ID: 562118
Sample Name:
tlBHrCrteFXy8Jz.exe
Cookbook: default.jbs
Time: 14:00:35
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

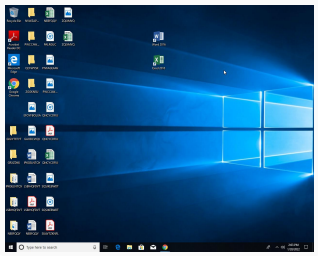
Windows Analysis Report

tlBHrCrteFXy8Jz.exe

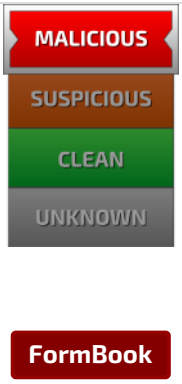
Overview

General Information

Sample Name:	tlBHrCrteFXy8Jz.exe
Analysis ID:	562118
MD5:	0e9943c0e2afaf5..
SHA1:	dc1c5f809a3e6e...
SHA256:	dc368951f1df68a..
Tags:	exe
Infos:	



Detection



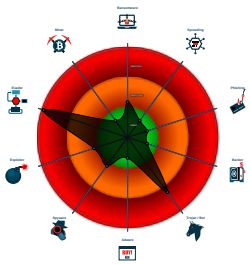
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e...
- Yara detected FormBook
- Malicious sample detected (through...
- Yara detected AntiVM3
- System process connects to networ...
- Antivirus detection for URL or domain
- Sample uses process hollowing tech...
- Maps a DLL or memory area into an...
- Tries to detect sandboxes and other...
- Machine Learning detection for sam...
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- tlBHrCrteFXy8Jz.exe (PID: 6248 cmdline: "C:\Users\user\Desktop\tlBHrCrteFXy8Jz.exe" MD5: 0E9943C0E2AFAF5E9ACEC16CE184B444)
  - tlBHrCrteFXy8Jz.exe (PID: 7160 cmdline: C:\Users\user\Desktop\tlBHrCrteFXy8Jz.exe MD5: 0E9943C0E2AFAF5E9ACEC16CE184B444)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 1292 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 5280 cmdline: /c del "C:\Users\user\Desktop\tlBHrCrteFXy8Jz.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.meizi.ltd/b3xd/"
  ],
  "decoy": [
    "nestonconstruction.com",
    "ratnainternational.com",
    "3bersaudara.com",
    "scottkmoody.store",
    "1metroband.com",
    "prechit.com",
    "desertbirdmercantile.com",
    "marciabernice.com",
    "packard.vote",
    "selo.global",
    "fourthandwhiteoak.com",
    "ecoplagas.online",
    "api-jipotvcom.xyz",
    "shabellafurniture.com",
    "maxmonacomarble.com",
    "imprimiruncalendario.com",
    "cochepordinero.net",
    "teamosu.club",
    "therightleftfoot.com",
    "mitt-masters.com",
    "transformeddestiny.com",
    "vzyz.top",
    "perfectotr.com",
    "rnhapr.com",
    "polebear.xyz",
    "tiatapa.com",
    "plick-click.com",
    "losfantasticos.com",
    "georgemacpherson.xyz",
    "sadiknitwears.com",
    "hpmetaverse.com",
    "smart-life-hacks.com",
    "gpowermall.com",
    "codegreenautomation.com",
    "investment-scientist.com",
    "igthksolution.com",
    "lrtlffnr.xyz",
    "ecomm-hub.com",
    "99ganbi.top",
    "quaked.net",
    "teliazepte.com",
    "www24fa.top",
    "nobleslim.com",
    "hsbsr9s.sbs",
    "yetiecoolerusa.com",
    "hourly.limo",
    "idesignuix.com",
    "fun4freegames.com",
    "wxqfilm.com",
    "auburnfuid.com",
    "chengxinyuan.online",
    "yzztx.com",
    "huggsforbubbs.com",
    "cdrbk.com",
    "eclipses.today",
    "sigmamu.com",
    "5pineridge.com",
    "lowfrictionvideo.com",
    "ord12route.art",
    "accreditslots.com",
    "madeitinhome.com",
    "insurance.pink",
    "thietkenoithatvanphong.asia",
    "gkynykj.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000000.358128872.000000000B7CA000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000D.00000000.358128872.000000000B7CA000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000D.00000000.358128872.000000000B7CA000.00000040.00000001.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ac9:$sqlite3step: 68 34 1C 7B E1 • 0x6bdc:$sqlite3step: 68 34 1C 7B E1 • 0x6af8:$sqlite3text: 68 38 2A 90 C5 • 0x6c1d:$sqlite3text: 68 38 2A 90 C5 • 0x6b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c33:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000000.299250808.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000000.299250808.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.0.tlBHrCrteFXy8Jz.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.0.tlBHrCrteFXy8Jz.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
11.0.tlBHrCrteFXy8Jz.exe.400000.6.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cc9:$sqlite3step: 68 34 1C 7B E1 • 0x15ddc:$sqlite3step: 68 34 1C 7B E1 • 0x15cf8:$sqlite3text: 68 38 2A 90 C5 • 0x15e1d:$sqlite3text: 68 38 2A 90 C5 • 0x15d0b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e33:$sqlite3blob: 68 53 D8 7F 8C
0.2.tlBHrCrteFXy8Jz.exe.335d944.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
11.0.tlBHrCrteFXy8Jz.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 24 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

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)

Stealing of Sensitive Information

Yara detected FormBook

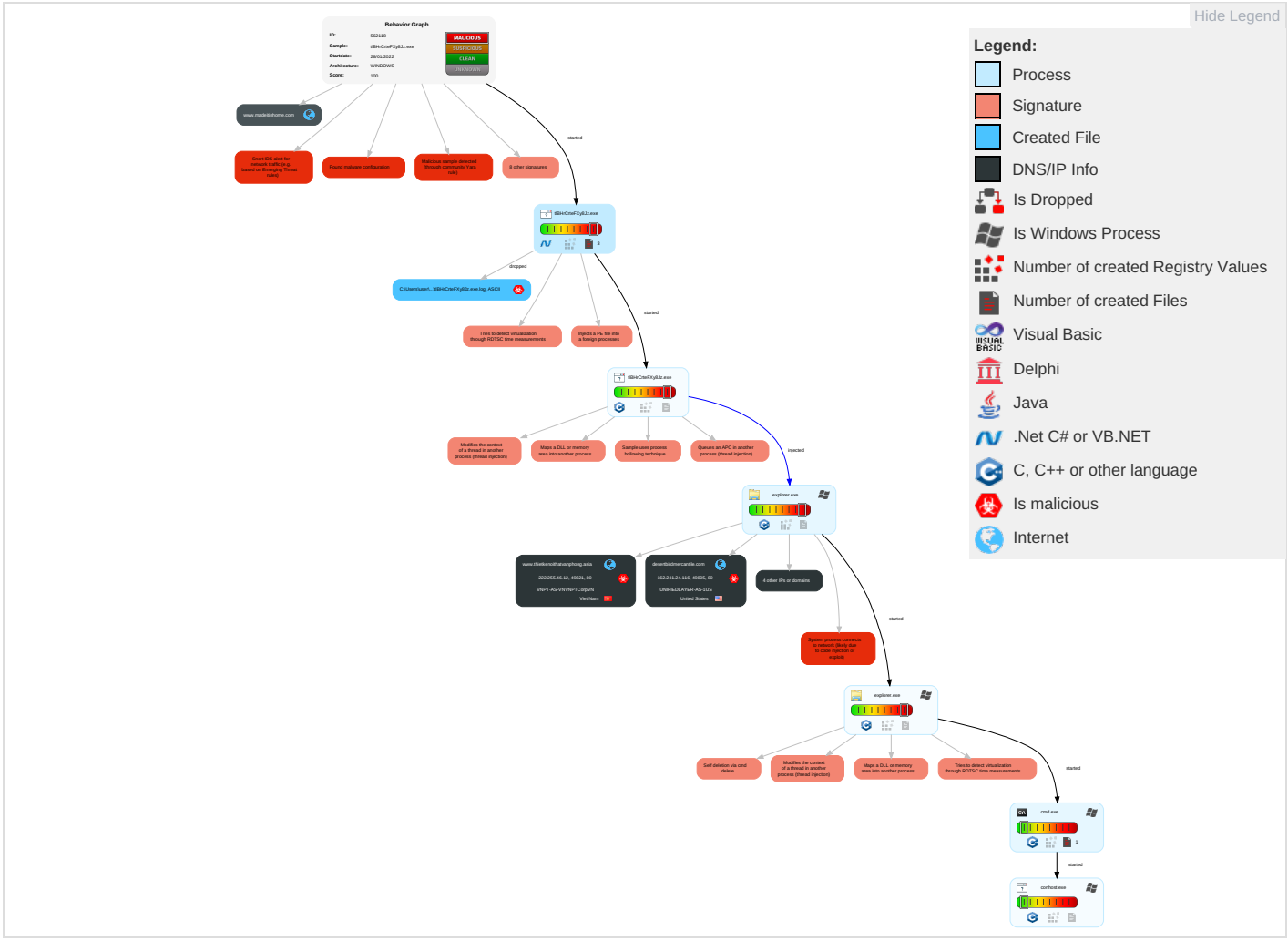
Remote Access Functionality

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 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 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 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	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 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
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

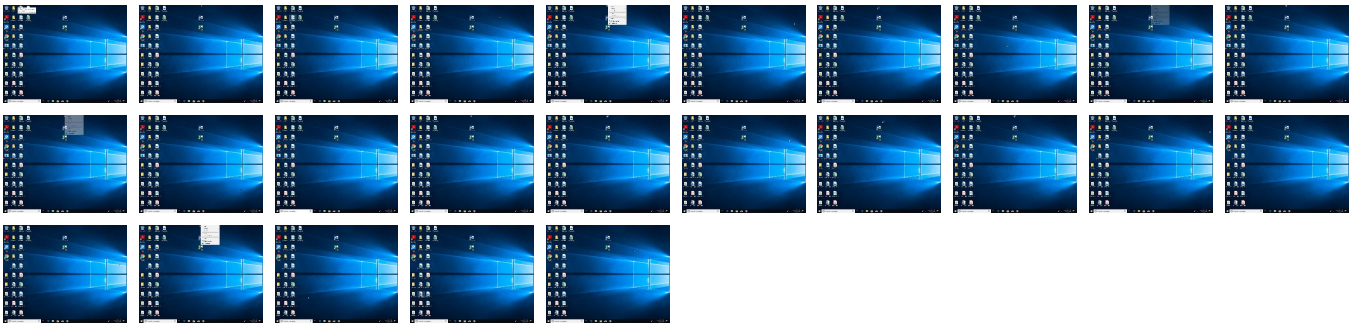
Behavior Graph



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
tlBHrCrteFXy8Jz.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.tlBHrCrteFXy8Jz.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.0.explorer.exe.b10000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.explorer.exe.b10000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.tlBHrCrteFXy8Jz.exe.3380000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.tlBHrCrteFXy8Jz.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.0.tlBHrCrteFXy8Jz.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.tlBHrCrteFXy8Jz.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.yzztx.com/b3xd/?qPYT=aV9tZ&iRah=u1+lAjLBA2+kcdvhq4UZu/nPbWuE94hnVKEDKIE9CxGJPgk2lSTbeIcckL5CyvhDdyZbFg7D5w==	0%	Avira URL Cloud	safe	
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://www.sigmamu.com/b3xd/?iRah=5GWj3iokSHma3YiDoT3m16TCcfPCT77oIBdOELLk89ETJqvKsRjgRlGfGSz2uWFXBl65BQRHGg==&qPYT=aV9tZ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.meizi.ltd/b3xd/	100%	Avira URL Cloud	malware	
http://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comoX	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
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://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.desertbirdmercantile.com/b3xd/?qPYT=aV9tZ&iRah=Ie1PhgByqbmAnBTD/2NTTWN841CMZzf2VbgiXa4AsIuYcZI/bp6cv0uoISKMiipyVSmV9CFFiA==	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.thietkenoithatvanphong.asia/b3xd/?iRah=JdJx4d7W9+IGJje0hU/QcPoKaGdRUKvyvIN3jQdk7kxI7FpVQbo1IF0KYDc1cvBgS1iZcvDTaA==&qPYT=aV9tZ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.thietkenoithatvanphong.asia	222.255.46.12	true	true		unknown
www.madeitinhome.com	23.230.105.134	true	false		unknown
sigmamu.com	160.153.136.3	true	true		unknown
www.yzztx.com	154.214.67.82	true	true		unknown
desertbirdmercantile.com	162.241.24.116	true	true		unknown
www.desertbirdmercantile.com	unknown	unknown	true		unknown
www.sigmamu.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.yzztx.com/b3xd/?qPYT=aV9tZ&iRah=u1+lAjLBA2+kcdvhq4UZu/nPbWuE94hnVKEDKIE9CxGJPgk2lSTbeIcckL5CyvhDdyZbFg7D5w==	true	• Avira URL Cloud: safe	unknown

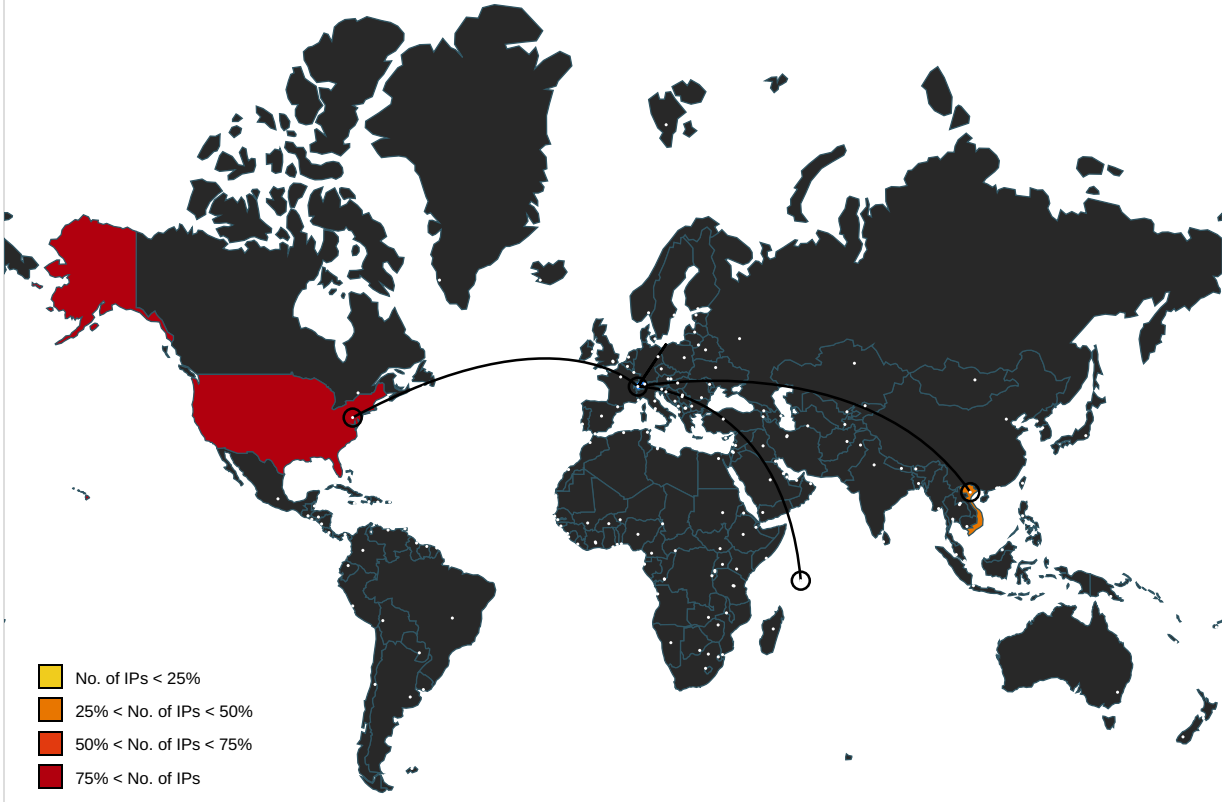
Name	Malicious	Antivirus Detection	Reputation
http://www.sigmamu.com/b3xd/?iRah=5GWj3iokSHma3YiDoT3m16TCcfPCT77oIBdOELLk89ETJqvKsRjgRlGfGSz2uWFXBl65BQRHGg==&qPYT=aV9tZ	true	• Avira URL Cloud: safe	unknown
www.meizi.ltd/b3xd/	true	• Avira URL Cloud: malware	low
http://www.desertbirdmercantile.com/b3xd/?qPYT=aV9tZ&iRah=Ie1PhgByqbmAnBTD/2NTTWN841CMZzf2VbgiXa4AsIuYcZI/bp6cv0uoISKMiipyVSmV9CFFiA==	true	• Avira URL Cloud: safe	unknown
http://www.thietkenoithatvanphong.asia/b3xd/?iRah=JdJx4d7W9+IGJje0hU/QcPoKaGdRUKvyvIN3jQdk7kxI7FpVQbo1IF0KYDc1cvBgS1iZcvDTaA==&qPYT=aV9tZ	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000D.00000000.40433009 0.0000000006870000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00D.00000000.347608168.0000000006840000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000D.00000000.317325369.000000 0006840000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 0000000D.0000 0000.331095005.0000000006840000.00000004 .00000001.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://blog.iandreev.com/	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 02694736.0000000003311000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://blog.iandreev.com	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 02694736.0000000003311000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comoX	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 02412697.0000000001977000.00000004.00000 020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fonts.com	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	tlBHrCrteFXy8Jz.exe, 00000000.00000002.3 05559596.00000000074B2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
222.255.46.12	www.thietkenoithatvanphong.asia	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.24.116	desertbirdmercantile.com	United States		46606	UNIFIEDLAYER-AS-1US	true
160.153.136.3	sigmamu.com	United States		21501	GODADDY-AMSDE	true
154.214.67.82	www.yzztx.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562118
Start date:	28.01.2022
Start time:	14:00:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tlBHrCrteFXy8Jz.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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@6/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.8% (good quality ratio 22.5%) • Quality average: 68.4% • Quality standard deviation: 34%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, dual-a-0001.dc-msedge.net, client.wns.windows.com, fs.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- VT rate limit hit for: tlBHrCrteFXy8Jz.exe

Simulations

Behavior and APIs

Time	Type	Description
14:01:54	API Interceptor	1x Sleep call for process: tlBHrCrteFXy8Jz.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\tlBHrCrteFXy8Jz.exe.log

Process:	C:\Users\user\Desktop\tlBHrCrteFXy8Jz.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):	6.390802601979872

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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	tlBHrCrteFXy8Jz.exe
File size:	793600
MD5:	0e9943c0e2afaf5e9acec16ce184b444
SHA1:	dc1c5f809a3e6e9a3358878d455cb235d2245460
SHA256:	dc368951f1df68a92c51f9afe6ad73c717b040fb9af6a278e9201b176362ed70
SHA512:	a7a7e54dc8a144266447b8c500a02adb2dcd855224f8780c6fbfe573ca3eedd1e78ab998aaa4adcfb1f717d670159b93d13cb340e2601fc936d0cc417b78eb50
SSDEEP:	6144:ORyHxmRYjO+Q45IX8LhyTa0oEpQOxRv9mu6hLlGATgBEWbs5gm0q2MKI9vTeiNzD:qY6to9OxRlmu6hpnTeVuf2Mfdun7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J..a.....>,... ...@....@.. ..... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c2c3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F3C14A [Fri Jan 28 10:11:22 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2bf0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc6000	0x5b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc2ba7	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	0xc0c44	0xc0e00	False	0.475148604585	data	6.39603433046	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xc4000	0x1e8	0x200	False	0.861328125	data	6.60844431455	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x5b0	0x600	False	0.425130208333	data	4.10455933281	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc60a0	0x324	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xc63c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

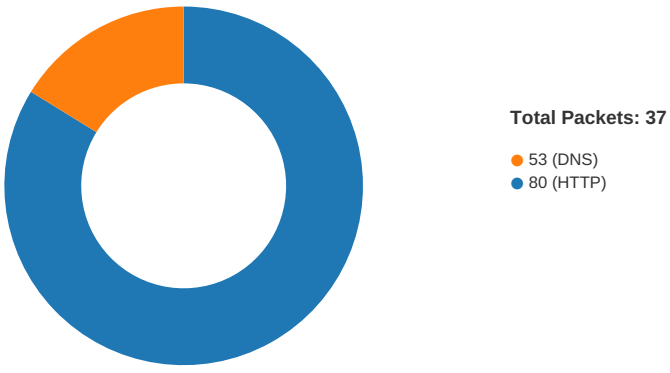
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	ASCIIEncodi.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	OthelloCS
ProductVersion	1.0.0.0
FileDescription	OthelloCS
OriginalFilename	ASCIIEncodi.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-14:03:13.623902	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49805	80	192.168.2.7	162.241.24.116
01/28/22-14:03:13.623902	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49805	80	192.168.2.7	162.241.24.116
01/28/22-14:03:13.623902	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49805	80	192.168.2.7	162.241.24.116
01/28/22-14:03:32.833166	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49824	80	192.168.2.7	160.153.136.3
01/28/22-14:03:32.833166	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49824	80	192.168.2.7	160.153.136.3
01/28/22-14:03:32.833166	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49824	80	192.168.2.7	160.153.136.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:03:13.486047983 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:13.623425961 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:13.623594999 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:13.623902082 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:13.763688087 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:14.139157057 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:14.316526890 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.450484991 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.450524092 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.450611115 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:15.450654030 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:15.467937946 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.468043089 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:15.469754934 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.469855070 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:15.470474005 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.470508099 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.470573902 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:15.470650911 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:15.471146107 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.471249104 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:15.487816095 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.487854004 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.487884998 CET	80	49805	162.241.24.116	192.168.2.7
Jan 28, 2022 14:03:15.487941980 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:15.487993956 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:15.488032103 CET	49805	80	192.168.2.7	162.241.24.116
Jan 28, 2022 14:03:21.198528051 CET	49821	80	192.168.2.7	222.255.46.12
Jan 28, 2022 14:03:21.423305988 CET	80	49821	222.255.46.12	192.168.2.7
Jan 28, 2022 14:03:21.423458099 CET	49821	80	192.168.2.7	222.255.46.12
Jan 28, 2022 14:03:21.434609890 CET	49821	80	192.168.2.7	222.255.46.12
Jan 28, 2022 14:03:21.659496069 CET	80	49821	222.255.46.12	192.168.2.7
Jan 28, 2022 14:03:21.936604977 CET	49821	80	192.168.2.7	222.255.46.12
Jan 28, 2022 14:03:22.200671911 CET	80	49821	222.255.46.12	192.168.2.7
Jan 28, 2022 14:03:22.344238997 CET	80	49821	222.255.46.12	192.168.2.7
Jan 28, 2022 14:03:22.344396114 CET	49821	80	192.168.2.7	222.255.46.12
Jan 28, 2022 14:03:22.344609022 CET	80	49821	222.255.46.12	192.168.2.7
Jan 28, 2022 14:03:22.344681025 CET	49821	80	192.168.2.7	222.255.46.12
Jan 28, 2022 14:03:27.366228104 CET	49822	80	192.168.2.7	154.214.67.82
Jan 28, 2022 14:03:27.551924944 CET	80	49822	154.214.67.82	192.168.2.7
Jan 28, 2022 14:03:27.552064896 CET	49822	80	192.168.2.7	154.214.67.82
Jan 28, 2022 14:03:27.552238941 CET	49822	80	192.168.2.7	154.214.67.82
Jan 28, 2022 14:03:27.739898920 CET	80	49822	154.214.67.82	192.168.2.7
Jan 28, 2022 14:03:27.739952087 CET	80	49822	154.214.67.82	192.168.2.7
Jan 28, 2022 14:03:27.739984035 CET	80	49822	154.214.67.82	192.168.2.7
Jan 28, 2022 14:03:27.740133047 CET	49822	80	192.168.2.7	154.214.67.82
Jan 28, 2022 14:03:27.740178108 CET	49822	80	192.168.2.7	154.214.67.82
Jan 28, 2022 14:03:27.740267038 CET	49822	80	192.168.2.7	154.214.67.82
Jan 28, 2022 14:03:27.924901009 CET	80	49822	154.214.67.82	192.168.2.7
Jan 28, 2022 14:03:32.806322098 CET	49824	80	192.168.2.7	160.153.136.3
Jan 28, 2022 14:03:32.832925081 CET	80	49824	160.153.136.3	192.168.2.7
Jan 28, 2022 14:03:32.833043098 CET	49824	80	192.168.2.7	160.153.136.3
Jan 28, 2022 14:03:32.833165884 CET	49824	80	192.168.2.7	160.153.136.3
Jan 28, 2022 14:03:32.859730005 CET	80	49824	160.153.136.3	192.168.2.7
Jan 28, 2022 14:03:32.862364054 CET	80	49824	160.153.136.3	192.168.2.7
Jan 28, 2022 14:03:32.862401009 CET	80	49824	160.153.136.3	192.168.2.7
Jan 28, 2022 14:03:32.862562895 CET	49824	80	192.168.2.7	160.153.136.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:03:32.862596035 CET	49824	80	192.168.2.7	160.153.136.3
Jan 28, 2022 14:03:32.889031887 CET	80	49824	160.153.136.3	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:03:13.452752113 CET	63744	53	192.168.2.7	8.8.8.8
Jan 28, 2022 14:03:13.472398043 CET	53	63744	8.8.8.8	192.168.2.7
Jan 28, 2022 14:03:19.160311937 CET	61457	53	192.168.2.7	8.8.8.8
Jan 28, 2022 14:03:20.203752995 CET	61457	53	192.168.2.7	8.8.8.8
Jan 28, 2022 14:03:20.496268988 CET	53	61457	8.8.8.8	192.168.2.7
Jan 28, 2022 14:03:20.521825075 CET	53	61457	8.8.8.8	192.168.2.7
Jan 28, 2022 14:03:26.958014965 CET	58367	53	192.168.2.7	8.8.8.8
Jan 28, 2022 14:03:27.365228891 CET	53	58367	8.8.8.8	192.168.2.7
Jan 28, 2022 14:03:32.782090902 CET	59571	53	192.168.2.7	8.8.8.8
Jan 28, 2022 14:03:32.805377960 CET	53	59571	8.8.8.8	192.168.2.7
Jan 28, 2022 14:03:37.876553059 CET	52689	53	192.168.2.7	8.8.8.8
Jan 28, 2022 14:03:38.058901072 CET	53	52689	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 14:03:13.452752113 CET	192.168.2.7	8.8.8.8	0xfd6f	Standard query (0)	www.desertbirdmercantile.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:19.160311937 CET	192.168.2.7	8.8.8.8	0xeac5	Standard query (0)	www.thietkenoithatvanphong.asia	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:20.203752995 CET	192.168.2.7	8.8.8.8	0xeac5	Standard query (0)	www.thietkenoithatvanphong.asia	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:26.958014965 CET	192.168.2.7	8.8.8.8	0xf897	Standard query (0)	www.yzztx.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:32.782090902 CET	192.168.2.7	8.8.8.8	0xa159	Standard query (0)	www.sigmamu.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:37.876553059 CET	192.168.2.7	8.8.8.8	0x87a	Standard query (0)	www.madeinhome.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 14:03:13.472398043 CET	8.8.8.8	192.168.2.7	0xfd6f	No error (0)	www.desertbirdmercantile.com	desertbirdmercantile.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:03:13.472398043 CET	8.8.8.8	192.168.2.7	0xfd6f	No error (0)	desertbirdmercantile.com		162.241.24.116	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:20.496268988 CET	8.8.8.8	192.168.2.7	0xeac5	No error (0)	www.thietkenoithatvanphong.asia		222.255.46.12	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:20.521825075 CET	8.8.8.8	192.168.2.7	0xeac5	No error (0)	www.thietkenoithatvanphong.asia		222.255.46.12	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:27.365228891 CET	8.8.8.8	192.168.2.7	0xf897	No error (0)	www.yzztx.com		154.214.67.82	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:32.805377960 CET	8.8.8.8	192.168.2.7	0xa159	No error (0)	www.sigmamu.com	sigmamu.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:03:32.805377960 CET	8.8.8.8	192.168.2.7	0xa159	No error (0)	sigmamu.com		160.153.136.3	A (IP address)	IN (0x0001)
Jan 28, 2022 14:03:38.058901072 CET	8.8.8.8	192.168.2.7	0x87a	No error (0)	www.madeinhome.com		23.230.105.134	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.desertbirdmercantile.com
- www.thietkenoithatvanphong.asia
- www.yzztx.com
- www.sigmamu.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49805	162.241.24.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 14:03:13.623902082 CET	10480	OUT	GET /b3xd/?qPYT=aV9tZ&iRah=Ie1PhgByqbmAnBTD/2NTTWN841CMZzf2VbgiXa4AsIuYcZI/bp6cv0uoISKMiipyVSmV9CFFiA== HTTP/1.1 Host: www.desertbirdmercantile.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 14:03:15.450484991 CET	10500	IN	HTTP/1.1 404 Not Found Date: Fri, 28 Jan 2022 13:03:13 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://www.desertbirdmercantile.com/wp-json/>; rel="https://api.w.org/" Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 65 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 61 76 61 64 61 2d 68 74 6d 6c 2d 6c 61 79 6f 75 74 2d 77 69 64 65 20 61 76 61 64 61 2d 68 74 6d 6c 2d 68 65 61 64 65 72 2d 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 2f 3e 0a 09 0d 0a Data Ascii: e9<!DOCTYPE html><html class="avada-html-layout-wide avada-html-header-position-top" lang="en-US"> <head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49821	222.255.46.12	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 14:03:21.434609890 CET	10521	OUT	GET /b3xd/?iRah=JdJx4d7W9+IGJje0hU/QcPoKaGdRUKvyvIN3jQdk7kxI7FpVQbo1IF0KYDc1cvBgS1iZcvDTaA==&qPYT=aV9tZ HTTP/1.1 Host: www.thietkenoithatvanphong.asia Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 14:03:22.344238997 CET	10521	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 28 Jan 2022 13:00:04 GMT Server: Apache/2 Upgrade: h2,h2c Connection: Upgrade, close X-Powered-By: PHP/7.2.22 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://www.thietkenoithatvanphong.asia/b3xd/?iRah=JdJx4d7W9+IGJje0hU/QcPoKaGdRUKvyvIN3jQdk7kxI7FpVQbo1IF0KYDc1cvBgS1iZcvDTaA==&qPYT=aV9tZ Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49822	154.214.67.82	80	C:\Windows\explorer.exe

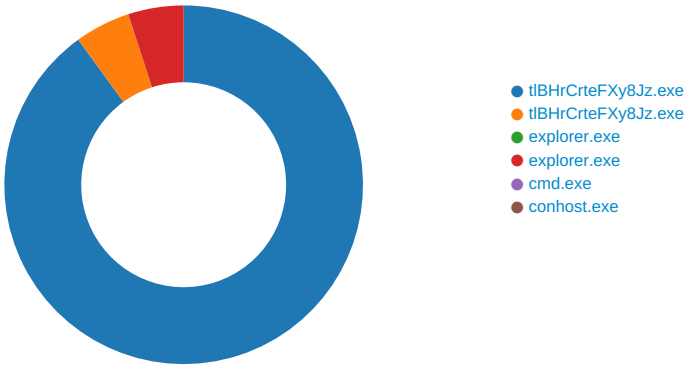
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 14:03:27.552238941 CET	10522	OUT	GET /b3xd/?qPYT=aV9tZ&iRah=u1+lAjLBA2+kcdvhq4UZu/nPbWuE94hnVKEDKIE9CxGJPgk2ISTbeIcckL5Cyvh DdyZbFg7D5w== HTTP/1.1 Host: www.yzztx.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 14:03:27.739898920 CET	10523	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 28 Jan 2022 13:03:27 GMT Content-Type: text/html Content-Length: 1755 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 c0 bc d6 dd d9 ca d0 d3 bb a5 c1 aa cd f8 c9 cc b3 c7 d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 35 34 30 32 3b 26 23 33 36 38 32 37 3b 26 23 32 36 33 37 39 3b 26 23 32 31 34 35 31 3b 26 23 32 30 31 35 34 3b 26 23 32 32 39 37 31 3b 26 23 33 30 33 34 30 3b 26 23 33 36 35 32 33 3b 26 23 32 30 33 30 37 3b 26 23 33 37 33 32 34 3b 2c 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 32 30 31 35 34 3b 26 23 32 35 31 30 34 3b 26 23 32 30 32 33 34 3b 26 23 32 30 31 35 34 3b 26 23 32 35 31 30 34 3b 26 23 32 30 32 33 34 3b 26 23 32 30 31 35 34 3b 26 23 32 35 31 30 34 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 33 32 35 39 33 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 31 3b 2c 26 23 31 39 39 36 38 3b 26 23 33 36 37 39 33 3b 26 23 32 35 37 32 30 3b 26 23 31 39 39 36 38 3b 26 23 33 36 37 39 33 3b 26 23 32 36 37 34 32 3b 26 23 31 39 39 36 38 3b 26 23 33 36 37 39 33 3b 26 23 33 33 30 37 33 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 2c 26 23 32 38 31 36 35 3b 26 23 33 32 34 33 31 3b 26 23 32 33 33 39 38 3b 26 23 32 39 39 38 33 3b 26 23 33 33 30 37 33 3b 26 23 33 35 30 33 33 3b 26 23 32 33 33 37 36 3b 26 23 33 32 34 33 31 3b 26 23 32 38 31 36 35 3b 26 23 32 32 35 34 30 32 3b 26 23 33 36 38 32 37 3b 26 23 32 36 33 37 39 3b 26 23 32 31 34 35 31 3b 26 23 32 30 31 35 34 3b 26 23 32 32 39 37 31 3b 26 23 33 30 33 34 30 3b 26 23 33 36 35 32 33 3b 26 23 32 30 33 30 37 3b 26 23 33 37 33 32 34 3b 2c 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 32 30 31 35 34 3b 26 23 32 35 31 30 34 3b 26 23 32 30 32 33 34 3b 26 23 32 30 31 35 34 3b 26 23 32 35 31 30 34 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 33 32 35 39 33 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 2c 26 23 31 39 39 36 38 3b 26 23 33 36 37 39 33 3b 26 23 32 36 37 34 32 3b 26 23 33 36 37 39 33 3b 26 23 33 33 30 37 33 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 2c 26 23 32 38 31 36 35 3b 26 23 33 32 34 33 31 3b 26 23 32 33 33 39 38 3b 26 23 32 39 39 38 33 3b 26 23 33 33 30 37 33 3b 26 23 32 33 33 37 36 3b 26 23 33 33 32 35 38 3b 26 23 32 34 39 34 34 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 35 34 30 32 3b 26 23 33 36 38 32 37 3b 26 23 32 36 33 37 39 3b 26 23 32 31 34 35 31 3b 26 23 32 30 31 35 34 3b 26 23 32 32 39 37 31 3b 26 23 33 30 33 34 30 3b 26 23 33 36 35 32 33 3b 26 23 32 30 33 30 37 3b 26 23 33 37 33 32 34 3b 2c 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 32 30 31 35 34 3b 26 23 32 35 31 30 34 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 33 32 35 39 33 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 2c 26 23 31 39 39 36 38 3b 26 23 33 36 37 39 33 3b 26 23 32 36 37 34 32 3b 26 23 33 36 37 39 33 3b 26 23 33 33 30 37 33 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 2c 26 23 32 38 31 36 35 3b 26 23 33 32 34 33 31 3b 26 23 32 33 33 39 38 3b 26 23 32 39 39 38 33 3b 26 23 33 33 30 37 33 3b 26 23 33 35 30 33 33 3b 26 23 32 33 33 37 36 3b 26 23 33 33 32 35 38 3b 26 23 32 34 39 34 34 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 35 34 30 32 3b 26 23 33 36 38 32 37 3b 26 23 32 36 33 37 39 3b 26 23 32 31 34 35 31 3b 26 23 32 30 31 35 34 3b 26 23 32 32 39 37 31 3b 26 23 33 30 33 34 30 3b 26 23 33 36 35 32 33 3b 26 23 32 30 33 30 37 3b 26 23 33 37 33 32 34 3b 2c 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 32 30 31 35 34 3b 26 23 32 35 31 30 34 3b 26 23 32 30 32 33 34 3b 26 23 32 30 31 35 34 3b 26 23 32 35 31 30 34 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 33 32 35 39 33 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 2c 26 23 31 39 39 36 38 3b 26 23 33 36 37 39 33 3b 26 23 32 36 37 34 32 3b 26 23 31 39 39 36 38 3b 26 23 33 36 37 39 33 3b 26 23 33 33 30 37 33 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 2c 26 23 32 38 31 36 35 3b 26 23 33 32 34 33 31 3b 26 23 32 33 33 39 38 3b 26 23 32 39 39 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>&#25402 ;进朋友人妻的身体里,亚洲人成伊人成综合网中文,一边摸一边桶一边脱免费,清纯学生脱裙子自慰</title><meta name="keywords" content="挺进朋友人妻的身体里,亚洲人成伊人成综合网中文,一边摸一边桶一边脱免费,清纯学生脱裙子自慰" /><meta name="description" content="挺进朋友人妻的身体里,亚洲人成伊人成综合网中文,一边摸一边桶一边脱免费,清纯学&#299

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49824	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 14:03:32.833165884 CET	10531	OUT	GET /b3xd/?iRah=5GWj3iokSHma3YiDoT3m16TCcfPCT77oIBdOELLk89ETJqvKsRjgRlGfGSz2uWFXBl65BQRHGg ==&qPYT=aV9tZ HTTP/1.1 Host: www.sigmamu.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 14:03:32.862364054 CET	10532	IN	HTTP/1.1 400 Bad Request Connection: close

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: tlBHrCrteFXy8Jz.exe PID: **6248**, Parent PID: **5676**

General

Target ID:	0
Start time:	14:01:29
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\tlBHrCrteFXy8Jz.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\tlBHrCrteFXy8Jz.exe"
Imagebase:	0xf00000
File size:	793600 bytes
MD5 hash:	0E9943C0E2AFAF5E9ACEC16CE184B444
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.304067071.0000000004319000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.304067071.0000000004319000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.304067071.0000000004319000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.303068640.00000000033C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.302694736.0000000003311000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: tlBHrCrteFXy8Jz.exe PID: **7160**, Parent PID: **6248**

General

Target ID:	11
Start time:	14:01:56
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\tlBHrCrteFXy8Jz.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\tlBHrCrteFXy8Jz.exe
Imagebase:	0xa20000
File size:	793600 bytes
MD5 hash:	0E9943C0E2AFAF5E9ACEC16CE184B444
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: 0000000B.00000000.299250808.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.299250808.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.299250808.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.373779572.0000000000F40000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.373779572.0000000000F40000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.373779572.0000000000F40000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.299753354.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.299753354.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.299753354.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.372769249.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.372769249.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.372769249.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.373929378.0000000000FC0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.373929378.0000000000FC0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.373929378.0000000000FC0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4186C7	NtReadFile

Analysis Process: explorer.exe PID: **3292**, Parent PID: **7160**

General

Target ID:	13
Start time:	14:02:00
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
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: 0000000D.00000000.358128872.000000000B7CA000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.358128872.000000000B7CA000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.358128872.000000000B7CA000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.337152454.000000000B7CA000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.337152454.000000000B7CA000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.337152454.000000000B7CA000.00000040.00000001.00040000.00000000.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: explorer.exe PID: 1292, Parent PID: 3292

General

Target ID:	16
Start time:	14:02:27
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xb10000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
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: 00000010.00000002.510355464.0000000004F80000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.510355464.0000000004F80000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.510355464.0000000004F80000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.509514447.0000000002F80000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.509514447.0000000002F80000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.509514447.0000000002F80000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.509765743.0000000004E60000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.509765743.0000000004E60000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.509765743.0000000004E60000.00000040.10000000.00040000.00000000.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	2F986C7	NtReadFile

Analysis Process: cmd.exe PID: 5280, Parent PID: 1292

General

Target ID:	19

Start time:	14:02:33
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\tlBHrCrteFXy8Jz.exe"
Imagebase:	0x870000
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: **4684**, Parent PID: **5280**

General

Target ID:	20
Start time:	14:02:35
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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