ID: 830388
Sample Name: d0#U10dc.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:32:12
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

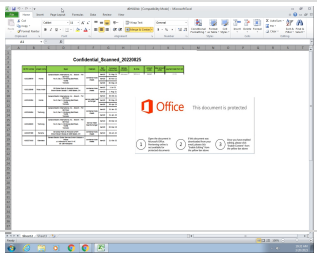
Windows Analysis Report

d0#U10dc.xls

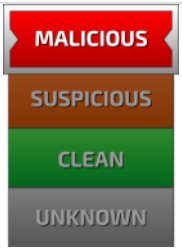
Overview

General Information

Sample Name:	d0#U10dc.xls
Original Sample Name:	P72215__7_-.xls
Analysis ID:	830388
MD5:	4f1aac1208442..
SHA1:	2eaf1072958ea..
SHA256:	b861cc02ce6a...
Tags:	CVE-2017-11882 xls
Infos:	



Detection



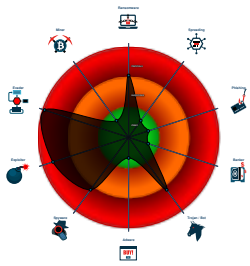
FormBook

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

Signatures

- Sigma detected: EQNEDT32.EXE c...
- System process connects to networ...
- Detected unpacking (changes PE se...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through...
- Office document tries to convince v...
- Antivirus / Scanner detection for sub...
- Sigma detected: File Dropped By EQ...
- Tries to steal Mail credentials (via fi...
- Maps a DLL or memory area into an...

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1236 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 544 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1928 cmdline: "C:\Users\Public\vbc.exe" MD5: 7DE990046A20E6666627273589B014A5)
    - mcwfy.exe (PID: 3004 cmdline: "C:\Users\user\AppData\Local\Temp\mcwfy.exe" C:\Users\user\AppData\Local\Temp\ytljtt.f MD5: 6CB712E482D150A185F713D75314A75A)
      - mcwfy.exe (PID: 1016 cmdline: C:\Users\user\AppData\Local\Temp\mcwfy.exe MD5: 6CB712E482D150A185F713D75314A75A)
        - explorer.exe (PID: 1860 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - wscript.exe (PID: 3360 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 979D74799EA6C8B8167869A68DF5204A)
            - firefox.exe (PID: 3768 cmdline: C:\Program Files (x86)\Mozilla Firefox\Firefox.exe MD5: C2D924CE9EA2EE3E7B7E6A7C476619CA)
- AcroRd32.exe (PID: 2704 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" -Embedding MD5: 2F8D93826B8CBF9290BC57535C7A6817)
  - RdrCEF.exe (PID: 1556 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 326A645391A97C760B60C558A35BB068)
- WINWORD.EXE (PID: 3148 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://asec.ahnlab.com/en/32149/https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.1184042628.00000000000E0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000010.00000002.1184042628.00000000000E0000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f0e0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae4f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x182f7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000010.00000002.1184042628.00000000000E0000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x180f5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17b91:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x181f7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1836f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xaa1a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16ddc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1de87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ee3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.1055408046.00000000003B0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000008.00000002.1055408046.00000000003B0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f0e0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae4f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x182f7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 16 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.mcwfy.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
8.2.mcwfy.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20f03:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xcc72:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1a11a:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
8.2.mcwfy.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19f18:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x199b4:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1a01a:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1a192:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xc83d:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18bff:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1fcaa:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x20c5d:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.2.mcwfy.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
8.2.mcwfy.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20103:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xbe72:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1931a:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 1 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

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

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

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

E-Banking Fraud

Yara detected FormBook

Spam, unwanted Advertisements and Ransom Demands

Found potential ransomware demand text

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)

Excel sheet contains many unusual embedded objects

Office equation editor drops PE file

Data Obfuscation

Detected unpacking (changes PE section rights)

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)

HIPS / PFW / Operating System Protection Evasion

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

Maps a DLL or memory area into another process

DLL side loading technique detected

Sample uses process hollowing technique

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

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

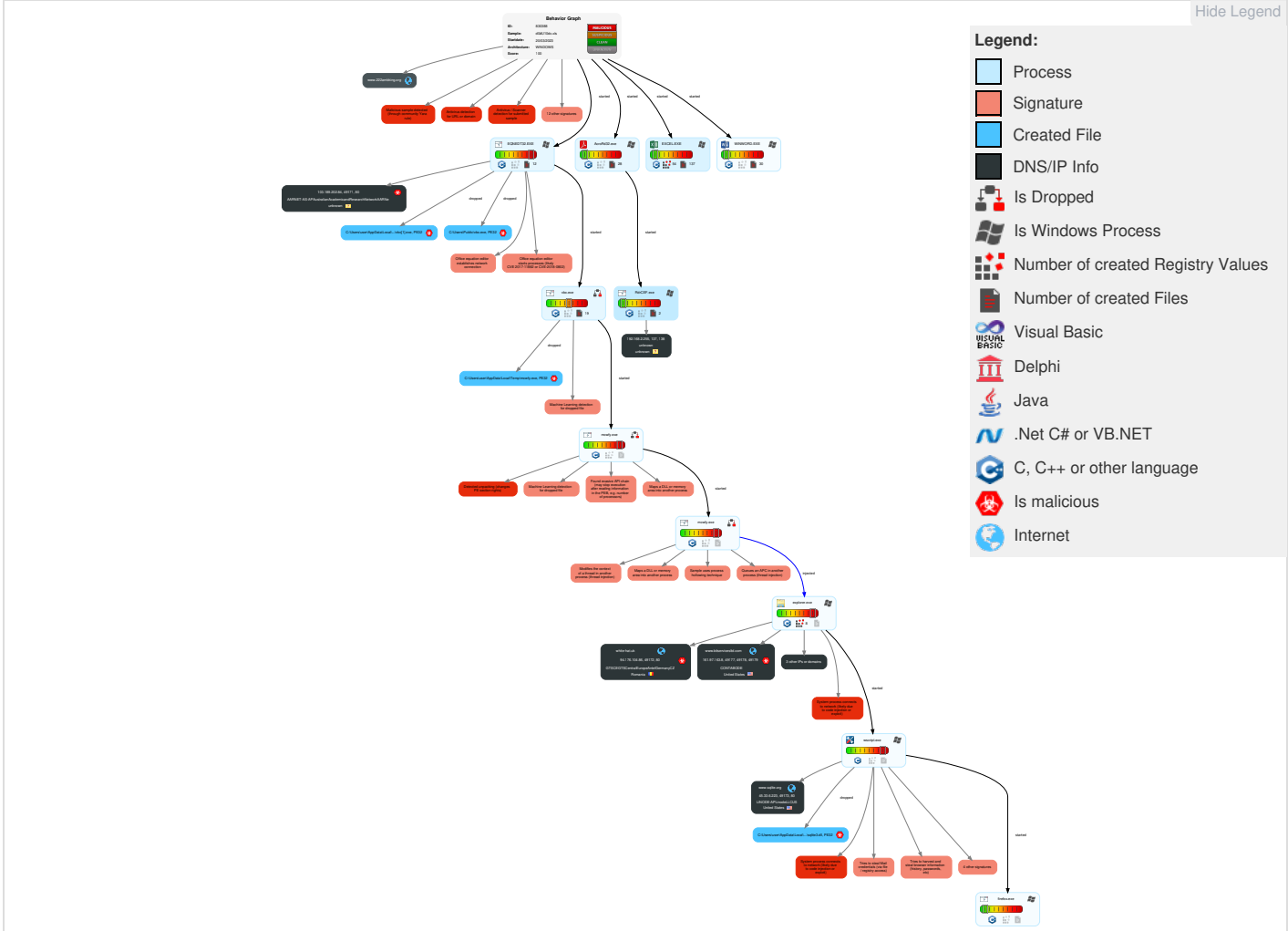
Yara detected FormBook

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 1 Scripting	1 1 DLL Side-Loading	1 1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 5 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Man in the Browser	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	5 1 2 Process Injection	1 1 Scripting	Security Account Manager	2 8 System Information Discovery	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 3 Exploitation for Client Execution	Logon Script (Mac)	Logon Script (Mac)	2 1 Obfuscated Files or Information	NTDS	4 1 Security Software Discovery	Distributed Component Object Model	1 Email Collection	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Software Packing	LSA Secrets	2 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 DLL Side-Loading	Cached Domain Credentials	2 Process 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 1 1 Masquerading	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Virtualization/Sandbox Evasion	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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Access Token Manipulation	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	5 1 2 Process Injection	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

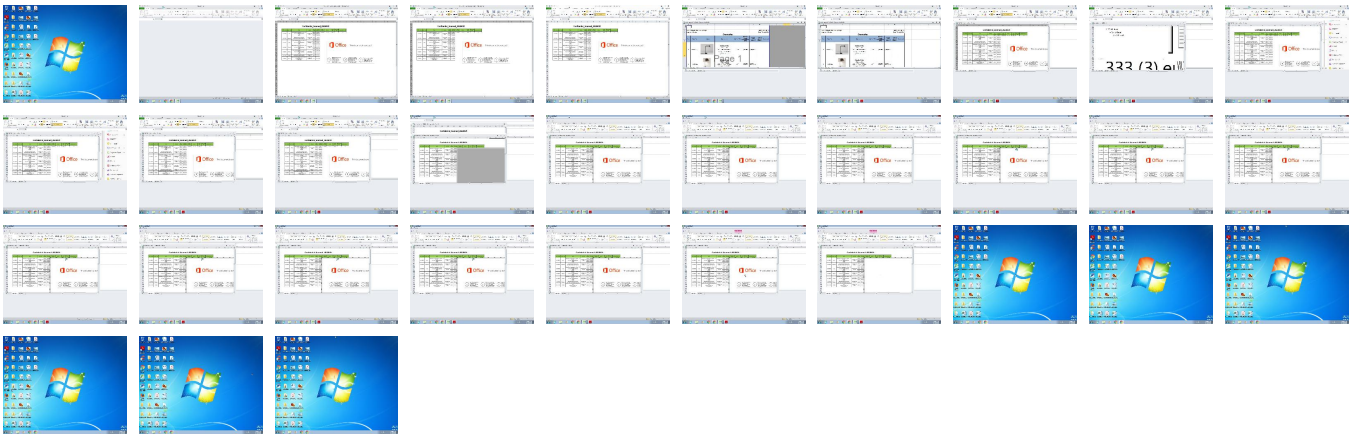
Behavior Graph

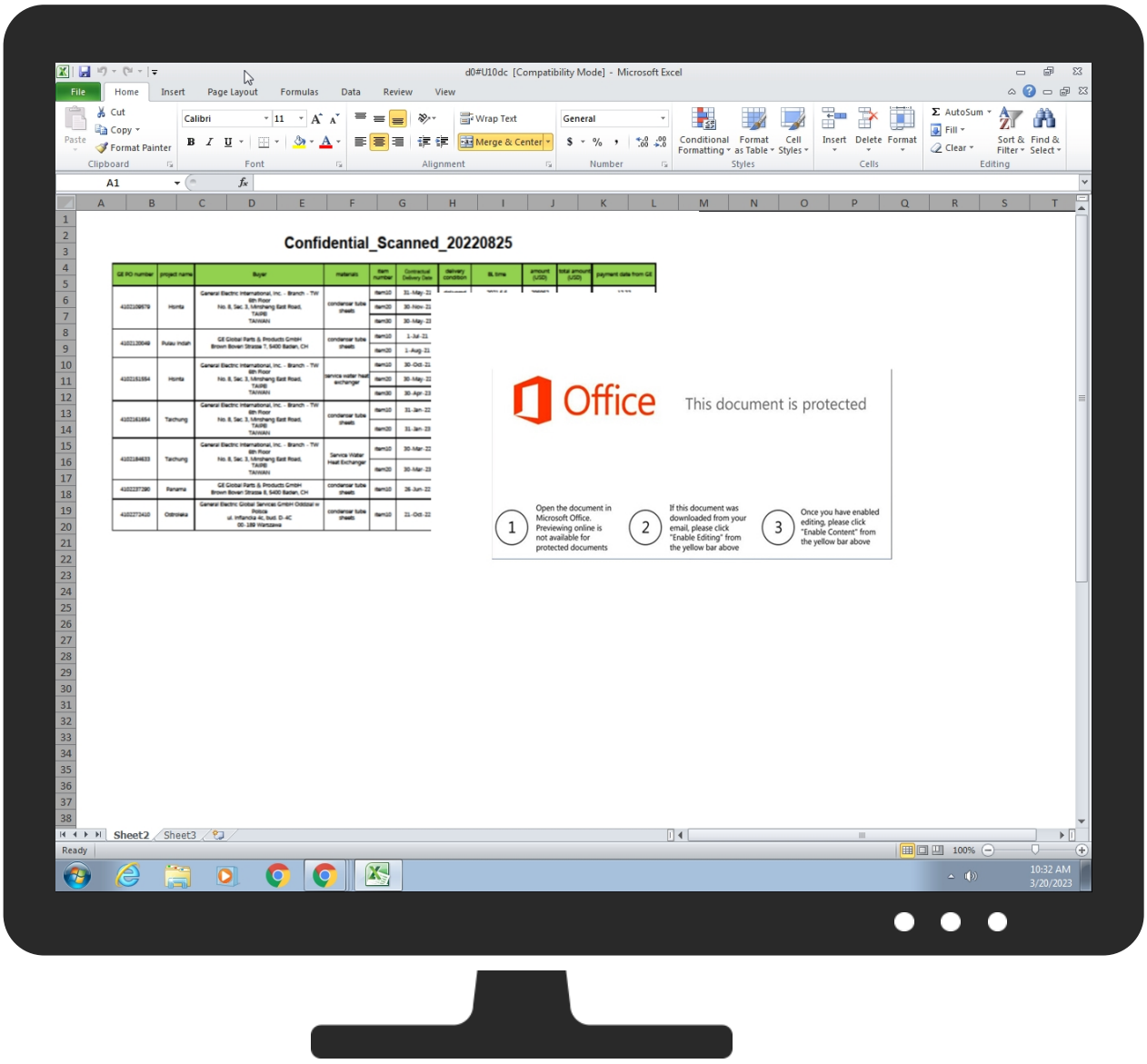


Screenshots

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
d0#U10dc.xls	31%	ReversingLabs	Document-OLE.Exploit.MathType	
d0#U10dc.xls	100%	Avira	EXP/CVE-2018-0798.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\mcwfy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\sqlite3.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.mcwfy.exe.280000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.mcwfy.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.white-hat.uk	0%	Avira URL Cloud	safe	
http://103.189.202.84/889r12/vbc.exe	100%	Avira URL Cloud	malware	
http://www.fclaimrewardccpointq.shopReferer:	0%	Avira URL Cloud	safe	
http://www.energyservicestation.comReferer:	0%	Avira URL Cloud	safe	
http://www.germanreps.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.avisrezervee.comReferer:	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.fclaimrewardccpointq.shop/u2kb/	100%	Avira URL Cloud	malware	
http://www.fclaimrewardccpointq.shop/u2kb/www.fclaimrewardccpointq.shop	100%	Avira URL Cloud	malware	
http://www.mygloballojistik.online/u2kb/	0%	Avira URL Cloud	safe	
http://www.bitservicesltd.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.un-object.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.energyservicestation.com/u2kb/www.energyservicestation.com	100%	Avira URL Cloud	malware	
http://www.gritslab.com/u2kb/www.gritslab.com	100%	Avira URL Cloud	malware	
http://www.thedivinerudraksha.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.white-hat.uk/u2kb/www.white-hat.uk	100%	Avira URL Cloud	malware	
http://www.gritslab.com/u2kb/	100%	Avira URL Cloud	malware	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.222ambking.orgReferer:	0%	Avira URL Cloud	safe	
http://www.thedivinerudraksha.com/u2kb/www.thedivinerudraksha.com	100%	Avira URL Cloud	malware	
http://www.mygloballojistik.online/u2kb/www.mygloballojistik.online	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.thedivinerudraksha.comReferer:	0%	Avira URL Cloud	safe	
http://white-hat.uk/u2kb/?MX=PXfMycAZpTAipct8YcIlv	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.younrock.com	0%	Avira URL Cloud	safe	
http://103.189.202.84/889r12/vbc.exehhC:	100%	Avira URL Cloud	malware	
http://www.un-object.com/u2kb/www.un-object.com	100%	Avira URL Cloud	malware	
http://www.ecomofietsen.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.shapshit.xyz/u2kb/	100%	Avira URL Cloud	malware	
http://www.avisrezervee.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.employerseervices.com	0%	Avira URL Cloud	safe	
http://www.un-object.comReferer:	0%	Avira URL Cloud	safe	
http://www.222ambking.org/u2kb/	100%	Avira URL Cloud	malware	
http://www.ecomofietsen.com/u2kb/www.ecomofietsen.com	100%	Avira URL Cloud	malware	
http://www.white-hat.ukReferer:	0%	Avira URL Cloud	safe	
http://www.bitservicesltd.com/u2kb/www.bitservicesltd.com	100%	Avira URL Cloud	malware	
http://103.189.202.84/889r12/vbc.exer	100%	Avira URL Cloud	malware	
http://www.avisrezervee.com/u2kb/www.avisrezervee.com	100%	Avira URL Cloud	malware	
http://www.bitservicesltd.comReferer:	0%	Avira URL Cloud	safe	
http://www.bitservicesltd.com/u2kb/?MX=rr+sOBvEXsBdGevUkpEFvjOGSuYjzi1YNHmXivr92FQhRIIYsedR2a+6GoV1WAKeGdj+MTdX512lJXnwfbSEi+kURcMlXNjU4ipRv+g=&uFI_=sroxa_9G7qh93	100%	Avira URL Cloud	malware	
http://www.thewildphotographer.co.uk/u2kb/www.thewildphotographer.co.uk	100%	Avira URL Cloud	malware	
http://localizability/practices/XML.asp	0%	Avira URL Cloud	safe	
http://103.189.202.84/889r12/vbc.exej	100%	Avira URL Cloud	malware	
http://www.white-hat.uk/u2kb/?MX=PXfMycAZpTAipct8YcIlv+jRzdgnyvgF2k7967nf/qU1A0mUqq9Jlnm9rK8XSf3D04yKTuePtKPnTC045fzMwSdM+ozxnu9rCO36QPo=&uFI_=sroxa_9G7qh93	100%	Avira URL Cloud	malware	
http://www.mygloballojistik.onlineReferer:	0%	Avira URL Cloud	safe	
http://www.shapshit.xyz	0%	Avira URL Cloud	safe	
http://www.mygloballojistik.online	0%	Avira URL Cloud	safe	
http://www.thedivinerudraksha.com	0%	Avira URL Cloud	safe	
http://www.ecomofietsen.com	0%	Avira URL Cloud	safe	
http://www.gritslab.com/u2kb/?MX=ydCzFiH7iMWnz6xHMbeyIS2EYayY5efYQUsmgPEoYCSsyD6HgT3yOGCjssC2N8mKn+GjlNYvhr7iKNK7QGdClLf278PMkWXjYWxIQds=&uFI_=sroxa_9G7qh93	100%	Avira URL Cloud	malware	
http://www.thewildphotographer.co.uk/u2kb/t	100%	Avira URL Cloud	malware	
http://www.ecomofietsen.com/u2kb/-wA	100%	Avira URL Cloud	malware	
http://www.germanreps.com/u2kb/5fQ	100%	Avira URL Cloud	malware	
http://www.avisrezervee.com	0%	Avira URL Cloud	safe	
http://www.bitservicesltd.com	0%	Avira URL Cloud	safe	
http://www.gritslab.com	0%	Avira URL Cloud	safe	
http://www.younrock.comReferer:	0%	Avira URL Cloud	safe	
http://www.thewildphotographer.co.uk/u2kb/	100%	Avira URL Cloud	malware	
http://www.white-hat.uk/u2kb/	100%	Avira URL Cloud	malware	
http://www.energyservicestation.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.germanreps.comReferer:	0%	Avira URL Cloud	safe	
http://www.employerseervices.com/u2kb/www.employerseervices.com	0%	Avira URL Cloud	safe	
http://www.thewildphotographer.co.uk	0%	Avira URL Cloud	safe	
http://www.222ambking.org/u2kb/www.222ambking.org	100%	Avira URL Cloud	malware	
http://www.shapshit.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.energyservicestation.com	0%	Avira URL Cloud	safe	
http://www.employerseervices.com/u2kb/	0%	Avira URL Cloud	safe	
http://www.222ambking.org/u2kb/l	100%	Avira URL Cloud	malware	
http://localizability/practices/XMLConfiguration.asp	0%	Avira URL Cloud	safe	
http://www.gritslab.comReferer:	0%	Avira URL Cloud	safe	
http://www.employerseervices.com/u2kb/EJ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bitservicesltd.com	161.97.163.8	true	true		unknown
www.222ambking.org	91.195.240.94	true	false		unknown
white-hat.uk	94.176.104.86	true	true		unknown
www.sqlite.org	45.33.6.223	true	false		high
gritslab.com	78.141.192.145	true	true		unknown
www.white-hat.uk	unknown	unknown	true		unknown
www.gritslab.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://103.189.202.84/889r12/vbc.exe	true	• Avira URL Cloud: malware	unknown
http://www.bitservicesltd.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.gritslab.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.bitservicesltd.com/u2kb/?MX=rr+sOBvEXsBdGevUkpEFvjOGSuYjzi1YNHmXivr92FQhRIIYsedR2a+6GoV1WAKeGdj+MTdX512lJXnwfbSEi+kURcMIXNjU4ipRv+g=&uFI_=sroxa_9G7qh93	true	• Avira URL Cloud: malware	unknown
http://www.white-hat.uk/u2kb/?MX=PXfMycAZpTAipct8Ycllv+jRzdgnyvgF2k7967nf/qU1A0mUqq9Jlnm9rK8XSf3D04yKTuePtKPnTC045fzMwSdM+ozxnu9rCO36QPo=&uFI_=sroxa_9G7qh93	true	• Avira URL Cloud: malware	unknown
http://www.sqlite.org/2017/sqlite-dll-win32-x86-3170000.zip	false		high
http://www.gritslab.com/u2kb/?MX=ydCzFiH7iMWnz6xHMbeyIS2EYayY5efYQUsmgPEoYCSsyD6HgT3yOGCjssC2N8mKn+GjlNYvhr7iKNK7QGdClLf278PMkWXjYWxlQds=&uFI_=sroxa_9G7qh93	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	wscript.exe, 00000010.00000003.1125814665.0000000006554000.00000004.00000020.00020000.00000000.sdmp, HI4NJ046K.16.dr	false		high
http://https://duckduckgo.com/ac/?q=	wscript.exe, 00000010.00000003.1125814665.0000000006554000.00000004.00000020.00020000.00000000.sdmp, HI4NJ046K.16.dr	false		high
http://www.gritslab.com/u2kb/www.gritslab.com	explorer.exe, 0000000C.00000002.1193741517.00000000086C9000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.iis.fhg.de/audioPA	explorer.exe, 0000000C.00000000.1040826982.00000000046D0000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.thedivinerudraksha.com/u2kb/	firefox.exe, 00000012.00000002.1137560692.0000000000080000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.mozilla.com0	wscript.exe, 00000010.00000003.1125600882.0000000006562000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://treyresearch.net	explorer.exe, 0000000C.00000000.1040826982.00000000046D0000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.germanreps.com	explorer.exe, 0000000C.00000002.1193741517.00000000086C9000.00000004.00000001.00020000.00000000.sdmp, firefox.exe, 00000012.00000002.1137560692.0000000000080000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.white-hat.uk/u2kb/www.white-hat.uk	explorer.exe, 0000000C.00000002.1193741517.00000000086C9000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.fclaimrewardccpointq.shopReferer:	firefox.exe, 00000012.00000002.1137560692.0000000000080000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.energyservicestation.com/u2kb/www.energyservicestation.com	explorer.exe, 0000000C.00000002.1193741517.00000000086C9000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.energyservicestation.comReferer:	firefox.exe, 00000012.00000002.1137560692.0000000000080000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.white-hat.uk	explorer.exe, 0000000C.00000002.1193741517.00000000086C9000.00000004.00000001.00020000.00000000.sdmp, firefox.exe, 00000012.00000002.1137560692.0000000000080000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

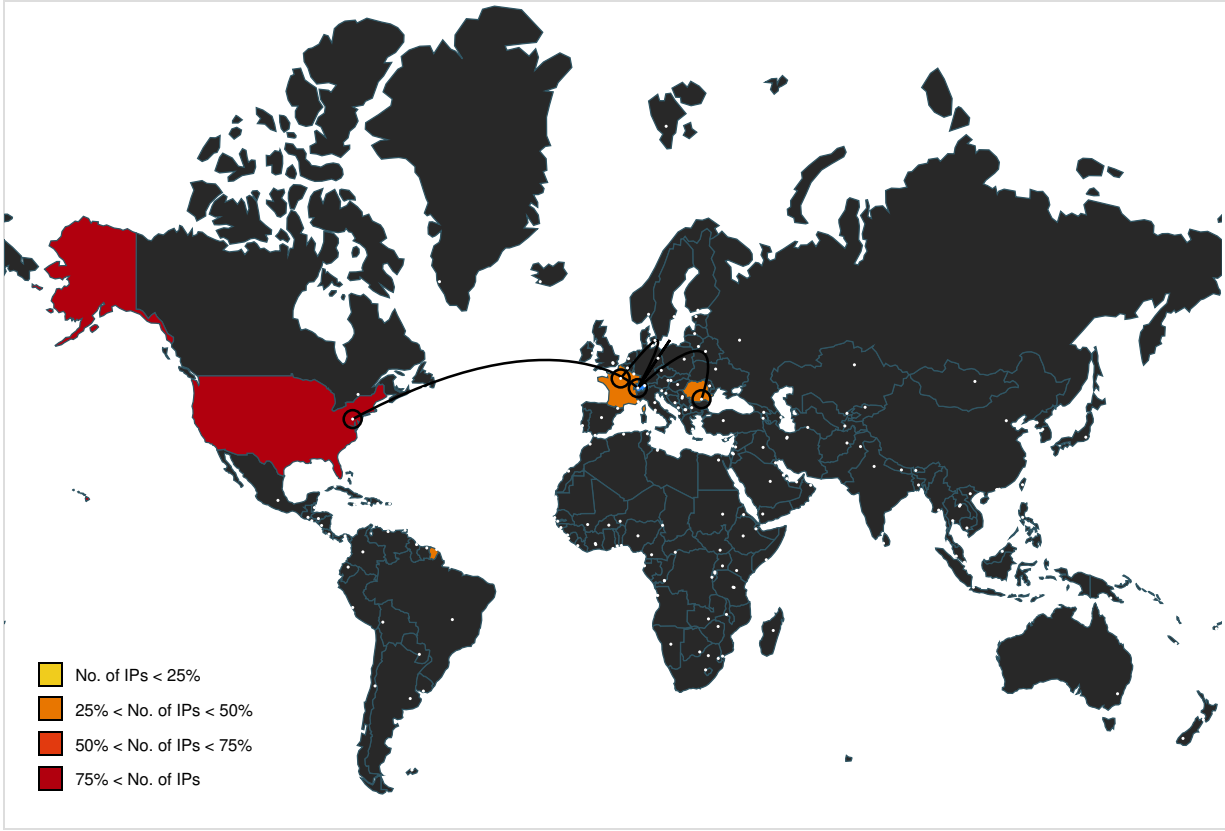
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.un-object.com/u2kb/	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.myglobalIojistik.online/u2kb/	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.avisrezervee.comReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://computername/printers/printername/.printer	explorer.exe, 0000000C.00000000.10408269 82.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 0000000C.00000002.11842858 79.0000000000335000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 000C.00000000.1003655931.0000000000335000 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://servername/isapibackend.dll	explorer.exe, 0000000C.00000000.10427270 06.0000000006450000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fclaimrewardccpointq.shop/u2kb/www.fclaimrewardccpointq.shop	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.fclaimrewardccpointq.shop/u2kb/	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.windows.com/pctv.	explorer.exe, 0000000C.00000000.10371085 61.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://103.189.202.84/889r12/vbc.exehhC:	EQNEDT32.EXE, 00000002.00000002.96945776 6.000000000068E000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.222ambking.orgReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://white-hat.uk/u2kb/?MX=PXfMycAZpTAipct8YcIlv	explorer.exe, 0000000C.00000002.11943444 86.000000000BD76000.00000004.80000000.00 040000.00000000.sdmp, wscript.exe, 00000 010.00000002.1185783285.0000000002CC6000 .00000004.10000000.00040000.00000000.sdmp, firefox.exe, 00000012.00000002.1138870439.00000 00001276000.00000004.80000000.00040000.0 0000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.younrock.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	wscript.exe, 00000010.00000003.112581466 5.0000000006554000.00000004.00000020.000 20000.00000000.sdmp, HI4NJ046K.16.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000005.00000000.968983697.000 000000040A000.00000008.00000001.01000000 .00000005.sdmp, vbc.exe, 00000005.000000 02.1002708792.000000000040A000.00000004. 00000001.01000000.00000005.sdmp, vbc.exe.2.dr	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 0000000C.00000000.10371085 61.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.un-object.com/u2kb/www.un-object.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.thedivinerudraksha.comReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.avisrezervee.com/u2kb/	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.myglobalIojistik.online/u2kb/www.myglobalIojistik.online	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thedivinerudraksha.com/u2kb/www.thedivinerudraksha.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/favicon.ico	HI4NJ046K.16.dr	false		high
http://java.sun.com	explorer.exe, 0000000C.00000002.11842858 79.0000000000335000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 000C.00000000.1003655931.000000000033500 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	explorer.exe, 0000000C.00000002.11849191 97.0000000001DD0000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.ecomofietsen.com/u2kb/	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.shapshit.xyz/u2kb/	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 0000000C.00000002.11937415 17.000000000869E000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000C.00000002.1184285879.00000000003A600 0.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000C.00000000.1046889553.000 0000008807000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000C.0 0000000.1003655931.00000000003A6000.0000 0004.00000020.00020000.00000000.sdmp, ex plorer.exe, 0000000C.00000000.1046750282 .000000000869E000.00000004.00000001.0002 0000.00000000.sdmp	false		high
http://www.employerseervices.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.222ambking.org/u2kb/	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.white-hat.ukReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ecomofietsen.com/u2kb/www.ecomofietsen.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.un-object.comReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bitservicesltd.com/u2kb/www.bitservicesltd.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://103.189.202.84/889r12/vbc.exer	EQNEDT32.EXE, 00000002.00000002.96945776 6.0000000000699000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.avisrezervee.com/u2kb/www.avisrezervee.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.msnbc.com/news/ticker.txt	explorer.exe, 0000000C.00000000.10371085 61.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.bitservicesltd.comReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://103.189.202.84/889r12/vbc.exej	EQNEDT32.EXE, 00000002.00000002.96991296 4.00000000035B0000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://localizability/practices/XML.asp	explorer.exe, 0000000C.00000000.10371085 61.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.piriform.com/ccleanerq	explorer.exe, 0000000C.00000000.10362833 89.0000000002CBF000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000C.00000002.1186521094.0000000002CBF00 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.thewildphotographer.co.uk/u2kb/www.thewildphotographer.co.uk	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mygloballojistik.online	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mygloballojistik.onlineReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.shapshit.xyz	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thewildphotographer.co.uk/u2kb/t	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.ecomofietsen.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thedivinerudraksha.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ecomofietsen.com/u2kb/-wA	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.icra.org/vocabulary/.	explorer.exe, 0000000C.00000000.10371085 61.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	wscript.exe, 00000010.00000003.112560088 2.0000000006562000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://www.employerseervices.com/u2kb/www.employerseervices.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.germanreps.com/u2kb/5fQ	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.energyservicestation.com/u2kb/	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://investor.msn.com/	explorer.exe, 0000000C.00000000.10371085 61.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.avisrezervee.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bitservicesltd.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000C.00000002.1190328364.0000000004B1200 0.00000040.80000000.00040000.00000000.sdmp, firefox.exe, 00000012.00000002.1137560692.0000 000000080000.00000004.00001000.00020000. 00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thewildphotographer.co.uk/u2kb/	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.white-hat.uk/u2kb/	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.younrock.comReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	explorer.exe, 0000000C.00000002.11849191 97.0000000001DD0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleanerv	explorer.exe, 0000000C.00000002.11892124 75.0000000004385000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000C.00000000.1039865017.0000000004385000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.germanreps.comReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gritslab.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thewildphotographer.co.uk	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sqlite.org/copyright.html.	wscript.exe, 00000010.00000002.118792081 5.0000000061EA3000.00000008.00000001.010 00000.00000008.sdmp	false		high
http:// www.222ambking.org/u2kb/www.222ambking.org	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.shapshit.xyzReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com	explorer.exe, 0000000C.00000000.10371085 61.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.energyservicestation.com	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gritslab.comReferer:	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://wellformedweb.org/CommentAPI/	explorer.exe, 0000000C.00000000.10408269 82.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://crash-reports.mozilla.com/submit?id=	wscript.exe, 00000010.00000003.112603888 4.00000000053D0000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://www.employerseervices.com/u2kb/	explorer.exe, 0000000C.00000002.11937415 17.00000000086C9000.00000004.00000001.00 020000.00000000.sdmp, firefox.exe, 00000 012.00000002.1137560692.0000000000080000 .00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.employerseervices.com/u2kb/EJ	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	wscript.exe, 00000010.00000003.112560088 2.0000000006562000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleaner1SPS0	explorer.exe, 0000000C.00000002.11934895 86.0000000008611000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000C.00000000.1046307432.0000000000861100 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.222ambking.org/u2kb/l	firefox.exe, 00000012.00000002.113756069 2.0000000000080000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://localizability/practices/XMLConfiguration.asp	explorer.exe, 0000000C.00000000.10371085 61.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http:// https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	wscript.exe, 00000010.00000003.112581466 5.0000000006554000.00000004.00000020.000 20000.00000000.sdmp, HI4NJ046K.16.dr	false		high
http://www.hotmail.com/oe	explorer.exe, 0000000C.00000000.10371085 61.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.33.6.223	www.sqlite.org	United States		63949	LINODE-APLinodeLLCUS	false
78.141.192.145	gritslab.com	France		20473	AS-CHOOPAUS	true
161.97.163.8	www.bitservicesltd.com	United States		51167	CONTABODE	true
103.189.202.84	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	true
94.176.104.86	white-hat.uk	Romania		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	true

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830388
Start date and time:	2023-03-20 10:32:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	18
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	d0#U10dc.xls
Original Sample Name:	P72215__7_-.xls
Detection:	MAL
Classification:	mal100.rans.troj.spyw.expl.evad.winXLS@27/74@6/6
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 40.6% (good quality ratio 38.1%) • Quality average: 75.1% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Active ActiveX Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 2.21.22.179, 2.21.22.155, 23.36.224.131
- Excluded domains from analysis (whitelisted): ssl.adobe.com.edgekey.net, armmf.adobe.com, acroipm2.adobe.com.edgesuite.net, e4578.dscb.akamaiedge.net, a122.dscd.akamai.net, acroipm2.adobe.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtEnumerateKey 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.
- VT rate limit hit for: d0#U10dc.xls

Simulations

Behavior and APIs

Time	Type	Description
10:32:44	API Interceptor	99x Sleep call for process: EQNEDT32.EXE modified
10:32:53	API Interceptor	591x Sleep call for process: AcroRd32.exe modified
10:33:01	API Interceptor	44x Sleep call for process: RdrCEF.exe modified
10:33:02	API Interceptor	17x Sleep call for process: mcwfy.exe modified
10:33:05	API Interceptor	2317x Sleep call for process: explorer.exe modified
10:33:30	API Interceptor	617x Sleep call for process: wscript.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\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Cache\data_1

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	270336
Entropy (8bit):	0.001953593414988235
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zEF/Cltw/ltl:/M/xT02zw/mml
MD5:	D1D7881FA66196F28CC6D03872FA6D46
SHA1:	BFDFF353504E73615317D45B2DBE46739FA9067A
SHA-256:	7E5756A6DF446E427FAD3354EA55C85E6401E0F7B3EB28F8B7D740E27E6D0F67
SHA-512:	6491853225A9BE97324D8FF049A63F220F0B72024BAFEC60E1A43D507CB80AFB20D05C21D992C8E908CEA6C849B912FEC1603854F498498D0E5946AFB86D575E
Malicious:	false
Preview:	....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.153762795765596
Encrypted:	false
SSDEEP:	6:kUHniyq2PP2nKuAl9OmbnIFUtdHnrX11ZmwvHn6cQRkwOP2nKuAl9OmbjLJ:koniyvWHAahFUtxnrXX//n3QR57HAaSJ
MD5:	3FA34ABD9ADA750BEA8FFBA661C3E25C
SHA1:	3D18F20392996F6420D9FC3C795E916B790AF16C
SHA-256:	B64C72F76B064FFEDE31FE5357EE1CC01E5D03029A0F2EF357E6C94EB28AA226
SHA-512:	7627135B849D3BCA49DAB5CB89616AA0F7CA1529C82A096E632AF6DD45328AA2AD0C31F154D795C0B8BA7CD691896149450E0A9FD575F44A949666BF0DC8DF7
Malicious:	false
Preview:	2023/03/20-10:33:03.641 1972 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/03/20-10:33:03.651 1972 Recovering log #3.2023/03/20-10:33:03.661 1972 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped

Size (bytes):	292
Entropy (8bit):	5.153762795765596
Encrypted:	false
SSDEEP:	6:kUHniyq2PP2nKuAl9OmbnIFUtdHnrX11ZmwvHn6cQRkwOP2nKuAl9OmbjLJ:koniyvWHAahFUtxnrXX//n3QR57HAaSJ
MD5:	3FA34ABD9ADA750BEA8FFBA661C3E25C
SHA1:	3D18F20392996F6420D9FC3C795E916B790AF16C
SHA-256:	B64C72F76B064FFEDE31FE5357EE1CC01E5D03029A0F2EF357E6C94EB28AA226
SHA-512:	7627135B849D3BCA49DAB5CB89616AA0F7CA1529C82A096E632AF6DD45328AA2AD0C31F154D795C0B8BA7CD691896149450E0A9FD575F44A949666BF0DC8DF7
Malicious:	false
Preview:	2023/03/20-10:33:03.641 1972 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/03/20-10:33:03.651 1972 Recovering log #3.2023/03/20-10:33:03.661 1972 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old~RF41d356.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.153762795765596
Encrypted:	false
SSDEEP:	6:kUHniyq2PP2nKuAl9OmbnIFUtdHnrX11ZmwvHn6cQRkwOP2nKuAl9OmbjLJ:koniyvWHAahFUtxnrXX//n3QR57HAaSJ
MD5:	3FA34ABD9ADA750BEA8FFBA661C3E25C
SHA1:	3D18F20392996F6420D9FC3C795E916B790AF16C
SHA-256:	B64C72F76B064FFEDE31FE5357EE1CC01E5D03029A0F2EF357E6C94EB28AA226
SHA-512:	7627135B849D3BCA49DAB5CB89616AA0F7CA1529C82A096E632AF6DD45328AA2AD0C31F154D795C0B8BA7CD691896149450E0A9FD575F44A949666BF0DC8DF7
Malicious:	false
Preview:	2023/03/20-10:33:03.641 1972 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/03/20-10:33:03.651 1972 Recovering log #3.2023/03/20-10:33:03.661 1972 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.008898238653846898
Encrypted:	false
SSDEEP:	3:ImtVnM1xVlt/rt/l3Sxdlt4dV1gt/lop:liV0xlzaxdX4m1lo
MD5:	3B8BF2F369CA7ABDF0636EE15DDEF161
SHA1:	4B82D483B79B555C62AA17F31F24F43C38F2C80F
SHA-256:	100201408FDCFA835C8699C6C2FCE748C5C3844C386053F9AA7CAD622373BFCA
SHA-512:	457D92EA15FA528E7BE3ED8136A267BD08A4D7866FDD7C353CFEB898F896983B40BB48156DC25D5E00EC118C6309337F3A9344226D1635F94D7F4A122D3DD87
Malicious:	false
Preview:	VLnk.....?.....LhXJ ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000, file counter 15, database pages 15, cookie 0x5, schema 4, UTF-8, version-valid-for 15
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	3.575535913153063
Encrypted:	false
SSDEEP:	384:neh9dThStELJ8DAcLKuZsLRGlKhsvXh+vSc:vAeZsLQhUSc
MD5:	BCAA03F72866441CBE9AF508D2AF7994
SHA1:	4E65AC57740F64C7A0B2F9678150CB79B4C97175
SHA-256:	E16BBDAABAF775FD6C09430D86B4780F907086E377E5AE1747C11F6602D2EFA0
SHA-512:	984E1A454FE4250BBA304608530816ACD1A41F4D4BAD10D61ABF7FD43149B9E8210C0DA9105889030E5DBDA555318127A7939E1ED43A212529C91AE6733E895A
Malicious:	false

Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.3093576730086833
Encrypted:	false
SSDEEP:	48:7M72iomVmBsmom1Ctiomxom1Nom1Aiom1RROiom1Com1pom1AiomVPiomgyqAlmT:79Cm6rtxh8CPyd49IVXEBodRBkV
MD5:	3A4DB9F200BA8A36D38EAF75B778C17B
SHA1:	13DB201253EB01039D5D7FB7FC2451A662E83883
SHA-256:	E969EBDB86AF91CECEC6CEE79249EBAE576E947883B71D00E22B5B96F2DDDFED
SHA-512:	A57FC82E3CD716859B4F00BA5ED0369FCB9821D6DAF1CFCCA5C7F1251C512A1162B5E1AD3F1259F33DFF1E9A32BE32C3BCC1127BF46A1D4C86723DE6D8F9E79B
Malicious:	false
Preview:	.... .c.....F..... .....W....X.W .L...y.....~..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	398613
Entropy (8bit):	2.1746478731407244
Encrypted:	false
SSDEEP:	1536:nnNTBeJFFFFFFp6LDyWnkGoGgpPortpyxxxxxxVzS:nBDyiFoGgpP
MD5:	E048CAA6DFA72DBBBA3A0C7869DC5B3F
SHA1:	0CE85D82BD02E1FDFA563ABBBE0A647A63834972
SHA-256:	6A8C2A62182DF333357CE5BA08FF2CF4F4CF6E74D3328AB47F844253512980DD
SHA-512:	62BEA535B786F67FCF96F371464DA5D4312F3A40BB264738FD304B5C0C36B1953FA223819C95CEA9C2D2DD217CC602E40533514ED0B64B34E6A15AE3D49D557
Malicious:	false
Preview:	Adobe Acrobat Reader DC 19.0....?A12_FindInDocument.....ppp.ppp`ppp.ppp.ppp.ppp.pppppp .....ppp.ppp.ppp.ppp.ppp.ppp.ppp.ppp.ppp.ppp .....ppp.ppp.ppp.ppp.ppp.ppp.ppp. ppp.ppp.ppp.ppp.ppp.ppp.ppp0.....ppp.ppp.ppp.ppp.pppP.....ppp0ppp.ppp.ppp.ppp.ppp0.....ppp.ppp.ppp.ppp.ppp..... .....ppp`ppp.ppp.ppp.....ppp.ppp.ppp.ppp.ppp.....ppp.ppp.ppp.ppp`.....ppp`ppp.ppp.pppP..... ....ppp.ppp.ppp.ppp.....ppp.ppp.ppp.....ppp.....ppp.....ppp.....ppp.ppp.ppp.....ppp.ppp.ppp.....ppp0ppp.ppp`....ppp`ppp.ppp0ppp.ppp.ppp.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\sqlite-dll-win32-x86-3170000[1].zip

Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	441750
Entropy (8bit):	**7.998736788620827**
Encrypted:	**true**
SSDEEP:	12288:kNYTTUBeH/mxYhfbJQ0BHxK30XfNd+6NwY8Ta6A:SYTT6ULhTndxmibH8u6A
MD5:	FA9B7C190006303EECDDFFA019D0BE06
SHA1:	A97CEBC176B3DAA453189F2C0B7CF2A5A70F9C92
SHA-256:	DC7F8B3493543DC086CB43B66401893597F993408F18B437E5C8E8B5544DB0BF
SHA-512:	4C293EF052A14F7527AA42D451BA5F4CFDF7FB7203F583EDA34EF24F4A2FD13975553C432A9354A0F8C1DE924B0C29A819BD34C7AAA03B642372496A75BE053
Malicious:	false
Preview:	PK.....x.MJ0..#....c.....sqlite3.defUT.....X..Xux.....d.....&....6.....9.$..\..nj....==O...F...4.O....._...%..*..Il..MD....>.&Y.St.~.6(g.x..=.....".=...|..`...[.....].Y.y$o.q..4k.L.u +...5'...@....S.....r.s..|}.Yo.U..M...nyP:...|..8.....`9. ..._.<..P..."..s.....H.8.F..../.....H..[.Nk.q...,..T.s@U2.G.1GR8..S."....L9N.....*?..S.R5....3..-s^m.|.Q..p....Ms2.&.a'_ .x.'.t.8].{.IW.....&..Of..a..*.....i.k.4.&^..5F_*..e..[..g.=.8.Cs2.qK.M>(.<.u...a)..V..%.)w.....ct..."...Q...w..`r.0.3M."...9...M`.>!Z.#R;.....k:.[.I.....Bl..>@.a.....(T..b1/.4..Px .I.)+...KLz...B..6...G.>..K..Gbu.#..c.`,.B.y.].....K{[A.....q..?..q6v^...of..V....];?#.v..I1=.m..R....]n.6.W..bv..]...'J.O....e3...@...E. 6..M..k..@.7.4.]@;.*..1.sq.P.v..MA/.....W!G..6. ...a.R<..XT5..U&.....(.N.f#.7.ck..].b>8....(.Xq`..p;...Ljt.....t.IW.....5O....3|}.=.....8..o.....Fn.....Lp..As.&..i8)....n-.....+".....q.....@.*...+...`....<.8..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	299979
Entropy (8bit):	7.926593256630463
Encrypted:	false
SSDEEP:	6144:PYa6J+5gUNIG+sCfq3V++iY3aub8kFiLGG9qFP2ipkHj3DR7gy7y:PYDghNESPX3ZZq9q1b6DRc
MD5:	7DE990046A20E6666627273589B014A5
SHA1:	55EBCCD35C2329C5816CD0240B0919651AC58321
SHA-256:	EBCE15AD53B98D7ABA7F7544EE947E88F58D696E22CA4BC5D15B2DED37B577AC
SHA-512:	850914621B366494BBA2A64AEF1B3DF7C619C7E6BB321A67BC1A1A97BD0182118A1E5648EE48D24449E6341AB7F7989369797114FA521DB8C26CCD5EB3386A4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L.....Oa.....h...*.....@6.....@.....@..... .....text...vf.....h..... ..`.rdata.....I.....@..@.data...x.....@....ndata.....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1A5CF463.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7296
Entropy (8bit):	3.5651429999741935
Encrypted:	false
SSDEEP:	48:SkII4EPVVypa2iq9YHnBfL9AG07kfAqN9XaZ7kV7kR3jCBgB:SxsPVMkzuWAG75aSWJjCSB
MD5:	BA57D54BD3285D95D18903CE0CF660E1
SHA1:	0C84E6EF9F025023659F5B6A70272B1C1FC4D6D6
SHA-256:	B8DBC0BBDD597E705EEFF35A415B149E0CE9214DA1F05F2E8ECA8BA5B5EEE741
SHA-512:	96D183A26CBA3D58FE66BA0E65D52A9E1F984DB2150BD7B317F763B1842856DF47DB09B99DABB3603ACFF55BB44434B3D5A0458702F1676EF968D4E82B61832 5
Malicious:	false
Preview:	....l.....X...<..... EMF.....8...X.....?.....c...C...R...p.....S.e.g.o.e. .U.l..... .....6.).X.....d.....d... .....p....\...d.....d.....p....d...\V.v...p....`..p8...zNw."..... Kw....$.....r.d.....^.p.....^.p....".. .....-.....&<Jw.....<...u.Z.v....X.b....8 .....vdv.....%.....r.....E...'.....(...(.....?.....?.....l...4.....(...(...(...(...(.... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\29F24F69.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	19100
Entropy (8bit):	3.4561252890903678
Encrypted:	false
SSDEEP:	192:KVuqi8qXS8qin47UqD8UqdBSS/qZUa7RqjJFqZ3fNqnpkL9qAQBqBlqOqT:KVLIXaDDUHCGaQCZ3YvAdmrT
MD5:	473866E4981DBB1AE9965320EAD15360
SHA1:	FB1E19BCF1AD583333FA3BF9D245C78435DD816A
SHA-256:	3CD00231E888E846B95A316223844E38F60E1D60BF95F62A21F8C18ABDD06D28
SHA-512:	F56D955D2EECD24750BC965BA75DEF90BE3093609583F54648CE805C58129676C4C6F9769C785E09F178D360C2C46A4A743300287B62CA58A620B8B80CCF1287
Malicious:	false
Preview:	....l.....1..#%.. EMF.....J.....\K..hC..F...,... ...EMF+.@.....X...X...F.....t...EMF+.@.....@.....0@.....?!@..... "@.....*@..$.....?.....?.....@.....!.....".....F.....EMF++@.....@.....!@.....@.....*@..$.....?.....?.....!@.....+@..... .@.....!@.....2@.....;E...E.@.....*@..$.....?.....?.....!@.....*@..$.....9.....9.....*@..$.....9.....9.....*@..$.....9..... +@.....*@..$.....9.....9.....*@..$.....9.....9.....@..$.....K J.J!.....b.....$...$.....>.....>.....%.....%.....V...0..... ....LF.]LF.].....%.....%.....$...$.....A.....A.....".....F...P...D...EMF+*@..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3DC2DB08.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped

Size (bytes):	7304
Entropy (8bit):	4.72619510322236
Encrypted:	false
SSDEEP:	192:2sP2AjNhh9u+2Vy5FiLT+BIbAc2Ct/iLEWFOuHc:2sP2AjNhh9u+2Vy5FMT+BIbAc2Ct/iL0
MD5:	1967B7B96BD5EEF298EBF909A00BA409
SHA1:	F7C4CA90A1659670D125762F743083D53719C452
SHA-256:	667B9A03BBC8768767352A8CFDDF94358974E9018C3F1FCCEC8696CC775A1088
SHA-512:	27F2FA0A7B357A0AD32059EF094A2E1937058652031B60D1E6C2B2E5509CFE9EFF76A264728B2A070C79936C8DC38489D5CD43398FBDE1D5AC8266E9D1A5D7A C
Malicious:	false
Preview:	....l..........S...<..... EMF.....8...X.....?.....^...C...R...p.....S.e.g.o.e. .U.l..... .....6.).X.....d.....d... .....p....\...d.....d.....p....d...\V.v...p....`..p8...zNw."..... Kw....$.....r.d.....^.p.....^.p....".. .....-.....&<Jw.....<..u.Z.v....X.b....8 .....vdv.....%.....r.....B...'.....(...(.....?.....?.....l...4.....(...(...(...(...(.... ....___.....???w.....www.sss.aaa.JJJ..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4F49BF6A.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1106864
Entropy (8bit):	2.1419000480872574
Encrypted:	false
SSDEEP:	3072:V7aN3JkKXiDPcp5jw7lPwsVb7ooxv+7/jJK:5aFJkKXiDU7w7lYav+7VK
MD5:	356DC4E99436992BD4706C8CE0069BB2
SHA1:	2FA1B51579AC35020AE714CCEA9AEDAEEE7E8234
SHA-256:	B8B68932AD77EA2457ADE5F7955E1B174E9ED08FF51F4969009F41AE11BC8516
SHA-512:	12CCA3AC063304D4B3590D1C2AB8F456087DFCBE430ED6A7986845705F3FDFAE70BAAA91C1155A085D53E51CBE88E7C039D0ECF8A2F4683D54940EB7439FC3 E0
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.....\$...H....f.].@W. %...$...h.....L...RQS^.....4.....$QS^..... ...Id.]..... .....d.].....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X...X.....8.\.. .....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....C.....L.....P... ...6...F.....EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5001E027.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	97824
Entropy (8bit):	4.15659389201526
Encrypted:	false
SSDEEP:	1536:pm4/WD/WeBPIKD4HC/QCavImrP+2kZQCtQJ2JEEEGtEEECtnS/Wx/WM:pmzBPIKD4i4CavImrP+2kZPKJ2JEEEGB
MD5:	0848CAA6A9DD00BE29F512337660DA2F
SHA1:	755DC9ED684CE58977DF5138C2D9F85DD9CBF9EC
SHA-256:	91970DFB03B2B86C767BCD128F7A0A74526B9D9E88DDDC72B2FC178B186A5C77
SHA-512:	4A112E017AC8FF3460DB198DE1F89F38F2DC0127D460000BC814E09C2DC21E88668A05362671412390A4519B88F3AA642A5AA304693FFAF183D53D041CD710EF
Malicious:	false
Preview:	....l.....?{...P.. EMF.... ~..+.....8...X.....?.....F...,... ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....".....l.....".....l.....".....l..... .....".....l.....".....l.....".....l.....".....l..... .....'.....%.....&.....%.....6.....%.....L...d.....!...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5607C5D.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=1], baseline, precision 8, 965x543, components 3
Category:	dropped
Size (bytes):	55370
Entropy (8bit):	7.732446166360939
Encrypted:	false

SSDEEP:	1536:93PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYsm:97aN3JkKXiDPcp5jwx
MD5:	990581CD06C4532D60580D7F639AAB73
SHA1:	232AA2CB41DCB013058ED1E9459C150C426D6F79
SHA-256:	AD06EF9115ED9A270D1DF4FF8F44D1F8FE68CE7538D70D5663EDF37CA778D8B5
SHA-512:	FFF5C8872C4FC05D2A3B593917AEE6243C8DA483CB47DBF1F7FFE3E313648E4248C8811F6A0D381D2A73F6D0DEB322067C3BBDD443FEC6EF32D7E9B24C062E 90
Malicious:	false
Preview:	......JFIF.....`.`.....NExif..MM.*.......i...,Photoshop 3.0.8BIM.%.................B~...C...C............. ...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvw xyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz...?.....(... (...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6E32DE56.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7272
Entropy (8bit):	3.562481485203936
Encrypted:	false
SSDEEP:	48:P+Il4EPV0ypa2iq9YHnBfL9AG07kfAqN9XaZ7kV7kR3jCIf0:PvsPVHkzuWAG75aSWJjCIf0
MD5:	3791BE9C61E48E7790C65E1C19D3994D
SHA1:	CA523D797A7F3613697AC593128B2D7ED6F67D6E
SHA-256:	12200520CDFF255DF215875CFED465225615DFA2AA0B37D5A605E239AAC0D12C
SHA-512:	94974E3A1ECB4F711AD1A96E1CB38383594362070211 73A7A620EB5529041960003494F4EDCFAF3A07167E32DB53CD388548D8BAAE9965C57D66DF0A219BE54E
Malicious:	false
Preview:	....l...........,...<................... EMF....h...........................8...X...................?.............................1...C...R...p..................................S.e.g.o.e. .U.I... ....6.).X.......d...................d... ......p....\...d.......d.........p....d...\V.v...p....`..p8...zNw."................Kw....$.....r.d............^.p.....^.p.....".. ....-.......&<Jw................<..u.Z.v....X.b....8 ....vdv......%..................................r...............,...'...........(...(..................?...........?................l...4...........(...(...(...(...(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\76C63CD.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1504468
Entropy (8bit):	1.053474355446965
Encrypted:	false
SSDEEP:	6144:mmA9GHd0sV3GzfRnt9lGnz+CdHKz91sLW9TOuKPUWkGWzAOvRbNAvY:mmndNGzJnYnz+1z997K0zD
MD5:	35E141964E2698FC12D087516D116C9A
SHA1:	E2E0713E181633BB4D5247D5B37A7FF854165538
SHA-256:	6A3A2ADDC5D6B554EED64B7C24B699E09BCF019E4F42AB14EC6D40C7CB749538
SHA-512:	70CF79F2CDAC3065E5EF644A666358ADAACAB8F1B4E458BAA9B9057AD1B3EE1DD432F6EDE973FB76A60F8945D31A8DDB5E04B34912DF292C7D8B752AE39F3 F4E
Malicious:	false
Preview:	....l...........I...R............:...).. EMF................................8...X...................?..:...)..........J...S...Q...............I...R...................J...S...P...(...x........... ....:...)..(. ..J...S.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\86F058AC.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3920
Entropy (8bit):	0.6238557764114945
Encrypted:	false
SSDEEP:	6:0zfhlOslsDwE1vfk+kSYR3PhlXxv/lhPmcROwMR/C+7khvSGq48uxUo++:0zrOEhcCJtbhv/7eSpM/0hvei
MD5:	B144C5DC2697405C54706532478FB8F4
SHA1:	4A336DC89AB41EA549248BF17732255450D43FFB
SHA-256:	A56486C90A658CC2107998846EA20FA6ACC722EF80550916DF1A496544835CF7
SHA-512:	AF415AE8AEF2595D71BE8EE89BD59B94DA500CBA64FC7332E74A750A004002744CA3FB5C2CCE564CD0F3644C52BA0C79C726EC4104FEB33D3E81757EDD083 C77

Malicious:	false
Preview:	....X.....a.....b... EMF....P.....d...d.....F...8.....EMF+.@.....`..`....@.....F...l...`...EMF+.@..$.....b...d..... .....PNG.....IHDR.....b.....:s....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.....Om..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\93918E5F.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3920
Entropy (8bit):	0.6238557764114945
Encrypted:	false
SSDEEP:	6:0zfhlOslsDwE1vfk+kSYR3PhlXxv/lhPmcROwMR/C+7khvSGq48uxUo++:0zrOEhcCJtbhv/7eSpM/0hvei
MD5:	B144C5DC2697405C54706532478FB8F4
SHA1:	4A336DC89AB41EA549248BF17732255450D43FFB
SHA-256:	A56486C90A658CC2107998846EA20FA6ACC722EF80550916DF1A496544835CF7
SHA-512:	AF415AE8AEF2595D71BE8EE89BD59B94DA500CBA64FC7332E74A750A004002744CA3FB5C2CCE564CD0F3644C52BA0C79C726EC4104FEB33D3E81757EDD083C77
Malicious:	false
Preview:	....X.....a.....b... EMF....P.....d...d.....F...8.....EMF+.@.....`..`....@.....F...l...`...EMF+.@..$.....b...d..... .....PNG.....IHDR.....b.....:s....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.....Om..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A58FA7F1.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	29944
Entropy (8bit):	2.799241780569642
Encrypted:	false
SSDEEP:	192:dHxXn27sc9dO+EV2BfSOrpjT9qS8suTngJwPWWkjeh6eN1nS4ItDPca:dHvc9cVMtrpwErWYehznS4Itf
MD5:	1CC9F00C5F6002C6467DD1FB62FE806D
SHA1:	099A6ABBEF29D8CF4ED5377DE8116176B58E2D51
SHA-256:	D73CC9F8FC1BC49FBEC6EFEC8144D68BC3BB3F68B55C16511F6AB8066731AA9D
SHA-512:	8412E55034163F33DF402140A1537B124E83D8107656778BB6897187DAC57CCC0D2C5AB3EFD28B00A71122C2F8EF8E3627716DFB31E89E7BCE25D8C2E6CEF05
Malicious:	false
Preview:	....l.....0...%.....K...8.. EMF....t..b.....8...X.....?.....F...,.. ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....".....l.....1...&...".....l..... .....1...&...".....l.....1...&...".....l.....1...&...".....l.....1...&...'..... ....%.....L...d.....W...0.....W...1...T...!.....?.....?.....R...p.....T.i.m.e.s. .N.e.w. .R.o.m. a.n.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B336EBFC.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1504016
Entropy (8bit):	0.6376230814613634
Encrypted:	false
SSDEEP:	1536:zmUE4ZVtO1ZKadEb/adPaa1LxakIaprMaHaDavag1a1mjMaJnaIah/axShMkGtaH:zmUE4ZVtO1Z9EbKPFLZ/rjHgMmOC
MD5:	4D59A7E93170340B5EC4009F7FA3AD31
SHA1:	E07421156DD87789F93F10904118343CA452BBB5
SHA-256:	83473215E5C2160333AA92EA7F9B1276D8ED7DD66AFC472DC92C88055D189D7D
SHA-512:	415102AD30DF62A63EC47D7B432AB397C2CFC8B6F7FE1E8A7057877379B65D344499089780E089AD2F5C08E3050F4DC2205E7C3C4FFE484C39D067027783AB5
Malicious:	false
Preview:	....l.....R...H.....)...;.. EMF.....8...X.....?.....)...;.....S...I...Q...T.....R...H.....S...I...P...(...x..... ....)...;.. (...S...I..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BBE8D3E.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1505804
Entropy (8bit):	1.0125563822616974
Encrypted:	false
SSDEEP:	768:v2CnnHbNB0IzJg3ittG70X8cwXqmZPYBIrpCupi8y0V3lruRBPnfmb6qJ+:vvnnHbN/zJUitA70XynCIlN1dfmb6qJ+
MD5:	FDEBFD1C0D731BF56A398ABEB7F221A5
SHA1:	7864F45CA62BC727A332DED751442B99265E065F
SHA-256:	19B8C1D2BFFB4FEAC1BDEB2FB14D79AC6D50B4CEB566C1F3C8E233A088C30EB2
SHA-512:	5747FD24D92139F6CFEC2EE7832AB44AF1DAEE3B1EEDB98FEC07E521E69A769AB1EEBCC91FEB94FE0292835BD32C034ECA545B7422E75FB67D3C3653AE76D83E
Malicious:	false
Preview:	....l.....R...l.....)...;.. EMF.....8...X.....?.....)...;.....S...J...Q...P.....R...l.....S...J...P...(...x..... ....)...;..(...S...J..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DB46BBB0.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	97824
Entropy (8bit):	4.154873870060106
Encrypted:	false
SSDEEP:	1536:pm4/W6/W+VaIKD4HC/QCavImraz2kZQCtQJ2JEEEGtEEECtne/WS/Wo:pm4VaIKD4i4CavImraz2kZPKJ2JEEEGo
MD5:	2666C077CBF5BEF474A4C303C62A22D2
SHA1:	9C6398B59914D5122D0716FC0FFA45E602CBF213
SHA-256:	7512C14E1AE1D96636A262A45C3AC3D6CA4D6CA171AA0077879F3F4927BD027E
SHA-512:	9569F78479DF66B42A474F7D55A1A0534448FAE30807170920D4B2E38229E32097C5360F4C16658AC7F331515B504A208DD75C9DB56005068D968E6D39E935D6
Malicious:	false
Preview:	....l.....?{...P.. EMF.... ~..+.....8...X.....?.....F...,.. ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....l.....".....l.....".....l.....".....l.....".....l.....".....l.....".....l.....".....l.....'.....%.....&.....%.....6.....%.....L...d.....!...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~$RD0003.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.479760646202031
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHoljpl0QelMWFlc2VbiVllln:vdsCkWt51p2tvHV6/l
MD5:	0ACDE4A3C820A366AC6C0AB821A72207
SHA1:	B6551E86B60D095E74D4F79B6B004D40FDA4BA72
SHA-256:	3F3701E84757747159396FB41AD88E0E51084F846EB8007A2FAEAC15CE9DBF2C
SHA-512:	CB974D0C6CFE9B9AF015DD9D92B8110FC9AFE7EEA9A8C03ECF9112F6EA642DBE5FE9531E39B5B52EAADE7FEBAF6C17E4DD92AF5841476BECEA8E8789E19C2FB0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~$RD0005.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.479760646202031
Encrypted:	false

SSDEEP:	3:vrJlaCkWtVyHoljpl0QelMWFlc2VbiVllln:vdsCkWt51p2tvHV6/l
MD5:	0ACDE4A3C820A366AC6C0AB821A72207
SHA1:	B6551E86B60D095E74D4F79B6B004D40FDA4BA72
SHA-256:	3F3701E84757747159396FB41AD88E0E51084F846EB8007A2FAEAC15CE9DBF2C
SHA-512:	CB974D0C6CFE9B9AF015DD9D92B8110FC9AFE7EEA9A8C03ECF9112F6EA642DBE5FE9531E39B5B52EAADE7FEBAF6C17E4DD92AF5841476BECEA8E8789E19C2FB0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~$RD3923.docx

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.479760646202031
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHoljpl0QelMWFlc2VbiVllln:vdsCkWt51p2tvHV6/l
MD5:	0ACDE4A3C820A366AC6C0AB821A72207
SHA1:	B6551E86B60D095E74D4F79B6B004D40FDA4BA72
SHA-256:	3F3701E84757747159396FB41AD88E0E51084F846EB8007A2FAEAC15CE9DBF2C
SHA-512:	CB974D0C6CFE9B9AF015DD9D92B8110FC9AFE7EEA9A8C03ECF9112F6EA642DBE5FE9531E39B5B52EAADE7FEBAF6C17E4DD92AF5841476BECEA8E8789E19C2FB0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~$RO0000.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.479760646202031
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHoljpl0QelMWFlc2VbiVllln:vdsCkWt51p2tvHV6/l
MD5:	0ACDE4A3C820A366AC6C0AB821A72207
SHA1:	B6551E86B60D095E74D4F79B6B004D40FDA4BA72
SHA-256:	3F3701E84757747159396FB41AD88E0E51084F846EB8007A2FAEAC15CE9DBF2C
SHA-512:	CB974D0C6CFE9B9AF015DD9D92B8110FC9AFE7EEA9A8C03ECF9112F6EA642DBE5FE9531E39B5B52EAADE7FEBAF6C17E4DD92AF5841476BECEA8E8789E19C2FB0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0001.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	68774
Entropy (8bit):	7.685434558972311
Encrypted:	false
SSDEEP:	1536:5Jqk3PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYstHUac:5J37aN3JkKXiDPcp5jwqXc
MD5:	A46EC904E7DA5870F7D9DD1104C8C452
SHA1:	53BF050834F00699C2335843DE5575A13CF980D1
SHA-256:	5DF39FDBFE0353DE555D09595D65943137D31855E0B58BDAA4AE8A1701C0BCD7
SHA-512:	8A0EF3CBF4749E227CCE3A5FE27DB6FC31EFAAD611E6EC0FF9EC662C4C65F7C1B553346E9372C4BCA5D75D6BF6AA445D450B270C75E2E8F329C371F9B9EDFC06
Malicious:	false
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TKO.@.....v..1..A.$b<..).v..Y^..i..H.(zi..~...\|..R...<*kR.M:,.#m..$e.....E...Da..l.....x..#B.L.4.w.9.)h..u`..[.E.W?.N.O1.~...piM...Pr.~..r1+B4\.... .....Z)S.$.....p.PR...Mv.,.J.Y...rxE.Y.BY.7.+..=.8.. .....&.\|a}.3+g..N..4..y.$....y+.....2[.....*.....D.7...<.l..}....d-..mW..hH..._.m.an.....s.C.j$.u....N....QS.....g.I...1I....)s./...D..i. .....).....D. k..U.....PK.....!.....N....._re

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0003.docx (copy)	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	68742
Entropy (8bit):	7.684708700306939
Encrypted:	false
SSDEEP:	1536:5Jj3PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYstHUO:5Jj7aN3JkKXiDPcp5jwqB
MD5:	26D08BF19E617D0A4CC0E8085928A680
SHA1:	059D6F0B8E71A96E5748AEBC301E2DCB7DC30239
SHA-256:	C787F7195BC4099C8EB908EFF2368BA9B8551E6A5B1E1969450C83EB58E36E58
SHA-512:	CEE7628F17D7425B14CAFEE26F8ED9B62DE49E1220DD3BD6509984B4772A0353769B462DC899457D0944A56DD343D361567306D3849E89B49D9D2761FC8A594
Malicious:	false
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TKO.@.....v..1..A.$b<..).v..Y^..i..H.(zi..~...\|..R...<*kR.M:,.#m..$e.....E...Da..l.....x..#B.L.4.w.9.)h..u`..[.E.W?.N.O1.~...piM...Pr.~..r1+B4\.... .....Z)S.$.....p.PR...Mv.,.J.Y...rxE.Y.BY.7.+..=.8.. .....&.\|a}.3+g..N..4..y.$....y+.....2[.....*.....D.7...<.I..}....d-..mW..hH..._.m.an.....s.C.j$.u....N....QS.....g.I...1I....)s./...D..i. .....).....D. k..U.....PK.....!.....N....._re

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0004.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	68742
Entropy (8bit):	7.684708700306939
Encrypted:	false
SSDEEP:	1536:5Jj3PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYstHUO:5Jj7aN3JkKXiDPcp5jwqB
MD5:	26D08BF19E617D0A4CC0E8085928A680
SHA1:	059D6F0B8E71A96E5748AEBC301E2DCB7DC30239
SHA-256:	C787F7195BC4099C8EB908EFF2368BA9B8551E6A5B1E1969450C83EB58E36E58
SHA-512:	CEE7628F17D7425B14CAFEE26F8ED9B62DE49E1220DD3BD6509984B4772A0353769B462DC899457D0944A56DD343D361567306D3849E89B49D9D2761FC8A594
Malicious:	false
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TKO.@.....v..1..A.$b<..).v..Y^..i..H.(zi..~...\|..R...<*kR.M:,.#m..$e.....E...Da..l.....x..#B.L.4.w.9.)h..u`..[.E.W?.N.O1.~...piM...Pr.~..r1+B4\.... .....Z)S.$.....p.PR...Mv.,.J.Y...rxE.Y.BY.7.+..=.8.. .....&.\|a}.3+g..N..4..y.$....y+.....2[.....*.....D.7...<.I..}....d-..mW..hH..._.m.an.....s.C.j$.u....N....QS.....g.I...1I....)s./...D..i. .....).....D. k..U.....PK.....!.....N....._re

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0005.docx (copy)	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	68742
Entropy (8bit):	7.684708700306939
Encrypted:	false
SSDEEP:	1536:5Jj3PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYstHUO:5Jj7aN3JkKXiDPcp5jwqB
MD5:	26D08BF19E617D0A4CC0E8085928A680
SHA1:	059D6F0B8E71A96E5748AEBC301E2DCB7DC30239
SHA-256:	C787F7195BC4099C8EB908EFF2368BA9B8551E6A5B1E1969450C83EB58E36E58
SHA-512:	CEE7628F17D7425B14CAFEE26F8ED9B62DE49E1220DD3BD6509984B4772A0353769B462DC899457D0944A56DD343D361567306D3849E89B49D9D2761FC8A594
Malicious:	false
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TKO.@.....v..1..A.$b<..).v..Y^..i..H.(zi..~...\|..R...<*kR.M:,.#m..$e.....E...Da..l.....x..#B.L.4.w.9.)h..u`..[.E.W?.N.O1.~...piM...Pr.~..r1+B4\.... .....Z)S.$.....p.PR...Mv.,.J.Y...rxE.Y.BY.7.+..=.8.. .....&.\|a}.3+g..N..4..y.$....y+.....2[.....*.....D.7...<.I..}....d-..mW..hH..._.m.an.....s.C.j$.u....N....QS.....g.I...1I....)s./...D..i. .....).....D. k..U.....PK.....!.....N....._re

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD2913.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	68742

Entropy (8bit):	7.684708700306939
Encrypted:	false
SSDEEP:	1536:5Jj3PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYstHUO:5Jj7aN3JkKXiDPcp5jwqB
MD5:	26D08BF19E617D0A4CC0E8085928A680
SHA1:	059D6F0B8E71A96E5748AEBC301E2DCB7DC30239
SHA-256:	C787F7195BC4099C8EB908EFF2368BA9B8551E6A5B1E1969450C83EB58E36E58
SHA-512:	CEE7628F17D7425B14CAFEE26F8ED9B62DE49E1220DD3BD6509984B4772A0353769B462DC899457D0944A56DD343D361567306D3849E89B49D9D2761FC8A594
Malicious:	false
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TKO.@.....v..1..A.$b<..).v..Y^..i..H.(zi..~...|..R...<*kR.M:,.#m..$e.....E...Da..l.....x..#B.L.4.w.9.)h..u`..[.E.W?.N.O1.~...piM...Pr.~..r1+B4\.... .....Z)S.$.....p.PR...Mv.,.J.Y...rxE.Y.BY.7.+..=.8.. .....&.|a}.3+g..N..4..y.$....y+.....2[.....*.....D.7...<.l..}....d-..mW..hH..._.m.an.....s.C.j$.u....N....QS.....g.l...1I....)s./...D..i. .....).....D. k..U.....PK.....!.....N....._re

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD3923.docx (copy)

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	68742
Entropy (8bit):	7.684708700306939
Encrypted:	false
SSDEEP:	1536:5Jj3PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYstHUO:5Jj7aN3JkKXiDPcp5jwqB
MD5:	26D08BF19E617D0A4CC0E8085928A680
SHA1:	059D6F0B8E71A96E5748AEBC301E2DCB7DC30239
SHA-256:	C787F7195BC4099C8EB908EFF2368BA9B8551E6A5B1E1969450C83EB58E36E58
SHA-512:	CEE7628F17D7425B14CAFEE26F8ED9B62DE49E1220DD3BD6509984B4772A0353769B462DC899457D0944A56DD343D361567306D3849E89B49D9D2761FC8A594
Malicious:	false
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TKO.@.....v..1..A.$b<..).v..Y^..i..H.(zi..~...|..R...<*kR.M:,.#m..$e.....E...Da..l.....x..#B.L.4.w.9.)h..u`..[.E.W?.N.O1.~...piM...Pr.~..r1+B4\.... .....Z)S.$.....p.PR...Mv.,.J.Y...rxE.Y.BY.7.+..=.8.. .....&.|a}.3+g..N..4..y.$....y+.....2[.....*.....D.7...<.l..}....d-..mW..hH..._.m.an.....s.C.j$.u....N....QS.....g.l...1I....)s./...D..i. .....).....D. k..U.....PK.....!.....N....._re

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD3923.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	68742
Entropy (8bit):	7.684708700306939
Encrypted:	false
SSDEEP:	1536:5Jj3PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYstHUO:5Jj7aN3JkKXiDPcp5jwqB
MD5:	26D08BF19E617D0A4CC0E8085928A680
SHA1:	059D6F0B8E71A96E5748AEBC301E2DCB7DC30239
SHA-256:	C787F7195BC4099C8EB908EFF2368BA9B8551E6A5B1E1969450C83EB58E36E58
SHA-512:	CEE7628F17D7425B14CAFEE26F8ED9B62DE49E1220DD3BD6509984B4772A0353769B462DC899457D0944A56DD343D361567306D3849E89B49D9D2761FC8A594
Malicious:	false
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TKO.@.....v..1..A.$b<..).v..Y^..i..H.(zi..~...|..R...<*kR.M:,.#m..$e.....E...Da..l.....x..#B.L.4.w.9.)h..u`..[.E.W?.N.O1.~...piM...Pr.~..r1+B4\.... .....Z)S.$.....p.PR...Mv.,.J.Y...rxE.Y.BY.7.+..=.8.. .....&.|a}.3+g..N..4..y.$....y+.....2[.....*.....D.7...<.l..}....d-..mW..hH..._.m.an.....s.C.j$.u....N....QS.....g.l...1I....)s./...D..i. .....).....D. k..U.....PK.....!.....N....._re

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRL0002.tmp (copy)

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	66096
Entropy (8bit):	7.6673327627733885
Encrypted:	false
SSDEEP:	1536:vYT3PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYsul:gT7aN3JkKXiDPcp5jw5l
MD5:	606E86DDF4A7C9B6AB8C67C5E07E9AA5

SHA1:	02D97F1B8693DEE4C016AEF0B52F881F5444D078
SHA-256:	B970B6D64F578A2F3A718ADA8DDBBA5FF337D5577E21F32500148724AADEC382
SHA-512:	74DA6FF7E54FE8F65A770B33C1B945450E7D5538034FBF83986C140CA327C1912E7D527DD9FC16B41F085DF87A18B64954FA62A5C96498679F0F586AFB5C2844
Malicious:	false
Preview:	PK.....!....us...T.....[Content_Types].xml ...(..... ....T.N.0..#....(q..!...#T.|.kOR.7....L.6*%M%J/...[.y..h.U....59.g=...VHS..c..$Df.S.@N...hx}5.....&.d..{.4..h.2..`..^..K_R...+...zw.[...4V.d8x...UL.W.{.. .AI....J+'RW.u..b<.p.a.).Y.....g..U..zO.I.n.:iW.*?M..lqo.....1..i.N...*,.k.;.i.i.Brh....C.xNZeME3iv....q. ....o.<..{.....jZ....p....1bd.h~...~=.....?;...d..h.....5y..I.K.._.=..#..q.....- SG.7q.....PK.....!.....N....._rels/.rels ...(.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRO0000.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	66096
Entropy (8bit):	7.6673327627733885
Encrypted:	false
SSDEEP:	1536:vYT3PFta9L335kzeMRXBPf0xWIqVDPcp5jxOPlFkYsul:gT7aN3JkKXiDPcp5jw5l
MD5:	606E86DDF4A7C9B6AB8C67C5E07E9AA5
SHA1:	02D97F1B8693DEE4C016AEF0B52F881F5444D078
SHA-256:	B970B6D64F578A2F3A718ADA8DDBBA5FF337D5577E21F32500148724AADEC382
SHA-512:	74DA6FF7E54FE8F65A770B33C1B945450E7D5538034FBF83986C140CA327C1912E7D527DD9FC16B41F085DF87A18B64954FA62A5C96498679F0F586AFB5C2844
Malicious:	false
Preview:	PK.....!....us...T.....[Content_Types].xml ...(..... ....T.N.0..#....(q..!...#T.|.kOR.7....L.6*%M%J/...[.y..h.U....59.g=...VHS..c..$Df.S.@N...hx}5.....&.d..{.4..h.2..`..^..K_R...+...zw.[...4V.d8x...UL.W.{.. .AI....J+'RW.u..b<.p.a.).Y.....g..U..zO.I.n.:iW.*?M..lqo.....1..i.N...*,.k.;.i.i.Brh....C.xNZeME3iv....q. ....o.<..{.....jZ....p....1bd.h~...~=.....?;...d..h.....5y..I.K.._.=..#..q.....- SG.7q.....PK.....!.....N....._rels/.rels ...(.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4596E15B-44F2-46EC-B7F0-548B7E499F6A}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8A733322-1ED0-47A6-9275-656451DAAFBA}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.11299086186625841
Encrypted:	false
SSDEEP:	3:llYdltn/lLQ+n:A3K+
MD5:	3E63486E4BEB395BEDDF4EADC8EAA7DF
SHA1:	3B1D6276345408B5F320AEE4A73AE71EF79ED78C
SHA-256:	5DAEC42472B3B45BA0D38072709BFEE8956D67AED379B39273758475162DB75F
SHA-512:	321453C0BF34BBFD094BA75B85BC3E15D7FE053F10F2BF3D89B926593DB02DA59970F8D619ACB46378753739C164396DE3A97A970D1A2F07E0441F7D24C073F
Malicious:	false

Preview:	../.....

C:\Users\user\AppData\Local\Temp\333 (2).emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3920
Entropy (8bit):	0.6238557764114945
Encrypted:	false
SSDEEP:	6:0zfhlOslsDwE1vfk+kSYR3PhlXxv/lhPmcROwMR/C+7khvSGq48uxUo++:0zrOEhcCJtbhv/7eSpM/0hvei
MD5:	B144C5DC2697405C54706532478FB8F4
SHA1:	4A336DC89AB41EA549248BF17732255450D43FFB
SHA-256:	A56486C90A658CC2107998846EA20FA6ACC722EF80550916DF1A496544835CF7
SHA-512:	AF415AE8AEF2595D71BE8EE89BD59B94DA500CBA64FC7332E74A750A004002744CA3FB5C2CCE564CD0F3644C52BA0C79C726EC4104FEB33D3E81757EDD083C77
Malicious:	false
Preview:	....X.....a.....b... EMF....P.....d...d.....F...8....,...EMF+.@.....`...`....@.....F...l...`...EMF+.@..$.....b...d.....PNG.....IHDR.....b.....:s....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.....Om.....

C:\Users\user\AppData\Local\Temp\333 (2).emf:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443B98
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Temp\333 (3).emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3920
Entropy (8bit):	0.6238557764114945
Encrypted:	false
SSDEEP:	6:0zfhlOslsDwE1vfk+kSYR3PhlXxv/lhPmcROwMR/C+7khvSGq48uxUo++:0zrOEhcCJtbhv/7eSpM/0hvei
MD5:	B144C5DC2697405C54706532478FB8F4
SHA1:	4A336DC89AB41EA549248BF17732255450D43FFB
SHA-256:	A56486C90A658CC2107998846EA20FA6ACC722EF80550916DF1A496544835CF7
SHA-512:	AF415AE8AEF2595D71BE8EE89BD59B94DA500CBA64FC7332E74A750A004002744CA3FB5C2CCE564CD0F3644C52BA0C79C726EC4104FEB33D3E81757EDD083C77
Malicious:	false
Preview:	....X.....a.....b... EMF....P.....d...d.....F...8....,...EMF+.@.....`...`....@.....F...l...`...EMF+.@..$.....b...d.....PNG.....IHDR.....b.....:s....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.....Om.....

C:\Users\user\AppData\Local\Temp\333 (3).emf:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 98
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Temp\87F4.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTILPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB 39E
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\HI4NJ046K

Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001, page size 2048, file counter 4, database pages 37, cookie 0x2f, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	1.1340767975888557
Encrypted:	false
SSDEEP:	96:rSGKaEdUDHN3ZMesTyWTJe7uKfeWb3d738Hsa/NlSGIdEd01YLvqAogv5KzzUG+H:OG8mZMDTJQb3OCaM0f6k81Vumi
MD5:	9A38AC1D3304A8EEFD9C54D4EADCCCD6
SHA1:	56E953B2827B37491BC80E3BFDBBF535F95EDFA7
SHA-256:	67960A6297477E9F2354B384ECFE698BEB2C1FA1F9168BEAC08D2E270CE3558C
SHA-512:	32281388C0DE6AA73FCFF0224450E45AE5FB970F5BA3E72DA1DE4E39F80BFC6FE1E27AAECC6C08165D2BF625DF57F3EE3FC1115BF1F4BA6DDE0EB4F69CD0 C77D
Malicious:	false
Preview:	SQLite format 3.....@ .....%...../.....C..... ....

C:\Users\user\AppData\Local\Temp\README (2).txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.144482923353892
Encrypted:	false
SSDEEP:	6:q4RLRyLk3Lfk+KKUwnXNgLB099EVk3Lfkq+ZEQh+y6oaQ4VQCs:BjyL9RqX0Bc909/ZEoooT
MD5:	38DE85DA0193E7AB300FDAFF24432A5A
SHA1:	F9C50ABA2CE25AA7C18C140352EC5F083DB00B7F

SHA-256:	E59C5729C72A6AB02ED18F740E72AC44FFB71171FB49A9405F5C3D1F2F056782
SHA-512:	41E2626CD5C3B739369C5FC5FA46605415F1F8367AB117EF4C5D0FE3D62480121AB7825011F2DC6F4E18F0C29DE78E17769E6674045A1B09CB91E5BF52EF67BD
Malicious:	false
Preview:	Installation Steps for Trillium Security MultiSploit Tool v6.5.25:....1. Copy your personal "user_license.bin" File and paste it to the "TDS_LicenseFile" Folder...2. Now you can run "Trillium Security MultiSploit Tool v6.5.25.exe".....w5456z4thrfhtfht-kgjhfdghj5utej-76r8ttrerhteitje-mhgjkftdzsretztrz657UIGZUurg-UHIgdfhdgrrdg97654

C:\Users\user\AppData\Local\Temp\README (2).txt:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E98
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Temp\README (3).txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.144482923353892
Encrypted:	false
SSDEEP:	6:q4RLRyLk3Lfk+KKUwnXNgLB099EVk3Lfkq+ZEQh+y6oaQ4VQCs:BjyL9RqX0Bc909/ZEoooT
MD5:	38DE85DA0193E7AB300FDAFF24432A5A
SHA1:	F9C50ABA2CE25AA7C18C140352EC5F083DB00B7F
SHA-256:	E59C5729C72A6AB02ED18F740E72AC44FFB71171FB49A9405F5C3D1F2F056782
SHA-512:	41E2626CD5C3B739369C5FC5FA46605415F1F8367AB117EF4C5D0FE3D62480121AB7825011F2DC6F4E18F0C29DE78E17769E6674045A1B09CB91E5BF52EF67BD
Malicious:	false
Preview:	Installation Steps for Trillium Security MultiSploit Tool v6.5.25:....1. Copy your personal "user_license.bin" File and paste it to the "TDS_LicenseFile" Folder...2. Now you can run "Trillium Security MultiSploit Tool v6.5.25.exe".....w5456z4thrfhtfht-kgjhfdghj5utej-76r8ttrerhteitje-mhgjkftdzsretztrz657UIGZUurg-UHIgdfhdgrrdg97654

C:\Users\user\AppData\Local\Temp\README (3).txt:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E98
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

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

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	95232

Entropy (8bit):	6.231519588351459
Encrypted:	false
SSDEEP:	1536:opZrDPCXLdr7zQN/GZGLaYeZjtBaKaedCRVLR8dpxekydJrD9iiU71aC4sWBlVmc:oHTCB7Y/GZGPeZxaGCRVLR9kydI7sCU5
MD5:	6CB712E482D150A185F713D75314A75A
SHA1:	0EE7D4AB0D46C6A668AA500470AAFB632F1ACD99
SHA-256:	C5E0F86A68DCBD03B9A506768F86C385C360D3CF67B9CC0B5760F7B3F1D91F48
SHA-512:	042C3B3A24C35686FA11FBF052A8F278C12535B5F90ECDE5319AA86B8F3616A9A00FBE5E86BD644E2101201B994648BCE2B1F6D6E1F4EDA6C8140F93421CD6E1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.8-?.V~?.V~?.V~t.U.5.V~t.S...V~t.R.+.V~..S...V~..R...V~..U.,. V~t.W.(.V~?.W~@.V~..^.>.V~..T.>.V~Rich?.V~.....PE..L...2'.d.....!.....z.....@.....<k..... .....^.....]..@.....text..... ..`.rdata...e.....f.....@..@.data...l.....j.....@..... ....

C:\Users\user\AppData\Local\Temp\nsl9C8E.tmp

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	329165
Entropy (8bit):	7.541945169368556
Encrypted:	false
SSDEEP:	6144:WVez7cuIYLUvLfkWAdTEkQUOM1sXFQveBUQZKQldIDMzCu/GZVZxML7L2+P:WKcsCftAdTEarq3BUQZKQfuMzCu/QZOS
MD5:	4ED3CB08EC2E744A786A87B5FEA1AA59
SHA1:	76A5A491D05D504A367C19F0E9669BAA474A8D12
SHA-256:	A3710AFDDF05886219EB7EBA3A85F0AD33EAC1BA6C4BB67F7B389C6CDA15875D
SHA-512:	EEA49222FD83CA261685EB282985906AF43B0020960961CA8141446E432D594BEC294EC2A76747D6B9F834ABCD3218CA5A014A769DBB7F3B8959360E8FD5ECDC
Malicious:	false
Preview:	.A.....-.....@.....A.....H..... .....G.....j.....I.....I..... ....

C:\Users\user\AppData\Local\Temp\o0whqph.zip

Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	441750
Entropy (8bit):	**7.998736788620827**
Encrypted:	**true**
SSDEEP:	12288:kNYTTUBeH/mxYhfbJQ0BHxK30XfNd+6NwY8Ta6A:SYTT6ULhTndxmibH8u6A
MD5:	FA9B7C190006303EECDDFFA019D0BE06
SHA1:	A97CEBC176B3DAA453189F2C0B7CF2A5A70F9C92
SHA-256:	DC7F8B3493543DC086CB43B66401893597F993408F18B437E5C8E8B5544DB0BF
SHA-512:	4C293EF052A14F7527AA42D451BA5F4CFDF7FB7203F583EDA34EF24F4A2FD13975553C432A9354A0F8C1DE924B0C29A819BD34C7AAA03B642372496A75BE053
Malicious:	false
Preview:	PK.....x.MJ0..#....c.....sqlite3.defUT.....X..Xux.....d.....&....6.....9.$..\..nj....==O...F...4.O....._...%..*..Il..MD....>.&Y.St.~.6(g.x..=.....".=...|..`...[.....].Y.y$o.q..4k.L.u +...5'...@....S.....r.s..|}.Yo.U..M...nyP:...|..8.....`9. ..._.<..P..."..s.....H.8.F..../.....H..[.Nk.q...,..T.s@U2.G.1GR8..S."......L9N.....*?..S.R5....3..-s^m.|.Q..p....Ms2.&.a'_ .x.'.t.8].{.IW.....&..Of..a..*.....i.k.4.&^..5F_*..e..[..g.=.8.Cs2.qK.M>(.<.u...a)..V..%.)w.....ct..."...Q...w..`r.0.3M."...9...M`.>!Z.#R;.....k:.[.l.....Bl..>@.a.....(T..b1/.4..Px .I.)+...KLz...B..6...G.>..K..Gbu.#..c.`,.B.y.].....K{[A.....q..?..q6v^...of..V....];?#.v..I1=.m..R....]n.6.W..bv..]...'J.O....e3...@...E. 6..M..k..@.7.4.]@;.*..1.sq.P.v..MA/.....W!G..6. ...a.R<..XT5..U&.....(.N.f#.7.ck..].b>8....(.Xq`..p;...Ljt.....t.lW.....5O....3|}.=.....8..o.....Fn.....Lp..As.&..i8)....n-.....+".....q.....@.*...+...`....<.8..

C:\Users\user\AppData\Local\Temp\ortnkgsjk.g

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	211209
Entropy (8bit):	**7.998782052319318**
Encrypted:	**true**
SSDEEP:	6144:7Vez7cuIYLUvLfkWAdTEkQUOM1sXFQveBUQZKQlu:7KcsCftAdTEarq3BUQZKQI
MD5:	0A629526F8AEC96658786151E6C3EA06

SHA1:	80B71B17469506F4023F5E3C35715A6A130AC4C5
SHA-256:	D61BEA82FCBA68CFBC5E6BBE882D5E373EAA26C0DD4AD9C5626EE13A780AB546
SHA-512:	848E3A46F2EAEF9656ADF2DAFE618C20BDDB19D98836F43065F219A58D14BEBB554A63B7844560CCF0EF2124F6D51AD2A6D71DA8AA0408EF639D6BB4FFF0A2F4
Malicious:	false
Preview:	...^.1s..E...g..0#YI.!.Dg.,$.K.....#>.....i..^...&..X..\|.,...\1....e.o.5.T`....;...>.Y..m.c.. ..X.}..mV_.6B]D...UQ.H.C.....x..?y..`...`...*.8.....K.z.x.o.;.}Z~]v.TO.....V.{...->i]..4-e.....[m^Bx.N..T!.[.E..yVD.q....."$m..0g.y.^\.B-.U.`.1s...QH.....4.Y....;...-.....@.#>....u.i..^.z.&..X.5|.....\.,.,Mrc?4....w+..'~&lO..5C.Y.*...I...'.5.}a..8/~.UQ.H.C...U<..*m$.xT..eQ...H...^.....j.w[m.H7..B..V.m.....qW.:..{.8....(.}v.....[.^~..,^..u.0.E..yVD....."....0....^\.B-.U.`.1s..QH.....MY....;....K.....#>.....i..^...&..X.5\|.....\.,.,Mrc?4....w+..'~&lO..5C.Y.*...I..'.5.}a..8/~.UQ.H.C...U<..*m$.xT..eQ...H...^.....j.w[m.H7..B..V.m.....V.{.d.-..(.}{6.....[.^~..,^.Tu.[.E..yVD....."....0....^\.B-.U.`.1s..QH.....MY....;....K.....#>.....i..^...&..X.5|.....\.,.,Mrc?4....w+..'~&lO..5C.Y.*...I...'.5.}a..8/~.UQ.H.C...U<..*m$.xT..eQ...H...^.....j.w[m.H7..B..V.m.....V.{.d.-..(.}{6.....[.^~..,^.Tu.[.E..yVD.

C:\Users\user\AppData\Local\Temp\sqlite3.def

Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	4963
Entropy (8bit):	4.34930488328599
Encrypted:	false
SSDEEP:	96:GcuN4gR+7Oc0XRMcCM3KVGOF95BlMtvrmNHY0ac:E4Q+7Oc0JKVBF95EvrmNHcc
MD5:	DE71633DE073966EB5D5F787EAC989BB
SHA1:	DD110A7666977B763F1CB540745D928A02A3AACA
SHA-256:	C810A7589A228352269413CC503647DF82B4320B7C0B596A15D2842DAC7F843A
SHA-512:	D10211BCD304EDE9CBF9CAD26852BBCF1C7F96D7615527DFA9097D97B5B94ABC3A28607E667C77D7E564676A3085C8C993036ED1D48BFCC77566D9C09A478BD
Malicious:	false
Preview:	EXPORTS.sqlite3_aggregate_context.sqlite3_aggregate_count.sqlite3_auto_extension.sqlite3_backup_finish.sqlite3_backup_init.sqlite3_backup_pagecount.sqlite3_backup_remaining.sqlite3_backup_step.sqlite3_bind_blob.sqlite3_bind_blob64.sqlite3_bind_double.sqlite3_bind_int.sqlite3_bind_int64.sqlite3_bind_null.sqlite3_bind_parameter_count.sqlite3_bind_parameter_index.sqlite3_bind_parameter_name.sqlite3_bind_text.sqlite3_bind_text16.sqlite3_bind_text64.sqlite3_bind_value.sqlite3_bind_zeroblob.sqlite3_bind_zeroblob64.sqlite3_blob_bytes.sqlite3_blob_close.sqlite3_blob_open.sqlite3_blob_read.sqlite3_blob_reopen.sqlite3_blob_write.sqlite3_busy_handler.sqlite3_busy_timeout.sqlite3_cancel_auto_extension.sqlite3_changes.sqlite3_clear_bindings.sqlite3_close.sqlite3_close_v2.sqlite3_collation_needed.sqlite3_collation_needed16.sqlite3_column_blob.sqlite3_column_bytes.sqlite3_column_bytes16.sqlite3_column_count.sqlite3_column_database_name.sqlite3_column_database_name16.sqlite3_column_decltype.sqlite3_co

C:\Users\user\AppData\Local\Temp\sqlite3.dll

Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	845402
Entropy (8bit):	6.501857871491562
Encrypted:	false
SSDEEP:	24576:i+S+SW56QlzJx2IzvTrSo46oeUVCkBtW6w0n:iZW4QltYlzv3So46oeUzn
MD5:	00A91261929192A7FACC32A9F330029A
SHA1:	7DF4FFDF48A6DF0BAC21A82D6DB56AA11DB470DC
SHA-256:	C1DE8ECA6419634C5F6E0E8C6EF14D9B3DAA28FA28E8D1C4CE0175DBC310A77F
SHA-512:	18A178CA0E70FA6E8F04B4AE229CFD6EF0DF252E3FD85D09CF79F89E69ADA89E3479DB83227095A8C16325B1DC27C9EC0C782AF304F7CE0AFA78C2E25B49B01E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....X....V.....!.....a.....5.....0..x.....@.. 0..... .....text...X.....`.P`.data...|.....@.`..rdata..T.....@.`@.bss.....`..edata..5.....@.0@.idata.....@.0..CRT.....@.0..tls.... ....@.0..rsrc...x....0.....@.0..reloc.. 0...@...2.....@.0B/4.....@.@B/19.....@..B/31.....0.....@..B/45.....P.....@..B/57.....p.....@.0B/70....i.....

C:\Users\user\AppData\Local\Temp\ytljtt.f

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	5854
Entropy (8bit):	7.162377453768944
Encrypted:	false
SSDEEP:	96:Farc6oY3g/DrYujk2XO5oSwYgCP7Yc3NdN6d35O4pTU15Fn9O2PGiMCmbvrfjXC:FarcRXrhX1S9PPN6d3ZpTU15EJLrLXC
MD5:	452A3EE71E9BA72BB78302A46C6D5B12
SHA1:	F86411F3F43C4351EF651B38A1402C63B90DB7AC

SHA-256:	521E94034E7166D401C6831BFEE91A92848BF821EAE75ADBD857F503C3D42BC2
SHA-512:	0BB5A96F91E37AB5B89A02C2B25D449C27D1A1E25EB42D461D4B52AE2FB067FDF288EF7F7A4C43955BD7A3A1B32CC514F1C4DD27DBFBB6FE6C7916763056DFD3
Malicious:	false
Preview:	.005m..f.F<...05o.:.....?v>.3.3.<.....M.knl.02a..c.E<...42c. .....4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r .D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX. ....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4.....F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0...^..M...3uc.....}<F...kloe.=8e...548.r...t..w.(058. q..v..l.0A..q..34.q.p.}..u.{.w....}.p013.....u.L.4F".u..04.t.t.q..p.x.u....q.8580..Y...}..E.4D'.q..80.}.t.t..w.p.p...X+AK..M.....v.ZXK.J.E.....}.]..O.F.....u.X_.M.M.....H...X...K.D.....}. \&....A..B....G...P5..O.E..P....\...Y...K.E..a....B...].4.T.4.q0.p..q..~<1|..x.q.>.t&.u.|1,.t..w.pe..\...w.p..u.T.4.Q.0.}.:.q%..5M%.}.:.qm..tL9.}.5013.6.].5.u...K...P3480..u...dR0. m...D4...B358.q.0342.}.e.....dX4R0]<048[3^2^8Z5..p...d.a..

C:\Users\user\AppData\Local\Temp\yy (2).txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with very long lines (599), with CRLF line terminators
Category:	dropped
Size (bytes):	3446
Entropy (8bit):	4.578411407233512
Encrypted:	false
SSDEEP:	96:k0mXWv0agGitiXOCPyXaqUH3V/W8b3+GFe4Qzl:k3aIJCO/K/bOGFe4y
MD5:	0CAB0C6F6888DE32D1EC8F600E3C1247
SHA1:	F612BA306D9E50FFC7BFE5AB2A995DA3F5EDB335
SHA-256:	970C719A58BC925CA596C9DDD7D4A3F2CEB6F6301AB06F556BAAB89307570816
SHA-512:	19BE3481380446B4E361AF55FCA9BC329173F01848432E82A002BEC0A40E19FF90F1E5D700EB6ABA647CD409AD7B985716F5C02B5DF72A8E0703F051FE82D7D4
Malicious:	false
Preview:	I just disabled SPy Option if you wish you can activate later if I am disconnected again but this option collect whole time all infos and interests of you , which programs you use, which websites you visit etc and send to microsoft and others for investigation did you knew ? i not know that. thank u bro np later if I am disconnected i recommend you go through this whole menu and disable things that all are only options which collected data from you / spy you if you want to be more anonym and secure you should disable can u do that for me are you using webcam on this systme ? no micro ?no done....btw do you have hf website here ? I mean can you open yaa oh 1 thin can I del ete the PM about the spritual things because all get watched its better to delete yaa do you know how I can see all my posted threads ? i not getting idea now np 1 sec i try something because I want show you important thing for deactivate spy on win 10 okay now much spy options disabled if you want disable more you can

C:\Users\user\AppData\Local\Temp\yy (2).txt:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443B98
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Temp\yy.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with very long lines (599), with CRLF line terminators
Category:	dropped
Size (bytes):	3446
Entropy (8bit):	4.578411407233512
Encrypted:	false
SSDEEP:	96:k0mXWv0agGitiXOCPyXaqUH3V/W8b3+GFe4Qzl:k3aIJCO/K/bOGFe4y
MD5:	0CAB0C6F6888DE32D1EC8F600E3C1247
SHA1:	F612BA306D9E50FFC7BFE5AB2A995DA3F5EDB335
SHA-256:	970C719A58BC925CA596C9DDD7D4A3F2CEB6F6301AB06F556BAAB89307570816
SHA-512:	19BE3481380446B4E361AF55FCA9BC329173F01848432E82A002BEC0A40E19FF90F1E5D700EB6ABA647CD409AD7B985716F5C02B5DF72A8E0703F051FE82D7D4
Malicious:	false

Preview:	I just disabled SPy Option if you wish you can activate later if I am disconnected again but this option collect whole time all infos and interests of you , which programs you use, which websites you visit etc and send to microsoft and others for investigation did you knew ? i not know that. thank u bro np later if I am disconnected i recommend you go through this whole menu and disable things that all are only options which collected data from you / spy you if you want to be more anonym and secure you should disable can u do that for me are you using webcam on this systme ? no micro ?no done....btw do you have hf website here ? I mean can you open yaa oh 1 thin can I del ete the PM about the spritual things because all get watched its better to delete yaa do you know how I can see all my posted threads ? i not getting idea now np 1 sec i try something because I want show you important thing for deactivate spy on win 10 okay now much spy options disabled if you want disable more you can

C:\Users\user\AppData\Local\Temp\yy.txt:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443B98
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Temp\~DF105CE6962F655752.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	7.577653575035039
Encrypted:	false
SSDEEP:	768:eT5BP++exJQohHN2WVFWbSFhEq8TFBxwd3ZZw9mCcUXiP4ymDiFLIhGHugk:eTPW+eTQaHN2uWuEq8TFBx2ZZwYCcUmm
MD5:	B6D766BDD546E92E549F8D1BA1C709D0
SHA1:	1C60C62B8D7419D25BAC3A72F98CE9F8312DC48F
SHA-256:	6E117BA8FCE0C5273BA74A4F70CB6ACEA970693EAED28534F6E738A169D607E1
SHA-512:	44737F3FB62F53484D3A414DD8F5AE6428A643C6CA416319EA0AB36D9C0CC2B528C403241E8A18564EA3AEEB762A4E5D421108D4C30FBE95F51F1610F0A856BB
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...[.....

C:\Users\user\AppData\Local\Temp\~DF2613BCA6826298A5.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	7.582513260576488
Encrypted:	false
SSDEEP:	768:pTktBP++exJwu+N2WVFWbSFhEq8TFBxwd3ZZw9mCcUXiP4ymDiFLIhQugk:pTkbW+eTwu+N2uWuEq8TFBx2ZZwYCcU7
MD5:	EB0EF657151A2795DFA4C524991EA55E
SHA1:	FA6D824C5B167ED0A6BE8889D0EE73B6CE4F91B7
SHA-256:	535E0C0B7C1416B3FA680A963E11498B43E9B0D235814972EE132C18FFE653C2
SHA-512:	7FA6F721F5D2F71DFC4A689AAD0FFB173B1D54EED764A8B4527C003DBC9DA09A57967CD499C12D7A78D4401C05560DDBAAE3DA0D1AAC7548453903C645897A2
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...[.....

C:\Users\user\AppData\Local\Temp\~DF3759C9448D2ED5D7.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	7.577868660379925
Encrypted:	false
SSDEEP:	768:AT5BP++exJQohHN2WVFWbSFhEq8TFBxwd3ZZw9mCcUXiP4ymDiFLIhlTgk:ATPW+eTQaHN2uWuEq8TFBx2ZZwYCcUm4
MD5:	1567F391B727410211B36EFB1FDB118D
SHA1:	C1ADC163163E92A2CB6CE0C4911B4715C994E257
SHA-256:	FBEDB2D394DCC615550C84EC5EF8B0D601D4B18B46CB81758C5AD1F43E68A0A8
SHA-512:	3610A0655FFD2727DFDB3AE62C9B01E49D451FDF77C24FCC8003601DDB8AB7B6271B19E9F2439975F11CD27726B77A370CF2B9BDF8AAD21A921264E3D16A43B
Malicious:	false
Preview:	.....>..... ....I..."...#...$...%...&...'...(...)...*...+...,...-...../...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...[.....

C:\Users\user\AppData\Local\Temp\~DF4DCF212DAF54DAAA.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	7.5831329381697605
Encrypted:	false
SSDEEP:	768:dTktBP++exJwu+N2WVFWbSFhEq8TFBxwd3ZZw9mCcUXiP4ymDiFLIhgtgk:dTkbW+eTwu+N2uWuEq8TFBx2ZZwYCcUy
MD5:	01FA5E410151521E31D6A02AC741FBB8
SHA1:	6C605C6D43A95B0FBCB50EFD18BF87E229552B34
SHA-256:	A2A2B877A3E971562BA5CCC7C64FC6B94F7018DF9CFB4F7234664A5A6715AF0A
SHA-512:	BFD65322955FC77A7F3C0607AC6222A85A47E16996282F5D609209C04A3D90D9D6637C052EAE745824C79A31AE4F6FFBCC32DD29653DC9CD5E828C2EB4E7963
Malicious:	false
Preview:	.....>..... ....I..."...#...$...%...&...'...(...)...*...+...,...-...../...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...[.....

C:\Users\user\AppData\Local\Temp\~DFAEEDEE6F10B6AFDD.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	7.582753965251375
Encrypted:	false
SSDEEP:	768:oTktBP++exJwu+N2WVFWbSFhEq8TFBxwd3ZZw9mCcUXiP4ymDiFLIhoIXgk:oTkbW+eTwu+N2uWuEq8TFBx2ZZwYCcUV
MD5:	69273511CB0A7F3C7962DF64FBAB4242
SHA1:	418073A4499F616249CD868D1CB02A34785FBDCD
SHA-256:	D868A8B6588232493CCC48273A33F7698E29E1D6167F7E5F7D182C03EC717552
SHA-512:	4739AE7D15EB411813849778E863ADEBDF4BB9545D7FA8F90637D95FF9F2CDA91E4B7212B523D7B684AA0F1905192D450B5547AF0783B7AE3A682D3BF3A8E2A3
Malicious:	false
Preview:	.....>..... ....I..."...#...$...%...&...'...(...)...*...+...,...-...../...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...[.....

C:\Users\user\AppData\Local\Temp\~DFCD0A74EBC3B8D0D3.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	7.582856886423914

Encrypted:	false
SSDEEP:	768:LTktBP++exJwu+N2WVFWbSFhEq8TFBxwd3ZZw9mCcUXiP4ymDiFLIhGHugk:LTkbW+eTwu+N2uWuEq8TFBx2ZZwYCcUt
MD5:	E7093D875FB8116FD59572267E89E70B
SHA1:	B11AA6698E0A554380E1B9908B985B7182A6B252
SHA-256:	A6C7449022EA4D31C1E17C4514BBE581A008B003E41C92C97074328056DAC45D
SHA-512:	AFF1B18032AED40493613006A06E8A971C07CD010547AD4DC55A10001A39DDD961F8919A1FDACE5FD1872DCECC2948A3822DD096A2990383859AE4E204FCE26
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...[.....

C:\Users\user\AppData\Local\Temp\~DFCE59EB4D76CCBC89.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.421630815922858
Encrypted:	false
SSDEEP:	24576:iLKZWQmmav30xr+MXUu94a6S+MXUu9FybVK+MXUu9yfbVYQo:iLKoQmmQ30l+MXV9Nr+MXV9FybVK+MXs
MD5:	2ECF3989803CC22790E4B09DBF1D7C13
SHA1:	FCB64CA8A168D8A1C1D18FB85C35B0DFC79FDB87
SHA-256:	64FA3051880E1D851ABEAF125D283B3A3BF107B7ACC84DFFA73CF83BC187AADA
SHA-512:	15F6BEC2EC98C995DAD583938ADE526603EADA83BD643A22E98F424ABAE29980666ACD3725D699E2ADD7924DD263E39B33FFAE202F0658BDAE0641A7204FEEC3
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFF3DB96A6682A15C6.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	7.5780781770787184
Encrypted:	false
SSDEEP:	768:vT5BP++exJQohHN2WVFWbSFhEq8TFBxwd3ZZw9mCcUXiP4ymDiFLIhigk:vTPW+eTQaHN2uWuEq8TFBx2ZZwYCcUmB
MD5:	ECC1C225AAEEB2C626A578564E03BF43
SHA1:	3B7A7D102B2F61FE9EABEF645E6FCC7DCE37145E
SHA-256:	FDFCB46BCEF1DD5C07FF051E1F8A256C56ED503FF29FD479CE17DBA325636EDB
SHA-512:	3EBE4BE2C7268F41F72B5ACEE345EFBE40215AEC0998DA4EE17B46295CD7CA41DC7926DF9EBE563E82AB935C95B954563A8B00F682F3B2E62AF4714118EBFE51
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...[.....

C:\Users\user\AppData\Local\Temp\~DFF43C2C98E1EF8FBE.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	7.577349403604213
Encrypted:	false
SSDEEP:	768:3T5BP++exJQohHN2WVFWbSFhEq8TFBxwd3ZZw9mCcUXiP4ymDiFLIhQugk:3TPW+eTQaHN2uWuEq8TFBx2ZZwYCcUm0
MD5:	73C204857EDD94212CDC4A3D2926F91D
SHA1:	835C78F6BC433491685A331C9EB42405D1161EEA
SHA-256:	B57FAC07E53B3CAB565A286FFFF67968C76F5A7966A7F997AFA2EE89A0C18C10

SHA-512:	84B9C01384EFBDDB0EDBAB056FCABFA8A3E332F6EC3B986F99CF03D52B2E37CB7755A5C475474AB66F4380C30AEEE095A0C6B35EA560B0A7DAC5732062529C7B
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...[.....

C:\Users\user\AppData\Local\Temp\~DFF502807A3587CE89.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1429504
Entropy (8bit):	7.051109271439765
Encrypted:	false
SSDEEP:	24576:/LKqWQmmav30x7+MXUu9/a6V+MXUu9LybVg+MXUu9mfbVtQo/LKmaEJQEzLKma2J:/LKPQmmQ305+MXV9iA+MXV9LybVg+MXa
MD5:	92DA3FCA9DB9F787A1DCC8EB8F888A30
SHA1:	E0ED570353A727F48B797BA05D507641286E04B6
SHA-256:	D01439144D9303C0507A8792889C7046AB2EBCB213466E292A8E2A6FBEB5A405
SHA-512:	AA2D09DAB8C841FD5708EA6525F002FB7A2D76F0D315208FD4AF020B566DDB9FCFA6A611512E4411B5ECEDF5C83C81C3E665C96D755A34D7F624C457ECD0D23
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_store

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	0.6739662216458647
Encrypted:	false
SSDEEP:	12:Ppb0slZp69PO9tauZ7nH2AaYSQ81v0t4TreIBUxFj87+k/R:RbG4WuZfKZ1c+reIAon/R
MD5:	C61F99FE7BEE945FC31B62121BE075CD
SHA1:	083BBD0568633FECB8984002EB4FE8FA08E17DD9
SHA-256:	1E0973F4EDEF345D1EA8E90E447B9801FABDE63A2A1751E63B91A8467E130732
SHA-512:	46D743C564A290EDFF307F8D0EF012BB01ED4AA6D9667E87A53976B8F3E87D78BEBE763121A91BA8FB5B0CF5A8C9FDE313D7FBD144FB929D98D7D39F4C9602C9
Malicious:	false
Preview:	....+..F..N..F).~].....\.">.. .....p.J..} /o...rLj-...FS..'x.o..%^ .....zr/..3.y.e4...MM.4..x9.f.D..{..(....'p.....9...Qn..d..+.....H..M.).....].....n-.].....n&.*.H`.sz...r.....1B.....e.."...A.....,-....n..$.<....CO..VO..P..'.....<.....n....&5s....z..$.{'IM-.o..(#N.-..(H...a&...y.S..`8.(./...1.P.. .....K.3.....I!]G....@N.....F.I.T=.0...`"..L....B...B`nI.<.....&F..2J2....1..Rs....h.Zq.`...t..CJ....@.....I.G.e..k..H.....F..G:..6.G.I=.Y.....:...C.....?[.ts...=....;.|...q...@....s..... ....

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storei

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	0.7532185028349225
Encrypted:	false
SSDEEP:	48:CMnfnO4FGtsFqN6t8nlztZKR6axR6uiozVb:ZnfO4kWKpZKdxR35
MD5:	520FE964934AF1AB0CEBA2366830D0FA
SHA1:	B90310ACA870261CB619FDFD1E54E1B1A25074FF
SHA-256:	DBD45EEA386D364B30BA189E079BFA05C2C40D9E5E83722C39A171998ED079C1
SHA-512:	A4839A6AB8DB522D9121A590B8C711E8C4F172D9CB71C918860F8048472920F3341B7BA624DFF514BE397809149E4471B2DF981DC81FE77C26B2DDF342A42F8(
Malicious:	false

Preview:	...W....K.h.E..g..0...!1sm.[t\.....A.....5_....N{Yf?.w..[.Y..A...a^..(._.=.....:.v.$*.....e...F....f.qo.]...B1{.8.%%...;.|..<....g ....I.7.`ny.h.n.y...~Y.../.. .WZ.'.....AI.|.._K}-$.i..<(.7Y.. .U....T.i.N.'Pt..c.[.....<zni.::. 8W.<S...8!.Wh..;T.?.^yf...E?...pQ....i.;>/..^...r.YsncP..@.. .["..^..A.|.0..$<bC.G.....~];..D.|.v.B.).g.E5.?... .N...}....i.,5..a.Fk.%.u.`..F...;xlw.}. 5.Jt..c.5.....v...~)..8b|.*.B.]-]jk....PQZ..T}..M.S...88.....?.*$..]..%V..D.<.5.d...[..Z.....2.....%.$E..+sb.....*...g...>Q[l.}.....@=..5L..._....Pi..HY.<[..I...H....9.\=u.v.....S8-&...,5..}t.. ....m...*..R.W.G.NZ....w.....{.iA.....G.f.TN.zk..(....q).....n....3..C...d./..... .....

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.479760646202031
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHoljpl0QelMWFlc2VbiVllln:vdsCkWt51p2tvHV6/l
MD5:	0ACDE4A3C820A366AC6C0AB821A72207
SHA1:	B6551E86B60D095E74D4F79B6B004D40FDA4BA72
SHA-256:	3F3701E84757747159396FB41AD88E0E51084F846EB8007A2FAEAC15CE9DBF2C
SHA-512:	CB974D0C6CFE9B9AF015DD9D92B8110FC9AFE7EEA9A8C03ECF9112F6EA642DBE5FE9531E39B5B52EAADE7FEBAF6C17E4DD92AF5841476BECEA8E8789E19C2FB0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

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):	299979
Entropy (8bit):	7.926593256630463
Encrypted:	false
SSDEEP:	6144:PYa6J+5gUNlG+sCfq3V++iY3aub8kFiLGG9qFP2ipkHj3DR7gy7y:PYDghNESPX3ZZq9q1b6DRc
MD5:	7DE990046A20E6666627273589B014A5
SHA1:	55EBCCD35C2329C5816CD0240B0919651AC58321
SHA-256:	EBCE15AD53B98D7ABA7F7544EE947E88F58D696E22CA4BC5D15B2DED37B577AC
SHA-512:	850914621B366494BBA2A64AEF1B3DF7C619C7E6BB321A67BC1A1A97BD0182118A1E5648EE48D24449E6341AB7F7989369797114FA521DB8C26CCD5EB3386A4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L.....Oa.....h...*.....@6.....@.....@..... .....text...vf.....h..... ..`.rdata.....l.....@..@.data...x.....@....ndata.....rsrc.....@..@..... ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Sun Mar 19 16:31:33 2023, Security: 0
Entropy (8bit):	7.7704162920128015
TrID:	• Microsoft PowerPoint document (31509/1) 33.51% • Microsoft Excel sheet (30009/1) 31.91% • Microsoft Excel sheet (alternate) (24509/1) 26.06% • Generic OLE2 / Multistream Compound File (8008/1) 8.52%
File name:	d0#U10dc.xls
File size:	1150464
MD5:	4f1aac12084426a909da47a49cf59193
SHA1:	2eaf1072958ea81e87c86b5ec7a63228d623854b
SHA256:	b861cc02ce6ad439e78219a4a0c154188de055794950d3e5d7fc51178f72971c
SHA512:	c2d2716d2c52ed75d9770353a3e9c15c12cbf546074909a81b9e9c56576aace47a7f84f288c6ff37fb0101a0bdd1ca7fbcc65f1782af1196940a2cb26918d4e3
SSDEEP:	24576:GLKkWQmmav30xL+MXUu9uGO+MXUu9c3bV/+MXUu9T3bVOZDNSq3mN1Ezh:GLK5QmmQ30x+MXV9++MXV9c3bV/+MXVc
TLSH:	3E350213E9C48D46D44247F96AE3B9C9131EBC227BD6A2C72748770F6F786E48A4710E

File Content Preview:	.....>.....u...v.....u.....w.....y.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "d0#U10dc.xls"

Indicators

Has Summary Info:	
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Summary

Code Page:	1252
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2023-03-19 16:31:33
Creating Application:	
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General

Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375192737
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 244

General

Stream Path:	\x5DocumentSummaryInformation

General	
File Type:	data
Stream Size:	244
Entropy:	2.889430592781307
Base64 Encoded:	False
Data ASCII:	. . . . + , 0 . . . . H . . . . P . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . W o r k s h e e t s . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 a1 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 200

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	200
Entropy:	3.244624082366348
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . + ' 0 . . . . @ . . . . H . . . . T . . . . ` . . . . x . . . . M i c r o s o f t E x c e l . @ . . . . | . # . @ . . .) D Z . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: MBD00A59CF0/\x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	MBD00A59CF0/\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.695694018334962
Base64 Encoded:	False
Data ASCII:	. . . . . . L u d @ K g 2 . . . . . . M i c r o s o f t O f f i c e W o r d D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 1 2 . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 9b 4c 75 f4 f5 64 40 4b 8a f4 67 97 32 ac 06 07 1f 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 57 6f 72 64 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 11 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 31 32 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF0/\x1Ole, File Type: data, Stream Size: 62

General	
Stream Path:	MBD00A59CF0/\x1Ole
File Type:	data
Stream Size:	62
Entropy:	2.7788384466112834
Base64 Encoded:	False
Data ASCII:	. . . . F . . . . ! . . . . . S h e e t 2 ! O b j e c t 5 .
Data Raw:	01 00 00 02 08 00 00 00 00 00 00 00 00 00 00 00 2e 00 00 00 04 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 02 00 00 00 21 00 10 00 00 00 53 68 65 65 74 32 21 4f 62 6a 65 63 74 20 35 00

Stream Path: MBD00A59CF0/Package, File Type: Microsoft Word 2007+, Stream Size: 66096

General	
Stream Path:	MBD00A59CF0/Package
File Type:	Microsoft Word 2007+
Stream Size:	66096
Entropy:	7.6673327627733885
Base64 Encoded:	True
Data ASCII:	P K . . . . ! . . . u s . . . T . . . . [C o n t e n t _ T y p e s] . x m l . . (. . . .
Data Raw:	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 1e 19 ef 75 73 01 00 00 54 05 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF1/\x1CompObj, File Type: data, Stream Size: 93

General	
Stream Path:	MBD00A59CF1/\x1CompObj
File Type:	data
Stream Size:	93
Entropy:	4.2892020709435155
Base64 Encoded:	False
Data ASCII:	. . . . . e . . D E S T . . . . . A c r o b a t D o c u m e n t . . . . . A c r o b a t . D o c u m e n t . D C . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 65 ca 01 b8 fc a1 d0 11 85 ad 44 45 53 54 00 00 11 00 00 00 41 63 72 6f 62 61 74 20 44 6f 63 75 6d 65 6e 74 00 00 00 00 00 14 00 00 00 41 63 72 6f 62 61 74 2e 44 6f 63 75 6d 65 6e 74 2e 44 43 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF1/\x1Ole, File Type: data, Stream Size: 62	
General	
Stream Path:	MBD00A59CF1/\x1Ole
File Type:	data
Stream Size:	62
Entropy:	2.7788384466112834
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . ! . . . . . S h e e t 2 ! O b j e c t 4 .
Data Raw:	01 00 00 02 08 00 00 00 00 00 00 00 00 00 00 00 2e 00 00 00 04 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 02 00 00 00 21 00 10 00 00 00 53 68 65 65 74 32 21 4f 62 6a 65 63 74 20 34 00

Stream Path: MBD00A59CF1/CONTENTS, File Type: PDF document, version 1.7, 1 pages, Stream Size: 141190	
General	
Stream Path:	MBD00A59CF1/CONTENTS
File Type:	PDF document, version 1.7, 1 pages
Stream Size:	141190
Entropy:	7.918921120478072
Base64 Encoded:	True
Data ASCII:	% P D F - 1 . 7 . % . . 1 0 o b j . . < < / O u t l i n e s 5 0 R . . / P a g e s 2 0 R . . / N a m e s < < / D e s t s 4 0 R . . > > . . / T y p e / C a t a l o g . . > > . . e n d o b j . . 2 0 o b j . . < < / C o u n t 1 . . / K i d s [6 0 R] . . / T y p e / P a g e s . . > > . . e n d o b j . . 3 0 o b j . . < < / C r e a t i o n D a t e (D : 2 0 2 2 0 7 0 1 1 0 0 4 1 7 + 0 2 ' 0 4 ') . . / M o d D a t e (D : 2 0 2 2 0 9 2 6 1 9 4 4 0 7 + 0 8 ' 0 0 '
Data Raw:	25 50 44 46 2d 31 2e 37 0d 25 e2 e3 cf d3 0d 0a 31 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 4f 75 74 6c 69 6e 65 73 20 35 20 30 20 52 0d 0a 2f 50 61 67 65 73 20 32 20 30 20 52 0d 0a 2f 4e 61 6d 65 73 20 3c 3c 2f 44 65 73 74 73 20 34 20 30 20 52 0d 0a 3e 3e 0d 0a 2f 54 79 70 65 20 2f 43 61 74 61 6c 6f 67 0d 0a 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 32 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 43 6f 75

Stream Path: MBD00A59CF2/\x1CompObj, File Type: data, Stream Size: 93	
General	
Stream Path:	MBD00A59CF2/\x1CompObj
File Type:	data
Stream Size:	93
Entropy:	4.2892020709435155
Base64 Encoded:	False
Data ASCII:	. . . . . e . . D E S T . . . . . A c r o b a t D o c u m e n t . . . . . A c r o b a t . D o c u m e n t . D C . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 65 ca 01 b8 fc a1 d0 11 85 ad 44 45 53 54 00 00 11 00 00 00 41 63 72 6f 62 61 74 20 44 6f 63 75 6d 65 6e 74 00 00 00 00 00 14 00 00 00 41 63 72 6f 62 61 74 2e 44 6f 63 75 6d 65 6e 74 2e 44 43 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF2/\x1Ole, File Type: data, Stream Size: 62	
General	
Stream Path:	MBD00A59CF2/\x1Ole
File Type:	data
Stream Size:	62
Entropy:	2.7788384466112834
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . ! . . . . . S h e e t 2 ! O b j e c t 3 .
Data Raw:	01 00 00 02 08 00 00 00 00 00 00 00 00 00 00 00 2e 00 00 00 04 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 02 00 00 00 21 00 10 00 00 00 53 68 65 65 74 32 21 4f 62 6a 65 63 74 20 33 00

Stream Path: MBD00A59CF2/CONTENTS, File Type: PDF document, version 1.7, 1 pages, Stream Size: 62293	
General	
Stream Path:	MBD00A59CF2/CONTENTS
File Type:	PDF document, version 1.7, 1 pages
Stream Size:	62293
Entropy:	7.949249248462166

General	
Base64 Encoded:	True
Data ASCII:	%PDF-1.7 .% .1 0 obj .<< ./Type /Catalog ./Pages 2 0 R ./PageMode /UseNone ./ViewerPreferences << ./FitWindow true ./PageLayout /SinglePage ./NonFullScreenPageMode /UseNone .> > .>> .endobj .5 0 obj .<< ./Length 1272 ./Filter [/FlateDecode] .>> .stream.xX
Data Raw:	25 50 44 46 2d 31 2e 37 20 0a 25 e2 e3 cf d3 20 0a 31 20 30 20 6f 62 6a 20 0a 3c 3c 20 0a 2f 54 79 70 65 20 2f 43 61 74 61 6c 6f 67 20 0a 2f 50 61 67 65 73 20 32 20 30 20 52 20 0a 2f 50 61 67 65 4d 6f 64 65 20 2f 55 73 65 4e 6f 6e 65 20 0a 2f 56 69 65 77 65 72 50 72 65 66 65 72 65 6e 63 65 73 20 3c 3c 20 0a 2f 46 69 74 57 69 6e 64 6f 77 20 74 72 75 65 20 0a 2f 50 61 67 65 4c 61 79

Stream Path: MBD00A59CF3/\x1CompObj, File Type: data, Stream Size: 93	
General	
Stream Path:	MBD00A59CF3/\x1CompObj
File Type:	data
Stream Size:	93
Entropy:	4.2892020709435155
Base64 Encoded:	False
Data ASCII:	......e..DEST......Acrobat Document.........Acrobat.Document.DC.9q.....
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 65 ca 01 b8 fc a1 d0 11 85 ad 44 45 53 54 00 00 11 00 00 00 41 63 72 6f 62 61 74 20 44 6f 63 75 6d 65 6e 74 00 00 00 00 00 14 00 00 00 41 63 72 6f 62 61 74 2e 44 6f 63 75 6d 65 6e 74 2e 44 43 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF3/\x1Ole, File Type: data, Stream Size: 62	
General	
Stream Path:	MBD00A59CF3/\x1Ole
File Type:	data
Stream Size:	62
Entropy:	2.746580382095154
Base64 Encoded:	False
Data ASCII:	.....F....!.....Sheet2!Object 2.
Data Raw:	01 00 00 02 08 00 00 00 00 00 00 00 00 00 00 00 2e 00 00 00 04 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 02 00 00 00 21 00 10 00 00 00 53 68 65 65 74 32 21 4f 62 6a 65 63 74 20 32 00

Stream Path: MBD00A59CF3/CONTENTS, File Type: PDF document, version 1.4, 1 pages, Stream Size: 78265	
General	
Stream Path:	MBD00A59CF3/CONTENTS
File Type:	PDF document, version 1.4, 1 pages
Stream Size:	78265
Entropy:	7.977302175246816
Base64 Encoded:	True
Data ASCII:	%PDF-1.4.%.1 0 obj.<<./CreationDate(D:20230316104232+00'00')./Creator(PDFsharp 1.50.5147 \\(www.pdfsharp.com\\)).Producer(PDFsharp 1.50.5147 \\(www.pdfsharp.com\\)).>>.endobj.20 obj.<<./Type/Catalog./Pages 3 0 R.>>.endobj.3 0 obj.<<./Type/Pages./Count 1./Kid
Data Raw:	25 50 44 46 2d 31 2e 34 0a 25 d3 f4 cc e1 0a 31 20 30 20 6f 62 6a 0a 3c 3c 0a 2f 43 72 65 61 74 69 6f 6e 44 61 74 65 28 44 3a 32 30 32 33 30 33 31 36 31 30 34 32 33 32 2b 30 30 27 30 30 27 29 0a 2f 43 72 65 61 74 6f 72 28 50 44 46 73 68 61 72 70 20 31 2e 35 30 2e 35 31 34 37 20 5c 28 77 77 77 2e 70 64 66 73 68 61 72 70 2e 63 6f 6d 5c 29 29 0a 2f 50 72 6f 64 75 63 65 72 28 50 44 46

Stream Path: MBD00A59CF4/\x1CompObj, File Type: data, Stream Size: 114	
General	
Stream Path:	MBD00A59CF4/\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.219515110876372
Base64 Encoded:	False
Data ASCII:	......0.....F!...Microsoft Office Excel Worksheet.....ExcelML12.....Excel.Sheet.12.9q.....
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 30 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 21 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 57 6f 72 6b 73 68 65 65 74 00 0a 00 00 00 45 78 63 65 6c 4d 4c 31 32 00 0f 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 31 32 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF4/Package, File Type: Microsoft Excel 2007+, Stream Size: 45183	
General	
Stream Path:	MBD00A59CF4/Package
File Type:	Microsoft Excel 2007+
Stream Size:	45183
Entropy:	7.806319843953119
Base64 Encoded:	True

General	
Data ASCII:	P K . . . . ! . < r . . . i . . . . . . [C o n t e n t _ T y p e s] . x m l . (. . . .
Data Raw:	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 3c 72 e1 d1 db 01 00 00 69 08 00 00 13 00 db 01 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 d7 01 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF5/\x1CompObj, File Type: data, Stream Size: 93	
General	
Stream Path:	MBD00A59CF5/\x1CompObj
File Type:	data
Stream Size:	93
Entropy:	4.2892020709435155
Base64 Encoded:	False
Data ASCII:	. . . . . . e . . D E S T . . . . . . A c r o b a t D o c u m e n t . . . . A c r o b a t . D o c u m e n t . D C . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 65 ca 01 b8 fc a1 d0 11 85 ad 44 45 53 54 00 00 11 00 00 00 41 63 72 6f 62 61 74 20 44 6f 63 75 6d 65 6e 74 00 00 00 00 00 14 00 00 00 41 63 72 6f 62 61 74 2e 44 6f 63 75 6d 65 6e 74 2e 44 43 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF5/\x1Ole, File Type: data, Stream Size: 64	
General	
Stream Path:	MBD00A59CF5/\x1Ole
File Type:	data
Stream Size:	64
Entropy:	2.892622069467395
Base64 Encoded:	False
Data ASCII:	. . . . 0 . . . . F . . . . ! . . . . . S h e e t 1 ! O b j e c t 5 3 1 .
Data Raw:	01 00 00 02 08 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 04 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 46 02 00 00 00 21 00 12 00 00 00 53 68 65 65 74 31 21 4f 62 6a 65 63 74 20 35 33 31 00

Stream Path: MBD00A59CF5/CONTENTS, File Type: PDF document, version 1.4, 1 pages, Stream Size: 78265	
General	
Stream Path:	MBD00A59CF5/CONTENTS
File Type:	PDF document, version 1.4, 1 pages
Stream Size:	78265
Entropy:	7.977302175246816
Base64 Encoded:	True
Data ASCII:	% P D F - 1 . 4 . % . 1 0 o b j . < < . / C r e a t i o n D a t e (D : 2 0 2 3 0 3 1 6 1 0 4 2 3 2 + 0 0 ' 0 0 ') . / C r e a t o r (P D F s h a r p 1 . 5 0 . 5 1 4 7 \\ (w w w . p d f s h a r p . c o m \\ )) . / P r o d u c e r (P D F s h a r p 1 . 5 0 . 5 1 4 7 \\ (w w w . p d f s h a r p . c o m \\ )) . > > . e n d o b j . 2 0 o b j . < < . / T y p e / C a t a l o g . / P a g e s 3 0 R . > > . e n d o b j . 3 0 o b j . < < . / T y p e / P a g e s . / C o u n t 1 . / K i d
Data Raw:	25 50 44 46 2d 31 2e 34 0a 25 d3 f4 cc e1 0a 31 20 30 20 6f 62 6a 0a 3c 3c 0a 2f 43 72 65 61 74 69 6f 6e 44 61 74 65 28 44 3a 32 30 32 33 30 33 31 36 31 30 34 32 33 32 2b 30 30 27 30 30 27 29 0a 2f 43 72 65 61 74 6f 72 28 50 44 46 73 68 61 72 70 20 31 2e 35 30 2e 35 31 34 37 20 5c 28 77 77 77 2e 70 64 66 73 68 61 72 70 2e 63 6f 6d 5c 29 29 0a 2f 50 72 6f 64 75 63 65 72 28 50 44 46

Stream Path: MBD00A59CF6/\x1CompObj, File Type: data, Stream Size: 114	
General	
Stream Path:	MBD00A59CF6/\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375192737
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF6/\x5DocumentSummaryInformation, File Type: data, Stream Size: 708	
General	
Stream Path:	MBD00A59CF6/\x5DocumentSummaryInformation
File Type:	data
Stream Size:	708
Entropy:	3.6235698530352805
Base64 Encoded:	True

General	
Data ASCII:	. . . . + , D . . . . + , ... (. . . . . . . 0 . . . . 8 . . . . @ . . . . H . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 44 00 00 00 05 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 20 02 00 00 dc 01 00 00 14 00 00 00 01 00 00 00 a8 00 00 00 02 00 00 00 b0 00 00 00 03 00 00 00 bc 00 00 00 0e 00 00 00 c8 00 00 00 0f 00 00 00 d4 00 00 00 04 00 00 00 e0 00 00 00 05 00 00 00

Stream Path: MBD00A59CF6/\x5SummaryInformation, File Type: data, Stream Size: 372	
General	
Stream Path:	MBD00A59CF6/\x5SummaryInformation
File Type:	data
Stream Size:	372
Entropy:	2.888140576289789
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . + ' 0 . . . D . . . . $ . . . . . . , ... 4 . . . . < . . . . v i v i e n 9 1
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 44 01 00 00 10 00 00 00 01 00 00 00 88 00 00 00 02 00 00 00 90 00 00 00 03 00 00 00 9c 00 00 00 04 00 00 00 a8 00 00 00 05 00 00 00 b8 00 00 00 06 00 00 00 c4 00 00 00 07 00 00 00 d0 00 00 00 08 00 00 00 dc 00 00 00 09 00 00 00 ec 00 00 00

Stream Path: MBD00A59CF6/Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 97808	
General	
Stream Path:	MBD00A59CF6/Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	97808
Entropy:	7.364561215625775
Base64 Encoded:	True
Data ASCII:	. . . . \\ . p . . . . 9 1 9 7 4 B . . . . a . . . . = ... = ... P . 9 . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 a9 1f cd 07 c1 00 01 00 06 04 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 39 31 39 37 34 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 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

Stream Path: MBD00A59CF6/_VBA_PROJECT_CUR/VBA/Sheet1, File Type: empty, Stream Size: 0	
General	
Stream Path:	MBD00A59CF6/_VBA_PROJECT_CUR/VBA/Sheet1
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: MBD00A59CF6/_VBA_PROJECT_CUR/VBA/ThisWorkbook, File Type: empty, Stream Size: 0	
General	
Stream Path:	MBD00A59CF6/_VBA_PROJECT_CUR/VBA/ThisWorkbook
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: MBD00A59CF6/_VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: empty, Stream Size: 0	
General	
Stream Path:	MBD00A59CF6/_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: MBD00A59CF7/\x1CompObj, File Type: data, Stream Size: 93	
General	
Stream Path:	MBD00A59CF7/\x1CompObj
File Type:	data
Stream Size:	93
Entropy:	4.2892020709435155
Base64 Encoded:	False
Data ASCII:	. . . . . e . . D E S T . . . . . A c r o b a t D o c u m e n t . . . . . A c r o b a t . D o c u m e n t . D C . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 65 ca 01 b8 fc a1 d0 11 85 ad 44 45 53 54 00 00 11 00 00 00 41 63 72 6f 62 61 74 20 44 6f 63 75 6d 65 6e 74 00 00 00 00 00 00 14 00 00 00 41 63 72 6f 62 61 74 2e 44 6f 63 75 6d 65 6e 74 2e 44 43 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF7/\x1Ole, File Type: data, Stream Size: 64	
General	
Stream Path:	MBD00A59CF7/\x1Ole
File Type:	data
Stream Size:	64
Entropy:	2.892622069467395
Base64 Encoded:	False
Data ASCII:	. . . . . 0 . . . . . F . . . . ! . . . . . S h e e t 1 ! O b j e c t 5 3 1 .
Data Raw:	01 00 00 02 08 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 04 03 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 02 00 00 00 21 00 12 00 00 00 53 68 65 65 74 31 21 4f 62 6a 65 63 74 20 35 33 31 00

Stream Path: MBD00A59CF7/CONTENTS, File Type: PDF document, version 1.4, 1 pages, Stream Size: 78265	
General	
Stream Path:	MBD00A59CF7/CONTENTS
File Type:	PDF document, version 1.4, 1 pages
Stream Size:	78265
Entropy:	7.977302175246816
Base64 Encoded:	True
Data ASCII:	% P D F - 1 . 4 . % . 1 0 o b j . < < . / C r e a t i o n D a t e (D : 2 0 2 3 0 3 1 6 1 0 4 2 3 2 + 0 0 ' 0 0 ') . / C r e a t o r (P D F s h a r p 1 . 5 0 . 5 1 4 7 \ \ (w w w . p d f s h a r p . c o m \ \ )) . / P r o d u c e r (P D F s h a r p 1 . 5 0 . 5 1 4 7 \ \ (w w w . p d f s h a r p . c o m \ \ )) . > > . e n d o b j . 2 0 o b j . < < . / T y p e / C a t a l o g . / P a g e s 3 0 R . > > . e n d o b j . 3 0 o b j . < < . / T y p e / P a g e s . / C o u n t 1 . / K i d
Data Raw:	25 50 44 46 2d 31 2e 34 0a 25 d3 f4 cc e1 0a 31 20 30 20 6f 62 6a 0a 3c 3c 0a 2f 43 72 65 61 74 69 6f 6e 44 61 74 65 28 44 3a 32 30 32 33 30 33 31 36 31 30 34 32 33 32 2b 30 30 27 30 30 27 29 0a 2f 43 72 65 61 74 6f 72 28 50 44 46 73 68 61 72 70 20 31 2e 35 30 2e 35 31 34 37 20 5c 28 77 77 77 2e 70 64 66 73 68 61 72 70 2e 63 6f 6d 5c 29 29 0a 2f 50 72 6f 64 75 63 65 72 28 50 44 46

Stream Path: MBD00A59CF8/\x1CompObj, File Type: data, Stream Size: 114	
General	
Stream Path:	MBD00A59CF8/\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375192737
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00A59CF8/\x5DocumentSummaryInformation, File Type: data, Stream Size: 708	
General	
Stream Path:	MBD00A59CF8/\x5DocumentSummaryInformation
File Type:	data
Stream Size:	708
Entropy:	3.6235698530352805
Base64 Encoded:	True
Data ASCII:	. . . . . + , D . . . . . + , ... (. . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 44 00 00 00 05 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 20 02 00 00 dc 01 00 00 14 00 00 00 01 00 00 00 a8 00 00 00 02 00 00 00 b0 00 00 00 03 00 00 00 bc 00 00 00 0e 00 00 00 c8 00 00 00 0f 00 00 00 d4 00 00 00 04 00 00 00 e0 00 00 00 05 00 00 00

Stream Path: MBD00A59CF8/\x5SummaryInformation, File Type: data, Stream Size: 372

General	
Stream Path:	MBD00A59CF8/\x5SummaryInformation
File Type:	data
Stream Size:	372
Entropy:	2.893869802613578
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . + ' 0 . . . D . . . . $ . . . . . . , ... 4 . . . . < . . . . v i v i e n 9 1
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 44 01 00 00 10 00 00 00 01 00 00 00 88 00 00 00 02 00 00 00 90 00 00 00 03 00 00 00 9c 00 00 00 04 00 00 00 a8 00 00 00 05 00 00 00 b8 00 00 00 06 00 00 00 c4 00 00 00 07 00 00 00 d0 00 00 00 08 00 00 00 dc 00 00 00 09 00 00 00 ec 00 00 00

Stream Path: MBD00A59CF8/Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 97808	
General	
Stream Path:	MBD00A59CF8/Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	97808
Entropy:	7.364373955658336
Base64 Encoded:	True
Data ASCII:	. . . . \\ . p . . . . 9 1 9 7 4 B . . . . a . . . . = ... = ... P . 9 . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 a9 1f cd 07 c9 00 02 00 06 04 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 39 31 39 37 34 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 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

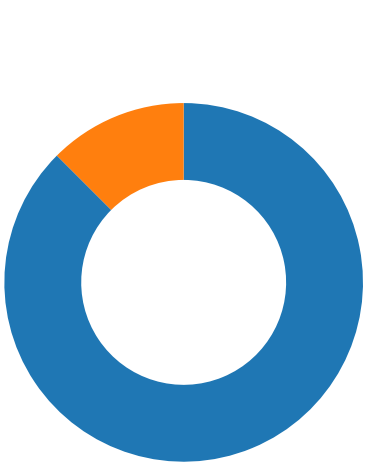
Stream Path: MBD00A59CF8/_VBA_PROJECT_CUR/VBA/Sheet1, File Type: empty, Stream Size: 0	
General	
Stream Path:	MBD00A59CF8/_VBA_PROJECT_CUR/VBA/Sheet1
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: MBD00A59CF8/_VBA_PROJECT_CUR/VBA/ThisWorkbook, File Type: empty, Stream Size: 0	
General	
Stream Path:	MBD00A59CF8/_VBA_PROJECT_CUR/VBA/ThisWorkbook
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: MBD00A59CF8/_VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: empty, Stream Size: 0	
General	
Stream Path:	MBD00A59CF8/_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 10:33:34.996516943 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.192823887 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.192950010 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.193614960 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.391124010 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.391180992 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.391227007 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.391247988 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.391272068 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.392350912 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.587097883 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.587151051 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.587300062 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.587953091 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.587989092 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.588020086 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.588051081 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.588069916 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.588093996 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.588114977 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.588129044 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.588180065 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.588247061 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.588320971 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.783282042 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.783312082 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.783332109 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.783355951 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.783430099 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.783431053 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.783792019 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.783818007 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.783839941 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.783855915 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.783868074 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.783906937 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.784305096 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.784334898 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.784357071 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.784377098 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.784396887 CET	80	49171	103.189.202.84	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 10:33:35.784444094 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.784542084 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.786840916 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.786881924 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.786911964 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.786950111 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.787065983 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.789401054 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.978729963 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.978760004 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.978779078 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.978800058 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.978830099 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.978854895 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.978873968 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.978898048 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.978898048 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.978924036 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.978950977 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.978965044 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.978997946 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.979630947 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.979737997 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980140924 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980161905 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980180979 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980206013 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980215073 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980226994 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980238914 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980252981 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980272055 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980289936 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980300903 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980310917 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980330944 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980341911 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980360985 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980370998 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980389118 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980401039 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980415106 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980427027 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980443954 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980463982 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980477095 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980484962 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980511904 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980520964 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980545998 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980559111 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980581999 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980592966 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980611086 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.980632067 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.980654001 CET	49171	80	192.168.2.22	103.189.202.84
Mar 20, 2023 10:33:35.982675076 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.982728004 CET	80	49171	103.189.202.84	192.168.2.22
Mar 20, 2023 10:33:35.982748032 CET	80	49171	103.189.202.84	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 10:33:38.322930098 CET	138	138	192.168.2.22	192.168.2.255
Mar 20, 2023 10:33:56.466960907 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:33:57.216228008 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:33:57.966264009 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:05.500899076 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:06.250477076 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:07.000554085 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:08.269311905 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:09.018851042 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:09.768990040 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:32.531739950 CET	54408	53	192.168.2.22	8.8.8.8
Mar 20, 2023 10:34:32.551840067 CET	53	54408	8.8.8.8	192.168.2.22
Mar 20, 2023 10:34:37.964605093 CET	50108	53	192.168.2.22	8.8.8.8
Mar 20, 2023 10:34:37.982831001 CET	53	50108	8.8.8.8	192.168.2.22
Mar 20, 2023 10:34:45.754302979 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:46.504328966 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:47.254437923 CET	137	137	192.168.2.22	192.168.2.255
Mar 20, 2023 10:34:53.680862904 CET	54723	53	192.168.2.22	8.8.8.8
Mar 20, 2023 10:34:53.700793028 CET	53	54723	8.8.8.8	192.168.2.22
Mar 20, 2023 10:35:03.932585001 CET	58062	53	192.168.2.22	8.8.8.8
Mar 20, 2023 10:35:04.944813013 CET	58062	53	192.168.2.22	8.8.8.8
Mar 20, 2023 10:35:04.964967012 CET	53	58062	8.8.8.8	192.168.2.22
Mar 20, 2023 10:35:05.968266964 CET	53	58062	8.8.8.8	192.168.2.22
Mar 20, 2023 10:35:09.961920023 CET	138	138	192.168.2.22	192.168.2.255
Mar 20, 2023 10:35:22.396008968 CET	56703	53	192.168.2.22	8.8.8.8
Mar 20, 2023 10:35:22.417706013 CET	53	56703	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Mar 20, 2023 10:35:05.968422890 CET	192.168.2.22	8.8.8.8	d01c	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 10:34:32.531739950 CET	192.168.2.22	8.8.8.8	0x2f5f	Standard query (0)	www.white-hat.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 10:34:37.964605093 CET	192.168.2.22	8.8.8.8	0x9912	Standard query (0)	www.sqlite.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 10:34:53.680862904 CET	192.168.2.22	8.8.8.8	0xceee	Standard query (0)	www.gritslab.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 10:35:03.932585001 CET	192.168.2.22	8.8.8.8	0xc4a9	Standard query (0)	www.bitservicesltd.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 10:35:04.944813013 CET	192.168.2.22	8.8.8.8	0xc4a9	Standard query (0)	www.bitservicesltd.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 10:35:22.396008968 CET	192.168.2.22	8.8.8.8	0x1666	Standard query (0)	www.222ambking.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 10:34:32.551840067 CET	8.8.8.8	192.168.2.22	0x2f5f	No error (0)	www.white-hat.uk	white-hat.uk		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 10:34:32.551840067 CET	8.8.8.8	192.168.2.22	0x2f5f	No error (0)	white-hat.uk		94.176.104.86	A (IP address)	IN (0x0001)	false
Mar 20, 2023 10:34:37.982831001 CET	8.8.8.8	192.168.2.22	0x9912	No error (0)	www.sqlite.org		45.33.6.223	A (IP address)	IN (0x0001)	false

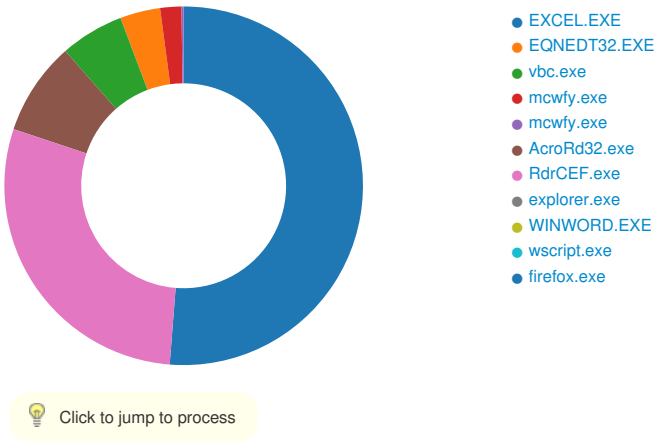
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 10:34:53.700793028 CET	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.gritslab.com	gritslab.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 10:34:53.700793028 CET	8.8.8.8	192.168.2.22	0xceee	No error (0)	gritslab.com		78.141.192.145	A (IP address)	IN (0x0001)	false
Mar 20, 2023 10:35:04.964967012 CET	8.8.8.8	192.168.2.22	0xc4a9	No error (0)	www.bitservicesltd.com		161.97.163.8	A (IP address)	IN (0x0001)	false
Mar 20, 2023 10:35:05.968266964 CET	8.8.8.8	192.168.2.22	0xc4a9	No error (0)	www.bitservicesltd.com		161.97.163.8	A (IP address)	IN (0x0001)	false
Mar 20, 2023 10:35:22.417706013 CET	8.8.8.8	192.168.2.22	0x1666	No error (0)	www.222ambking.org		91.195.240.94	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 103.189.202.84
- www.white-hat.uk
- www.sqlite.org
- www.gritslab.com
- www.bitservicesltd.com

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **1236**, Parent PID: **576**

General

Target ID:	0
Start time:	10:32:22

Start date:	20/03/2023
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:	0x13f120000
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

Analysis Process: EQNEDT32.EXE PID: **544**, Parent PID: **576**

General

Target ID:	2
Start time:	10:32:44
Start date:	20/03/2023
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	35B064A	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	35B064A	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	35B064A	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	35B064A	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	35B064A	URLDownloadToFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	35B064A	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	35B064A	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	35B064A	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	35B064A	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	35B064A	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	0	694	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 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 50 45 00 00 4c 01 05 00 1f fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOah*	success or wait	1	35B064A	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\vbc[1].exe	694	4120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	35B064A	URLDownloadToFileW
C:\Users\Public\vbc.exe	0	4814	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 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 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 50 45 00 00 4c 01 05 00 1f fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOah*	success or wait	1	35B064A	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\vbc[1].exe	6100	8192	09 6a 22 fd fd 09 00 00 fd fd 6a fd fd fd 09 00 00 50 53 57 56 fd 15 4c fd 40 00 fd fd fd fd fd fd 10 fd 40 00 6a 01 fd 45 08 fd 09 00 00 6a 12 fd fd fd 09 00 00 6a 49 45 fd fd 09 00 00 50 68 fd 03 00 00 fd 45 08 57 50 fd 75 fd 56 fd 15 50 fd 40 00 66 fd 3f 0a fd 1d fd fd fd 39 5d fd fd 75 fd 75 2b 6a 02 fd 09 00 00 fd fd 3b fd 0f fd fd 04 00 00 6a 33 fd 52 09 00 00 50 56 fd 15 14 fd 40 00 56 fd fd fd 15 10 fd 40 00 fd 16 6a 22 fd 38 09 00 00 fd 4d fd fd fd 51 50 56 fd fd 09 00 00 fd fd 3b fd 0f fd fd 07 00 00 fd 04 00 00 fd 75 fd fd fd fd 45 fd 6a 02 fd 45 fd fd 0a 09 00 00 6a 11 fd 45 fd fd 00 09 00 00 6a 02 50 57 fd 45 fd 01 00 00 00 fd 09 00 00 3b c9 45 08 0f fd 69 07 00 00 33 fd fd fd 01 fd fd fd 40 00 75 11 6a 23 fd fd 08 00	j"jPSWVL@@jEjjEPhEWPuVP@f?9]uu+j;j3RPV@V@j"8MQPV;uEjEjEjPWE;Ei3@uj#	success or wait	38	35B064A	URLDownloadToFileW
C:\Users\Public\vbc.exe	4814	10288	68 fd fd 40 00 fd 15 58 fd 40 00 fd 5a 07 00 00 53 fd 0e 00 00 6a 01 fd fd fd 55 fd fd 0e 00 00 39 5d fd 59 59 fd 55 fd 50 56 75 0b fd 15 50 fd 40 00 fd 23 0d 00 00 fd 15 78 fd 40 00 fd 18 0d 00 00 53 fd 0e 00 00 6a 31 fd fd fd 0e 00 00 6a 22 fd fd fd 7c 0e 00 00 6a 15 fd fd fd 73 0e 00 00 6a fd fd fd fd fd fd fd 45 fd fd fd 78 fd fd fd fd 45 fd fd fd 7c fd fd fd fd 45 09 45 fd 66 fd 06 66 fd fd 1b fd fd 5d fd 23 89 45 fd 66 fd 07 66 fd fd 1b fd fd 45 fd 00 60 43 00 23 c9 45 fd fd fd 74 fd fd fd 50 fd 0c 3d 00 00 fd fd 0f fd fd 09 00 00 fd fd 78 fd fd fd 40 0f fd fd 0c 00 00 fd 75 fd fd 41 4b 00 00 fd 75 fd fd 47 53 fd fd 0d 00 00 fd fd 56 6a fd fd 16 37 00 00 56 fd 3c 00 00 fd fd 3b fd 0f fd 6a 09 00 00 39 5d fd 74 21 56 fd 11 4b	h@X@ZSjU9]YYUPVuP@#x@Sj1j"|jsjExE|EEff]#EffE`C#EtP=x@uAKuGSVj7V<;j9]t!VK	success or wait	6	35B064A	URLDownloadToFileW
C:\Users\Public\vbc.exe	269730	30249	39 73 fd fd 5f 0c 7c fd 3f fd fd 02 fd 50 fd 24 fd 5d 4a 7e fd 02 fd fd fd 03 fd 0c 17 cf fd 06 60 fd 65 16 fd 33 0b f8 fd 01 fd 18 60 fd fd fd 03 fd 47 fd 2b 7f fd fd 18 fd 6b 20 5c fd 12 fd fd fd 40 fd fd 40 fd 6f fd fd bf 1b fd fd fd 09 fd fd fd fd fd fd 42 17 fd 3d fd fd 31 dc fd 21 43 48 4d fd 33 fd 48 fd fd 07 fd 78 fd fd 15 0c 6b 44 fd 0d 33 e7 2a fd 17 fd 5d 29 2a fd fd fd 42 46 63 fd 69 77 fd fd 10 63 6f 1b fd ba fd fd a0 76 fd fd fd fd fd fd 5c 70 51 03 6c fd 4d 4b 7e fd 6f 5a 17 4c fd 05 71 32 fd fd fd fd fd fd 12 fd 3f 7c 12 6c 2c fd fd 1c fd fd fd 57 fd 6d fd 37 13 fd 53 26 39 fd 59 fd 3f 3f 45 4c 15 1e 50 34 fd fd 14 6f fd 4f fd 69 79 2c fd 07 fd 3b fd fd 57 4a fd 33 2e fd fd 29 26 74 53 19 47 28	9_|?P$]J~`e3`G+k\@@oB=1!CHM3HxkD3*])*BFciwcov\pQlMK~oZLq2?|l,Wm7S&9Y??ELP4oOiy;WJ.&tSG(	success or wait	1	35B064A	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: **1928**, Parent PID: **544**

General

Target ID:	5
Start time:	10:32:49
Start date:	20/03/2023
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	299979 bytes
MD5 hash:	7DE990046A20E6666627273589B014A5
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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsl9C8D.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsl9C8E.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsl9C8F.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	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	405C22	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	405C22	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	405C22	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	405C22	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsl9C8F.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	405BE2	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	405C22	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	405C22	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	405C22	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	405C22	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\ortnkgsjk.g	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\ytljtt.f	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\mcwfy.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsl9C8D.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsl9C8F.tmp	success or wait	1	405DA3	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\nsl9C8E.tmp	0	32768	fd 41 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 03 00 00 00 fd 19 00 00 fd 00 00 00 fd 2d 00 00 00 00 00 00 fd 40 00 00 01 00 00 00 fd 41 00 00 00 00 00 00 00 00 00 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 48 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	A,-@AH	success or wait	18	406224	WriteFile
C:\Users\user\AppData\Local\Temp\ortnkgsjk.g	0	16384	13 fd fd 5e 1a 31 73 fd fd 45 1f fd fd 67 fd 00 30 23 59 49 fd 21 fd 44 67 1c 2c 24 13 4b fd fd c2 fd 03 fd fd 23 3e fd fd fd fd fd 08 69 fd fd 5e fd fd fd 26 fd f5 58 04 1e 7c fd fd 2c fd fd 16 5c 31 fd fd fd fd 65 fd 6f 09 35 fd 54 60 fd fd fd fd 3b fd fd 7f 3e fd 59 fd fd 6d fd 63 fd fd 20 fd fd 58 09 7d fd fd 6d 56 5f 0b 36 42 5d 44 fd fd fd 55 51 fd 48 7f 43 fd fd 12 03 10 fd 78 fd fd 3f 79 fd fd 60 0f 0f fd 60 fd fd fd 2a 0b 38 fd 06 fd 16 fd 15 4b 4c 7a fd 78 fd 6f 04 3b fd 7d 5a 7e 5d 76 fd 54 4f fd fd fd fd a4 fd fd fd fd fd 56 05 7b fd fd fd 2d fd 3e 69 5d fd fd 34 2d 65 fd fd e7 fd 1c fd 5b 6d 5e 42 78 fd 4e fd fd 54 21 fd 5b 0d 45 fd fd 79 56 44 fd 71 10 fd ff fd 1d fd 22 24 6d 1c fd 30 67 68 79 fd 5e 5c 0f 42	^1sEg0#YI!Dg,$K#>i^&X\| ,\1eo5T`;>Ymc X}mV_6B]DUQHCx? y``*8Kzxo;}Z~]vTOV{- >i]4-e[m^BxNT![EyVD q"$m0gy^\B	success or wait	13	406224	WriteFile
C:\Users\user\AppData\Local\Temp\ytljtt.f	0	5854	c6 30 30 35 6d fd fd 66 fd 46 3c fd 12 1b 30 35 6f fd 3a fd fd fd fd fd fd 3f 76 3e fd 33 fd 33 fd 3c fd 0c fd fd fd fd 4d fd 6b 6e 6c fd 30 32 61 fd fd 63 fd 45 3c fd 17 10 34 32 63 fd 20 fd fd fd fd fd fd 34 fd 44 36 33 fd 36 fd 33 fd 3f fd 0d fd fd fd 45 fd 67 6e 69 fd 35 33 50 fd 04 38 30 35 fd 70 38 fd 71 3f fd 32 fd 38 fd 75 20 fd 61 fd fd 62 65 61 62 6f fd 48 30 03 bb 76 0f fd 76 0c 40 33 fd 60 14 fd 69 2f 37 fd 70 14 36 fd 74 28 32 fd fd 67 31 7d 71 75 3c fd fd 47 2d fd 30 fd 33 fd 68 fd 66 fd fd fd 0f 77 38 4c 24 fd 6d fd 72 0b 44 3b 46 fd 07 fd 6f 6b 63 fd fd 6d fd 3b 34 fd 71 fd 3f fd 3c 40 fd 34 fd 30 fd fd fd 6d fd 73 75 3c 66 fd f1 fd 40 25 fd 60 34 fd fd 44 27 64 fd 4f 24 fd fd 41 35 1b fd 3d 01 fd 3c 72 fd	005mfF<05o:? v>33<Mknl02acE<42c 4D6363? Egni53P805p8q?28u abea boH0vv@3`i/7p6t(2g}u<G -03hfw8L $mrD;Fokcm;4q? <@40mu<f@%`4D'dO $A5=<r	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mcwfy.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 00 00 01 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 7b fd 38 2d 3f fd 56 7e 3f fd 56 7e 3f fd 56 7e 74 fd 55 7f 35 fd 56 7e 74 fd 53 7f fd fd 56 7e 74 fd 52 7f 2b fd 56 7e fd fd 53 7f 19 fd 56 7e fd fd 52 7f 2e fd 56 7e fd fd 55 7f 2c fd 56 7e 74 fd 57 7f 28 fd 56 7e 3f fd 57 7e 40 fd 56 7e fd fd 5e 7f 3e fd 56 7e fd fd 54 7f 3e fd 56 7e 52 69 63 68 3f fd 56 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.${8-?V~?V~?V~tU 5V~tSV~tR+V~SV~R.V~ U,V~tW(V~?W ~@V~^>V~T>V~Rich?V~	success or wait	6	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	75	4061F5	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	16	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsl9C8E.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsl9C8E.tmp	unknown	16854	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsl9C8E.tmp	unknown	4	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsl9C8E.tmp	unknown	16384	success or wait	20	4061F5	ReadFile

Analysis Process: mcwfy.exe PID: **3004**, Parent PID: **1928**

General

Target ID:	6
Start time:	10:32:49
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\mcwfy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\mcwfy.exe" C:\Users\user\AppData\Local\Temp\ytljtt.f
Imagebase:	0x400000
File size:	95232 bytes
MD5 hash:	6CB712E482D150A185F713D75314A75A
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ytljtt.f	unknown	4096	success or wait	1	4077E4	ReadFile
C:\Users\user\AppData\Local\Temp\ytljtt.f	unknown	4096	success or wait	1	4077E4	ReadFile
C:\Users\user\AppData\Local\Temp\ortnkgsjk.g	unknown	190464	success or wait	1	260A2C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	260EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	260EFF	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	260EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	260EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	260EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	260EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	260EFF	ReadFile

Analysis Process: mcwfy.exe PID: **1016**, Parent PID: **3004**

General

Target ID:	8
Start time:	10:32:50
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\mcwfy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\mcwfy.exe
Imagebase:	0x400000
File size:	95232 bytes
MD5 hash:	6CB712E482D150A185F713D75314A75A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.1055408046.00000000003B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.1055408046.00000000003B0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1055408046.00000000003B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.1055247288.0000000000260000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.1055247288.0000000000260000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1055247288.0000000000260000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.1055435528.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.1055435528.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1055435528.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
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	41E74A	NtReadFile

Analysis Process: AcroRd32.exe PID: **2704**, Parent PID: **576**

General

Target ID:	10
Start time:	10:32:53
Start date:	20/03/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" -Embedding
Imagebase:	0x1320000
File size:	2525680 bytes
MD5 hash:	2F8D93826B8CBF9290BC57535C7A6817

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13556E3	CreateDirectoryExW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	135699C	SHCreateDirectoryExW
C:\Users\user\AppData\LocalLow\Adobe\Linguistics	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	135699C	SHCreateDirectoryExW
C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	135699C	SHCreateDirectoryExW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	135699C	SHCreateDirectoryExW
C:\Users\user\AppData\Local\Adobe\Color	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	135699C	SHCreateDirectoryExW
C:\Users\user\AppData\Roaming\Adobe\Linguistics	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	135699C	SHCreateDirectoryExW
C:\Users\user\AppData\Roaming\Adobe\LogTransport2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	135699C	SHCreateDirectoryExW
C:\Users\user\AppData\Roaming\Adobe\Headlights	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	135699C	SHCreateDirectoryExW
C:\Users\user\AppData\Roaming\Microsoft\Speech	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	135699C	SHCreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13793E5	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rbq0qja_cepn9a_20o.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	136D40E	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	136D40E	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R29jerp_cepn9b_20o.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	136D40E	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1aneui4_cepn9c_20o.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	136D40E	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rldwxs_cepn9d_20o.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	136D40E	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rrzusa9_cepn9e_20o.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	136D40E	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\BroadcastMsg_1679333654.txt	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	136D40E	NtCreateFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	136B8C9	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\IPMContextAPI	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\IPMContextAPI\cIPMContextAPICache	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c1	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c1\cViewDef	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c1\cViewDef\cBottomView	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c1\cViewDef\cLeftView	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c1\cViewDef\cTopLeftView	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c1\cViewDef\cTopLeftView\cocgStates	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c1\cViewDef\cocgStates	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c2	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c2\cViewDef	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c2\cViewDef\cBottomView	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c2\cViewDef\cLeftView	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c2\cViewDef\cTopLeftView	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c2\cViewDef\cTopLeftView\cocgStates	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c2\cViewDef\cocgStates	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c3	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c3\cViewDef	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c3\cViewDef\cBottomView	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c3\cViewDef\cLeftView	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c3\cViewDef\cTopLeftView	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c3\cViewDef\cTopLeftView\cocgStates	success or wait	1	136BDC4	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\RememberedViews\cNoCategoryFiles\c3\cViewDef\cocgStates	success or wait	1	136BDC4	NtCreateKey

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

Analysis Process: RdrCEF.exe PID: **1556**, Parent PID: **2704**

General

Target ID:	11
Start time:	10:33:01
Start date:	20/03/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043
Imagebase:	0xef0000
File size:	9805808 bytes

MD5 hash:	326A645391A97C760B60C558A35BB068
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	89	FFBCE3	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	154	FFBD3B	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	1	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	2	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	324	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	10	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	5	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	33	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	12	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	5	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	24	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	3174	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	84	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	5	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	18	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	11	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	5	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	6	FF241A	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	5	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	11	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	36	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	36	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	81	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	90	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	220	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	5	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	4	FF241A	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	84	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	12	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	8	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	90	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	27	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	16	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	28	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	30	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	29	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	6	FF241A	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	349	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	336	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	16	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	425	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	395	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	31	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	645	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	100	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	4	FF241A	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	8	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	295	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	24	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	64	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	20	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	6	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	3	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	388	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	40	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	5	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	4	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	12	FF241A	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	4	FF241A	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	FFBCE3	ReadFile

Analysis Process: explorer.exe PID: **1860**, Parent PID: **1016**

General

Target ID:	12
Start time:	10:33:03
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xff040000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: WINWORD.EXE PID: **3148**, Parent PID: **576**

General

Target ID:	14
Start time:	10:33:14
Start date:	20/03/2023
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" -Embedding
Imagebase:	0x13f790000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
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	Completion	Count	Source Address	Symbol

Old File Path	New File Path	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

Analysis Process: wscript.exe PID: **3360**, Parent PID: **1860**

General	
Target ID:	16
Start time:	10:33:26
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0x40000
File size:	141824 bytes
MD5 hash:	979D74799EA6C8B8167869A68DF5204A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000010.00000002.1184042628.00000000000E0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000010.00000002.1184042628.00000000000E0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.1184042628.00000000000E0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000010.00000002.1184129727.00000000002B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000010.00000002.1184129727.00000000002B0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.1184129727.00000000002B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000010.00000002.1184187420.00000000002E0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000010.00000002.1184187420.00000000002E0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.1184187420.00000000002E0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com

Analysis Process: firefox.exe PID: **3768**, Parent PID: **3360**

General	
Target ID:	18
Start time:	10:34:02
Start date:	20/03/2023
Path:	C:\Program Files (x86)\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Mozilla Firefox\Firefox.exe
Imagebase:	0xe10000
File size:	517064 bytes
MD5 hash:	C2D924CE9EA2EE3E7B7E6A7C476619CA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000012.00000002.1137588402.0000000000230000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000012.00000002.1137588402.0000000000230000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.1137588402.0000000000230000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com

Disassembly

No disassembly