ID: 432719
Sample Name: 5SXTKXCnqS
Cookbook: default.jbs
Time: 17:41:33
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report 5SXTKXCnqS

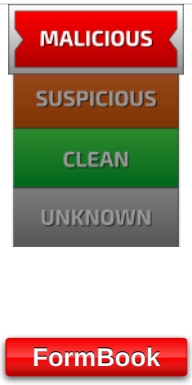
Overview

General Information

Sample Name:	5SXTKXCnqS (renamed file extension from none to exe)
Analysis ID:	432719
MD5:	cb4947e5c78ada..
SHA1:	eb2c2d329e9be0..
SHA256:	02230fb80db0fe0..
Tags:	exe
Infos:	

Most interesting Screenshot:

Detection



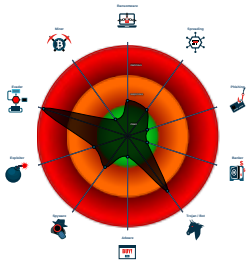
FormBook

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…
- 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…
- Queues an APC in another process …

Classification



- **System is w10x64**
- 5SXTKXCnqS.exe (PID: 5828 cmdline: 'C:\Users\user\Desktop\5SXTKXCnqS.exe' MD5: CB4947E5C78ADA624D22C28EE9079871)
  - 5SXTKXCnqS.exe (PID: 4328 cmdline: 'C:\Users\user\Desktop\5SXTKXCnqS.exe' MD5: CB4947E5C78ADA624D22C28EE9079871)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 4940 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 1384 cmdline: /c del 'C:\Users\user\Desktop\5SXTKXCnqS.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.updatesz.com/hlx/"
  ],
  "decoy": [
    "firo.store",
    "unmeasured-grace.com",
    "burger-ff.com",
    "alcargomoversllc.com",
    "brianratkevich.com",
    "semugaralara01.net",
    "ngalvision.com",
    "texaslearningpods.com",
    "ontarioboatcharters.com",
    "kleinrugcleaning.com",
    "michaelvancebromfield.com",
    "habitameya.com",
    "elyoma.com",
    "worldtvepisode.com",
    "masatakahorie.com",
    "jumpinginfo.com",
    "hfjxhs.com",
    "bf-swiss.com",
    "rvingbus.com",
    "suxfi.com",
    "schoolcardtrades.com",
    "motion-airsoft.com",
    "123netflix.moe",
    "ic200mdl750.com",
    "silkensarees.com",
    "digitalmarketingtraining.xyz",
    "foypay.com",
    "eudoraacantik.com",
    "healthyandwealthie.com",
    "print-postcards-fast.com",
    "alpha-psych.com",
    "merthyrrock.com",
    "mss52.com",
    "cddcsw.com",
    "istanbulbisiklettamircisi.com",
    "ertugrulbey.net",
    "katarina-yoga.com",
    "findholmesinlaurelmaryland.com",
    "sabciu.net",
    "shipthuocnhanh24h.com",
    "veganonthegreens.com",
    "ailil-alvarez.com",
    "thefashionszone.com",
    "geminicomputerofficial.com",
    "terraveda.net",
    "ruhstorfer-gruppe.info",
    "suderstr.com",
    "yunjichem.com",
    "priyadubai.com",
    "sofierceboutique.com",
    "nealcurtiss.com",
    "mcgdinner.com",
    "steplife.info",
    "pwagih.com",
    "cpzgzcw.com",
    "wierzewzwierze.com",
    "asbestosconsultancyservices.com",
    "centerstageacademyaz.com",
    "skip1-dndasasd.com",
    "successteamrealty.com",
    "mijninboxe.com",
    "berkeleyrehab.com",
    "tfjxw.com",
    "mcluxuryrentals.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.314505627.00000000008D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.314505627.00000000008D0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.314505627.00000000008D0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.496732172.0000000000720000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.496732172.0000000000720000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.5SXTKXCnqS.exe.2170000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.5SXTKXCnqS.exe.2170000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.5SXTKXCnqS.exe.2170000.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
0.2.5SXTKXCnqS.exe.2170000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.5SXTKXCnqS.exe.2170000.3.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

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:

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

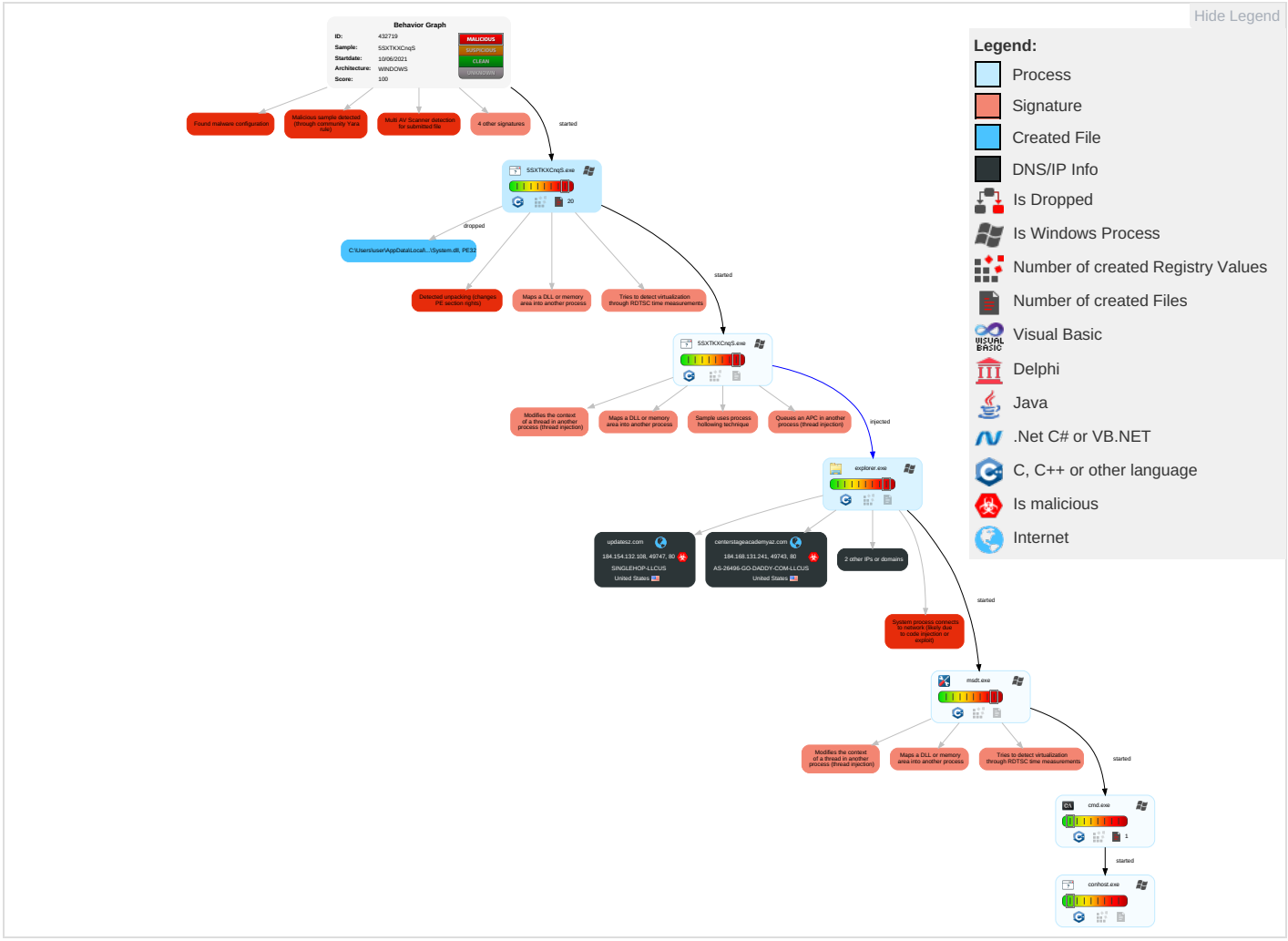
Remote Access Functionality:

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	Input Capture 1	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Input Capture 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	Archive Collected 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	Clipboard Data 1	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 3	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
5SXTKXCnqS.exe	30%	Virustotal		Browse
5SXTKXCnqS.exe	30%	ReversingLabs	Win32.Spyware.Noon	
5SXTKXCnqS.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsaC26E.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsaC26E.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.5SXTKXCnqS.exe.2170000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.5SXTKXCnqS.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.5SXTKXCnqS.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
14.2.msdt.exe.b552b0.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.5SXTKXCnqS.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
2.1.5SXTKXCnqS.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
14.2.msdt.exe.509f834.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.5SXTKXCnqS.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File

Domains

No Antivirus matches

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.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	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://centerstage.academy/hlx/?wVSH=B58lx/xaXAfqMrblDg0CPLD4IpEHx1MuvfXEetjmXTR5BJPCAvCKa/uMIPwGmDq	0%	Avira URL Cloud	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.centerstageacademyaz.com/hlx/?wVSH=B58lx/xaXAfqMrblDg0CPLD4IpEHx1MuvfXEetjmXTR5BJPCAvCKa/uMIPwGmDqbiG+v&i0D=adKPlr	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://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	
www.updatesz.com/hlx/	0%	Avira URL Cloud	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	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.updatesz.com/hlx/?wVSH=1q0nvnuESuCKkKkbLudmlC1kRF8eq+dUTLEJwYL638OOvnGjESXIW61pqUjqlD08HWSv&i0D=adKPlr	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
centerstageacademyaz.com	184.168.131.241	true	true		unknown
updatesz.com	184.154.132.108	true	true		unknown
www.updatesz.com	unknown	unknown	true		unknown
www.centerstageacademyaz.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.centerstageacademyaz.com/hlx/?wVSH=B58lx/xaXAfqMrblDg0CPLD4IpEHx1MuvfXEetjmXTR5BJPCAvCKa/uMIPwGmDqbiG+v&i0D=adKPlr	true	• Avira URL Cloud: safe	unknown
www.updatesz.com/hlx/	true	• Avira URL Cloud: safe	low
http://www.updatesz.com/hlx/?wVSH=1q0nvnuESuCKkKkbLudmlC1kRF8eq+dUTLEJwYL638OOvnGjESXIW61pqUjqlD08HWSv&i0D=adKPlr	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.168.131.241	centerstageacademyaz.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
184.154.132.108	updatesz.com	United States		32475	SINGLEHOP-LLCUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432719
Start date:	10.06.2021
Start time:	17:41:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5SXTKXCnqS (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/4@2/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.1% (good quality ratio 20.8%) • Quality average: 75.8% • Quality standard deviation: 31.7%
HCA Information:	• Successful, ratio: 86% • 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
184.168.131.241	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	• www.centerstageacademyaz.com/hlx/?5jSp=B58lx/xfXHfuM7XpBg0CPLD4IpEHx1MuvfPUCu/nTzR4B4jEH/TGM7WOLp8Aty+Q3gKYZw==&JR-laV=zN90U
	#U00a0Import Custom Duty invoice & its clearance documents.exe	Get hash	malicious	Browse	• www.mnanoramaonline.com/dp3a/?6l6x=JpPDbdpPqJah&F4ClVX_=HMSedmBm6/hlWbSmMxUxYZbRrtDTwFsk+TyYRjGVNzdErelZVoFwy82MvW0W4Pxo5ExE
	Payment receipt MT103.exe	Get hash	malicious	Browse	• www.2006almadenrd.com/n86i/?3fDpH=EncZcG68c0UFvrfaep8p5kHr59rKeBqDHDmJoTlHDlH5Q19q6THcE1BV1jQP2/4tmveZ&Vjo=1bT0vz7
	New Order.exe	Get hash	malicious	Browse	• www.flockuplabs.com/uqf5/?mVS=CH5D6h5PGn4ts&3fCDL=kpO7L1Lkp8iY+ON3mW6Oq8CK0aWMRalGagQzJa0PwjziroypQJ68geE/ArNV1zcwD6YY

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW ORDER ZIP.exe	Get hash	malicious	Browse	• www.cohorsetrails.com/j7e/?iP_T-V=s4TxBF2&F8EdvhY=0uFKBmvmOY3N1cR6tfDjvpZ4XCwo5tCp3URJWx4vIEcYZHH/ZYklCf5hgzXfIPGP0WLm
	oVA5JBAJutcna88.exe	Get hash	malicious	Browse	• www.covid-19-411.com/c6ss/?P6AT72s=DB71Bym9Rr14TfwtieeaSq+XP6MPPP3k6OJ3eYsEhcCNhSwkByfhm8SfoYhSpsTVm4Za&j6A4qv=gJBt3
	qXDtb88hht.exe	Get hash	malicious	Browse	• www.thriveglucose.com/p2io/?Z8E=bgEje2qoIMshrcRflwWQjpUULYzLZlDcA+elzyDX4pz+rZVwSlMQ2+HN9bOaKrviR/d6&b0GDi6=Q6Ahtfox
	a8eC6O6okf.exe	Get hash	malicious	Browse	• www.oceancollaborative.com/bp3i/?PF=5jiDaNi8a4RT0&V0Gp=+tA82deiMnBv5x6tQvXabF4qHjy6FJLdLGXe/FevxPH8etKnEP6uMBOxOeXG6ZsHsCfG
	Telex_Payment.exe	Get hash	malicious	Browse	• www.avaatraelegant.com/m3rc/?hTk8tpm=TSQTGbGl+UafldaDY7iOrPnVdHYt9Ypfw/QiU1mtcNJ1KwlNQbFG4EVzsaDm0ZQusGTd&l4=5jxX5BaX4hy8-j8
	QyKNw7NioL.exe	Get hash	malicious	Browse	• www.thriveglucose.com/p2io/?m4=PditjTvx4PwX_x-&ad=bgEje2qoIMshrcRflwWQjpUULYzLZlDcA+elzyDX4pz+rZVwSlMQ2+HN9YuKFK/aPa09
	Payment_Advice.exe	Get hash	malicious	Browse	• www.ingenious.care/uqf5/?9rw=IyvMBxqM8mznciPJtkomKlfF/kq/6zAZ/NulsdYJ5cntVs/S9fIvdvtMsAQ76USE273s&s6=bPYXfd3Xq0VHDp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SOA #093732.exe	Get hash	malicious	Browse	• www.xn--arepasantabrbara-pmb.com/hme1/?jPw=2SPw7LQlaa7cti3Mn2rz6TCjd7lU8jHnPITUh2R4n2dBA+x2SVgAgss/958kYo9ATjis&y2JhS=6lr41hZpgNXtF
	rHk5KU7bfT.exe	Get hash	malicious	Browse	• www.rvvikings.com/dxe/?TfTl=jHjQ1sEHwNXw4n+A/8fpKnaO6SpchAkuZ+GgFHi7AN8kb2XA0i8OmoFepGcQzHHYqc9c&7nGt5=h6Altfix
	Order.exe	Get hash	malicious	Browse	• www.complexscale.net/jogt/?w6ATB0=mM0Ck4zU/d9hG5lVEWeH7uQPwyvlCbjgstqvdurAh1ZdTH4Yqc2sgGmD0X7Q/SemRdxv&Jxox=Er6tXhMxl
	VubYcOdGjQ.exe	Get hash	malicious	Browse	• www.theguyscave.com/k8n/?wR-T-=ETYdeRC&5jn=ffRSpgj0URUgPhDkzfA3YdlDQQz5pJJRybkyQxcySljT84fGDbAnWSnhJv/zp2N19SZb
	Payment_Advice.exe	Get hash	malicious	Browse	• www.getthistle.com/q4kr/?w2MLb=6lux&QtRl=Jt1JO2t971959LrdDM/EJ1cvA97Pwm/HDqPg7v3P69I8XU+CUZlUHoU2RjaRLLQwrinB
	Neworder.exe	Get hash	malicious	Browse	• www.kanitanailloungе.com/jogt/?PlQ8j=jKXq1ZQHcPBM/dFmsG96Rrq7SiC5kuIPSSiD8Dd2ip+Nb1yUpyUL4OnlzbOoJzgaBXqf&2db=g0G0iLxxPHIT
	Request for Price W912D2-19-Q-0004.exe	Get hash	malicious	Browse	• www.blackwomencamp.net/egem/?2dCHQ=s0ILlWrMQzsGp3p1RmAY3qUukEAkmJAYYPkleJQvQBxBfoOdmLxTHansmvlw5WkCayf3&7nDtA=f2JDOtyx2xtDzteP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ack0527073465.exe	Get hash	malicious	Browse	• www.cohenasssets.net/5yue/?3fJx=KYutaNEAlvarQ918ErbJ+YDUvzOLVJKXYG8C/UFRJ6ixESNgaf8eKtytrZ1l6vvKrhJX&2dC4V=P48T-VYXSzrLax
	Product_Samples.exe	Get hash	malicious	Browse	• www.drlisatharler.com/m3rc/?j48=S9zQlxIAxlHw3AhG2oij4tyqbwYeiyo/TLihsL6vT2Jmjs5l/Hr2XRCnRYAhYdjvl6NmGr7rCg==&vRC=5jdD624HmJID8lJP

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	• 184.168.131.241
	619wGDCTZA.exe	Get hash	malicious	Browse	• 23.229.215.137
	Documents_13134976_1377491379.xlsb	Get hash	malicious	Browse	• 107.180.50.232
	#U00a0Import Custom Duty invoice & its clearance documents.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment receipt MT103.exe	Get hash	malicious	Browse	• 184.168.131.241
	research-531942606.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-121105165.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-76934760.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-1960540844.xlsx	Get hash	malicious	Browse	• 72.167.211.83
	research-1110827633.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	DocumentScanCopy2021_pdf.exe	Get hash	malicious	Browse	• 148.66.138.158
	New Order.exe	Get hash	malicious	Browse	• 184.168.131.241
	DocumentScanCopy202_pdf.exe	Get hash	malicious	Browse	• 148.66.138.158
	NEW ORDER ZIP.exe	Get hash	malicious	Browse	• 184.168.131.241
	oVA5JBAJutcna88.exe	Get hash	malicious	Browse	• 184.168.131.241
	qXDtb88hht.exe	Get hash	malicious	Browse	• 184.168.131.241
	a8eC6O6okf.exe	Get hash	malicious	Browse	• 184.168.131.241
	Telex_Payment.exe	Get hash	malicious	Browse	• 184.168.131.241
	QyKNw7NioL.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment_Advice.exe	Get hash	malicious	Browse	• 184.168.131.241
SINGLEHOP-LLCUS	Payment slip.exe	Get hash	malicious	Browse	• 198.20.110.232
	PO4358492133-REF30.doc	Get hash	malicious	Browse	• 184.154.190.82
	1092991(JB#082).exe	Get hash	malicious	Browse	• 198.20.110.232
	Qgc2Nreer3.exe	Get hash	malicious	Browse	• 198.143.164.252
	OoFyX2nTbB.exe	Get hash	malicious	Browse	• 184.154.132.108
	Payment.html	Get hash	malicious	Browse	• 63.251.14.14
	proforma invoice.exe	Get hash	malicious	Browse	• 198.20.110.232
	$RAULIU9.exe	Get hash	malicious	Browse	• 172.96.187.217

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BN45.vbs	Get hash	malicious	Browse	• 198.20.110.126
	LMNF434.vbs	Get hash	malicious	Browse	• 172.96.187.2
	SF65G55121E0FE25552.vbs	Get hash	malicious	Browse	• 172.96.187.2
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 184.154.83.252
	export of bill 896621.xlsm	Get hash	malicious	Browse	• 184.154.83.252
	scan of invoice 4366307.xlsm	Get hash	malicious	Browse	• 184.154.83.252
	FY9Z5TR6rr.exe	Get hash	malicious	Browse	• 198.20.110.126
	cf9f3c05-00c9-4008-846e-7d9a88232305.exe	Get hash	malicious	Browse	• 184.154.27.242
	Spetrum-invoice-95144511.vbs	Get hash	malicious	Browse	• 172.96.187.2
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 173.236.127.29
	DX35.vbs	Get hash	malicious	Browse	• 172.96.186.134
	Y8G0OTN7.htm	Get hash	malicious	Browse	• 173.236.35.188

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsaC26E.tmp\System.dll	i6xFULh8J5.exe	Get hash	malicious	Browse	
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	
	090049000009000.exe	Get hash	malicious	Browse	
	dYy3yfSkwY.exe	Get hash	malicious	Browse	
	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	UGGJ4NnzFz.exe	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	3arZKnr21W.exe	Get hash	malicious	Browse	
	Shipping receipt.exe	Get hash	malicious	Browse	
	New Order TL273723734533.pdf.exe	Get hash	malicious	Browse	
	YZ8OvkljWm.exe	Get hash	malicious	Browse	
	U03c2doc.exe	Get hash	malicious	Browse	
	QUOTE061021.exe	Get hash	malicious	Browse	
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	
	PO187439.exe	Get hash	malicious	Browse	
	090009000000090.exe	Get hash	malicious	Browse	
	NEWORDERLIST.exe	Get hash	malicious	Browse	
	00404000004.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\02vqprgl0atfidc	
Process:	C:\Users\user\Desktop\5SXTKXCnqS.exe
File Type:	data
Category:	dropped
Size (bytes):	185856
Entropy (8bit):	**7.998940517618347**
Encrypted:	**true**
SSDEEP:	3072:sGXmBfAYT/4RnQPu5PBTgJApkOdFuKxnZMfSWVgVBratxWRHkFlhFQ:sbVZanguBdgJ2JdF/ZMqNbatxWREr
MD5:	378DDC5CCA93C62AF29C52E3A139BB7A
SHA1:	04C1B1F9C5AF921764E29E654D2D87E80D47C470
SHA-256:	7AFCBE7E43FFCFC7268EFAF45629E6B6ED931145C9E5E820D60C5C9B50B0A1C5
SHA-512:	977D9A3F41B3AE1D5ADC32926F522BDAB3A77A5472C0A47E63565D8CF6EAEC98C94A3776EA21538E4AFB122F1046F9BB916375B5B632889FFC8ED3430BB0360A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\02vqprgl0atfidc	
Preview:	)..\.L...b~zy....R...u,....B.pp..pb...u<.-V...1....>o.V.Pw....k..:...h.n.Y@M....T..?1.._2....$H.....E..G.....S.j....S...;..t..,...kY..t..a&...w=..("'...G..6[=..V$...YR..&T..JN..T.i...F.. .%....a.....H.....F...&.r.,.....x.K..]C.....v..N...V..GC.&D...Z9)..39t.i0.....+j..I..+...)._.$.~1.+7.H@.W..N.E,z..1.....lQ.....'7...)I&.1....'I\.<..!..5.....Q*..C...}.=..q#q.Rf.Tf.?h. SD...R.K..Q[1..n.b.V1.#.Y.....6..t.6..Y.....8.+7.}.~...K_..B.J.....|.R..Q...:.J!....q...{..[F...;...i...e...}...+[.S.....IV?9..)F.....Q..IT.j.%zh.u:.....L(..R.).6"..Dd.....-.y.lC.bZ.. .....~. .....T..'...}.m.UC.[6...Z ....!Z#...a.....u#....jp..OM.p.-XM.N.r.x.D...c_M..{;.....#.N.&8.a.3B>.Ht.....}m5....K.....p..Q...R..{Z$.Y..qE...#..c.sZ..;.b.O.u. .....U+....6^.D.... MQ.#.%..<..@.....v.n.....+&.t.r.3..[.af...R=UL.....6.v..c.v.....m.E.a@c.R:...hJ.T....4w.<.od2\....z,..\..{...V..:~r.....D.8.q..`V.19....]=...a)U`..'9..K....n!qN.E#.E.w...2i....q.N.9.).

C:\Users\user\AppData\Local\Temp\nsaC26D.tmp	
Process:	C:\Users\user\Desktop\5SXTKXCnqS.exe
File Type:	data
Category:	dropped
Size (bytes):	278770
Entropy (8bit):	7.448079444634977
Encrypted:	false
SSDEEP:	6144:OtbVZanguBdgJ2JdF/ZMqNbatxWREwXeQumQ4T3t:qINkc7RTVXeQued
MD5:	C4CB16A32F9F83E70EAE2EDB6FD01FF3
SHA1:	9E86174F2952237E5170B532A69BC080FCD59765
SHA-256:	C8FE712473694B00B45F2AC8C83E57C0527751C6BA118E2A95F3F5B699B7EE57
SHA-512:	8D9FC4DB04C2538B792F720A183A337043F77A846B7A71F3D66405C15F975D98CFF7E63ADDD2CB677454765A7D3C2295E522457DB6A479F7F84753C3F4E119CF
Malicious:	false
Reputation:	low
Preview:	._.....,.....xH.....^.....y_..... .....J.....#...j.....j..... ....

C:\Users\user\AppData\Local\Temp\nsaC26E.tmp\System.dll	
Process:	C:\Users\user\Desktop\5SXTKXCnqS.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
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: i6xFULh8J5.exe, Detection: malicious, Browse • Filename: AWB00028487364 -000487449287.doc, Detection: malicious, Browse • Filename: 090049000009000.exe, Detection: malicious, Browse • Filename: dYy3yfSkwY.exe, Detection: malicious, Browse • Filename: PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx, Detection: malicious, Browse • Filename: Purchase Order Price List 061021.xlsx, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: UGGJ4NnzFz.exe, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: 3arZKnr21W.exe, Detection: malicious, Browse • Filename: Shipping receipt.exe, Detection: malicious, Browse • Filename: New Order TL273723734533.pdf.exe, Detection: malicious, Browse • Filename: YZ8OvkljWm.exe, Detection: malicious, Browse • Filename: U03c2doc.exe, Detection: malicious, Browse • Filename: QUOTE061021.exe, Detection: malicious, Browse • Filename: PAYMENT CONFIRMATION.exe, Detection: malicious, Browse • Filename: PO187439.exe, Detection: malicious, Browse • Filename: 090009000000090.exe, Detection: malicious, Browse • Filename: NEWORDERLIST.exe, Detection: malicious, Browse • Filename: 00404000004.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\wkxohdeyqvvyr	
Process:	C:\Users\user\Desktop\5SXTKXCnqS.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\wkxohdeyqvvyr	
Size (bytes):	56657
Entropy (8bit):	4.975811547605918
Encrypted:	false
SSDEEP:	1536:5usA23WeP0CJgK679CbFutzrcnrz42c9nvpVid:012meP0Ikuwtvcz4pBWd
MD5:	33CC7C9385899984348854239577060l
SHA1:	D57862368225F9240C279B0C1C1FA9BA7EB4E8CC
SHA-256:	F0738E409A7008B653A4E5C86D90CC73021988D59CAE648772305C41D6668BB1
SHA-512:	23F7DA5A861CAB4D0F06174BD78978F325B1D19DCECA6ED7A520B7957529B7D1A3EC1CC838EC140C426B0C64784B744AF6E3A4BB4C4514FE30A40E89CDEFF AF
Malicious:	false
Preview:	U.....@...8.A.....B.....C...i.D...i.E...l.F.....G...=.H.....I.....J...e.K...i.L...l.M.....N...=.O.....P...=.Q.....R.....S...i.T...i.U.....V.....W...m.X...i.Y.....Z...\.[.....\.....]...i.^...i._...i.`.....a...\.b.. ...c.....d...\.e...l.f.....g.....h.....i...i.j...U.k.....l.....m...\.n...l.o.....p...i.q...i.r.....s...\.t...l.u...).v.....w...\.x...l.y.....z...\.{.....|...!.}.....~...\.....%.....i.....i.....i..... .....\.....i.....U.....\.....i.....i.....\.....).....\.....\.....!.....\.....a.....i.....i.....i..... .....\.....i.....U.....\.....i.....i.....\.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.92465625934964
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:	5SXTKXCnqS.exe
File size:	245650
MD5:	cb4947e5c78ada624d22c28ee9079871
SHA1:	eb2c2d329e9be0b3a74582a4fd9c257bc795a690
SHA256:	02230fb80db0fe0055730a0af8b3a0c66a578b2c3152060 53b80bae250c5561d
SHA512:	7582aed1984c65c550532ab4a97d6bc5bc45bfceeacdf32 9467b39667dbcaaa6a28175aa29fef30146e16cbdae903c 5381b3d1ea47888f8d29b9f4119a581b26
SSDEEP:	3072:DQIURTXJ+McCmF7tC1eb4lhkULBwRLuJTqDW2 CLd+d/Lpz3JAdFu4V65bRvSC5aL:Ds9cCmF5SnwvmL d+d/FcU4Y5bRvbRAaa
File Content Preview:	MZ.....@.....!..L.!Th is 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:	

General

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
.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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 17:43:43.679322004 CEST	192.168.2.5	8.8.8.8	0x8cf7	Standard query (0)	www.centerstageacademyaz.com	A (IP address)	IN (0x0001)
Jun 10, 2021 17:44:22.509793997 CEST	192.168.2.5	8.8.8.8	0x19c5	Standard query (0)	www.updatesz.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 17:43:43.745172024 CEST	8.8.8.8	192.168.2.5	0x8cf7	No error (0)	www.centerstageacademyaz.com	centerstageacademyaz.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 17:43:43.745172024 CEST	8.8.8.8	192.168.2.5	0x8cf7	No error (0)	centerstageacademyaz.com		184.168.131.241	A (IP address)	IN (0x0001)
Jun 10, 2021 17:44:22.607316017 CEST	8.8.8.8	192.168.2.5	0x19c5	No error (0)	www.updatesz.com	updatesz.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 17:44:22.607316017 CEST	8.8.8.8	192.168.2.5	0x19c5	No error (0)	updatesz.com		184.154.132.108	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.centerstageacademyaz.com
- www.updatesz.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49743	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 17:43:43.946809053 CEST	3035	OUT	GET /hlx/?wVSH=B58lx/xaXAfqMrblDg0CPLD4IpEHx1MuvfXEetjmXTR5BJPCAvCKa/uMIPwGmDqbiG+v&i0D=adKPlr HTTP/1.1 Host: www.centerstageacademyaz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 17:43:44.176570892 CEST	3036	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Thu, 10 Jun 2021 15:43:44 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://centerstage.academy/hlx/?wVSH=B58lx/xaXAfqMrblDg0CPLD4IpEHx1MuvfXEetjmXTR5BJPCAvCKa/uMIPwGmDqbiG+v&i0D=adKPlr Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49747	184.154.132.108	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 17:44:22.758177042 CEST	3088	OUT	GET /hlx/?wVSH=1q0nvnuESuCKkKkbLudmlC1kRF8eq+dUTLEJwYL638OOvnGjESXIW61pqUjqlD08HWSv&i0D=adKPlr HTTP/1.1 Host: www.updatesz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 17:44:25.261095047 CEST	3089	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 10 Jun 2021 15:44:21 GMT Server: Apache/2.4.46 (cPanel) OpenSSL/1.1.1k mod_bwlimited/1.4 Phusion_Passenger/6.0.7 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://updatesz.com/hlx/?wVSH=1q0nvnuESuCKkKkbLudmlC1kRF8eq+dUTLEJwYL638OOvnGjESXIW61pqUjqlD08HWSv&i0D=adKPlr Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

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: 5SXTKXCnqS.exe PID: 5828 Parent PID: 5720

General

Start time:	17:42:26
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\5SXTKXCnqS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\5SXTKXCnqS.exe'
Imagebase:	0x400000
File size:	245650 bytes
MD5 hash:	CB4947E5C78ADA624D22C28EE9079871
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: 00000000.00000002.240364615.0000000002170000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.240364615.0000000002170000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.240364615.0000000002170000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: 5SXTKXCnqS.exe PID: 4328 Parent PID: 5828

General

Start time:	17:42:27
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\5SXTKXCnqS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\5SXTKXCnqS.exe'
Imagebase:	0x400000
File size:	245650 bytes
MD5 hash:	CB4947E5C78ADA624D22C28EE9079871
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: 00000002.00000002.314505627.00000000008D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.314505627.00000000008D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.314505627.00000000008D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.237002642.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.237002642.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.237002642.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.314179672.00000000008A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.314179672.00000000008A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.314179672.00000000008A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.313248208.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.313248208.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.313248208.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 4328

General

Start time:	17:42:31
Start date:	10/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
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: msdt.exe PID: 4940 Parent PID: 3472

General

Start time:	17:43:03
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x10f0000
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: 0000000E.00000002.496732172.0000000000720000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.496732172.0000000000720000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.496732172.0000000000720000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.499467789.00000000047C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.499467789.00000000047C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.499467789.00000000047C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.499102168.0000000004680000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.499102168.0000000004680000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.499102168.0000000004680000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1384 Parent PID: 4940

General

Start time:	17:43:06
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\5SXTKXCnqS.exe'
Imagebase:	0x1f0000
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: 5388 Parent PID: 1384

General

Start time:	17:43:06
Start date:	10/06/2021
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