ID: 528622
Sample Name:
S9yf6BkjhTQUbHE.exe
Cookbook: default.jbs
Time: 15:11:30
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

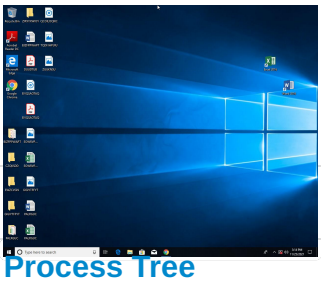
Windows Analysis Report S9yf6BkjhTQUbHE.exe

Overview

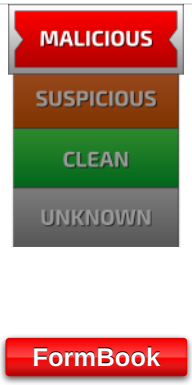
General Information

Sample Name:	S9yf6BkjhTQUbHE.exe
Analysis ID:	528622
MD5:	812861ad5cbb91..
SHA1:	ca092e52319047..
SHA256:	a649d216b55b0f0.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



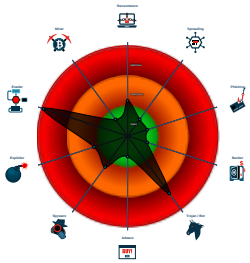
FormBook

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- S9yf6BkjhTQUbHE.exe (PID: 6344 cmdline: "C:\Users\user\Desktop\S9yf6BkjhTQUbHE.exe" MD5: 812861AD5CBB91BFA01A6A15C2CEF128)
  - S9yf6BkjhTQUbHE.exe (PID: 6408 cmdline: C:\Users\user\Desktop\S9yf6BkjhTQUbHE.exe MD5: 812861AD5CBB91BFA01A6A15C2CEF128)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autoconv.exe (PID: 6488 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - msdt.exe (PID: 6472 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 6572 cmdline: /c del "C:\Users\user\Desktop\S9yf6BkjhTQUbHE.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.peptidepowder.com/czh8/"
  ],
  "decoy": [
    "ekkyo-business.com",
    "anamentor.com",
    "criptodigital.online",
    "smart-device.tech",
    "piano-tomimoto.com",
    "sergiojuradomunera.com",
    "xn----pl8a630b0whm6t.com",
    "exploitslozdz.xyz",
    "peregorodki.store",
    "authenticationtd.net",
    "ichelbrousset.com",
    "amboyshops.com",
    "hengtaigyl.com",
    "iliubo.com",
    "overtimersanonymous.com",
    "crimsonrangellc.com",
    "otterburnelanding.com",
    "ping-ken.info",
    "belezaweb.digital",
    "elementkultury.com",
    "heireply.xyz",
    "membranbakar.xyz",
    "babygirlletsheal.com",
    "alpe.paris",
    "fuslonnd.com",
    "massaora.com",
    "geatarotista.com",
    "namethatsetup.com",
    "igdxir.com",
    "tokatyapimarket.com",
    "soundnox.com",
    "ase3baeb4p.com",
    "uniteddatavault.com",
    "savageequipment.biz",
    "cutos2.com",
    "thietketrangtrinhacua.store",
    "mways-vintage.com",
    "cloudscapephotos.com",
    "padelscuolaroma.store",
    "medeiros.store",
    "green-umbrella.academy",
    "kobaran.com",
    "ilmkibahar.com",
    "blueworldaquariums.com",
    "bigjohnblues.com",
    "e2adriasec.online",
    "pufaawareskincare.com",
    "sumerchemicals.com",
    "epubgame.net",
    "nuditecouverte.com",
    "tbpadvogados.website",
    "cryptoentering.com",
    "dahliahearing.com",
    "annellata.xyz",
    "barberking.online",
    "cpw882.com",
    "dock-weiler.com",
    "dianyuwang.com",
    "fitpromax.xyz",
    "deckingtoronto.com",
    "boundlessentgroup.com",
    "metricwombat.com",
    "emergencyhomerepairnetwork.com",
    "fullerhomeloans.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.314660733.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.314660733.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.314660733.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000000.250860288.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000000.250860288.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.S9yf6BkjhTQUbHE.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.0.S9yf6BkjhTQUbHE.exe.400000.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.0.S9yf6BkjhTQUbHE.exe.400000.6.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
1.0.S9yf6BkjhTQUbHE.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.0.S9yf6BkjhTQUbHE.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

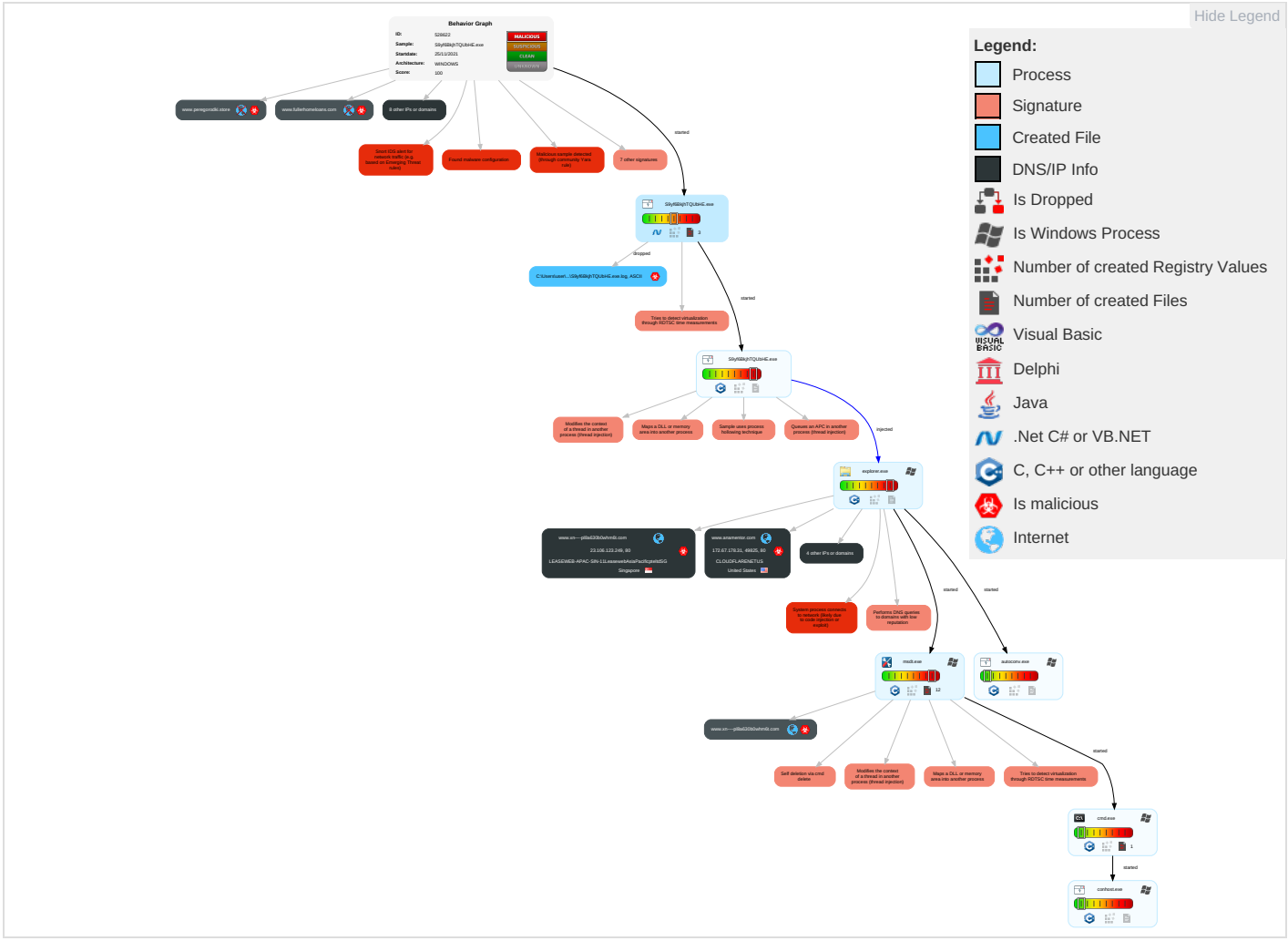
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 5 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect Pl Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Application Window 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	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi- Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
S9yf6BkjhTQUbHE.exe	22%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.S9yf6BkjhTQUbHE.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.S9yf6BkjhTQUbHE.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.S9yf6BkjhTQUbHE.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.S9yf6BkjhTQUbHE.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.xn----pl8a630b0whm6t.com/czh8/?7n=WfBFmY7eHt5QBShHhdd2jwwFQU0Qfs4ciJop7u3ZFFtbwI7iz04mk8i	0%	Avira URL Cloud	safe	
http://www.anamentor.com/czh8/?7n=IRLjoLIXlWieDd548KoJS/rowvlX7n5q7mSRLwbc7H8jLvnjYG+pwFiMTHdBlEYfNNBf&t4b=Zn-L	0%	Avira URL Cloud	safe	
www.peptidepowder.com/czh8/	0%	Avira URL Cloud	safe	
http://https://www.anamentor.com/czh8/?7n=IRLjoLIXlWieDd548KoJS/rowvlX7n5q7mSRLwbc7H8jLvnjYG	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.xn----pl8a630b0whm6t.com	23.106.123.249	true	true		unknown
td-ccm-168-233.wixdns.net	34.117.168.233	true	true		unknown
cryptoentering.com	127.0.0.1	true	true		unknown
parkingpage.namecheap.com	198.54.117.218	true	false		high
www.ichelbrousset.com	209.17.116.163	true	false		unknown
www.anamentor.com	172.67.178.31	true	true		unknown
www.fuslonnd.com	unknown	unknown	true		unknown
www.dock-weiler.com	unknown	unknown	true		unknown
www.peregorodki.store	unknown	unknown	true		unknown
www.annellata.xyz	unknown	unknown	true		unknown
www.metricwombat.com	unknown	unknown	true		unknown
www.fullerhomeloans.com	unknown	unknown	true		unknown
www.epubgame.net	unknown	unknown	true		unknown
www.exploitslozdz.xyz	unknown	unknown	true		unknown
www.cryptoentering.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.anamentor.com/czh8/?7n=IRLjoLIXlWieDd548KoJS/rowvlX7n5q7mSRLwbc7H8jLvnjYG+pwFiMTHdBlEYfNNBf&t4b=Zn-L	true	• Avira URL Cloud: safe	unknown
www.peptidepowder.com/czh8/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.106.123.249	www.xn----pl8a630b0whm6t.com	Singapore		59253	LEASEWEB-APAC-SIN-11LeasewebAsiaPacificptteltdSG	true
172.67.178.31	www.anamentor.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528622
Start date:	25.11.2021
Start time:	15:11:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 15s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	S9yf6BkjhTQUbHE.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:	29
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@8/1@13/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.5% (good quality ratio 15.5%) • Quality average: 72.4% • Quality standard deviation: 32.4%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:12:29	API Interceptor	22x Sleep call for process: S9yf6BkjhTQUbHE.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.106.123.249	gJvdHdeawX.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKDZ.74048.21519.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Ransom.Stop.P6.19307.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.7393.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.2200.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware2.22585.exe	Get hash	malicious	Browse	
	ZcCHi8mKVk.exe	Get hash	malicious	Browse	
172.67.178.31	40rsuPoRyW.exe	Get hash	malicious	Browse	• www.aname ntor.com/shjn/?sbWx=tv0gbh/Fir1M81j+EOOET4kbqB9H6LwHpkw5oua6kbgwj0sH1g9v33R+7+13J6QYFzuS&e0=s8Vty2Ip

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_DELIVERY_ADDRESS_CONFIRMATION.xlsx	Get hash	malicious	Browse	• www.anamentor.com/shjn/?lL=tv0gbh/Ais1l8lvyGOOET4kbqB9H6LwHpkop0tG7g7gxjFABywsjhzp84Y5xCLETQValQA==&NRX4i6=BxoHnNf8mX1

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
td-ccm-168-233.wixdns.net	ORDER K0-9110.exe	Get hash	malicious	Browse	• 34.117.168.233
	vbc.exe	Get hash	malicious	Browse	• 34.117.168.233
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	• 34.117.168.233
	Revised Shipping Documents 385099_pdf.exe	Get hash	malicious	Browse	• 34.117.168.233
	vGULtWc6Jh.exe	Get hash	malicious	Browse	• 34.117.168.233
	rfq.exe	Get hash	malicious	Browse	• 34.117.168.233
	DHL50458006SHP.exe	Get hash	malicious	Browse	• 34.117.168.233
	New order 7nbm471.exe	Get hash	malicious	Browse	• 34.117.168.233
	Swift Copy MT103.exe	Get hash	malicious	Browse	• 34.117.168.233
	triage_dropped_file.exe	Get hash	malicious	Browse	• 34.117.168.233
	DHL_Delivery_Confirmation.exe	Get hash	malicious	Browse	• 34.117.168.233
	Swift Payment Copy.exe	Get hash	malicious	Browse	• 34.117.168.233
	SWIFT Transfer 103 000000999315.xlsx	Get hash	malicious	Browse	• 34.117.168.233
	Order 0091.exe	Get hash	malicious	Browse	• 34.117.168.233
	EwrGOFT5pd.exe	Get hash	malicious	Browse	• 34.117.168.233
	UT6Bihk8wY.exe	Get hash	malicious	Browse	• 34.117.168.233
parkingpage.namecheap.com	JUSTIFICANTE.exe	Get hash	malicious	Browse	• 198.54.117.216
	Swift Copy TT.doc	Get hash	malicious	Browse	• 198.54.117.212
	8M5ZqXSa28.exe	Get hash	malicious	Browse	• 198.54.117.218
	XKLyPH8fil.exe	Get hash	malicious	Browse	• 198.54.117.218
	eFSFIMudyc.exe	Get hash	malicious	Browse	• 198.54.117.217
	MT103_RECEIPT241121.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Quote Request - Linde Tunisia.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	vbc.exe	Get hash	malicious	Browse	• 198.54.117.218
	VSL_MV HANNOR.exe	Get hash	malicious	Browse	• 198.54.117.217
	oIDAuDVIqp.exe	Get hash	malicious	Browse	• 198.54.117.212
	wYW5AsM930.exe	Get hash	malicious	Browse	• 198.54.117.216
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	HG0uDx2zkt.exe	Get hash	malicious	Browse	• 198.54.117.211
	NxYNG6zxNe.exe	Get hash	malicious	Browse	• 198.54.117.212
	97Pl742Uow.exe	Get hash	malicious	Browse	• 198.54.117.217
	aD1yIqGIQS.exe	Get hash	malicious	Browse	• 198.54.117.217
	Purchase Order 2890.exe	Get hash	malicious	Browse	• 198.54.117.218
	50% TT advance copy.doc	Get hash	malicious	Browse	• 198.54.117.215
	Drawing-FS3589_Surra-Unprice BOQ - Lock file - 28. 1.2021.xlsx 788K.doc	Get hash	malicious	Browse	• 198.54.117.215
	5F38FE3232085EC3BCF1411036241F6F23E58764 1B4E9.exe	Get hash	malicious	Browse	• 198.54.117.212

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-APAC-SIN-11LeasewebAsiaPacificpteltdSG	HXSFwEhM8m	Get hash	malicious	Browse	• 209.58.183.52
	TRANFER SLIP.exe	Get hash	malicious	Browse	• 209.58.177.241
	t0oNRqzxIc.exe	Get hash	malicious	Browse	• 198.252.110.227
	Whg8jgqeOs.exe	Get hash	malicious	Browse	• 198.252.110.227
	q2NdLgh8pk.exe	Get hash	malicious	Browse	• 198.252.110.227
	SecuriteInfo.com.Variant.Babar.29261.28155.exe	Get hash	malicious	Browse	• 198.252.110.227

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BrIL7GBTq6.exe	Get hash	malicious	Browse	• 198.252.110.227
	vd6dk7Pd2i.exe	Get hash	malicious	Browse	• 198.252.110.227
	Yob73TQCPI.exe	Get hash	malicious	Browse	• 198.252.110.227
	htP4fuQKSM.exe	Get hash	malicious	Browse	• 198.252.110.227
	DCF4ECC6D3B70A3E11077862B9E3830806191F0718EEC.exe	Get hash	malicious	Browse	• 198.252.110.227
	R F Q 2000051165.exe	Get hash	malicious	Browse	• 209.58.177.241
	R F Q 2000051165.exe	Get hash	malicious	Browse	• 209.58.177.241
	R F Q 2000051165.exe	Get hash	malicious	Browse	• 209.58.177.241
	65TYFXU6E9 BANK DATAILS.exe	Get hash	malicious	Browse	• 209.58.177.241
	TRANSFER SLIP.exe	Get hash	malicious	Browse	• 209.58.177.241
	TRANSFER SLIP.exe	Get hash	malicious	Browse	• 209.58.177.241
	TRANSFER SLIP.exe	Get hash	malicious	Browse	• 209.58.177.241
	TRANSFER SLIP.exe	Get hash	malicious	Browse	• 209.58.177.241
	JKgYJ56rZs	Get hash	malicious	Browse	• 172.96.190.95
CLOUDFLARENETUS	Halbank Ekstre 2021101 073653 270424.exe	Get hash	malicious	Browse	• 172.67.188.154
	yH8giB6jJ2.exe	Get hash	malicious	Browse	• 162.159.135.233
	pwY5ozOzpY	Get hash	malicious	Browse	• 172.64.209.6
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 104.21.76.223
	VXsVZBllD099876.exe	Get hash	malicious	Browse	• 172.67.206.244
	OPKyR75fJn.exe	Get hash	malicious	Browse	• 104.21.50.241
	COMPROBANTE DE CONSIGNACION #0000012992-882383393293293.vbs	Get hash	malicious	Browse	• 172.67.68.88
	DOC20212411003001001.exe	Get hash	malicious	Browse	• 104.21.19.200
	V-M RTAmpcapital5EG1-TGQO2F-IOC8.htm	Get hash	malicious	Browse	• 104.16.19.94
	AO7gki3UTr.exe	Get hash	malicious	Browse	• 162.159.129.233
	6docs'pdf.ppam	Get hash	malicious	Browse	• 104.16.202.237
	Product Inquiry.exe	Get hash	malicious	Browse	• 66.235.200.147
	JUSTIFICANTE.exe	Get hash	malicious	Browse	• 104.21.29.122
	Purchase Order.exe	Get hash	malicious	Browse	• 162.159.133.233
	Swift Copy TT.doc	Get hash	malicious	Browse	• 23.227.38.74
	sfhJLQhj84.exe	Get hash	malicious	Browse	• 104.23.98.190
	TOH09847465353.COM.exe	Get hash	malicious	Browse	• 104.21.49.41
	ESP095744532.BAT.exe	Get hash	malicious	Browse	• 104.21.79.226
	New PO.exe	Get hash	malicious	Browse	• 172.67.188.154
	lQzTg5PyVw.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\S9yf6BkjhTQUbHE.exe.log

Process:	C:\Users\user\Desktop\S9yf6BkjhTQUbHE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntIxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\S9yf6BkjhTQUbHE.exe.log	
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.847097424496743
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	S9yf6BkjhTQUbHE.exe
File size:	446976
MD5:	812861ad5cbb91bfa01a6a15c2cef128
SHA1:	ca092e52319047d609cb6fcca1821a8f873416df
SHA256:	a649d216b55b0f0597a16690b8469b6b44b9cdc73560d8237387b2df225ab20b
SHA512:	67f95b15cf249be43324f73de874fc5ca2f2b1d7255c1bb99b6d103b8d9c7414ebbf3ce1bdf7bb9df225c020d79836985c89fa687049892fa6323c535579e05d
SSDEEP:	12288:iDW+U0QixBFmqI9AY9aVrwRn+BbxGmG5tquMAQ52RJeHEO:iDvU0Qi1hIhaVASx85tquMAQ52HdO
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...QM.a.....0.....v.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46e776
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F4D51 [Thu Nov 25 08:46:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0

General

Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6c78c	0x6c800	False	0.884828629032	data	7.85954100497	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x70000	0x5c4	0x600	False	0.4296875	data	4.13698409708	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x72000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-15:14:49.156551	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.5	34.117.168.233
11/25/21-15:14:49.156551	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.5	34.117.168.233
11/25/21-15:14:49.156551	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.5	34.117.168.233
11/25/21-15:15:02.896670	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49837	80	192.168.2.5	198.54.117.218
11/25/21-15:15:02.896670	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49837	80	192.168.2.5	198.54.117.218
11/25/21-15:15:02.896670	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49837	80	192.168.2.5	198.54.117.218

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 15:13:46.186501980 CET	192.168.2.5	8.8.8.8	0x5f4f	Standard query (0)	www.epubgame.net	A (IP address)	IN (0x0001)
Nov 25, 2021 15:13:51.264303923 CET	192.168.2.5	8.8.8.8	0xabac	Standard query (0)	www.fuslonnd.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:13:56.359602928 CET	192.168.2.5	8.8.8.8	0xd8e9	Standard query (0)	www.annellata.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:01.449800968 CET	192.168.2.5	8.8.8.8	0xaf65	Standard query (0)	www.xn----pl8a630b0whm6t.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 15:14:25.505644083 CET	192.168.2.5	8.8.8.8	0xfd5f	Standard query (0)	www.xn---- pl8a630b0w hm6t.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:27.600068092 CET	192.168.2.5	8.8.8.8	0x7843	Standard query (0)	www.anamen tor.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:32.799489021 CET	192.168.2.5	8.8.8.8	0x9ebd	Standard query (0)	www.metric wombat.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:37.889867067 CET	192.168.2.5	8.8.8.8	0xc5e9	Standard query (0)	www.crypto entering.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:43.999562979 CET	192.168.2.5	8.8.8.8	0x63f6	Standard query (0)	www.dock-w eiler.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:49.062454939 CET	192.168.2.5	8.8.8.8	0xb316	Standard query (0)	www.perego rodki.store	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:54.248440027 CET	192.168.2.5	8.8.8.8	0xc76e	Standard query (0)	www.ichelb rousset.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:15:02.666291952 CET	192.168.2.5	8.8.8.8	0x6e0f	Standard query (0)	www.exploi tslozdz.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 15:15:08.072524071 CET	192.168.2.5	8.8.8.8	0x5d8a	Standard query (0)	www.fuller homeloans.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 15:13:46.241841078 CET	8.8.8.8	192.168.2.5	0x5f4f	Name error (3)	www.epubga me.net	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:13:51.343818903 CET	8.8.8.8	192.168.2.5	0xabac	Name error (3)	www.fuslon nd.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:13:56.414275885 CET	8.8.8.8	192.168.2.5	0xd8e9	Name error (3)	www.annell ata.xyz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:01.513969898 CET	8.8.8.8	192.168.2.5	0xaf65	No error (0)	www.xn---- pl8a630b0w hm6t.com		23.106.123.249	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:25.582798958 CET	8.8.8.8	192.168.2.5	0xfd5f	No error (0)	www.xn---- pl8a630b0w hm6t.com		23.106.123.249	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:27.668248892 CET	8.8.8.8	192.168.2.5	0x7843	No error (0)	www.anamen tor.com		172.67.178.31	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:27.668248892 CET	8.8.8.8	192.168.2.5	0x7843	No error (0)	www.anamen tor.com		104.21.51.95	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:32.882380962 CET	8.8.8.8	192.168.2.5	0x9ebd	Name error (3)	www.metric wombat.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:37.956604958 CET	8.8.8.8	192.168.2.5	0xc5e9	No error (0)	www.crypto entering.com	cryptoentering.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:14:37.956604958 CET	8.8.8.8	192.168.2.5	0xc5e9	No error (0)	cryptoente ring.com		127.0.0.1	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:44.050005913 CET	8.8.8.8	192.168.2.5	0x63f6	Name error (3)	www.dock-w eiler.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:49.133816957 CET	8.8.8.8	192.168.2.5	0xb316	No error (0)	www.perego rodki.store	gcdn0.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:14:49.133816957 CET	8.8.8.8	192.168.2.5	0xb316	No error (0)	gcdn0.wixd ns.net	td-ccm-168-233.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:14:49.133816957 CET	8.8.8.8	192.168.2.5	0xb316	No error (0)	td-ccm-168-233.wixdns.net		34.117.168.233	A (IP address)	IN (0x0001)
Nov 25, 2021 15:14:54.410651922 CET	8.8.8.8	192.168.2.5	0xc76e	No error (0)	www.ichelb rousset.com		209.17.116.163	A (IP address)	IN (0x0001)
Nov 25, 2021 15:15:02.729429960 CET	8.8.8.8	192.168.2.5	0x6e0f	No error (0)	www.exploi tslozdz.xyz	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:15:02.729429960 CET	8.8.8.8	192.168.2.5	0x6e0f	No error (0)	parkingpag e.namechea p.com		198.54.117.218	A (IP address)	IN (0x0001)
Nov 25, 2021 15:15:02.729429960 CET	8.8.8.8	192.168.2.5	0x6e0f	No error (0)	parkingpag e.namechea p.com		198.54.117.217	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 15:15:02.729429960 CET	8.8.8.8	192.168.2.5	0x6e0f	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Nov 25, 2021 15:15:02.729429960 CET	8.8.8.8	192.168.2.5	0x6e0f	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Nov 25, 2021 15:15:02.729429960 CET	8.8.8.8	192.168.2.5	0x6e0f	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Nov 25, 2021 15:15:02.729429960 CET	8.8.8.8	192.168.2.5	0x6e0f	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Nov 25, 2021 15:15:02.729429960 CET	8.8.8.8	192.168.2.5	0x6e0f	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Nov 25, 2021 15:15:08.158160925 CET	8.8.8.8	192.168.2.5	0x5d8a	Name error (3)	www.fullerhomeloans.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.anamentor.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49825	172.67.178.31	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:14:27.703845978 CET	11243	OUT	GET /czh8/?7n=IRLjoLIXlWieDd548KoJS/rowvlX7n5q7mSRLwbc7H8jLvnjYG+pwFiMTHdBlEYfNNBf&t4b=Zn-L HTTP/1.1 Host: www.anamentor.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:14:27.778224945 CET	11244	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 25 Nov 2021 14:14:27 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 25 Nov 2021 15:14:27 GMT Location: https://www.anamentor.com/czh8/?7n=IRLjoLIXlWieDd548KoJS/rowvlX7n5q7mSRLwbc7H8jLvnjYG+pwFiMTHdBlEYfNNBf&t4b=Zn-L Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=RzIWNo2qqeDFO2t1MpA%2FOdaqEXCSt3i%2FGZmLkcZpm6f76Mci07Yzcq5ZRvSRwDOez1hTdzS4aWfPMe8ywl3LNUDv%2B4Z%2Fh5hPMNAVAwFYiHWORPRPU5x6BxLWPT9j1tYPoJT5TQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Server: cloudflare CF-RAY: 6b3b7bc73b736b36-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: S9yf6BkjhTQUbHE.exe PID: 6344 Parent PID: 1928

General

Start time:	15:12:27
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\S9yf6BkjhTQUbHE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\S9yf6BkjhTQUbHE.exe"
Imagebase:	0xa80000
File size:	446976 bytes
MD5 hash:	812861AD5CBB91BFA01A6A15C2CEF128
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.256688867.00000000041A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.256688867.00000000041A8000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.256688867.00000000041A8000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.254291450.000000000304A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.254885571.0000000003F8D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.254885571.0000000003F8D000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.254885571.0000000003F8D000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.254094379.0000000002F81000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: S9yf6BkjhTQUbHE.exe PID: 6408 Parent PID: 6344

General

Start time:	15:12:30
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\S9yf6BkjhTQUbHE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\S9yf6BkjhTQUbHE.exe
Imagebase:	0x450000
File size:	446976 bytes
MD5 hash:	812861AD5CBB91BFA01A6A15C2CEF128
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.314660733.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.314660733.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.314660733.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.250860288.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.250860288.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.250860288.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.314889663.0000000000A20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.314889663.0000000000A20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.314889663.0000000000A20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.251285298.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.251285298.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.251285298.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.314919624.0000000000A50000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.314919624.0000000000A50000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.314919624.0000000000A50000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 6408

General

Start time:	15:12:33
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.288279316.000000000EC4A000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.288279316.000000000EC4A000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.288279316.000000000EC4A000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.305725796.000000000EC4A000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.305725796.000000000EC4A000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.305725796.000000000EC4A000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autoconv.exe PID: 6488 Parent PID: 3472

General

Start time:	15:12:58
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x1080000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msdt.exe PID: 6472 Parent PID: 3472

General

Start time:	15:12:58
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x9f0000
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: 00000012.00000002.514724044.00000000008D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.514724044.00000000008D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.514724044.00000000008D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.518773545.0000000002FA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.518773545.0000000002FA0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.518773545.0000000002FA0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.518592905.0000000002E90000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.518592905.0000000002E90000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.518592905.0000000002E90000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 6572 Parent PID: 6472

General

Start time:	15:13:02
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\S9yf6BkjhTQUbHE.exe"
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6368 Parent PID: 6572

General

Start time:	15:13:04
Start date:	25/11/2021
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