ID: 532909
Sample Name: Y1p8VPvyU2
Cookbook: default.jbs
Time: 19:58:13
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

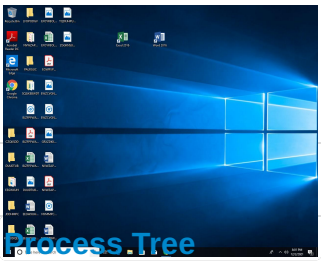
Windows Analysis Report Y1p8VPvyU2

Overview

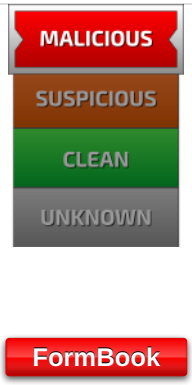
General Information

Sample Name:	Y1p8VPvyU2 (renamed file extension from none to exe)
Analysis ID:	532909
MD5:	83be105c9fa2427.
SHA1:	1430baa740d2cd..
SHA256:	8cd61259417101..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

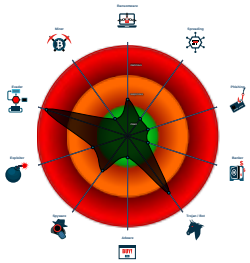


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…
- Queues an APC in another process …
- Tries to detect virtualization through…

Classification



- **System is w10x64**
- Y1p8VPvyU2.exe (PID: 7100 cmdline: "C:\Users\user\Desktop\Y1p8VPvyU2.exe" MD5: 83BE105C9FA2427BD6079F5D19659596)
  - Y1p8VPvyU2.exe (PID: 1304 cmdline: "C:\Users\user\Desktop\Y1p8VPvyU2.exe" MD5: 83BE105C9FA2427BD6079F5D19659596)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 4816 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 3192 cmdline: /c del "C:\Users\user\Desktop\Y1p8VPvyU2.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.tgalegail.quest/n6fr/"
  ],
  "decoy": [
    "magnetic-island-qld.com",
    "yr-golf.com",
    "udyam-registration.com",
    "paulsamaco.com",
    "mimisminiatureboutique.store",
    "csspadding.com",
    "gujaratigyaan.com",
    "findphotographersonline.com",
    "clevelawareness.com",
    "purelyhawaii.com",
    "2axx.com",
    "tricktodance.com",
    "getstoic.com",
    "globexglobalstore.com",
    "mysticnail.net",
    "handejqr.com",
    "letswatch.online",
    "lnfddttoyof6.xyz",
    "tdc-trust.com",
    "federalimmigrationgola.com",
    "cinasing.com",
    "614721.com",
    "pumpizy.com",
    "satsumauosen-official.com",
    "fairytalesinc.com",
    "fastbest.host",
    "assisttm.com",
    "triniautotrader.com",
    "alissanoume.xyz",
    "ma-manger.com",
    "twinpick.paris",
    "easycv4u.com",
    "xn--2i0bm4p1b62jv8dxz3b7uj.com",
    "ventleetailoronline.com",
    "8355512.win",
    "catlyfoundation.com",
    "mygeorgecolemanfordstory.com",
    "haiphongmap.com",
    "canvasb.net",
    "salvationhubtv.com",
    "teamisenberg.com",
    "innoclubs.com",
    "glwcn.net",
    "byshelly.biz",
    "commongroundcowork.com",
    "zhonglucredit.com",
    "tyjgfuke.com",
    "caixadepandora.club",
    "webuywholesalerhouses.com",
    "hundvardag.com",
    "nchh02.xyz",
    "oqnr.top",
    "rapidfreecredit.com",
    "alquilarorihuela.com",
    "medicijnenshop.com",
    "somoslaostra.com",
    "luvvlyjubblyshop.com",
    "housestephenson.com",
    "39abxx.com",
    "gsjbd1.club",
    "luisantonioenedina.com",
    "xn--pckwb0cye6947ajzku8opzi.com",
    "jakihmentha.quest",
    "clothingteesshop.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000001.304934739.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000001.304934739.0000000000400000.00000040.00020000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000001.304934739.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000000.304424908.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000000.304424908.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$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
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Y1p8VPvyU2.exe.2420000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Y1p8VPvyU2.exe.2420000.1.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.Y1p8VPvyU2.exe.2420000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cd9:$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:$sqlite3blob: 68 53 D8 7F 8C
1.0.Y1p8VPvyU2.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.0.Y1p8VPvyU2.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$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 28 entries				

Copyright Joe Security LLC 2021

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

Multi AV Scanner detection for dropped file

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)

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

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

Copyright Joe Security LLC 2021

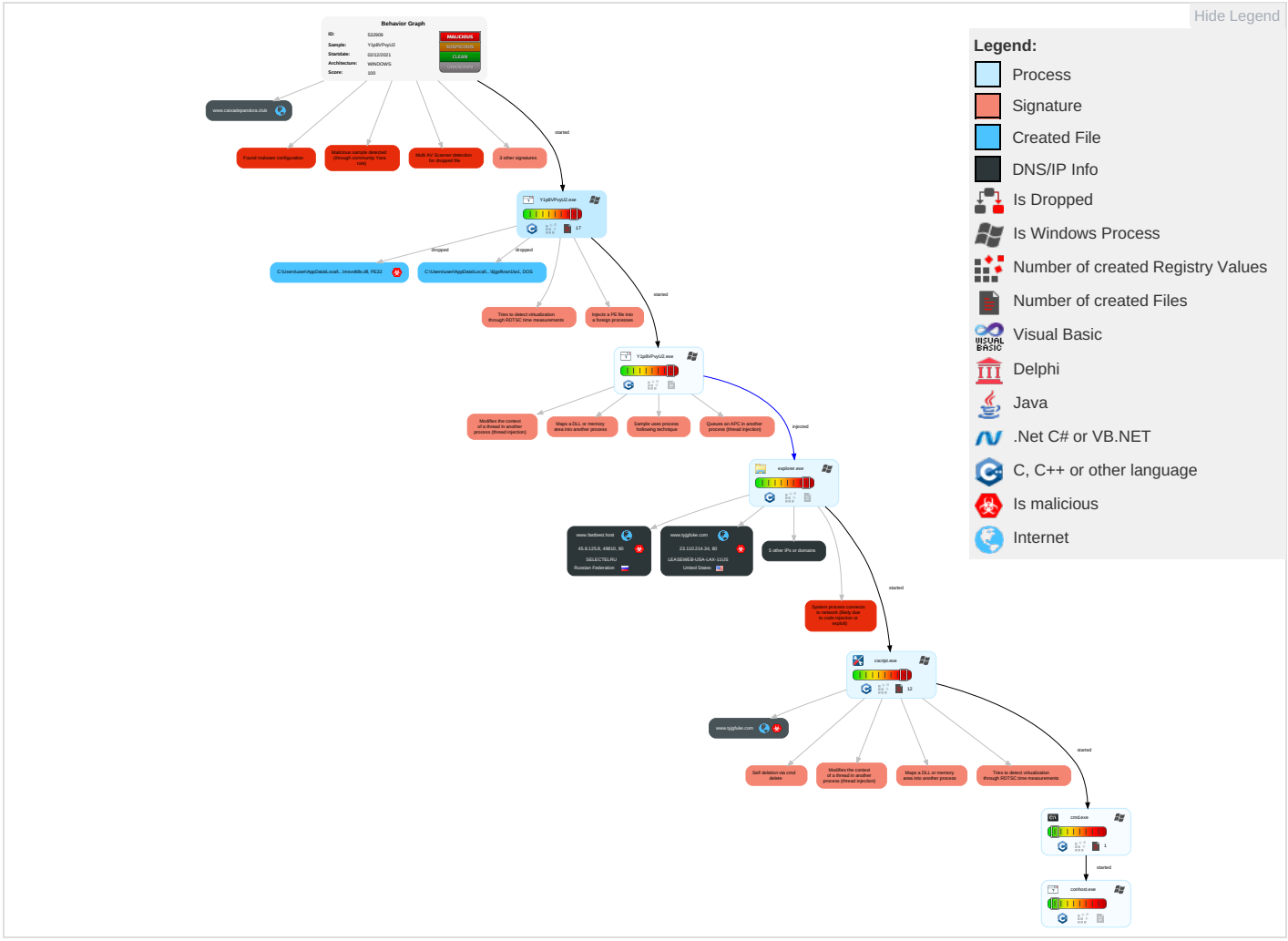
Remote Access Functionality:

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 6 1 2	Virtualization/Sandbox Evasion 2	Input Capture 1	Security Software Discovery 2 5 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 6 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
Y1p8VPvyU2.exe	35%	Virustotal		Browse
Y1p8VPvyU2.exe	9%	Metadefender		Browse
Y1p8VPvyU2.exe	64%	ReversingLabs	Win32.Trojan.Swotter	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsj1052.tmp\msvofdls.dll	50%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.Y1p8VPvyU2.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Y1p8VPvyU2.exe.2420000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.Y1p8VPvyU2.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
6.2.cscript.exe.592796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.1.Y1p8VPvyU2.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.Y1p8VPvyU2.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.Y1p8VPvyU2.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.Y1p8VPvyU2.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.Y1p8VPvyU2.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
1.0.Y1p8VPvyU2.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
6.2.cscript.exe.35c8670.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.Y1p8VPvyU2.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
yr-golf.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fastbest.host/n6fr/?W0Gd5=_zrxFrQh&r8Yhe8X=RitrxMT4CF2430UT8yTHljH4YcWCFGycH+KnQUedz6G1CLl+fZ1eccWunXIbAos2Mzom	0%	Avira URL Cloud	safe	
http://https://fastbest.host	0%	Avira URL Cloud	safe	
http://www.assisttm.com/n6fr/?r8Yhe8X=GhRWdiRsNNJH8eQL+yxTqcpdK2zUc5yAzRv8ilcs8c/60sXMgS13/r7ilAGjTWuYzon7&W0Gd5=_zrxFrQh	0%	Avira URL Cloud	safe	
www.tgalegail.quest/n6fr/	0%	Avira URL Cloud	safe	
http://www.yr-golf.com/n6fr/?W0Gd5=_zrxFrQh&r8Yhe8X=BQDMjsZC/MHMhOokLNCZ8NvLdfoNcIlcbjuvjCJyzVYcZRVM3RE3M6YlVSnQ+pY87GBB	0%	Avira URL Cloud	safe	
http://www.tyjgfuke.com/$t	0%	Avira URL Cloud	safe	
http://www.tyjgfuke.com/n6fr/?r8Yhe8X=LSrsi9BeeNNPJfOX4A9nLsTLbEdx4M4dJGVYJBt	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.tyjgfuke.com	23.110.214.34	true	true		unknown
assisttm.com	34.102.136.180	true	false		unknown
yr-golf.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.fastbest.host	45.8.125.8	true	true		unknown
www.caixadepandora.club	137.184.111.224	true	false		unknown
www.assisttm.com	unknown	unknown	true		unknown
www.gsjbd1.club	unknown	unknown	true		unknown
www.yr-golf.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.fastbest.host/n6fr/?W0Gd5=_zrxFrQh&r8Yhe8X=RitrxMT4CF2430UT8yTHljH4YcWCFGycH+KnQUedz6G1CLl+fZ1eccWunXIbAos2Mzom	true	• Avira URL Cloud: safe	unknown
http://www.assisttm.com/n6fr/?r8Yhe8X=GhRWdiRsNNJH8eQL+yxTqcpdK2zUc5yAzRv8ilcs8c/60sXMgS13/r7ilAGjTWuYzon7&W0Gd5=_zrxFrQh	false	• Avira URL Cloud: safe	unknown
www.tgalegail.quest/n6fr/	true	• Avira URL Cloud: safe	low
http://www.yr-golf.com/n6fr/?W0Gd5=_zrxFrQh&r8Yhe8X=BQDMjsZC/MHMhOokLNCZ8NvLdfoNcIlcbjuvjCJyzVYcZRVM3RE3M6YlVSnQ+pY87GBB	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	assisttm.com	United States		15169	GOOGLEUS	false
23.110.214.34	www.tyjgfuke.com	United States		395954	LEASEWEB-USA-LAX-11US	true
45.8.125.8	www.fastbest.host	Russian Federation		49505	SELECTELRU	true

Copyright Joe Security LLC 2021

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532909
Start date:	02.12.2021
Start time:	19:58:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Y1p8VPvyU2 (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:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/2@7/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.8% (good quality ratio 19.7%) • Quality average: 74.7% • Quality standard deviation: 31.6%
HCA Information:	• Successful, ratio: 87% • 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

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.fastbest.host	Medtronics Product catalog and prices_pdf.exe	Get hash	malicious	Browse	• 194.54.163.227

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-LAX-11US	RFQ - SST#2021111503.exe	Get hash	malicious	Browse	• 108.187.86.48
	YjKK5XYBzB	Get hash	malicious	Browse	• 172.255.161.176
	JUyE95BLaL	Get hash	malicious	Browse	• 172.255.161.168
	9hyE41yNDB	Get hash	malicious	Browse	• 23.86.78.90
	triage_dropped_file.exe	Get hash	malicious	Browse	• 23.110.31.106
	vbc.exe	Get hash	malicious	Browse	• 23.110.31.106
	xd.x86	Get hash	malicious	Browse	• 23.80.138.175
	eKmL8hvXz2	Get hash	malicious	Browse	• 108.187.220.76
	TsOl2c6Yc6	Get hash	malicious	Browse	• 23.83.26.237
	SALES CONFIRMATION 153_154 SN.xlsx	Get hash	malicious	Browse	• 23.110.31.106
	oQANZnrt9d	Get hash	malicious	Browse	• 23.83.26.245
	xzKS6P1qDo.exe	Get hash	malicious	Browse	• 23.104.53.233
	apep.mips	Get hash	malicious	Browse	• 108.187.80.246
	7H5yVEypQX	Get hash	malicious	Browse	• 23.85.79.155
	7OjVU04f8q.exe	Get hash	malicious	Browse	• 23.110.31.75
	DuxgwH47QB.exe	Get hash	malicious	Browse	• 23.110.128.234
	ORDER.doc	Get hash	malicious	Browse	• 23.110.128.234
	SWIFT-MLSB-11,546__doc.exe	Get hash	malicious	Browse	• 23.110.95.195
	BwJriVGrt5.exe	Get hash	malicious	Browse	• 23.110.31.77
	29383773738387477474774.exe	Get hash	malicious	Browse	• 142.234.161.17
SELECTELRU	uATT8vAUK9.exe	Get hash	malicious	Browse	• 95.213.165.249
	1Y0xc70fbX.exe	Get hash	malicious	Browse	• 95.213.165.249
	SecuriteInfo.com.Packed-GDV0304D0F07C5D.24466.exe	Get hash	malicious	Browse	• 95.213.165.249
	SecuriteInfo.com.W32.AIDetect.malware1.19028.exe	Get hash	malicious	Browse	• 95.213.165.249
	8VvzOu0uHY.exe	Get hash	malicious	Browse	• 95.213.165.249
	koCttsCjGY.exe	Get hash	malicious	Browse	• 95.213.165.249
	oCBC1EaZ9G.exe	Get hash	malicious	Browse	• 95.213.165.249
	LF6pwW1llz.exe	Get hash	malicious	Browse	• 37.9.13.169
	DvWDF1pMu7.exe	Get hash	malicious	Browse	• 95.213.165.249
	gSSvliK2kn.exe	Get hash	malicious	Browse	• 95.213.165.249
	gjYAgorDLm.exe	Get hash	malicious	Browse	• 95.213.165.249
	zPeXh7zbd3.exe	Get hash	malicious	Browse	• 95.213.165.249
	2KWErWhXoQ.exe	Get hash	malicious	Browse	• 95.213.165.249
	Nh3xqMPynb.exe	Get hash	malicious	Browse	• 95.213.165.249
	MN5wZ55l17.exe	Get hash	malicious	Browse	• 95.213.165.249
	QMn13jz6nj.exe	Get hash	malicious	Browse	• 95.213.165.249
	v72n86vFFq.exe	Get hash	malicious	Browse	• 95.213.165.249
	DOC-BRAD _ 26TH_NOVEMBER_2021 _.HTM	Get hash	malicious	Browse	• 92.53.68.205
	t2yFh0lOxM.exe	Get hash	malicious	Browse	• 185.189.167.130
	vwLliS25F5.exe	Get hash	malicious	Browse	• 95.213.165.229

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsj1052.tmp\msvofdls.dll	product list.xlsx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\6jgsfkran1lw1	product list.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\6jgsfkran1lw1

Process:	C:\Users\user\Desktop\Y1p8VPvyU2.exe
File Type:	DOS executable (COM, 0x8C-variant)

C:\Users\user\AppData\Local\Temp\6jgsfkran1lw1	
Category:	dropped
Size (bytes):	217235
Entropy (8bit):	**7.9937809161987765**
Encrypted:	**true**
SSDEEP:	6144:W4FmTjet9fxOzh9Ky33TDMfVwr37hQnll6V:GE9YzhogvMfm3oll
MD5:	75ACE7B8440CE829D653343E18EAE33A
SHA1:	09F23DD8962701C4D5213E2A7AA395985E8963DE
SHA-256:	A4CAE10880D0DD180CC5B92E38F449EE244E83186725BD1257312DCC05AA4E48
SHA-512:	F4BC54E1396D9AF6E61ED270B068D60475F357BD3258ABF4E659D75FD81D27D173BBB2126D646BA51736B3EA82CEC03F5D4A1D9D8FEFC6E1599333827B7AB2A0
Malicious:	false
Joe Sandbox View:	• Filename: product list.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	..;.7w.GJ0s...TS.G.4.%..zI..E.,...f.....be.....T{..;Q.....";.D=..Z.t...!...Gkl..Jy...;.G.....4.$...5.\..}M&.....B.#}..f...\...fj.=4.8.@.....d.JmH...8A...Ua6..G...vr.jC..c..\.^ ....w...y..1.6....j#.B}.G.Z=..I.O.. .".XN...]..7w.\.....G..E.T.,k...f...,..be.....&T{...E.....W..U^.j...}...N..oU.y.....P)..... P..S%..4.$...5....,....9...D..F?..^.e.c..`c.m.@o.%n_8.L..I :..w.8A...U..D...v..jC..c.....?..q...w...y....@....j.B}.J.Zx..I.O.....".XN....]..7w.y..K.....3..E.,...f.....be.....&T{...E.....W..U^.j...}...N..oU.y.....P)..... P..S%..4.$...5....,.... .9...D..F?..^.e.c..`c.m.@o.%n_8.L..lJmH...8AV..U..D.n..vr.jC..c.....?..q...w...y....@....j.B}.J.Zx..I.O.....".XN....]..7w.y..K.....3..E.,...f.....be.....&T{...E.....W..U^.j...}. ..N..oU.y.....P)..... P..S%..4.$...5....,....9...D..F?..^.e.c..`c.m.@o.%n_8.L..lJmH...8AV..U..D.n..vr.jC..c.....?..q...w...y....@....

C:\Users\user\AppData\Local\Temp\nsj1052.tmp\msvofdls.dll	
Process:	C:\Users\user\Desktop\Y1p8VPvyU2.exe
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137728
Entropy (8bit):	6.411397085063496
Encrypted:	false
SSDEEP:	1536:gmPsLrHeJTgGJPLlr0VOGfTRisu0/8UgCUoXD2/Y+z4o8QqbfvZ2BksWjcd8EmjN:sLz0gGJPprwr/dXDZE2Z2B8E8
MD5:	4881ED27473CD15B3FCC072F11465658
SHA1:	37A29E690965E233CA4B89538A77188DC2048BFF
SHA-256:	13FA843E8D2B2E3A9699F9F71A8AD152EA94995B1045891B6B91CFA9674B69F8
SHA-512:	ED198137652861DB9A6595FEDC6E376EA2BC730E5D6BC8D58B203F07814200529597AD5B24EE8409942222CB18674DDE38422B82FFCD057E63ACC9233E6EAFF
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50%
Joe Sandbox View:	• Filename: product list.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;6.A.W...W...W..r.s.^W..r.M.oW..r.r..W....\.|W....Y.lW...W...W .....~W.....~W....m.~W.....~W..Rich.W.....PE..L....R.a.....!.....p.....T.....L.....`.....0..... .....P...@.....<.....text...L..... ..`.rdata...R.....T.....@..@.data....U.....:.....@....rsrc.....`.....@..B.... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.939366323187133
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	Y1p8VPvyU2.exe
File size:	318467
MD5:	83be105c9fa2427bd6079f5d19659596
SHA1:	1430baa740d2cd40a507cbfa8fe62e3d78424315
SHA256:	8cd6125941710166af38133bce6cae9f9cc41c8d88ff774cd691081d193015a1

General

SHA512:	09a2c3c9d9b147e6c25d824c931b2c0f4f9daaccdbde4a28ad0955be63642e11cb23df8f1d85e719b2b0b535e55b0c2cfb7168312c0f082d8b4f9d1072efdd3e
SSDEEP:	6144:rGiw8TRbniXVRaPCuyCxGfYy33TGBbXU2gx7hQn+l6aFu00D/4e3aKize/q:bTwXVRACauYgFo+q0K4VKizR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030e3
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:	0x48EFCDCD [Fri Oct 10 21:49:01 2008 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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b68	0x5c00	False	0.67722486413	data	6.48746502716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.4337890625	data	5.04904254867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.58203125	data	4.76995537906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x900	0xa00	False	0.4078125	data	3.93441125971	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Copyright Joe Security LLC 2021

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-20:00:36.476668	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49777	34.102.136.180	192.168.2.3
12/02/21-20:00:41.788599	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49793	34.102.136.180	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 20:00:36.186220884 CET	192.168.2.3	8.8.8.8	0x10ba	Standard query (0)	www.yr-golf.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:41.495348930 CET	192.168.2.3	8.8.8.8	0xc7e4	Standard query (0)	www.assisttm.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:46.807691097 CET	192.168.2.3	8.8.8.8	0x498e	Standard query (0)	www.gsjbd1.club	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:51.858485937 CET	192.168.2.3	8.8.8.8	0x9dd7	Standard query (0)	www.tyjgfuke.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:16.770849943 CET	192.168.2.3	8.8.8.8	0x9969	Standard query (0)	www.tyjgfuke.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:18.165642023 CET	192.168.2.3	8.8.8.8	0x7c7d	Standard query (0)	www.fastbest.host	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:23.519859076 CET	192.168.2.3	8.8.8.8	0xe521	Standard query (0)	www.caixadepandora.club	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 20:00:36.210366011 CET	8.8.8.8	192.168.2.3	0x10ba	No error (0)	www.yr-golf.com	yr-golf.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:00:36.210366011 CET	8.8.8.8	192.168.2.3	0x10ba	No error (0)	yr-golf.com		34.102.136.180	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:41.519289017 CET	8.8.8.8	192.168.2.3	0xc7e4	No error (0)	www.assisttm.com	assisttm.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:00:41.519289017 CET	8.8.8.8	192.168.2.3	0xc7e4	No error (0)	assisttm.com		34.102.136.180	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:46.831301928 CET	8.8.8.8	192.168.2.3	0x498e	Name error (3)	www.gsjbd1.club	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:52.032300949 CET	8.8.8.8	192.168.2.3	0x9dd7	No error (0)	www.tyjgfuke.com		23.110.214.34	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:16.942539930 CET	8.8.8.8	192.168.2.3	0x9969	No error (0)	www.tyjgfuke.com		23.110.214.34	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 20:01:18.359935045 CET	8.8.8.8	192.168.2.3	0x7c7d	No error (0)	www.fastbest.host		45.8.125.8	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:23.555322886 CET	8.8.8.8	192.168.2.3	0xe521	No error (0)	www.caixadepandora.club		137.184.111.224	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.yr-golf.com
- www.assisttm.com
- www.fastbest.host

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49777	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:36.234204054 CET	8401	OUT	GET /n6fr/?W0Gd5=_zrxFrQh&r8Yhe8X=BQDMjsZC/MHMhOokLNCZ8NvLdfoNcIlcbjuvjCJyzVYcZRVM3RE3M6YlVSnQ+pY87GBB HTTP/1.1 Host: www.yr-golf.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:00:36.476667881 CET	8403	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 02 Dec 2021 19:00:36 GMT Content-Type: text/html Content-Length: 275 ETag: "61973ffe-113" Via: 1.1 google 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 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49793	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:41.543401957 CET	8436	OUT	GET /n6fr/?r8Yhe8X=GhRWdiRsNNJH8eQL+yxTqcpdK2zUc5yAzRv8ilcs8c/60sXMgS13/r7ilAGjTWuYzon7&W0Gd5=_zrxFrQh HTTP/1.1 Host: www.assisttm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:41.788599014 CET	8437	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 02 Dec 2021 19:00:41 GMT Content-Type: text/html Content-Length: 275 ETag: "61a4f026-113" Via: 1.1 google 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 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49810	45.8.125.8	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:01:18.436930895 CET	8482	OUT	GET /n6fr/?W0Gd5=_zrxFrQh&r8Yhe8X=RitrxMT4CF2430UT8yTHljH4YcWCFGycH+KnQUedz6G1CLl+fZ1eccWunXIbAos2Mzom HTTP/1.1 Host: www.fastbest.host Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:01:18.510102034 CET	8483	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 02 Dec 2021 19:01:18 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 7081 Connection: close Last-Modified: Mon, 27 Sep 2021 00:52:07 GMT ETag: "1ba9-5ccef81a2c93b" Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 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 2e 30 22 3e 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 20 63 6f 6e 74 65 6e 74 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 66 61 73 74 62 65 73 74 20 2d 20 d0 a5 d0 be d1 81 d1 82 d0 b8 d0 bd d0 b3 20 d0 b4 d0 bb d1 8f 20 d0 ba d0 b0 d0 b6 d0 b4 d0 be d0 b3 d0 be 20 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 70 6e 67 22 20 68 72 65 66 3d 22 73 71 55 49 6d 44 43 56 4b 41 73 37 2e 69 63 6f 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 67 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 32 3f 66 61 6d 69 6c 79 3d 4f 70 65 6e 2b 53 61 6e 73 3a 77 67 68 74 40 33 30 30 3b 34 30 30 3b 36 30 30 3b 37 30 30 3b 38 30 30 26 61 6d 70 3b 64 69 73 70 6c 61 79 3d 73 77 61 70 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 32 3f 66 61 6d 69 6c 79 3d 4a 6f 73 65 66 69 6e 2b 53 61 6e 73 3a 77 67 68 74 40 34 30 30 3b 35 30 30 3b 36 30 30 3b 37 30 30 26 61 6d 70 3b 64 69 73 70 6c 61 79 3d 73 77 61 70 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 73 73 2f 51 44 54 38 59 66 4e 30 42 46 63 4d 2e 63 73 73 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 73 73 2f 6f 6f 68 4f 71 6c 77 38 70 6c 39 6e 68 2e 63 73 73 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 73 73 2f 4c 43 50 36 72 75 4c 70 4d 48 5a 58 2e 63 73 73 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 73 73 2f 4a 35 68 6c 79 71 37 76 34 4c 71 49 2e 63 73 73 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 73 73 2f 65 75 76 7a 64 30 52 4f 37 4d 6e 75 2e 63 73 73 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 73 73 2f 72 56 4b 65 49 68 34 52 47 67 34 30 2e 63 73 73 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta name="description" content> <title>fastbest - </title> <link rel="icon" type="image/png" href="sqUImDCVKAs7.ico"> <link href="https://fonts.googleapis.com/css2?family=Open+Sans:wght@300;400;600;700;800&display=swap" rel="stylesheet"> <link rel="preconnect" href="https://fonts.gstatic.com"> <link href="https://fonts.googleapis.com/css2?family=Josefin+Sans:wght@400;500;600;700&display=swap" rel="stylesheet"> <link rel="stylesheet" href="css/QDT8YfN0BFcM.css"> <link rel="stylesheet" href="css/hKfqNjwXPSze.css"> <link rel="stylesheet" href="css/atTcsRJOLoMl.css"> <link rel="stylesheet" href="css/ohOqlw8pl9nh.css"> <link rel="stylesheet" href="css/LCP6ruLpMHZX.css"> <link rel="stylesheet" href="css/J5hlyq7v4LqI.css"> <link rel="stylesheet" href="css/euvzd0RO7Mnu.css"> <link rel="stylesheet" href="css/rVKeIh4RGg40.css"> <link rel="stylesh

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Y1p8VPvyU2.exe PID: 7100 Parent PID: 1688

General

Start time:	19:59:12
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Y1p8VPvyU2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Y1p8VPvyU2.exe"
Imagebase:	0x400000
File size:	318467 bytes
MD5 hash:	83BE105C9FA2427BD6079F5D19659596
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: 00000000.00000002.305776988.0000000002420000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.305776988.0000000002420000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.305776988.0000000002420000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Y1p8VPvyU2.exe PID: 1304 Parent PID: 7100

General

Start time:	19:59:14
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Y1p8VPvyU2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Y1p8VPvyU2.exe"

Copyright Joe Security LLC 2021

Imagebase:	0x400000
File size:	318467 bytes
MD5 hash:	83BE105C9FA2427BD6079F5D19659596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.304934739.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.304934739.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.304934739.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.304424908.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.304424908.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.304424908.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.303509344.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.303509344.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.303509344.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.361567881.0000000000670000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.361567881.0000000000670000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.361567881.0000000000670000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.361497642.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.361497642.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.361497642.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.361714769.00000000009E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.361714769.00000000009E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.361714769.00000000009E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 1304

General

Start time:	19:59:18
Start date:	02/12/2021
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: 00000003.00000000.336290310.0000000010086000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.336290310.0000000010086000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.336290310.0000000010086000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cscript.exe PID: 4816 Parent PID: 3352

General

Start time:	19:59:40
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x1300000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
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: 00000006.00000002.565875481.0000000001220000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.565875481.0000000001220000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.565875481.0000000001220000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.567386686.00000000038B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.567386686.00000000038B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.567386686.00000000038B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.566653867.0000000003440000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.566653867.0000000003440000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.566653867.0000000003440000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 3192 Parent PID: 4816

General

Start time:	19:59:44
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Y1p8VPvyU2.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: 2332 Parent PID: 3192

General

Start time:	19:59:46
Start date:	02/12/2021
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021