ID: 491359
Sample Name: EH5ro3Hyug
Cookbook: default.jbs
Time: 14:06:45
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

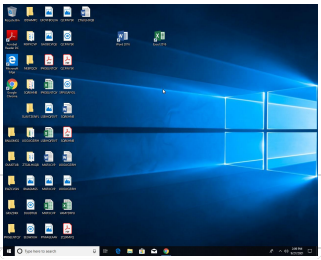
Windows Analysis Report EH5ro3Hyug

Overview

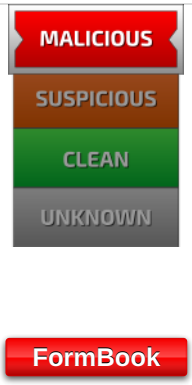
General Information

Sample Name:	EH5ro3Hyug (renamed file extension from none to exe)
Analysis ID:	491359
MD5:	dff3bf025dcd487…
SHA1:	1ff59c9410fb281…
SHA256:	230b56b1d07272..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



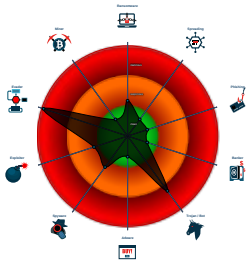
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- EH5ro3Hyug.exe (PID: 6400 cmdline: 'C:\Users\user\Desktop\EH5ro3Hyug.exe' MD5: DFF3BF025DCD487A2F0FB22B4CCF8998)
  - EH5ro3Hyug.exe (PID: 5412 cmdline: C:\Users\user\Desktop\EH5ro3Hyug.exe MD5: DFF3BF025DCD487A2F0FB22B4CCF8998)
  - EH5ro3Hyug.exe (PID: 5660 cmdline: C:\Users\user\Desktop\EH5ro3Hyug.exe MD5: DFF3BF025DCD487A2F0FB22B4CCF8998)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autoconv.exe (PID: 7104 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - WWAHost.exe (PID: 7092 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 4972 cmdline: /c del 'C:\Users\user\Desktop\EH5ro3Hyug.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.eastwestasia-thailand.com/hht8/"
  ],
  "decoy": [
    "chenghuaikj.com",
    "lovegames.site",
    "namalon.com",
    "ltxxiu.com",
    "yaotiaoshiguang.top",
    "serversshipping.com",
    "animationwageshare.com",
    "rh-et.com",
    "cutepets1.com",
    "chantforpeace.com",
    "techmazakatta.com",
    "amoorelive.com",
    "bisexualnft.com",
    "k5truckingexpress.com",
    "6e1eturzmu9ustbnrfe2404.com",
    "allday.coach",
    "prettyrisque.com",
    "stripeer.com",
    "ktranspass.com",
    "salinibros.com",
    "alzayantourism.com",
    "vilitex.com",
    "c10todkqnmixtkwzw2xq.pro",
    "alicama.com",
    "lyssna-miss.xyz",
    "vinoonline.cloud",
    "ip-15-235-154.net",
    "mylinkedbook.com",
    "sugarbombed.com",
    "blufftonga.com",
    "discocl.xyz",
    "conversationaldatacloud.com",
    "chancebig190.xyz",
    "empoweringcommunityrewards.com",
    "yournfts.one",
    "shopskinara.com",
    "zoltun.design",
    "mightyasianfood.com",
    "kingtreemusic.com",
    "kle638ske.com",
    "fsfurnitureking.com",
    "pl-id86979577.xyz",
    "hollandmediapromotion.com",
    "tansx.top",
    "ig-businessverifyaccount.com",
    "btcwpg.com",
    "eagles5050.com",
    "simplyblessedcrafts.com",
    "bestjob.solutions",
    "cikgu-alirays.xyz",
    "ceasa.club",
    "boutiques333.com",
    "sherwoodmastiff.com",
    "zljrsy.com",
    "tuberbytes.com",
    "gentciu.com",
    "lax2k.com",
    "hotelsanfelipeycasinos.com",
    "pungentvrtwan.xyz",
    "plein-exclusive.com",
    "juliareda.xyz",
    "tasq.digital",
    "spdrum.com",
    "anartravertine.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.730557103.0000000006BF F000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000000.730557103.0000000006BF F000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x26a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x2191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x27a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x291f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x140c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x991a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
00000007.00000000.730557103.0000000006BF F000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x5839:$sqlite3step: 68 34 1C 7B E1 • 0x594c:$sqlite3step: 68 34 1C 7B E1 • 0x5868:$sqlite3text: 68 38 2A 90 C5 • 0x598d:$sqlite3text: 68 38 2A 90 C5 • 0x587b:$sqlite3blob: 68 53 D8 7F 8C • 0x59a3:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.691567196.0000000003BF 1000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.691567196.0000000003BF 1000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x6fda8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x70012:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9d1c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9d432:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb45:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xa8f65:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x7b631:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xa8a51:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x7bc47:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xa9067:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x7bdbf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa91df:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x70a2a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 0 2 83 E3 0F C1 EA 06 • 0x9de4a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 0 2 83 E3 0F C1 EA 06 • 0x7a8ac:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa7ccc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x71723:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x9eb43:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x81db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xaf1d7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x82dba:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.EH5ro3Hyug.exe.2c48584.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
6.2.EH5ro3Hyug.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.EH5ro3Hyug.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.EH5ro3Hyug.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
6.2.EH5ro3Hyug.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

Injects a PE file into a foreign processes

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

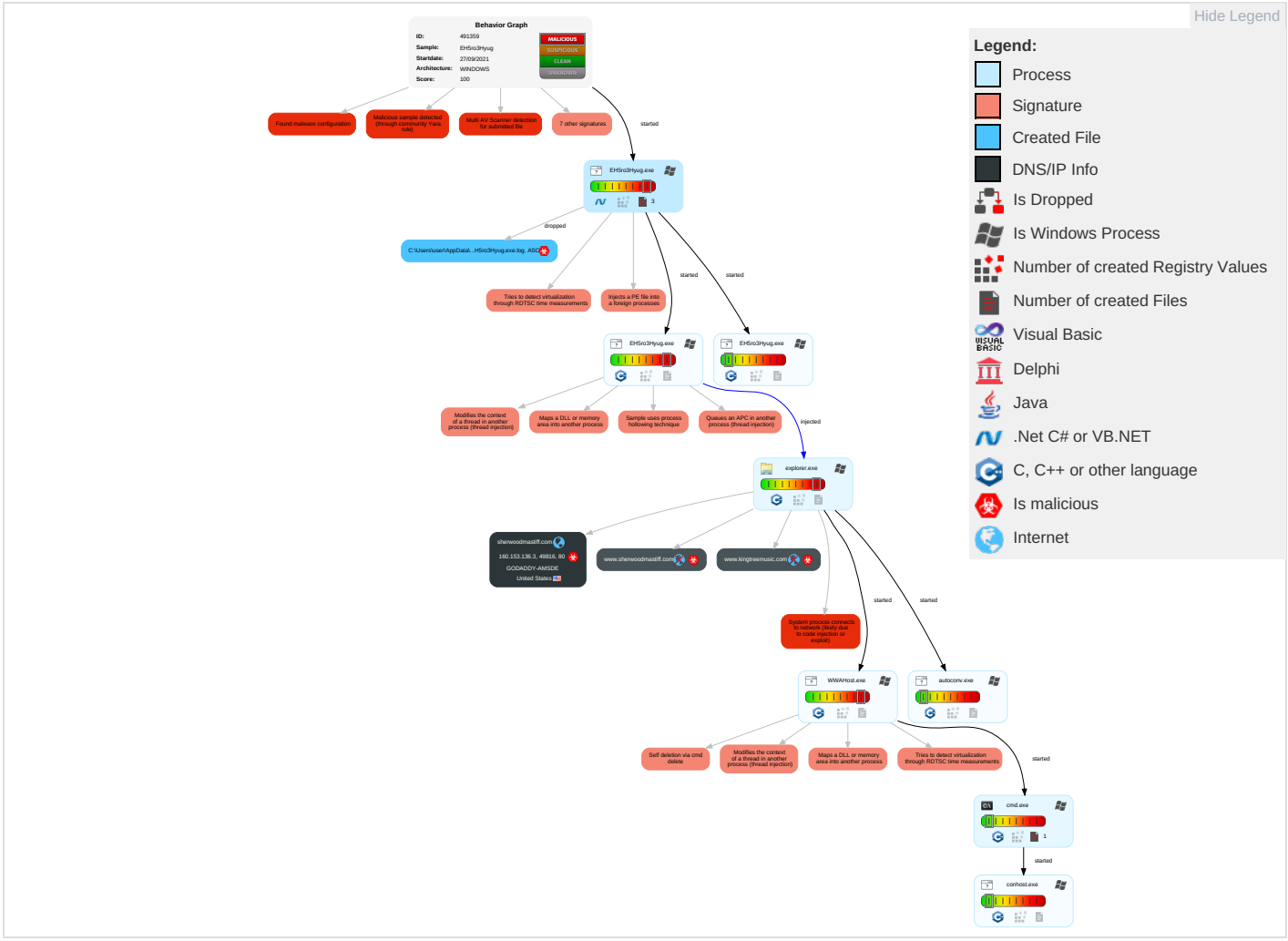
Remote Access Functionality:

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
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

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
EH5ro3Hyug.exe	32%	Virustotal		Browse
EH5ro3Hyug.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.EH5ro3Hyug.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comF	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.rspb.org.uk/wildlife/birdguide/name/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sherwoodmastiff.com/hht8/?V2=UdJvmcuMRIp/sNw0TNsoQAu26okuAPtZrfHvhR73KElz+11bxdQbtsNL5cLMDPcOzFi3&5j=SVeDzJKXh	0%	Avira URL Cloud	safe	
http://www.fontbureau.comma	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
www.eastwestasia-thailand.com/hht8/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sherwoodmastiff.com	160.153.136.3	true	true		unknown
www.sherwoodmastiff.com	unknown	unknown	true		unknown
www.kingtreemusic.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.sherwoodmastiff.com/hht8/?V2=UdJvmcuMRIp/sNw0TNsoQAu26okuAPtZrfHvhR73KElz+11bxdQbtsNL5cLMDPcOzFi3&5j=SVeDzJKXh	true	• Avira URL Cloud: safe	unknown
www.eastwestasia-thailand.com/hht8/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
160.153.136.3	sherwoodmastiff.com	United States		21501	GODADDY-AMSDE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491359
Start date:	27.09.2021
Start time:	14:06:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 43s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EH5ro3Hyug (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/1@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15% (good quality ratio 13.6%) • Quality average: 73.3% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:07:50	API Interceptor	1x Sleep call for process: EH5ro3Hyug.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
160.153.136.3	HSBC94302,pdf.exe	Get hash	malicious	Browse	• www.bowersllc.com/dhua/?dXj87bfP=DZJno2lRgPkpRcdocWJrBMQZQjsJd79nG0M0QfwGCvK21BDxR+MasdVU7jGMzvw95wLv&xXE=6lxdAHgP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EWVNnyXoRS.exe	Get hash	malicious	Browse	• www.freshstartdaycarecenterinc.com/9gdg/?f2JXBT=1v3lpljBMJCYkWxoO9X4xNLGQeZZzV6uKpc2hvA5k3bzcKM1l1sCAvVyxTYVjtF2eHPY&axoHc=0DKH6PKhnz
	h0nSzCFt9G.exe	Get hash	malicious	Browse	• www.theklownz.com/n092/?Tprx=X2JtatpP&nDKxbVC=xZ6zTG1wCRdW0FqK4OgDrOSOP6aEPheXUTUGB1IE7px35dVeIs23Fr9+4uCU9GYqzXnjYpRUWg==
	Noua comanda de achizitie.exe	Get hash	malicious	Browse	• www.mysekrit.com/bc3s/?aJEPmr=DJBLJBWp7PolwH&c67H=E5WphFATnbnaRyuRPAh/WM7mxWtd+hXJM8jzg0hRzLi18WQzRQA1DtRaKp9ybJtfHuLm
	1gKjQPdvon.exe	Get hash	malicious	Browse	• www.glassicsrentals.com/m8g0/?SHi8X8e=kIFpnZs5z0+/nBdZobov2JWoYGnsZajPGBKYo9xNlu1rTqVgFGN8GSwN3myxq3kKTQHE&eBZT=4hu4ZpopK40tQtZ
	ryfAIJHmKETyAPz.exe	Get hash	malicious	Browse	• www.elenabub.com/p90g/?EPlpdD=uE62JYvV/5U2/fRWjwpnPJKU4slz1TWRV2Vk0lZZok+3XHkdz6W6i967c7YQi5hog0lm&BVqH=e2J4M8j0PxD8N
	NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe	Get hash	malicious	Browse	• www.everythingswallow.com/kbl2/?X8sl8h70=Uk/4fiNFIrAENImNkq5NhDo1aeiSVlAy2lomCsVKXqRgqDXOUaCk1Fhsw/s2uep8GWm3&t48xlt=YTUh7PIXtPD8u2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	3RBawvxxeY.exe	Get hash	malicious	Browse	• www.theuptownstudios.info/9t6k/?4hSpe=TAUv81DSxy6V0s2DjsmVmlW9dThxq9Qh3VfSYdLZXbEdBy5Gfl0S0MTO7hpfTQbXNA8O7IBSiw==&vR-=9r04i4FhmzChinQP
	QUOTATION.exe	Get hash	malicious	Browse	• www.cash4homesutah.com/m4ts/?KHDXBF=Rm3izdospj+ubKB1yr5SLsgzRwjgsOIy5NO+YIygSe5cIeRylzQwpySVQfBc/5LYjUag&tR-DU=ETYX
	Wire Payment Instruction Copy.exe	Get hash	malicious	Browse	• www.inspirestudioprо.com/i6sj/?uXcXQBqH=t94SsO8+42teq3sPOf9U6i98tzsKIq7U/jnQ7PxqyfWoFehf0hfwbKSeXhGkM6wYPtS6&lJE=FtxTAri
	PO9887655.exe	Get hash	malicious	Browse	• www.urbanbrewlabs.com/b4nj/?cN6l=OTytRx&8pvtZZdH=c/k3B/qQLoWLUtYfSPtZzw/khWdVw3wR4gj5VtwnNNWeNzkUnQiITB7HG61rruTH1UQr
	CAGE8UjZmt.exe	Get hash	malicious	Browse	• www.communityalliances.info/sqwo/?BTcPlT=x54d9I74DaJAzviN+MS1pXoHUOdqhv+JR+CMH1qSiS+1nVekSYfxY910zMpU1pmlAJ3l/q09+w==&Lhh8C=k6AlV0GXb27dex6P
	Remmittance Advise.exe	Get hash	malicious	Browse	• www.therainbowmixpodcast.com/bqt25/?W6AlNtFX=/xKfFjhN+eyAVC6Cv1YZzoYouCAFleQi0yIHJdsCK3Y4L+/h2gPFpir6/wIzmD6ygeO8&3flpd=02MtKD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	gBMggUztPR.exe	Get hash	malicious	Browse	• www.incrementumgroup.net/r48a/?SBC=kgPRCp7FmQ1qwWhzLbVAL/f7zP1ea2V3mquIzjYnI+EbjRJ+tMFg9KWn0p67f8gCzaX/&t6ALcX=-ZWd9lh
	Arrival Notice.exe	Get hash	malicious	Browse	• www.trinitydevelopmentalcenter.com/ez2z/?5jol=fae+nqjkhrGHKaYu76qMZLgdHLYZuj/Lwm0k8H3w4k3+ncw63blTPeHnDJhmTCDQCDjeRLnTew==&YL0xrT=s8XX2FyPDZHtkN7
	REQUEST FOR QUOTATION.xlsx	Get hash	malicious	Browse	• www.travelscappadocia.com/att3/?xfL0sV=XrhpH4yhFbv&btxhA=+5e0lDgZQLIqG33OgwJ5eoDVaUzG8FsHDr0RYq+9Lz8oFts6A/WK7VPjrJB5GIMdGrEi/g==
	yioor3yi8n.exe	Get hash	malicious	Browse	• www.narrowpathwc.com/n8ba/?qj=RqoVB/kRDotnM81a68VGCKAD0SwVXhGBA2hw7fPCanVTcO/r0wYF2QFNLO8FObh2ftta&UR-=0xo0sHb06TyDihHP
	b123456.exe	Get hash	malicious	Browse	• www.filigreefilly.com/lt0h/?bPyXK=opnRKy5/zw2X/Pt/cp5raUaYUp/6F7xuOQIFNBYlrKALcWEu8e763T/HRu+eZeWA7ApY&6luD_=EBZlQlwxEd8T
	Pending DHL Shipment Notification REF 82621.exe	Get hash	malicious	Browse	• www.upstaff.info/ssee/?1b_l=4ho4nNKX7&vZAd4=pl6vF5RSB6Zko6xDNSoMUKF8L1+fNrh6HiwbFcH81l+QKpdcXo1xe9+iG1J+/pT7YSi+VPJCUw==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BIN.exe	Get hash	malicious	Browse	• www.narrowpathwc.com/n8ba/?l6El7rEX=RqoVB/kRDotnM81a68VGCKAD0SwVXhGBA2hw7fPCanVTcO/r0wYF2QFNLO8FObh2ftta&yBZ02=2df8xb-H6hatkZkp

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GODADDY-AMSDE	HSBC94302,pdf.exe	Get hash	malicious	Browse	• 160.153.136.3
	EWVNnyXoRS.exe	Get hash	malicious	Browse	• 160.153.136.3
	h0nSzCFt9G.exe	Get hash	malicious	Browse	• 160.153.136.3
	Noua comanda de achizitie.exe	Get hash	malicious	Browse	• 160.153.136.3
	1gKjQPdvon.exe	Get hash	malicious	Browse	• 160.153.136.3
	ryfAIJHmKETyAPz.exe	Get hash	malicious	Browse	• 160.153.136.3
	NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe	Get hash	malicious	Browse	• 160.153.136.3
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 160.153.249.159
	sora.arm	Get hash	malicious	Browse	• 160.153.212.153
	WIRE TRANSFER FOR $255,114.77 THROUGH OUR ACCOUNT OFFICER.exe	Get hash	malicious	Browse	• 160.153.129.29
	3RBawvxxeY.exe	Get hash	malicious	Browse	• 160.153.136.3
	qB6P2WfUjb.exe	Get hash	malicious	Browse	• 160.153.249.159
	8ft2Xvqgx2.exe	Get hash	malicious	Browse	• 160.153.249.159
	QUOTATION.exe	Get hash	malicious	Browse	• 160.153.136.3
	Wire Payment Instruction Copy.exe	Get hash	malicious	Browse	• 160.153.136.3
	WJRyvbvOD7.exe	Get hash	malicious	Browse	• 160.153.249.159
	o06RIULPrN.exe	Get hash	malicious	Browse	• 160.153.249.159
	wpljwjYfor.exe	Get hash	malicious	Browse	• 160.153.249.159
	ebBm41wULr.exe	Get hash	malicious	Browse	• 160.153.249.159
	PO9887655.exe	Get hash	malicious	Browse	• 160.153.136.3

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\EH5ro3Hyug.exe.log	
Process:	C:\Users\user\Desktop\EH5ro3Hyug.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1309
Entropy (8bit):	5.3528008810928345

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\EH5ro3Hyug.exe.log	
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84aE4Ks:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzg
MD5:	542338C5A30B02E372089FECDC54D607
SHA1:	6FAD29FF14686FC847B160E876C1E078333F6DCB
SHA-256:	6CEA4E70947B962733754346CE49553BE3FB6E1FB3949C29EC22FA9CA4B7E7B6
SHA-512:	FE4431305A8958C4940EB4AC65723A38DA6057C3D30F789C6EDDEBA8962B62E9C0583254E74740855027CF3AE9315E3001A7EEB54168073ED0D2AB9B1F05503A
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.790198320706062
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	EH5ro3Hyug.exe
File size:	860672
MD5:	dff3bf025dcd487a2f0fb22b4ccf8998
SHA1:	1ff59c9410fb281ffc8d2c3c1fc3268eacd5dba1
SHA256:	230b56b1d072725eff3a0e100515ba924377c9f0a79308bbfa3123269ee23d56
SHA512:	088c3395be1bf0ef0de2135d0588c6106c5a5f279b9b40761f58298db8368a31107820dd621d66d2656b18417bf06e025a8cd3700075daeaa393ab5a62b5e899
SSDEEP:	12288:JIR5so4GVamo1M3de8zo70QuynMwr/amKEDm4fgGvSw24MLGhovWdo9S7LCn1tNP:3fqIFUF+W2L0YvUrzmOSha+u
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..... .....@.. .....@.....

File Icon

Icon Hash:	138e8ecece8cccc

Static PE Info

General

Entrypoint:	0x4ba7d2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61511619 [Mon Sep 27 00:53:45 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb87d8	0xb8800	False	0.678409235264	data	7.04755215007	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x1944c	0x19600	False	0.391750692734	data	4.29647851076	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 14:09:05.803047895 CEST	192.168.2.4	8.8.8.8	0xc3f5	Standard query (0)	www.sherwoodmastiff.com	A (IP address)	IN (0x0001)
Sep 27, 2021 14:09:24.108165026 CEST	192.168.2.4	8.8.8.8	0x48b9	Standard query (0)	www.kingtreemusic.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 14:09:05.840178967 CEST	8.8.8.8	192.168.2.4	0xc3f5	No error (0)	www.sherwoodmastiff.com	sherwoodmastiff.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 14:09:05.840178967 CEST	8.8.8.8	192.168.2.4	0xc3f5	No error (0)	sherwoodmastiff.com		160.153.136.3	A (IP address)	IN (0x0001)
Sep 27, 2021 14:09:24.331362009 CEST	8.8.8.8	192.168.2.4	0x48b9	Name error (3)	www.kingtreemusic.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.sherwoodmastiff.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49816	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:09:05.876187086 CEST	5733	OUT	GET /hht8/?V2=UdJvmcuMRIp/sNw0TNsoQAu26okuAPtZrfHvhR73KElz+11bxdQbtsNL5cLMDPcOzFi3&5j=SVeDzJKXh HTTP/1.1 Host: www.sherwoodmastiff.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 14:09:05.902458906 CEST	5734	IN	HTTP/1.1 400 Bad Request Connection: close

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

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EH5ro3Hyug.exe PID: 6400 Parent PID: 6056

General

Start time:	14:07:41
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\EH5ro3Hyug.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\EH5ro3Hyug.exe'
Imagebase:	0x810000
File size:	860672 bytes
MD5 hash:	DFF3BF025DCD487A2F0FB22B4CCF8998
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.691567196.0000000003BF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.691567196.0000000003BF1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.691567196.0000000003BF1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.689143123.0000000002BF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.689245304.0000000002C6F000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: EH5ro3Hyug.exe PID: 5412 Parent PID: 6400

General

Start time:	14:07:51
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\EH5ro3Hyug.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\EH5ro3Hyug.exe
Imagebase:	0xc0000
File size:	860672 bytes
MD5 hash:	DFF3BF025DCD487A2F0FB22B4CCF8998
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: EH5ro3Hyug.exe PID: 5660 Parent PID: 6400

General

Start time:	14:07:51
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\EH5ro3Hyug.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\EH5ro3Hyug.exe
Imagebase:	0xf20000
File size:	860672 bytes
MD5 hash:	DFF3BF025DCD487A2F0FB22B4CCF8998
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: 00000006.00000002.753692091.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.753692091.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.753692091.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.754960764.0000000001890000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.754960764.0000000001890000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.754960764.0000000001890000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.754337166.0000000001860000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.754337166.0000000001860000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.754337166.0000000001860000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 5660

General

Start time:	14:07:53
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000007.00000000.730557103.0000000006BFF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.730557103.0000000006BFF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.730557103.0000000006BFF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.714656452.0000000006BFF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.714656452.0000000006BFF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.714656452.0000000006BFF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autoconv.exe PID: 7104 Parent PID: 3424

General

Start time:	14:08:19
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0xd50000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: WWAHost.exe PID: 7092 Parent PID: 3424

General

Start time:	14:08:20
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0x9b0000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
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: 0000000C.00000002.934957623.00000000037B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.934957623.00000000037B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.934957623.00000000037B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.934785962.0000000003080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.934785962.0000000003080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.934785962.0000000003080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.934221004.0000000002A80000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.934221004.0000000002A80000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.934221004.0000000002A80000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4972 Parent PID: 7092

General

Start time:	14:08:24
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\EH5ro3Hyug.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5548 Parent PID: 4972

General

Start time:	14:08:24
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis