL Cloud	malware	
http://www.hervelegerdressshop.co.uk/nu06/www.edu-degrees-89998.com	100%	Avira URL Cloud	malware	
http://www.alexwright.xyz/nu06/	100%	Avira URL Cloud	malware	
http://www.edu-degrees-89998.com/nu06/	100%	Avira URL Cloud	malware	
http://www.heikeshuwu.com/nu06/	100%	Avira URL Cloud	malware	
http://www.ballinc.online/nu06/	100%	Avira URL Cloud	malware	
http://www.hervelegerdressshop.co.uk/nu06/	100%	Avira URL Cloud	malware	
http://www.smartmetersystems.co.uk/nu06/	100%	Avira URL Cloud	malware	
http://www.eltres-iot.infoReferer:	0%	Avira URL Cloud	safe	
http://www.evaluatemyathlete.com/nu06/www.coiffeur-kosmetik-basel1.ch	100%	Avira URL Cloud	malware	
http://www.languageforall.africa/nu06/www.eltres-iot.info	100%	Avira URL Cloud	malware	
http://www.zwangerschapvanweektotweek.net/nu06/www.gonulserezart.com	100%	Avira URL Cloud	malware	
http://www.eltres-iot.info/nu06/	100%	Avira URL Cloud	malware	
http://www.languageforall.africa/nu06/	100%	Avira URL Cloud	malware	
http://www.evaluatemyathlete.comReferer:	0%	Avira URL Cloud	safe	
http://www.pyvob.xyz	100%	Avira URL Cloud	malware	
http://www.smartmetersystems.co.uk/nu06/www.alexwright.xyz	100%	Avira URL Cloud	malware	
http://www.evaluatemyathlete.com/nu06/?4h8xq=AAU7dHxOAmD1XA8vVT3AMGpmmEX+lZnDYwXHz32oiklDU/SqaBIxIuHdufVlmX9k3aqv&UrZ=9rv4vpj	100%	Avira URL Cloud	malware	
http://www.evaluatemyathlete.com	0%	Avira URL Cloud	safe	
http://www.letstalkreparation.com	0%	Avira URL Cloud	safe	
http://www.arrindellnotary.comReferer:	0%	Avira URL Cloud	safe	
http://www.languageforall.africa	0%	Avira URL Cloud	safe	
http://www.gonulserezart.com	0%	Avira URL Cloud	safe	
http://www.pyvob.xyz/nu06/www.heikeshuwu.com	100%	Avira URL Cloud	malware	
www.eltres-iot.info/nu06/	100%	Avira URL Cloud	malware	
http://www.ballinc.onlineReferer:	0%	Avira URL Cloud	safe	
http://www.gonulserezart.comReferer:	0%	Avira URL Cloud	safe	
http://www.edu-degrees-89998.comReferer:	0%	Avira URL Cloud	safe	
http://www.coiffeur-kosmetik-basel1.ch/nu06/www.pyvob.xyz	100%	Avira URL Cloud	malware	
http://www.gonulserezart.com/nu06/www.evaluatemyathlete.com	100%	Avira URL Cloud	malware	
http://www.gonulserezart.com/nu06/?UrZ=9rv4vpj&4h8xq=XguJjl6AKJ7iGHg0sIvbxor8PKuuNZIswUYLv8brtIVcEL19nblZmBuHZOHdf2lpP/kE	100%	Avira URL Cloud	malware	
http://www.arrindellnotary.com	0%	Avira URL Cloud	safe	
http://www.smartmetersystems.co.uk	0%	Avira URL Cloud	safe	
http://www.hervelegerdressshop.co.uk	0%	Avira URL Cloud	safe	
http://www.gonulserezart.com/nu06/	100%	Avira URL Cloud	malware	
http://www.alexwright.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.edu-degrees-89998.com	0%	Avira URL Cloud	safe	
http://www.evaluatemyathlete.com/nu06/	100%	Avira URL Cloud	malware	
http://www.smartmetersystems.co.ukReferer:	0%	Avira URL Cloud	safe	
http://www.letstalkreparation.comReferer:	0%	Avira URL Cloud	safe	
http://www.coiffeur-kosmetik-basel1.ch/nu06/	100%	Avira URL Cloud	malware	
http://www.pyvob.xyz/nu06/	100%	Avira URL Cloud	malware	
http://www.ballinc.online/nu06/www.hervelegerdressshop.co.uk	100%	Avira URL Cloud	malware	
http://www.pyvob.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.alessandromargonari.comReferer:	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.zwangerschapvanweektotweek.net/nu06/?4h8xq=RzhUDSljQ8La7qrFgsCqcMZ5F/GKaWYSy/YExKb0zDK6Qw0jyiEXU4SBBDL3oY4sWHH+&UrZ=9rv4vpj	100%	Avira URL Cloud	malware	
http://www.zwangerschapvanweektotweek.netReferer:	0%	Avira URL Cloud	safe	
http://www.heikeshuwu.comReferer:	0%	Avira URL Cloud	safe	
http://www.heikeshuwu.com	0%	Avira URL Cloud	safe	
http://www.hervelegerdressshop.co.ukReferer:	0%	Avira URL Cloud	safe	
http://www.languageforall.africaReferer:	0%	Avira URL Cloud	safe	
http://www.alessandromargonari.com	0%	Avira URL Cloud	safe	
http://www.ballinc.online	0%	Avira URL Cloud	safe	
http://www.alexwright.xyz/nu06/www.ballinc.online	100%	Avira URL Cloud	malware	
http://www.zwangerschapvanweektotweek.net/nu06/	100%	Avira URL Cloud	malware	
http://www.letstalkreparation.com/nu06/	100%	Avira URL Cloud	malware	
http://www.coiffeur-kosmetik-basel1.ch	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
td-ccm-168-233.wixdns.net	34.117.168.233	true	true		unknown
evaluatemyathlete.com	34.98.99.30	true	false		unknown
www.zwangerschapvanweektotweek.net	91.218.127.118	true	true		unknown
letstalkreparation.com	34.102.136.180	true	false		unknown
www.letstalkreparation.com	unknown	unknown	true		unknown
www.evaluatemyathlete.com	unknown	unknown	true		unknown
www.gonulserezart.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.evaluatemyathlete.com/nu06/?4h8xq=AAU7dHxOAmD1XA8vVT3AMGpmmEX+IZnDYwXHz32oiklDU/SqaBlxIuHdufVlmX9k3aqv&UrZ=9rv4vpj	false	• Avira URL Cloud: malware	unknown
www.eltres-iot.info/nu06/	true	• Avira URL Cloud: malware	low
http://www.gonulserezart.com/nu06/?UrZ=9rv4vpj&4h8xq=XguJjl6AKJ7iGHg0sIvbxor8PKuuNZIswUYLv8brtIVcEL19nblZmBuHZOHdf2lpP/kE	true	• Avira URL Cloud: malware	unknown
http://www.zwangerschapvanweektotweek.net/nu06/?4h8xq=RzhUDSljQ8La7qrFgsCqcMZ5F/GKaWYSy/YExKb0zDK6Qw0jyiEXU4SBBDL3oY4sWHH+&UrZ=9rv4vpj	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.alexwright.xyz/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.smartmetersystems.co.uk/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.alessandromargonari.com/nu06/www.languageforall.africa	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.alessandromargonari.com/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.zwangerschapvanweektotweek.net	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.alexwright.xyz	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.eltres-iot.info	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ballinc.online/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.edu-degrees-89998.com/nu06/www.arrindellnotary.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.arrindellnotary.com/nu06/	explorer.exe, 00000001.00000003.53380057 1.000000000ED55000.00000004.00000001.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.hervelegerdressshop.co.uk/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.coiffeur-kosmetik-basel1.chReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hervelegerdressshop.co.uk/nu06/www.edu-degrees-89998.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.heikeshuwu.com/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.letstalkreparation.com/nu06/www.zwangerschapvanweektotweek.net	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.eltres-iot.info/nu06/www.smartmetersystems.co.uk	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.heikeshuwu.com/nu06/www.alessandromargonari.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.edu-degrees-89998.com/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.eltres-iot.infoReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.evaluatemyathlete.com/nu06/www.coiffeur-kosmetik-basel1.ch	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.zwangerschapvanweektotweek.net/nu06/www.gonulserezart.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.languageforall.africa/nu06/www.eltres-iot.info	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.languageforall.africa/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.smartmetersystems.co.uk/nu06/www.alexwright.xyz	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.evaluatemyathlete.comReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pyvob.xyz	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.eltres-iot.info/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.evaluatemyathlete.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.letstalkreparation.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.arrindellnotary.comReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.languageforall.africa	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pyvob.xyz/nu06/www.heikeshuwu.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.gonulserezart.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

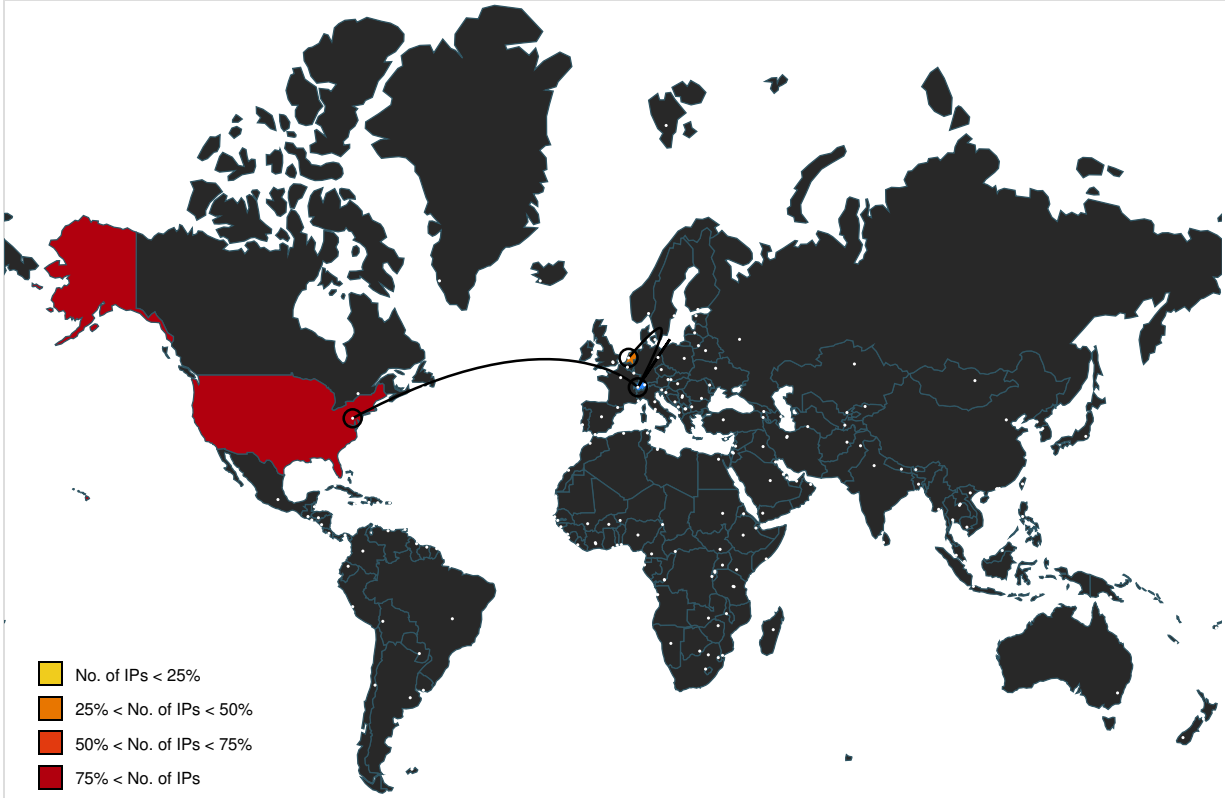
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.gonulserezart.comReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ballinc.onlineReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.edu-degrees-89998.comReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.coiffeur-kosmetik-basel1.ch/nu06/www.pyvob.xyz	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000001.00000000.30878400 9.000000000091F000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.573479962.0000000000921000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://www.gonulserezart.com/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.gonulserezart.com/nu06/www.evaluatemyathlete.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.arrindellnotary.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hervelegerdressshop.co.uk	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.smartmetersystems.co.uk	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.alexwright.xyzReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.edu-degrees-89998.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.evaluatemyathlete.com/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.smartmetersystems.co.ukReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.coiffeur-kosmetik-basel1.ch/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.letstalkreparation.comReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ballinc.online/nu06/www.hervelegerdressshop.co.uk	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.pyvob.xyzReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pyvob.xyz/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.alessandromargonari.comReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zwangerschapvanweektotweek.netReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.heikeshuwu.comReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hervelegerdressshop.co.ukReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.heikeshuwu.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.languageforall.africaReferer:	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.alessandromargonari.com	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.letstalkreparation.com/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.alexwright.xyz/nu06/www.ballinc.online	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.zwangerschapvanweektotweek.net/nu06/	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.coiffeur-kosmetik-basel1.ch	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ballinc.online	explorer.exe, 00000001.00000003.53397821 1.000000000ED66000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000002.584394622.000000000ED69000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.533800571.000000 000ED55000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	letstalkreparation.com	United States		15169	GOOGLEUS	false
34.98.99.30	evaluatemyathlete.com	United States		15169	GOOGLEUS	false
34.117.168.233	td-ccm-168-233.wixdns.net	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	true
91.218.127.118	www.zwangerschapvanwee ktotweek.net	Netherlands		50673	SERVERIUS-ASNL	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830325
Start date and time:	2023-03-20 09:09:36 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	7
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
Sample file name:	Hbi8WUpShm.exe
Original Sample Name:	9739b15bd8493e99e281d62d213ddc4cce684b1e833af4634932c57a669035fc.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/1@4/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.2% (good quality ratio 56.5%) • Quality average: 68.6% • Quality standard deviation: 33.1%
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, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: Hbi8WUpShm.exe

Simulations

Behavior and APIs

Time	Type	Description
09:10:42	API Interceptor	809x Sleep call for process: explorer.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\PenWorkspace\DiscoverCacheData.dat

Process:	C:\Windows\explorer.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.2414849034866355
Encrypted:	false
SSDEEP:	24:Yq6CUXyhmbmPlbNdB6hmYmPlz0JahmNmPlHZ6T06Mhm6mPlbxdB6hm3mPl7KTdB2:YqDUXycSNbNdUcVNz0JacQNHZ6T06Mcs
MD5:	4816271302882BDFB06EE40F624169D1
SHA1:	A8F07F0A5940C4A9D4DAD112787FE109CCACA869
SHA-256:	26D30DFFC5E2C493FF97B32C775C98630F0466D49144778BAE2688BA0716C760
SHA-512:	3D46AA6777AF386524E65D8D158201B699F766A5640A3E917CFA78E337475F910A839B93E0097C6651D2FCBE02ED7BFAF9EF8274C9632A88D06985168087823B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"RecentItems":[{"AppID":"Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim","PenUsageSec":15,"LastSwitchedLowPart":4155601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.WindowsMaps_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":4145601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint","PenUsageSec":15,"LastSwitchedLowPart":4135601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge","PenUsageSec":15,"LastSwitchedLowPart":4125601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.Windows.Photos_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":4115601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.Getstarted_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":4105601904,"LastSwitchedHighPart":30747926,"PrePopulated":true}]}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.395887090595119
TrID:	• Win32 Executable (generic) a (10002005/4) 99.98% • DOS Executable Generic (2002/1) 0.02%
File name:	Hbi8WUpShm.exe
File size:	185856
MD5:	00a41a4804673581f675471bffa2bafc
SHA1:	a9ebc4956b89e080451dbe619176a7e9ab8c8dd9
SHA256:	9739b15bd8493e99e281d62d213ddc4cce684b1e833af4634932c57a669035fc
SHA512:	f5136ac20e83e69492288e70de29c628517983f4e32e4f07bf61cdae8273d7eebbdef35febec348189a79433abb65f23943cd62cf40a16711eca3751c4a3a8cb
SSDEEP:	3072:9SBtkUimUbUffP36DCEtnaBlVTeWR5vcLtWA0AN87GqgodtpVu:SFHP62laBlVyW7sQK87GAjpw
TLSH:	A004BF32D642C031F2B211B4B6BD1B7B483D0E343295A4E6E3E525E06EE59A9F43931F
File Content Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....f...f...f.....f.....f.....f.Rich..f.....PE..L...-rxA.....P.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41f150
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x4178722D [Fri Oct 22 02:36:29 2004 UTC]

TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 64h
call 00007F6008C17D7Ah
mov esp, ebp
pop ebp
ret
call 00007F6008C1B565h
pop eax
ret
call 00007F6008C1B565h
pop eax
ret
call 00007F6008C17DC3h
ret
call 00007F6008C1B565h
pop eax
ret
jmp 00007F6008C17E26h
ret
call 00007F6008C1B565h
pop eax
ret
push 88888888h
jmp 00007F6008C19794h
ret
call 00007F6008C1B565h
pop eax
ret
push 88888888h
jmp 00007F6008C19797h
ret
call 00007F6008C1B565h
pop eax
ret
push 88888888h
jmp 00007F6008C1979Ah
ret
call 00007F6008C1B565h
pop eax
ret
push 88888888h
jmp 00007F6008C1979Dh
ret
call 00007F6008C1B565h
pop eax
ret
push 88888888h

Instruction
jmp 00007F6008C197A0h
ret
call 00007F6008C1B565h
pop eax
ret
push 88888888h
jmp 00007F6008C197A3h
ret
call 00007F6008C1B565h
pop eax
ret
push 88888888h
jmp 00007F6008C197A6h
ret
call 00007F6008C1B565h
pop eax
ret
push 88888888h
jmp 00007F6008C197A9h
ret
call 00007F6008C1B565h
pop eax
ret

Rich Headers

Programming Language:	• [C++] VS2010 SP1 build 40219 • [ASM] VS2010 SP1 build 40219 • [LNK] VS2010 SP1 build 40219

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

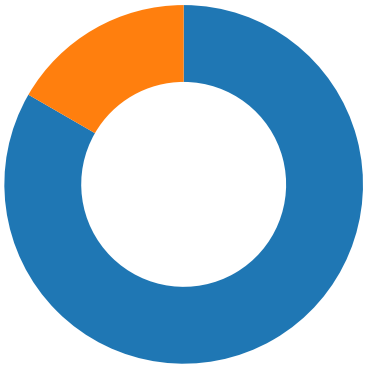
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2d1b4	0x2d200	False	0.7626547351108033	data	7.411530981126198	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.534.102.136.18049699802031412 03/20/23-09:11:34.950454	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49699	80	192.168.2.5	34.102.136.180
192.168.2.534.102.136.18049699802031449 03/20/23-09:11:34.950454	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49699	80	192.168.2.5	34.102.136.180
192.168.2.534.117.168.23349701802031412 03/20/23-09:12:16.158626	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49701	80	192.168.2.5	34.117.168.233
192.168.2.534.117.168.23349701802031453 03/20/23-09:12:16.158626	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49701	80	192.168.2.5	34.117.168.233
192.168.2.534.117.168.23349701802031449 03/20/23-09:12:16.158626	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49701	80	192.168.2.5	34.117.168.233
192.168.2.534.102.136.18049699802031453 03/20/23-09:11:34.950454	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49699	80	192.168.2.5	34.102.136.180

Network Port Distribution



Total Packets: 24

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:11:34.930716991 CET	49699	80	192.168.2.5	34.102.136.180
Mar 20, 2023 09:11:34.950098038 CET	80	49699	34.102.136.180	192.168.2.5
Mar 20, 2023 09:11:34.950277090 CET	49699	80	192.168.2.5	34.102.136.180
Mar 20, 2023 09:11:34.950453997 CET	49699	80	192.168.2.5	34.102.136.180
Mar 20, 2023 09:11:34.969583988 CET	80	49699	34.102.136.180	192.168.2.5
Mar 20, 2023 09:11:35.066672087 CET	80	49699	34.102.136.180	192.168.2.5
Mar 20, 2023 09:11:35.066715956 CET	80	49699	34.102.136.180	192.168.2.5
Mar 20, 2023 09:11:35.066847086 CET	49699	80	192.168.2.5	34.102.136.180
Mar 20, 2023 09:11:35.066898108 CET	49699	80	192.168.2.5	34.102.136.180
Mar 20, 2023 09:11:35.083978891 CET	80	49699	34.102.136.180	192.168.2.5
Mar 20, 2023 09:11:55.570101023 CET	49700	80	192.168.2.5	91.218.127.118
Mar 20, 2023 09:11:55.598764896 CET	80	49700	91.218.127.118	192.168.2.5
Mar 20, 2023 09:11:55.599045038 CET	49700	80	192.168.2.5	91.218.127.118
Mar 20, 2023 09:11:55.599268913 CET	49700	80	192.168.2.5	91.218.127.118
Mar 20, 2023 09:11:55.627808094 CET	80	49700	91.218.127.118	192.168.2.5
Mar 20, 2023 09:11:55.629206896 CET	80	49700	91.218.127.118	192.168.2.5
Mar 20, 2023 09:11:55.629324913 CET	80	49700	91.218.127.118	192.168.2.5
Mar 20, 2023 09:11:55.629522085 CET	49700	80	192.168.2.5	91.218.127.118
Mar 20, 2023 09:11:55.629584074 CET	49700	80	192.168.2.5	91.218.127.118

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:11:55.658082008 CET	80	49700	91.218.127.118	192.168.2.5
Mar 20, 2023 09:12:16.138863087 CET	49701	80	192.168.2.5	34.117.168.233
Mar 20, 2023 09:12:16.158241034 CET	80	49701	34.117.168.233	192.168.2.5
Mar 20, 2023 09:12:16.158474922 CET	49701	80	192.168.2.5	34.117.168.233
Mar 20, 2023 09:12:16.158626080 CET	49701	80	192.168.2.5	34.117.168.233
Mar 20, 2023 09:12:16.177845001 CET	80	49701	34.117.168.233	192.168.2.5
Mar 20, 2023 09:12:16.229779959 CET	80	49701	34.117.168.233	192.168.2.5
Mar 20, 2023 09:12:16.229813099 CET	80	49701	34.117.168.233	192.168.2.5
Mar 20, 2023 09:12:16.229986906 CET	49701	80	192.168.2.5	34.117.168.233
Mar 20, 2023 09:12:16.230048895 CET	49701	80	192.168.2.5	34.117.168.233
Mar 20, 2023 09:12:16.247335911 CET	80	49701	34.117.168.233	192.168.2.5
Mar 20, 2023 09:12:38.660048008 CET	49702	80	192.168.2.5	34.98.99.30
Mar 20, 2023 09:12:38.677489042 CET	80	49702	34.98.99.30	192.168.2.5
Mar 20, 2023 09:12:38.677763939 CET	49702	80	192.168.2.5	34.98.99.30
Mar 20, 2023 09:12:38.677958965 CET	49702	80	192.168.2.5	34.98.99.30
Mar 20, 2023 09:12:38.695177078 CET	80	49702	34.98.99.30	192.168.2.5
Mar 20, 2023 09:12:38.795730114 CET	80	49702	34.98.99.30	192.168.2.5
Mar 20, 2023 09:12:38.795758009 CET	80	49702	34.98.99.30	192.168.2.5
Mar 20, 2023 09:12:38.796055079 CET	49702	80	192.168.2.5	34.98.99.30
Mar 20, 2023 09:12:38.798008919 CET	49702	80	192.168.2.5	34.98.99.30
Mar 20, 2023 09:12:38.815126896 CET	80	49702	34.98.99.30	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:11:34.884437084 CET	60841	53	192.168.2.5	8.8.8.8
Mar 20, 2023 09:11:34.924032927 CET	53	60841	8.8.8.8	192.168.2.5
Mar 20, 2023 09:11:55.532341003 CET	61893	53	192.168.2.5	8.8.8.8
Mar 20, 2023 09:11:55.567677021 CET	53	61893	8.8.8.8	192.168.2.5
Mar 20, 2023 09:12:16.103852034 CET	60649	53	192.168.2.5	8.8.8.8
Mar 20, 2023 09:12:16.136781931 CET	53	60649	8.8.8.8	192.168.2.5
Mar 20, 2023 09:12:38.624042988 CET	51441	53	192.168.2.5	8.8.8.8
Mar 20, 2023 09:12:38.657809973 CET	53	51441	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 09:11:34.884437084 CET	192.168.2.5	8.8.8.8	0xd21b	Standard query (0)	www.letstalkreparation.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:55.532341003 CET	192.168.2.5	8.8.8.8	0xe7f5	Standard query (0)	www.zwangerschapvanweektotweek.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:16.103852034 CET	192.168.2.5	8.8.8.8	0x9aa5	Standard query (0)	www.gonulserezart.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:38.624042988 CET	192.168.2.5	8.8.8.8	0xfcc9	Standard query (0)	www.evaluatemyathlete.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
Mar 20, 2023 09:11:34.924032927 CET	8.8.8.8	192.168.2.5	0xd21b	No error (0)	www.letstalkreparation.com	letstalkreparation.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:11:34.924032927 CET	8.8.8.8	192.168.2.5	0xd21b	No error (0)	letstalkreparation.com		34.102.136.180	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:55.567677021 CET	8.8.8.8	192.168.2.5	0xe7f5	No error (0)	www.zwangerschapvanweektotweek.net		91.218.127.118	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:16.136781931 CET	8.8.8.8	192.168.2.5	0x9aa5	No error (0)	www.gonulserezart.com	gcdn0.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 09:12:16.136781931 CET	8.8.8.8	192.168.2.5	0x9aa5	No error (0)	gcdn0.wixdns.net	td-ccm-168-233.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:12:16.136781931 CET	8.8.8.8	192.168.2.5	0x9aa5	No error (0)	td-ccm-168-233.wixdns.net		34.117.168.233	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:38.657809973 CET	8.8.8.8	192.168.2.5	0xfcc9	No error (0)	www.evaluatemyathlete.com	evaluatemyathlete.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:12:38.657809973 CET	8.8.8.8	192.168.2.5	0xfcc9	No error (0)	evaluatemyathlete.com		34.98.99.30	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.letstalkreparation.com
- www.zwangerschapvanweektotweek.net
- www.gonulserezart.com
- www.evaluatemyathlete.com

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

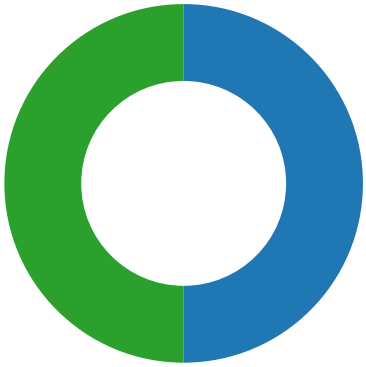
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE4
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE4
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE4
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE4

Statistics

Behavior

- Hbi8WUpShm.exe
- explorer.exe
- chkdsk.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: Hbi8WUpShm.exe PID: **5868**, Parent PID: **3324**

General	
Target ID:	0
Start time:	09:10:35
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\Hbi8WUpShm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Hbi8WUpShm.exe
Imagebase:	0x830000
File size:	185856 bytes
MD5 hash:	00A41A4804673581F675471BFFA2BAFC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.340187458.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000000.00000000.304875108.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000000.304875108.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000000.304875108.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000000.304875108.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000000.304875108.0000000000831000.00000020.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000000.00000002.343561110.0000000000D50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.343561110.0000000000D50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.343561110.0000000000D50000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.343561110.0000000000D50000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.343561110.0000000000D50000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000000.00000002.343352693.0000000000D20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.343352693.0000000000D20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.343352693.0000000000D20000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.343352693.0000000000D20000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.343352693.0000000000D20000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: explorer.exe PID: **3324**, Parent PID: **5868**

General

Target ID:	1
Start time:	09:10:36
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
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: Windows_Trojan_Formbook_772cc62d, Description: unknown, Source: 00000001.00000002.585228598.000000000FBA3000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000001.00000002.586228708.00000000152CF000.00000004.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.586228708.00000000152CF000.00000004.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.586228708.00000000152CF000.00000004.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.586228708.00000000152CF000.00000004.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.586228708.00000000152CF000.00000004.80000000.00040000.00000000.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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chkdsk.exe PID: **6012**, Parent PID: **3324**

General

Target ID:	2
Start time:	09:10:47
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\chkdsk.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0x1370000
File size:	23040 bytes
MD5 hash:	2D5A2497CB57C374B3AE3080FF9186FB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.573760954.0000000000DC0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.573760954.0000000000DC0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.573760954.0000000000DC0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.573760954.0000000000DC0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.573760954.0000000000DC0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.573525615.0000000000AE4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.573525615.0000000000AE4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.573525615.0000000000AE4000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.573525615.0000000000AE4000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.573525615.0000000000AE4000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.573684424.0000000000D90000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.573684424.0000000000D90000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.573684424.0000000000D90000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.573684424.0000000000D90000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.573684424.0000000000D90000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.575081559.00000000058AF000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.575081559.00000000058AF000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.575081559.00000000058AF000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.575081559.00000000058AF000.00000004.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.575081559.00000000058AF000.00000004.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.573431641.00000000008F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.573431641.00000000008F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.573431641.00000000008F0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.573431641.00000000008F0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.573431641.00000000008F0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	90A457	NtReadFile

Analysis Process: cmd.exe PID: **4208**, Parent PID: **6012**

General

Target ID:	3
Start time:	09:10:54
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Hbi8WUpShm.exe"
Imagebase:	0x11d0000
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: **3536**, Parent PID: **4208**

General

Target ID:	4
Start time:	09:10:54
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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