ID: 402842
Sample Name:
74ed218c_by_Libranalysis
Cookbook: default.jbs
Time: 14:41:46
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 74ed218c_by_Libranalysis 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
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 11
Contacted Domains 11
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 13
Public 13
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 19
ASN 20
JA3 Fingerprints 21
Dropped Files 21
Created / dropped Files 21
Static File Info 21
General 21
File Icon 22
Static PE Info 22
General 22
Entrypoint Preview 22
Data Directories 24

Sections 24
Resources 24
Imports 25
Version Infos 25
Network Behavior 25
Snort IDS Alerts 25
Network Port Distribution 26
TCP Packets 26
UDP Packets 27
DNS Queries 29
DNS Answers 29
HTTP Request Dependency Graph 30
HTTP Packets 30
Code Manipulations 32
Statistics 32
Behavior 32
System Behavior 32
Analysis Process: 74ed218c_by_Libranalysis.exe PID: 6800 Parent PID: 5876 32
General 32
File Activities 33
File Created 33
File Written 33
File Read 34
Analysis Process: 74ed218c_by_Libranalysis.exe PID: 6940 Parent PID: 6800 34
General 34
File Activities 35
File Read 35
Analysis Process: explorer.exe PID: 3440 Parent PID: 6940 35
General 35
File Activities 35
Analysis Process: cmd.exe PID: 4704 Parent PID: 3440 35
General 35
File Activities 36
File Read 36
Analysis Process: cmd.exe PID: 5936 Parent PID: 4704 36
General 36
File Activities 36
Analysis Process: conhost.exe PID: 5800 Parent PID: 5936 36
General 36
Disassembly 37
Code Analysis 37

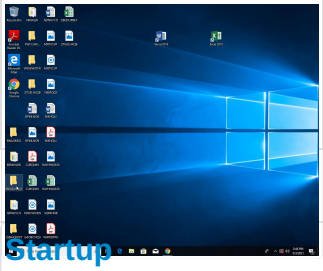
Analysis Report 74ed218c_by_Libranalysis

Overview

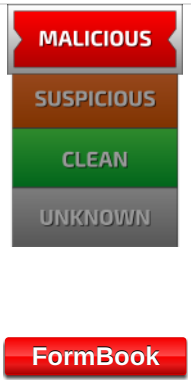
General Information

Sample Name:	74ed218c_by_Libranalysis (renamed file extension from none to exe)
Analysis ID:	402842
MD5:	74ed218c2c421e..
SHA1:	16d950eae07654..
SHA256:	b32ad3bf2b79e41.
Tags:	Formbook
Infos:	

Most interesting Screenshot:



Detection

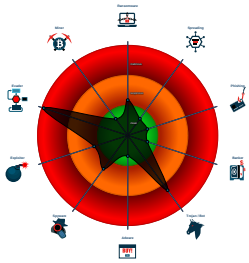


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- 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 …

Classification



Startup

- **System is w10x64**
- 74ed218c_by_Libranalysis.exe (PID: 6800 cmdline: 'C:\Users\user\Desktop\74ed218c_by_Libranalysis.exe' MD5: 74ED218C2C421E3978445A1EDBE40A08)
  - 74ed218c_by_Libranalysis.exe (PID: 6940 cmdline: C:\Users\user\Desktop\74ed218c_by_Libranalysis.exe MD5: 74ED218C2C421E3978445A1EDBE40A08)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 4704 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cmd.exe (PID: 5936 cmdline: /c del 'C:\Users\user\Desktop\74ed218c_by_Libranalysis.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.cats16.com/8u3b/"
  ],
  "decoy": [
    "pipienta.com",
    "wisdomfest.net",
    "jenniferreich.com",
    "bigcanoehomesforless.com",
    "kayandbernard.com",
    "offerbuildingsecrets.com",
    "benleefoto.com",
    "contactlesssoftware.tech",
    "statenislandplumbing.info",
    "lifestylemedicineservices.com",
    "blazerplanning.com",
    "fnatic-skins.club",
    "effectivemarketinginc.com",
    "babyshopit.com",
    "2000deal.com",
    "k12paymentcemter.com",
    "spwakd.com",
    "lesreponses.com",
    "abundando.com",
    "hawkspremierfhc.com",
    "midwestmadeclothing.com",
    "kamuakuinisiapa.com",
    "swirlingheadjewelry.com",
    "donelys.com",
    "stiloksero.com",
    "hoangphucsolar.com",
    "gb-contracting.com",
    "girlboyfriends.com",
    "decadejam.com",
    "glassfullcoffee.com",
    "todoparaconstruccion.com",
    "anygivenrunday.com",
    "newgalaxyindia.com",
    "dahlonegaforless.com",
    "blue-light.tech",
    "web-evo.com",
    "armmotive.com",
    "mollysmulligan.com",
    "penislandbrewer.com",
    "wgrimao.com",
    "dxm-int.net",
    "sarmaayagroup.com",
    "timbraunmusician.com",
    "amazoncovid19tracer.com",
    "peaknband.com",
    "pyqxlz.com",
    "palomachurch.com",
    "surfboardwarehouse.net",
    "burundiacademyst.com",
    "pltcoin.com",
    "workinglifestyle.com",
    "vickybowskill.com",
    "ottawahomevalues.info",
    "jtrainterrain.com",
    "francescoiocca.com",
    "metallitypiercing.com",
    "lashsavings.com",
    "discjockeydelraybeach.com",
    "indicraftsvilla.com",
    "tbq.xyz",
    "arfjkacsgatfzbazpdth.com",
    "appsend.online",
    "cunerier.com",
    "orospucocuguatmaca.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.377542690.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.377542690.0000000000400000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.377542690.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.378047898.0000000001680000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.378047898.0000000001680000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 15 entries				

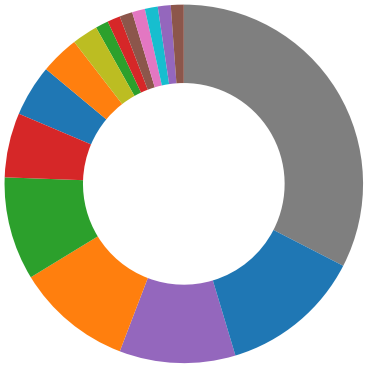
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.74ed218c_by_Libranalysis.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.74ed218c_by_Libranalysis.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.74ed218c_by_Libranalysis.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
3.2.74ed218c_by_Libranalysis.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.74ed218c_by_Libranalysis.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$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
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

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)

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

Stealing of Sensitive Information:

Yara detected FormBook

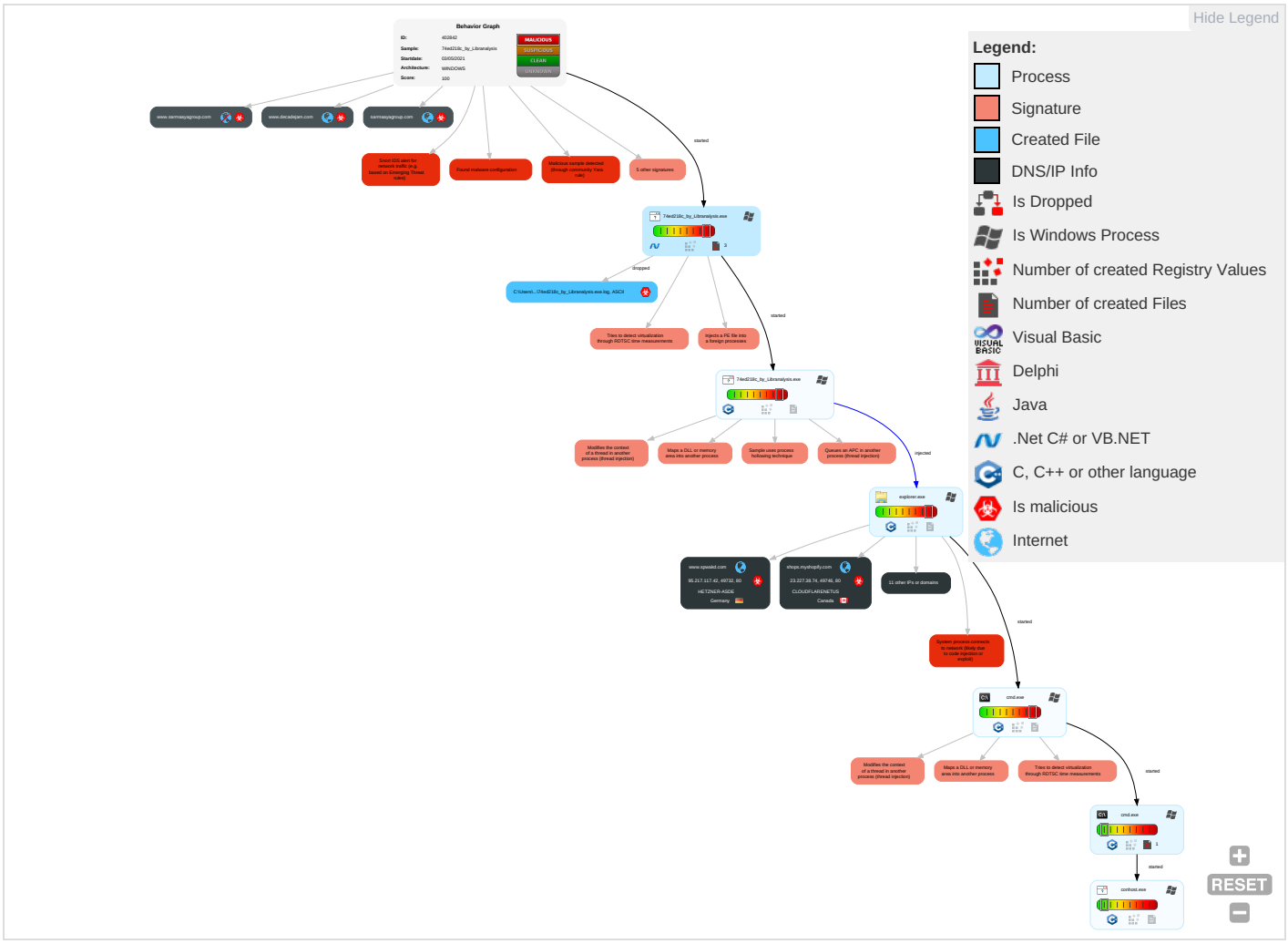
Remote Access Functionality:

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 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop c Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 2 4 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 6 1 2	Access Token Manipulation 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Virtualization/Sandbox Evasion 3 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	Virtualization/Sandbox Evasion 3 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 6 1 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Deobfuscate/Decode Files or Information 1	DCSync	System Information Discovery 1 2 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 4	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statior

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
74ed218c_by_Libranalysis.exe	14%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.74ed218c_by_Libranalysis.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
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.cats16.com/8u3b/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pyqxlz.com	34.102.136.180	true	false		unknown
sarmaayagroup.com	166.62.10.48	true	true		unknown
www.spwakd.com	95.217.117.42	true	true		unknown
www.decadejam.com	74.50.52.136	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.arfjkacsgatfzbazpdth.com	103.5.116.132	true	true		unknown
www.babyshopit.com	unknown	unknown	true		unknown
www.amazoncovid19tracer.com	unknown	unknown	true		unknown
www.pyqxlz.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.sarmaayagroup.com	unknown	unknown	true		unknown
www.jenniferreich.com	unknown	unknown	true		unknown
www.newgalaxyindia.com	unknown	unknown	true		unknown
www.kamuakuinisiapa.com	unknown	unknown	true		unknown
www.appsend.online	unknown	unknown	true		unknown
www.cats16.com	unknown	unknown	true		unknown

Contacted URLs

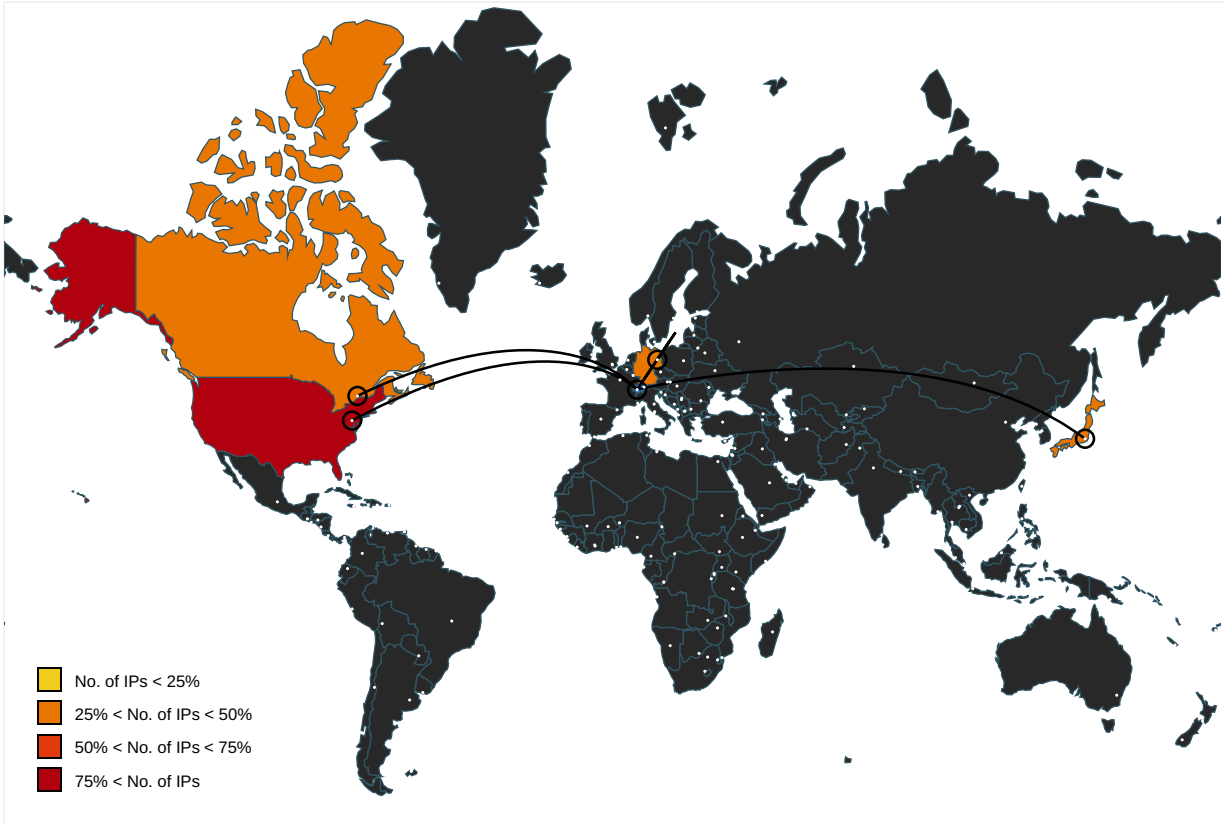
Name	Malicious	Antivirus Detection	Reputation
www.cats16.com/8u3b/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000005.00000000.341165696.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.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	74ed218c_by_Libranalysis.exe, 00000001.00000002.340709877.000000003215000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000005.00000000.364055555.000000000B1A6000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000005.0000000 0.364055555.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.0000000 0.364055555.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000005.0000000 0.364055555.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000005.0000000 0.364055555.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000005.0000000 0.364055555.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000005.0000000 0.364055555.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000005.0000000 0.364055555.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	74ed218c_by_Libranalysis.exe, 00000001.00000002.340649422.00 000000031C1000.00000004.000000 01.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000005.0000000 0.364055555.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/unguest	74ed218c_by_Libranalysis.exe	false		high
http:// https://github.com/unguest9WinForms_RecursiveFormCreate5 WinForms_SeeInnerExceptionGProperty	74ed218c_by_Libranalysis.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.5.116.132	www.arfjkacsgatfzbazpdth.com	Japan		17408	ABOVE-AS-APAboveNetCommunicationsTaiwanTW	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	pyqxlz.com	United States		15169	GOOGLEUS	false
95.217.117.42	www.spwakd.com	Germany		24940	HETZNER-ASDE	true
74.50.52.136	www.decadejam.com	United States		36024	AS-TIERP-36024US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402842
Start date:	03.05.2021
Start time:	14:41:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	74ed218c_by_Libranalysis (renamed file extension from none to 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:	29
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@13/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.9% (good quality ratio 6.6%) • Quality average: 75% • Quality standard deviation: 25.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 52.147.198.201, 92.122.145.220, 13.88.21.125, 104.43.193.48, 13.107.4.50, 13.64.90.137, 20.82.210.154, 92.122.213.249, 92.122.213.247, 205.185.216.10, 205.185.216.42, 51.103.5.186, 52.155.217.156, 20.54.26.129, 104.84.56.60 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, b1ns.c-0001.c-msedge.net, wu-fg-shim.trafficmanager.net, 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, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.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, b1ns.au-msedge.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, c-0001.c-msedge.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, download.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/402842/sample/74ed218c_by_Libranalysis.exe

Simulations

Behavior and APIs

Time	Type	Description
14:42:39	API Interceptor	2x Sleep call for process: 74ed218c_by_Libranalysis.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.5.116.132	MRQUolkoK7.exe	Get hash	malicious	Browse	• www.arfjkacsgatfzbazpdth.com/8u3b/?9rwxC4Lh=PWNBDH2hPCb1us8Ao8B+54WayNfcYj50QVchuC7xNQJC497qOyaPHph0Z/J570kZBf62v/9E1Q==&o2=iN68aFPHs
23.227.38.74	don.exe	Get hash	malicious	Browse	• www.funnyfootballmugs.com/uoe8/?BR=cjlpd&Y4plXns=oRF9sMnf9PdLhjUOIBAEDWVppNUvEE2O6ED6s7IbEJi5z3I9xavY20aFrDWDg7pV30V8
	WaybillDoc_7349796565.pdf.exe	Get hash	malicious	Browse	• www.theestellawear.com/sbqi/?JtxL=Ofv0h5DUcgF1HBnP9jQv4WLSG1M3kjn+2XlmTbHkz/cbhvSYry19ohgdWpI3v2dkGCKs&pph=kJBTslxPNNKLxNz
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• www.exuberantemodafeminina.com/ued5/?t8o8ntU=P+YSthdRkosM1Kkk+FGYkcUIeENu2yCNDkfR3XxxXKvwa5X+dXL5WZZdMs5u6SZ4VnDl&kRm0q=J48P
	wMqdemYyHm.exe	Get hash	malicious	Browse	• www.raiseamerican.com/f0sg/?7n0lqHm=YNkyISHPJk/bibwJBhOHtZm0DRLrV9PaArDWVr56RQ+cEQwRll7Xlbem2zoOENnktRSV&CP=chrxU
	PO#10244.exe	Get hash	malicious	Browse	• www.dreamlikeliving.com/uv34/?xV8HslL8=5UaGcRQVNBURRiJV+9v1SQNlNBIBrH6pS93qQ4ZjH/IbytUWJvzWBvUcaoCYSFJ+DAMYTluhcw==&1bz=o8rHa

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• www.advionpowergel.com/8njn/?CTvX=cvRh_lYP&uFNl=SvxnXnxPZ6/RXiCEA5gpWOUe8/6ZD7+WedveK6ILzn6yPy4OJmK7t7jGBRqeY+TLnjv1
	DocNo2300058329.exe	Get hash	malicious	Browse	• www.exuberantemodafeminina.com/ued5/?RL0=P+YSthdRkosM1Kkk+FGYkcUIeENu2yCNDkfR3XxxXKvwa5X+dXL5WZZdMvZ+1zJALCqi&BR-d4N=7nMpkDO0IdLxFH6P
	x16jmZMFrN.exe	Get hash	malicious	Browse	• www.covidpreventionshop.com/h6fe/?idCt3l3x=lvVfZQo4A24dNSGxxPwiOsdgHIv5tWk/cS3b4qunPdJKlwuQQcnTCZP3mbjBL0nYndss&Rv=Y2MpoVAxKRFDj0y
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• www.heoslight.com/maw9/?0V0hlZ=WKgLlhFhEzeNjFMge4LpHm5g+ODrZerh8srqhGFWn5kwTJLJyZ0r84PSd6yLMthvhFEa&OVolp8=AZ9lQ6QHS8EdPrG0
	z5Wqivscwd.exe	Get hash	malicious	Browse	• www.raiseamerican.com/f0sg/?9rQPJl=YNkyISHPJk/bibwJBhOHtZm0DRLrV9PaArDWVr56RQ+cEQwRll7Xlbem2zokb9XkpTaV&EzrtFB=4hL05l3xNH1L
	DVO100024000.doc	Get hash	malicious	Browse	• www.ameri canstatesapparel.com/f0sg/?tDK=3tuwmvhMi7pGvx+mmUPwBEVcP0da4WtROkbfwo1L944cWBUw2PlAV4md2HmgZSuKmmCfDA==&LPYP_=Sfgd

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	100005111.exe	Get hash	malicious	Browse	• www.dreamlikeliving.com/uv34/?tXEd=9r4tEpsH-L5HP&2dspJx=5UaGcRQVNBURRiJV+9v1SQNlNBIBrH6pS93qQ4ZjH/IbytUWJvzWBvUcaruiRElFA3tJ
	1103305789.exe	Get hash	malicious	Browse	• www.dreamlikeliving.com/uv34/?rZ=5UaGcRQVNBURRiJV+9v1SQNlNBIBrH6pS93qQ4ZjH/IbytUWJvzWBvUcaoChN0p9NWQfTlumPA==&sBvD8F=GxopsDgxOz1D0R
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• www.weirdkult.com/b3gc/?ndkHzH=-Z20XnRx36xD&ARn=fdxwzo3oR3+60ycRzpiGgZCohcHl+5WU1+HTjmZXhP2AlGDanZS5zFmFBLd5xguXKjuO
	zDUYXIqwi4.exe	Get hash	malicious	Browse	• www.recovatek.com/hx3a/?YVMtavf=fCmUcBRhMrUy3w+kl11B/xiypSW2fUD8cU7Pu3gqArK5c3pJn3j9k/DsIYuCZjxFqiyLV4XQ2A==&EBZ=ZTIHdV4XjtnXb
	HbnmVuxDIc.exe	Get hash	malicious	Browse	• www.manicolada.com/oerg/?xBZ4k4xH=VrJFN02EWUtV1rIt9g/j1QSdUuEw0Uf1/z3ywhG+Y3UeSqedxSn0wL7pECCF3FrbmHhMvfLpdA==&tHr8=gdfDsdw8
	Invoice.exe	Get hash	malicious	Browse	• www.cjaccessories.net/eqas/?v4Xp-=zlzoH+ErGdORI3KgnipEDQmAM+5mnlewXlSz4LF6ZDcdx8ultHTjoqljxUMZx7tHvLXvbS3vgg==&0nGP-6=LhrLJ4-pzBedz

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	OuuJQ2R6v5.exe	Get hash	malicious	Browse	• www.trumpchix.com/g8bi/?7n=zq4LXs77W3q9n4caIdqAltHL4o48M8oiqlf9nZ5gHtwqOaWe9U5+XgrVJla/dPCaliP2&lHK8=X2JX02PxcH_p0rM
	MV UNIVERSE-VSLS PARTICULARS.xlsx	Get hash	malicious	Browse	• www.jeepleakfix.com/g8bi/?Bxl07=m24teDGumfLdhubkEoQ3vTFb65+EzEIQ3uP3ktaAm8QAzLszxgXzDa7IljZf3XZM8rNvuQ==&3f=WpU4Ex
	pdf Re revised PI 900tons.exe	Get hash	malicious	Browse	• www.trendyheld.com/edbs/?mHId9X=d74BDEXnxoADciMbQzj0eCjrMELcvf+wOrQFIjwVZdGJg+vXDTJsALwkgrbDA7hrk8UtLYkwRQ==&ExlldL=Udg8Tf2pOFu
95.217.117.42	MRQUolkoK7.exe	Get hash	malicious	Browse	• www.spwakd.com/8u3b/?o2=iN68aFPHs&9rwxC4Lh=ApmP+YWYCK6vLVfjcl0EWRKNz1AqTOP9eBXy99nVLHRI2g8p2qSHut9K1XPoIIT5Jec57i/T8w==
	PO20210429.xlsx	Get hash	malicious	Browse	• www.spwakd.com/8u3b/?WBZXQ8j=ApmP+YWdCN6rLFTvel0EWRKNz1AqTOP9eBPih+7UPnRJ2RQvx6DL4pFI2xPXPYryL+0fiQ==&Mz=ltx0qfi0x45
	PO_29_00412.exe	Get hash	malicious	Browse	• www.dpok.network/hw6d/?rVEt3p=S0D0v04&SPx=ls4KrYyf4XWOBM5SK/TIhyWi005n2zKHC8sQkWkcGenl5Mi6K3ubve8XeBiUJJUq8V1yzgpX8A==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.spwakd.com	MRQUolkoK7.exe	Get hash	malicious	Browse	• 95.217.117.42
	PO20210429.xlsx	Get hash	malicious	Browse	• 95.217.117.42
www.arfjkacsgatfzbazpdth.com	MRQUolkoK7.exe	Get hash	malicious	Browse	• 103.5.116.132
shops.myshopify.com	don.exe	Get hash	malicious	Browse	• 23.227.38.74
	WaybillDoc_7349796565.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#10244.exe	Get hash	malicious	Browse	• 23.227.38.74
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	DocNo2300058329.exe	Get hash	malicious	Browse	• 23.227.38.74
	x16jmZMFrN.exe	Get hash	malicious	Browse	• 23.227.38.74
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• 23.227.38.74
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 23.227.38.74
	DVO100024000.doc	Get hash	malicious	Browse	• 23.227.38.74
	100005111.exe	Get hash	malicious	Browse	• 23.227.38.74
	1103305789.exe	Get hash	malicious	Browse	• 23.227.38.74
	New order.04272021.DOC.exe	Get hash	malicious	Browse	• 23.227.38.74
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	zDUYXIqwi4.exe	Get hash	malicious	Browse	• 23.227.38.74
	HbnmVuxDIc.exe	Get hash	malicious	Browse	• 23.227.38.74
	Invoice.exe	Get hash	malicious	Browse	• 23.227.38.74
	OuuJQ2R6v5.exe	Get hash	malicious	Browse	• 23.227.38.74
	MV UNIVERSE-VSLS PARTICULARS.xlsx	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-TIERP-36024US	c98768e6_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	0af9d688_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	85c45fa1_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	66849b38_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	61c611ad_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	d81cbf02_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	b12b4f2b_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	d5fc03b1_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	cc0fd026_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	c0e07b7a_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	c6f70722_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	1206ac3c_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	8c736bc5_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	51092ff9_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	3bf3256b_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	625b54c1_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	abb13f4d_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	75266cb3_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	b81e5436_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
	b9471641_by_Libranalysis.dll	Get hash	malicious	Browse	• 72.249.22.245
HETZNER-ASDE	c98768e6_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	0af9d688_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	85c45fa1_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	66849b38_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	61c611ad_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	d81cbf02_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	b12b4f2b_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	d5fc03b1_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	cc0fd026_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	c0e07b7a_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	c6f70722_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	ff878909_by_Libranalysis.exe	Get hash	malicious	Browse	• 195.201.225.248
	e17486cd_by_Libranalysis.exe	Get hash	malicious	Browse	• 188.34.193.205
	1206ac3c_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	SecuriteInfo.com.Trojan.PackedNET.624.6293.exe	Get hash	malicious	Browse	• 78.46.5.205
	8c736bc5_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	51092ff9_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	3bf3256b_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	625b54c1_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	abb13f4d_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
ABOVE-AS-APAboveNetCommunicationsTaiwanTW	MRQUolkoK7.exe	Get hash	malicious	Browse	• 103.5.116.132
CLOUDFLARENETUS	Bank payment return x.exe	Get hash	malicious	Browse	• 104.21.19.200

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Trojan.GenericKD.36812138.16843.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4.dll	Get hash	malicious	Browse	• 104.20.184.68
	LAjei2S8bg.exe	Get hash	malicious	Browse	• 104.21.19.200
	HFTeISi0wZQeZi6.exe	Get hash	malicious	Browse	• 104.21.19.200
	don.exe	Get hash	malicious	Browse	• 172.67.218.244
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.18.24.31
	QEpa8OLm9Z.exe	Get hash	malicious	Browse	• 172.67.188.154
	c7b8f5dc_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.19.200
	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.159.133.233
	e17486cd_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.17.62.50
	O1E623TjjW.exe	Get hash	malicious	Browse	• 104.21.24.135
	calvary petroleum.doc	Get hash	malicious	Browse	• 104.21.19.200
	34zNZUh9hTEGU4a.exe	Get hash	malicious	Browse	• 104.21.19.200
	b75e7348_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.184.68
	PV GAS THI VAI LNG RECEIVING TERMINAL EXPANSION PROJECT.exe	Get hash	malicious	Browse	• 104.21.19.200
	eHV0IaHe2btEhvP.exe	Get hash	malicious	Browse	• 172.67.188.154
	BOQ and specifications.exe	Get hash	malicious	Browse	• 104.21.19.200
	WaybillDoc_7349796565.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\74ed218c_by_Libranalysis.exe.log

Process:	C:\Users\user\Desktop\74ed218c_by_Libranalysis.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):	7.885893866459429

General

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:	74ed218c_by_Libranalysis.exe
File size:	793600
MD5:	74ed218c2c421e3978445a1edbe40a08
SHA1:	16d950eae07654c9805d4476928c4c8d7d12fcc1
SHA256:	b32ad3bf2b79e411ca0450c1d5430d12c9bb73c269e0838ee512bc816fcce3b7
SHA512:	0cb4af6ad1434d4140d0e055fc77de2543c9ea9babe077ce27184b1628cbdc8f32530c5f0c2f4b3e1199459c0521e67415421525070c0870e75dc09105bf94d6
SSDEEP:	24576:cuiV+Sy45VNaxhYxuPiRmE6zJ/sC44nJRT:5iV+vkaFKRmt/sKn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(..`.....P..<.....[... ...`....@.. .....`.....@.....

File Icon

Icon Hash:	ce27232d2d2327c8

Static PE Info

General

Entrypoint:	0x4b5bb2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x608FA828 [Mon May 3 07:37:12 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb5b60	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0xda5c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc4000	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	0xb3bb8	0xb3c00	False	0.938543115438	data	7.92660309365	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0xda5c	0xdc00	False	0.463245738636	data	6.04896979773	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb6340	0x2e8	data		
RT_ICON	0xb6628	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0xb6750	0xea8	data		
RT_ICON	0xb75f8	0x8a8	data		
RT_ICON	0xb7ea0	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0xb8408	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xbc630	0x25a8	data		
RT_ICON	0xbebd8	0x1a68	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc0640	0x10a8	data		
RT_ICON	0xc16e8	0x988	data		
RT_ICON	0xc2070	0x6b8	data		
RT_ICON	0xc2728	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xc2b90	0xae	data		
RT_VERSION	0xc2c40	0x394	data		
RT_MANIFEST	0xc2fd4	0xa85	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	IBuiltInPermission.exe
FileVersion	1.0.1.35
CompanyName	Unguest
LegalTrademarks	Unguest
Comments	A light media player
ProductName	LightWatch
ProductVersion	1.0.1.35
FileDescription	LightWatch
OriginalFilename	IBuiltInPermission.exe

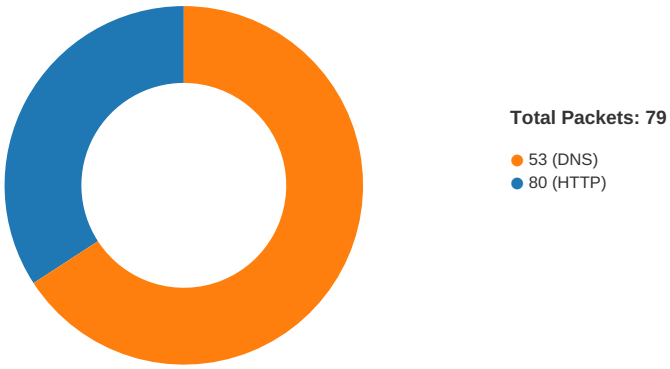
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-14:42:36.051325	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:42:36.086400	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/03/21-14:42:36.087379	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:42:36.123092	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
05/03/21-14:42:36.123519	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:42:36.158814	ICMP	449	ICMP Time-To-Live Exceeded in Transit			91.206.52.152	192.168.2.6
05/03/21-14:42:36.159190	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:42:39.761683	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:42:43.762166	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:42:47.762259	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:42:51.763140	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:42:55.763001	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:42:59.763250	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:43:03.763604	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:43:07.768561	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-14:43:11.764955	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:43:15.780771	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:43:19.765195	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:43:23.765601	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-14:43:23.801579	ICMP	408	ICMP Echo Reply			13.107.4.50	192.168.2.6
05/03/21-14:43:52.496176	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49746	23.227.38.74	192.168.2.6
05/03/21-14:43:57.795477	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49747	34.102.136.180	192.168.2.6
05/03/21-14:44:49.609591	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.6	166.62.10.48
05/03/21-14:44:49.609591	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.6	166.62.10.48
05/03/21-14:44:49.609591	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.6	166.62.10.48

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:43:30.841694117 CEST	49732	80	192.168.2.6	95.217.117.42
May 3, 2021 14:43:30.906488895 CEST	80	49732	95.217.117.42	192.168.2.6
May 3, 2021 14:43:30.906631947 CEST	49732	80	192.168.2.6	95.217.117.42
May 3, 2021 14:43:30.906847954 CEST	49732	80	192.168.2.6	95.217.117.42
May 3, 2021 14:43:30.971499920 CEST	80	49732	95.217.117.42	192.168.2.6
May 3, 2021 14:43:30.971549034 CEST	80	49732	95.217.117.42	192.168.2.6
May 3, 2021 14:43:30.971558094 CEST	80	49732	95.217.117.42	192.168.2.6
May 3, 2021 14:43:30.971837997 CEST	49732	80	192.168.2.6	95.217.117.42
May 3, 2021 14:43:30.987694979 CEST	49732	80	192.168.2.6	95.217.117.42
May 3, 2021 14:43:31.052467108 CEST	80	49732	95.217.117.42	192.168.2.6
May 3, 2021 14:43:41.450367928 CEST	49736	80	192.168.2.6	103.5.116.132
May 3, 2021 14:43:41.728737116 CEST	80	49736	103.5.116.132	192.168.2.6
May 3, 2021 14:43:41.729068041 CEST	49736	80	192.168.2.6	103.5.116.132
May 3, 2021 14:43:41.729366064 CEST	49736	80	192.168.2.6	103.5.116.132
May 3, 2021 14:43:42.006519079 CEST	80	49736	103.5.116.132	192.168.2.6
May 3, 2021 14:43:42.007214069 CEST	80	49736	103.5.116.132	192.168.2.6
May 3, 2021 14:43:42.007230043 CEST	80	49736	103.5.116.132	192.168.2.6
May 3, 2021 14:43:42.007375956 CEST	49736	80	192.168.2.6	103.5.116.132
May 3, 2021 14:43:42.009159088 CEST	49736	80	192.168.2.6	103.5.116.132
May 3, 2021 14:43:42.286375046 CEST	80	49736	103.5.116.132	192.168.2.6
May 3, 2021 14:43:52.275767088 CEST	49746	80	192.168.2.6	23.227.38.74
May 3, 2021 14:43:52.317616940 CEST	80	49746	23.227.38.74	192.168.2.6
May 3, 2021 14:43:52.317800045 CEST	49746	80	192.168.2.6	23.227.38.74

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:43:52.317936897 CEST	49746	80	192.168.2.6	23.227.38.74
May 3, 2021 14:43:52.361114979 CEST	80	49746	23.227.38.74	192.168.2.6
May 3, 2021 14:43:52.496176004 CEST	80	49746	23.227.38.74	192.168.2.6
May 3, 2021 14:43:52.496205091 CEST	80	49746	23.227.38.74	192.168.2.6
May 3, 2021 14:43:52.496217012 CEST	80	49746	23.227.38.74	192.168.2.6
May 3, 2021 14:43:52.496228933 CEST	80	49746	23.227.38.74	192.168.2.6
May 3, 2021 14:43:52.496248007 CEST	80	49746	23.227.38.74	192.168.2.6
May 3, 2021 14:43:52.496260881 CEST	80	49746	23.227.38.74	192.168.2.6
May 3, 2021 14:43:52.496437073 CEST	49746	80	192.168.2.6	23.227.38.74
May 3, 2021 14:43:52.496493101 CEST	49746	80	192.168.2.6	23.227.38.74
May 3, 2021 14:43:52.496622086 CEST	49746	80	192.168.2.6	23.227.38.74
May 3, 2021 14:43:52.497508049 CEST	80	49746	23.227.38.74	192.168.2.6
May 3, 2021 14:43:52.497575998 CEST	49746	80	192.168.2.6	23.227.38.74
May 3, 2021 14:43:57.617427111 CEST	49747	80	192.168.2.6	34.102.136.180
May 3, 2021 14:43:57.658473015 CEST	80	49747	34.102.136.180	192.168.2.6
May 3, 2021 14:43:57.658669949 CEST	49747	80	192.168.2.6	34.102.136.180
May 3, 2021 14:43:57.658832073 CEST	49747	80	192.168.2.6	34.102.136.180
May 3, 2021 14:43:57.699692011 CEST	80	49747	34.102.136.180	192.168.2.6
May 3, 2021 14:43:57.795476913 CEST	80	49747	34.102.136.180	192.168.2.6
May 3, 2021 14:43:57.795511961 CEST	80	49747	34.102.136.180	192.168.2.6
May 3, 2021 14:43:57.795660973 CEST	49747	80	192.168.2.6	34.102.136.180
May 3, 2021 14:43:57.795696974 CEST	49747	80	192.168.2.6	34.102.136.180
May 3, 2021 14:43:57.836584091 CEST	80	49747	34.102.136.180	192.168.2.6
May 3, 2021 14:44:23.204823971 CEST	49751	80	192.168.2.6	74.50.52.136
May 3, 2021 14:44:26.210383892 CEST	49751	80	192.168.2.6	74.50.52.136
May 3, 2021 14:44:32.224039078 CEST	49751	80	192.168.2.6	74.50.52.136
May 3, 2021 14:44:44.975044966 CEST	49753	80	192.168.2.6	74.50.52.136
May 3, 2021 14:44:47.959772110 CEST	49753	80	192.168.2.6	74.50.52.136

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:42:28.731353045 CEST	62044	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:28.803082943 CEST	53	62044	8.8.8.8	192.168.2.6
May 3, 2021 14:42:29.333442926 CEST	63791	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:29.384006977 CEST	53	63791	8.8.8.8	192.168.2.6
May 3, 2021 14:42:30.144805908 CEST	64267	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:30.202353954 CEST	53	64267	8.8.8.8	192.168.2.6
May 3, 2021 14:42:30.643338919 CEST	49448	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:30.702867031 CEST	53	49448	8.8.8.8	192.168.2.6
May 3, 2021 14:42:30.938601017 CEST	60342	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:30.992634058 CEST	53	60342	8.8.8.8	192.168.2.6
May 3, 2021 14:42:31.803185940 CEST	61346	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:31.853010893 CEST	53	61346	8.8.8.8	192.168.2.6
May 3, 2021 14:42:33.014483929 CEST	51774	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:33.063134909 CEST	53	51774	8.8.8.8	192.168.2.6
May 3, 2021 14:42:34.276711941 CEST	56023	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:34.325309038 CEST	53	56023	8.8.8.8	192.168.2.6
May 3, 2021 14:42:35.176676989 CEST	58384	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:35.229954004 CEST	53	58384	8.8.8.8	192.168.2.6
May 3, 2021 14:42:35.982534885 CEST	60261	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:36.023857117 CEST	56061	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:36.039100885 CEST	53	60261	8.8.8.8	192.168.2.6
May 3, 2021 14:42:36.072993994 CEST	53	56061	8.8.8.8	192.168.2.6
May 3, 2021 14:42:38.431483984 CEST	58336	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:38.480279922 CEST	53	58336	8.8.8.8	192.168.2.6
May 3, 2021 14:42:39.348581076 CEST	53781	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:39.399909973 CEST	53	53781	8.8.8.8	192.168.2.6
May 3, 2021 14:42:40.590265989 CEST	54064	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:40.640347004 CEST	53	54064	8.8.8.8	192.168.2.6
May 3, 2021 14:42:41.799211025 CEST	52811	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:41.850986004 CEST	53	52811	8.8.8.8	192.168.2.6
May 3, 2021 14:42:43.501785040 CEST	55299	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:43.563138008 CEST	53	55299	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:42:44.497627974 CEST	63745	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:44.554634094 CEST	53	63745	8.8.8.8	192.168.2.6
May 3, 2021 14:42:45.477952003 CEST	50055	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:45.526963949 CEST	53	50055	8.8.8.8	192.168.2.6
May 3, 2021 14:42:46.594819069 CEST	61374	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:46.643687963 CEST	53	61374	8.8.8.8	192.168.2.6
May 3, 2021 14:42:48.026428938 CEST	50339	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:48.087661028 CEST	53	50339	8.8.8.8	192.168.2.6
May 3, 2021 14:42:49.008661032 CEST	63307	53	192.168.2.6	8.8.8.8
May 3, 2021 14:42:49.060020924 CEST	53	63307	8.8.8.8	192.168.2.6
May 3, 2021 14:43:07.185836077 CEST	49694	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:07.234436989 CEST	53	49694	8.8.8.8	192.168.2.6
May 3, 2021 14:43:22.216257095 CEST	54982	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:22.276076078 CEST	53	54982	8.8.8.8	192.168.2.6
May 3, 2021 14:43:24.142365932 CEST	50010	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:24.195888996 CEST	53	50010	8.8.8.8	192.168.2.6
May 3, 2021 14:43:24.935106039 CEST	63718	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:25.009084940 CEST	53	63718	8.8.8.8	192.168.2.6
May 3, 2021 14:43:25.305160999 CEST	62116	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:25.366305113 CEST	53	62116	8.8.8.8	192.168.2.6
May 3, 2021 14:43:30.018943071 CEST	63816	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:30.087877989 CEST	53	63816	8.8.8.8	192.168.2.6
May 3, 2021 14:43:31.656812906 CEST	55014	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:31.714086056 CEST	53	55014	8.8.8.8	192.168.2.6
May 3, 2021 14:43:36.005229950 CEST	62208	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:36.081224918 CEST	53	62208	8.8.8.8	192.168.2.6
May 3, 2021 14:43:40.042953014 CEST	57574	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:40.188538074 CEST	53	57574	8.8.8.8	192.168.2.6
May 3, 2021 14:43:40.809952974 CEST	51818	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:40.900835991 CEST	53	51818	8.8.8.8	192.168.2.6
May 3, 2021 14:43:41.126205921 CEST	56628	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:41.448692083 CEST	53	56628	8.8.8.8	192.168.2.6
May 3, 2021 14:43:41.539508104 CEST	60778	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:41.600740910 CEST	53	60778	8.8.8.8	192.168.2.6
May 3, 2021 14:43:42.190650940 CEST	53799	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:42.250555038 CEST	53	53799	8.8.8.8	192.168.2.6
May 3, 2021 14:43:42.835406065 CEST	54683	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:42.896348000 CEST	53	54683	8.8.8.8	192.168.2.6
May 3, 2021 14:43:43.280991077 CEST	59329	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:43.338252068 CEST	53	59329	8.8.8.8	192.168.2.6
May 3, 2021 14:43:44.073010921 CEST	64021	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:44.133064985 CEST	53	64021	8.8.8.8	192.168.2.6
May 3, 2021 14:43:45.212090015 CEST	56129	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:45.310631990 CEST	53	56129	8.8.8.8	192.168.2.6
May 3, 2021 14:43:46.398830891 CEST	58177	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:46.455845118 CEST	53	58177	8.8.8.8	192.168.2.6
May 3, 2021 14:43:47.022499084 CEST	50700	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:47.102418900 CEST	53	50700	8.8.8.8	192.168.2.6
May 3, 2021 14:43:48.281198025 CEST	54069	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:48.340060949 CEST	53	54069	8.8.8.8	192.168.2.6
May 3, 2021 14:43:49.868282080 CEST	61178	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:49.925497055 CEST	53	61178	8.8.8.8	192.168.2.6
May 3, 2021 14:43:52.115824938 CEST	57017	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:52.263573885 CEST	53	57017	8.8.8.8	192.168.2.6
May 3, 2021 14:43:57.542874098 CEST	56327	53	192.168.2.6	8.8.8.8
May 3, 2021 14:43:57.616167068 CEST	53	56327	8.8.8.8	192.168.2.6
May 3, 2021 14:44:02.803395987 CEST	50243	53	192.168.2.6	8.8.8.8
May 3, 2021 14:44:02.900130987 CEST	53	50243	8.8.8.8	192.168.2.6
May 3, 2021 14:44:07.881709099 CEST	62055	53	192.168.2.6	8.8.8.8
May 3, 2021 14:44:07.913749933 CEST	61249	53	192.168.2.6	8.8.8.8
May 3, 2021 14:44:07.940939903 CEST	53	62055	8.8.8.8	192.168.2.6
May 3, 2021 14:44:07.983449936 CEST	53	61249	8.8.8.8	192.168.2.6
May 3, 2021 14:44:13.017112970 CEST	65252	53	192.168.2.6	8.8.8.8
May 3, 2021 14:44:13.081286907 CEST	53	65252	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:44:23.119055033 CEST	64367	53	192.168.2.6	8.8.8.8
May 3, 2021 14:44:23.203619957 CEST	53	64367	8.8.8.8	192.168.2.6
May 3, 2021 14:44:29.683831930 CEST	55066	53	192.168.2.6	8.8.8.8
May 3, 2021 14:44:29.735109091 CEST	53	55066	8.8.8.8	192.168.2.6
May 3, 2021 14:44:44.905441046 CEST	60211	53	192.168.2.6	8.8.8.8
May 3, 2021 14:44:44.968118906 CEST	53	60211	8.8.8.8	192.168.2.6
May 3, 2021 14:44:49.245368004 CEST	56570	53	192.168.2.6	8.8.8.8
May 3, 2021 14:44:49.319710016 CEST	53	56570	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 14:43:24.935106039 CEST	192.168.2.6	8.8.8.8	0x1cad	Standard query (0)	www.amazoncovid19tracer.com	A (IP address)	IN (0x0001)
May 3, 2021 14:43:30.018943071 CEST	192.168.2.6	8.8.8.8	0x2ef3	Standard query (0)	www.spwakd.com	A (IP address)	IN (0x0001)
May 3, 2021 14:43:36.005229950 CEST	192.168.2.6	8.8.8.8	0x304b	Standard query (0)	www.jenniferreich.com	A (IP address)	IN (0x0001)
May 3, 2021 14:43:41.126205921 CEST	192.168.2.6	8.8.8.8	0x6fa2	Standard query (0)	www.arfjkacsgatfzbazpdth.com	A (IP address)	IN (0x0001)
May 3, 2021 14:43:47.022499084 CEST	192.168.2.6	8.8.8.8	0x310f	Standard query (0)	www.newgalaxyindia.com	A (IP address)	IN (0x0001)
May 3, 2021 14:43:52.115824938 CEST	192.168.2.6	8.8.8.8	0x1535	Standard query (0)	www.babyshopit.com	A (IP address)	IN (0x0001)
May 3, 2021 14:43:57.542874098 CEST	192.168.2.6	8.8.8.8	0x62da	Standard query (0)	www.pyqxlz.com	A (IP address)	IN (0x0001)
May 3, 2021 14:44:02.803395987 CEST	192.168.2.6	8.8.8.8	0xa939	Standard query (0)	www.appsend.online	A (IP address)	IN (0x0001)
May 3, 2021 14:44:07.913749933 CEST	192.168.2.6	8.8.8.8	0xcb70	Standard query (0)	www.kamuakuinisiapa.com	A (IP address)	IN (0x0001)
May 3, 2021 14:44:13.017112970 CEST	192.168.2.6	8.8.8.8	0x41ca	Standard query (0)	www.cats16.com	A (IP address)	IN (0x0001)
May 3, 2021 14:44:23.119055033 CEST	192.168.2.6	8.8.8.8	0x1e94	Standard query (0)	www.decadejam.com	A (IP address)	IN (0x0001)
May 3, 2021 14:44:44.905441046 CEST	192.168.2.6	8.8.8.8	0x9efd	Standard query (0)	www.decadejam.com	A (IP address)	IN (0x0001)
May 3, 2021 14:44:49.245368004 CEST	192.168.2.6	8.8.8.8	0xc3a8	Standard query (0)	www.sarmaayagroup.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:43:25.009084940 CEST	8.8.8.8	192.168.2.6	0x1cad	Name error (3)	www.amazoncovid19tracer.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:43:30.087877989 CEST	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	www.spwakd.com		95.217.117.42	A (IP address)	IN (0x0001)
May 3, 2021 14:43:36.081224918 CEST	8.8.8.8	192.168.2.6	0x304b	Name error (3)	www.jenniferreich.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:43:41.448692083 CEST	8.8.8.8	192.168.2.6	0x6fa2	No error (0)	www.arfjkacsgatfzbazpdth.com		103.5.116.132	A (IP address)	IN (0x0001)
May 3, 2021 14:43:47.102418900 CEST	8.8.8.8	192.168.2.6	0x310f	Name error (3)	www.newgalaxyindia.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:43:52.263573885 CEST	8.8.8.8	192.168.2.6	0x1535	No error (0)	www.babyshopit.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:43:52.263573885 CEST	8.8.8.8	192.168.2.6	0x1535	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 3, 2021 14:43:57.616167068 CEST	8.8.8.8	192.168.2.6	0x62da	No error (0)	www.pyqxlz.com	pyqxlz.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:43:57.616167068 CEST	8.8.8.8	192.168.2.6	0x62da	No error (0)	pyqxlz.com		34.102.136.180	A (IP address)	IN (0x0001)
May 3, 2021 14:44:02.900130987 CEST	8.8.8.8	192.168.2.6	0xa939	Server failure (2)	www.appsend.online	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:44:07.983449936 CEST	8.8.8.8	192.168.2.6	0xcb70	Name error (3)	www.kamuakuinisiapa.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:44:13.081286907 CEST	8.8.8.8	192.168.2.6	0x41ca	Name error (3)	www.cats16.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:44:23.203619957 CEST	8.8.8.8	192.168.2.6	0x1e94	No error (0)	www.decadejam.com		74.50.52.136	A (IP address)	IN (0x0001)
May 3, 2021 14:44:44.968118906 CEST	8.8.8.8	192.168.2.6	0x9efd	No error (0)	www.decadejam.com		74.50.52.136	A (IP address)	IN (0x0001)
May 3, 2021 14:44:49.319710016 CEST	8.8.8.8	192.168.2.6	0xc3a8	No error (0)	www.sarmaayagroup.com	sarmaayagroup.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:44:49.319710016 CEST	8.8.8.8	192.168.2.6	0xc3a8	No error (0)	sarmaayagroup.com		166.62.10.48	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.spwakd.com
- www.arfjkacsgatfzbazpdth.com
- www.babyshopit.com
- www.pyqxlz.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49732	95.217.117.42	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:43:30.906847954 CEST	1274	OUT	GET /8u3b/?EzrxUr=ApmP+YWYCK6vLVfjcl0EWRKNz1AqTOP9eBXy99nVLHRI2g8p2qSHut9K1XPRX5z6HIA+7i/UvA==&0VMt8D=3fJTbJlpxpVT_2d0 HTTP/1.1 Host: www.spwakd.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 14:43:30.971549034 CEST	1275	IN	HTTP/1.1 404 Not Found Server: nginx/1.10.3 Date: Mon, 03 May 2021 12:43:30 GMT Content-Type: text/html Content-Length: 169 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 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 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 2f 31 2e 31 30 2e 33 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx/1.10.3 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49736	103.5.116.132	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:43:41.729366064 CEST	8371	OUT	GET /8u3b/?EzrxUr=PWNBDH2hPCb1us8Ao8B+54WayNfcYj50QVchuC7xNQJC497qOyaPHph0Z/JAkFEaPJmxv/9Dmg==&0VMt8D=3fJTbJlpxpVT_2d0 HTTP/1.1 Host: www.arfjkacsgatfzbazpdth.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:43:42.007214069 CEST	8396	IN	HTTP/1.1 302 Found Date: Mon, 03 May 2021 12:43:41 GMT Server: Apache Location: http://choco.mhnebsadebugpctkuryt.com/8u3b/?EzrxUr=PWNBDH2hPCb1us8Ao8B+54WayNfcYj50QVchuC7xNQJC497qOyaPHph0Z/JAkFEaPJmxv/9Dmg==&0VMt8D=3fJTbJlpxpVT_2d0 Content-Length: 339 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 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 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 3a 2f 2f 63 68 6f 63 6f 2e 6d 68 6e 65 62 73 61 64 65 62 75 67 70 63 74 6b 75 72 79 74 2e 63 6f 6d 2f 38 75 33 62 2f 3f 45 7a 72 78 55 72 3d 50 57 4e 42 44 48 32 68 50 43 62 31 75 73 38 41 6f 38 42 2b 35 34 57 61 79 4e 66 63 59 6a 35 30 51 56 63 68 75 43 37 78 4e 51 4a 43 34 39 37 71 4f 79 61 50 48 70 68 30 5a 2f 4a 41 6b 46 45 61 50 4a 6d 78 76 2f 39 44 6d 67 3d 3d 26 61 6d 70 3b 30 56 4d 74 38 44 3d 33 66 4a 54 62 4a 6c 70 78 70 56 54 5f 32 64 30 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>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49746	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:43:52.317936897 CEST	9097	OUT	GET /8u3b/?EzrxUr=TE3r3Po/80I3A7BjdmOrtV2X1cXMdBXcsPlehNMo8xFrjXCGEx4PM+IgH3zoRtc5Tgzkp+uvDw==&0VMt8D=3fJTbJlpxpVT_2d0 HTTP/1.1 Host: www.babyshopit.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 14:43:52.496176004 CEST	9098	IN	HTTP/1.1 403 Forbidden Date: Mon, 03 May 2021 12:43:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Dc: gcp-us-central1 X-Request-ID: 364811d9-8667-4d12-8d2f-25d3d9733dfc X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none CF-Cache-Status: DYNAMIC cf-request-id: 09d3dab89e0000074aaeb00000000001 Server: cloudflare CF-RAY: 649993d43b76074a-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 34 63 30 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d Data Ascii: 4c0<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;display:flex;min-height:100vh;flex-direction:column}.text-

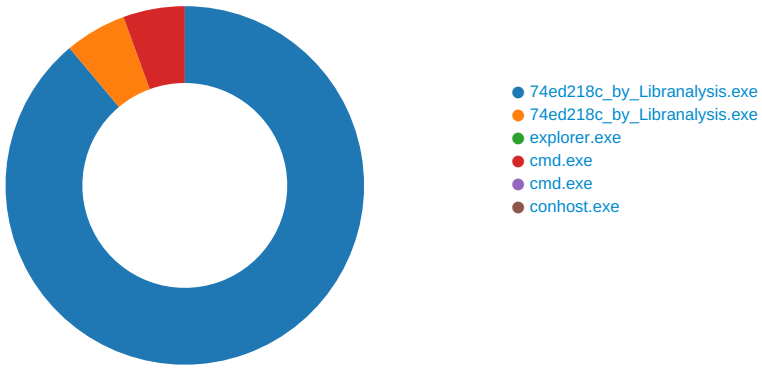
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49747	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:43:57.658832073 CEST	9126	OUT	GET /8u3b/?0VMt8D=3fJTbJlpxpVT_2d0&EzrxUr=QhGT3fvyIg/Tdu+peJX/18F82XojpghVKKtPaYcZWPnpiCRWL9VDuvxnUE1ISN8qX8wj4FmhpA== HTTP/1.1 Host: www.pyqxlz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 14:43:57.795476913 CEST	9127	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 03 May 2021 12:43:57 GMT Content-Type: text/html Content-Length: 275 ETag: "6089be8c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 74ed218c_by_Libranalysis.exe PID: 6800 Parent PID: 5876

General

Start time:	14:42:37
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\74ed218c_by_Libranalysis.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\74ed218c_by_Libranalysis.exe'
Imagebase:	0xdd0000
File size:	793600 bytes
MD5 hash:	74ED218C2C421E3978445A1EDBE40A08
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.340709877.0000000003215000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.341386451.00000000041C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.341386451.00000000041C9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.341386451.00000000041C9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6E0CCF06	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	6E0CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\74ed218c_by_Libranalysis.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	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\74ed218c_by_Libranalysis.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	6E3DC907	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile

Analysis Process: 74ed218c_by_Libranalysis.exe PID: 6940 Parent PID: 6800

General

Start time:	14:42:41
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\74ed218c_by_Libranalysis.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\74ed218c_by_Libranalysis.exe
Imagebase:	0xc00000
File size:	793600 bytes
MD5 hash:	74ED218C2C421E3978445A1EDBE40A08
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: 00000003.00000002.377542690.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.377542690.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.377542690.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.378047898.0000000001680000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.378047898.0000000001680000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.378047898.0000000001680000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.378002260.0000000001650000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.378002260.0000000001650000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.378002260.0000000001650000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3440 Parent PID: 6940

General

Start time:	14:42:43
Start date:	03/05/2021
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: cmd.exe PID: 4704 Parent PID: 3440

General

Start time:	14:42:57
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.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
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.594461458.0000000002880000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.594461458.0000000002880000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.594461458.0000000002880000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.593997073.0000000002780000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.593997073.0000000002780000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.593997073.0000000002780000.00000040.00000001.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	27982A7	NtReadFile

Analysis Process: cmd.exe PID: 5936 Parent PID: 4704

General

Start time:	14:43:02
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\74ed218c_by_Libranalysis.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: 5800 Parent PID: 5936

General

Start time:	14:43:02
Start date:	03/05/2021
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