ID: 680530
Sample Name:
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.27077
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:40:24
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

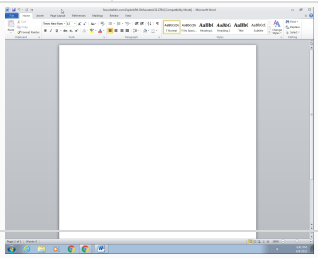
Windows Analysis Report

SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.27077

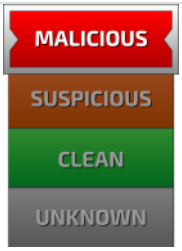
Overview

General Information

Sample Name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.27077 (renamed file extension from 27077 to rtf)
Analysis ID:	680530
MD5:	a5b0c571197ee2..
SHA1:	a4355fe45e321b..
SHA256:	00915bcbff87b2e..
Tags:	rtf
Infos:	



Detection



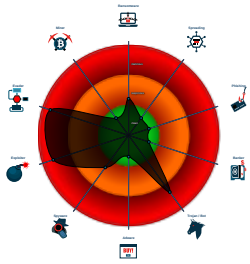
FormBook

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

Signatures

- Yara detected FormBook
- Document exploit detected (drops P…
- Malicious sample detected (through…
- Document contains OLE streams w…
- Document exploit detected (creates…
- Antivirus detection for dropped file
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Office process drops PE file
- Writes to foreign memory regions
- Document contains OLE streams w…
- Office equation editor starts process…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 3024 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1740 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - cmd.exe (PID: 972 cmdline: CmD.exe /C %tmp%\Client.exe A C MD5: AD7B9C14083B52BC532FBA5948342B98)
    - Client.exe (PID: 152 cmdline: C:\Users\user\AppData\Local\Temp\Client.exe A C MD5: 599BB05227A88A5C83E36E05D67DA0EA)
      - notepad.exe (PID: 280 cmdline: C:\Windows\SysWOW64\notepad.exe /Processid:{E9404046-8D8A-4DD0-8368-370A12D9C21C} MD5: A4F6DF0E33E644E802C8798ED94D80EA)
        - explorer.exe (PID: 1860 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - autochk.exe (PID: 1708 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: F88A52EB62019D6A62FDD9E08034DBD8)
          - colorcpl.exe (PID: 2564 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 031183B7923637CBB3E99CBBE5E821CA)
            - cmd.exe (PID: 800 cmdline: /c del "C:\Windows\SysWOW64\notepad.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
            - explorer.exe (PID: 968 cmdline: "C:\Windows\explorer.exe" MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.kambilemuntupan.space/sy31/"
  ],
  "decoy": [
    "saranatv.online",
    "xwrwdl.xyz",
    "tradecoin-investments.com",
    "cas-559.com",
    "liandli.biz",
    "hexglow.com",
    "jewelstorefront.com",
    "fukkd.com",
    "peliculasponder.com",
    "zourasecuritieslitgation.com",
    "armaxglobal.com",
    "postnarkapp.com",
    "wordhardeatbold.com",
    "greatdanedirects.site",
    "expressbelgium.com",
    "sophie-allport.com",
    "say-it-loud.org.uk",
    "selltoejfast.com",
    "kasaautomotriz.com",
    "stalkingbigcarp.site",
    "floral-poetry.com",
    "tacobellsurvey.xyz",
    "expansioncon.com",
    "208573.com",
    "expocartoon.com",
    "sakkaboom.site",
    "brewat.online",
    "alien-store.store",
    "beachdaygames.com",
    "sidedishpgh.com",
    "weekpaidhouse.top",
    "serv3can.online",
    "cumbreenvases.com",
    "wxfssl.com",
    "noahsdata.com",
    "e-blmail.org.uk",
    "swampkmaj.com",
    "idyllnewfoundland.com",
    "aerobrasil.net",
    "makotog4blog.com",
    "manuacevedo.com",
    "awakenedsaints.com",
    "hwps.us",
    "roxycinemamiddlesbrough.com",
    "am023.ltd",
    "xc-novel.com",
    "credit-cards-96409.com",
    "robotica-electronica.com",
    "syglhs.com",
    "zlhcyljy.com",
    "glanceid.net",
    "victoring.com",
    "d08765.com",
    "lazada44.com",
    "fernielodging.company",
    "mysiriusgear.com",
    "universalemotions.com",
    "jfql.xyz",
    "risingsauce.com",
    "scotwastebathgate.co.uk",
    "clarencesp.com",
    "adiversaoemfailia.online",
    "brandisaw.xyz",
    "3670tom.com"
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf	MAL_RTF_Embedded_OLE_PE	Detects a suspicious string often used in PE files in a hex encoded object stream	Florian Roth	• 0x178c:$a1: 546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f6465 • 0x16f0:$m1: 4d5a90000300000004000000ffff
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x1276:$obj2: \objdata • 0x1e867e:$obj2: \objdata • 0x2c8c94:$obj3: \objupdate • 0x8e3:$obj4: \objemb • 0x1e7ceb:$obj4: \objemb

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{5A3C8D88-A016-4151-9911-DB6F195FA0DD}.tmp	rtf_cve2017_11882_ole	Attempts to identify the exploit CVE 2017 11882	John Davison	• 0xf2000:$headers: 1C 00 00 00 02 00 9E C4 A9 00 00 00 00 00 00 00 C8 A7 5C 00 C4 EE 5B 00 00 00 00 00 03 01 01 03 0A • 0xf2021:$font: 0A 01 08 5A 5A • 0xf2052:$winexec: 12 0C 43 00
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{5A3C8D88-A016-4151-9911-DB6F195FA0DD}.tmp	EXP_potential_CVE_2017_11882	unknown	ReversingLabs	• 0x0:$docfilemagic: D0 CF 11 E0 A1 B1 1A E1 • 0xf1f00:$equation1: Equation Native • 0x920:$equation2: Microsoft Equation 3.0 • 0x2a0c:$exe: .exe • 0x2a1f:$exe: .exe • 0x2a3a:$exe: .exe • 0xf2029:$exe: .exe • 0xf203d:$exe: .exe • 0xf2052:$address: 12 0C 43 00

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000000.946833187.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000000.946833187.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000009.00000000.946833187.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000000.946833187.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
0000000C.00000002.1179366947.0000000000270000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 54 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.notepad.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.notepad.exe.400000.2.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
9.0.notepad.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.0.notepad.exe.400000.2.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
9.0.notepad.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 44 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Yara detected FormBook

Antivirus 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

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

PE file contains section with special chars

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

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

Remote Access Functionality

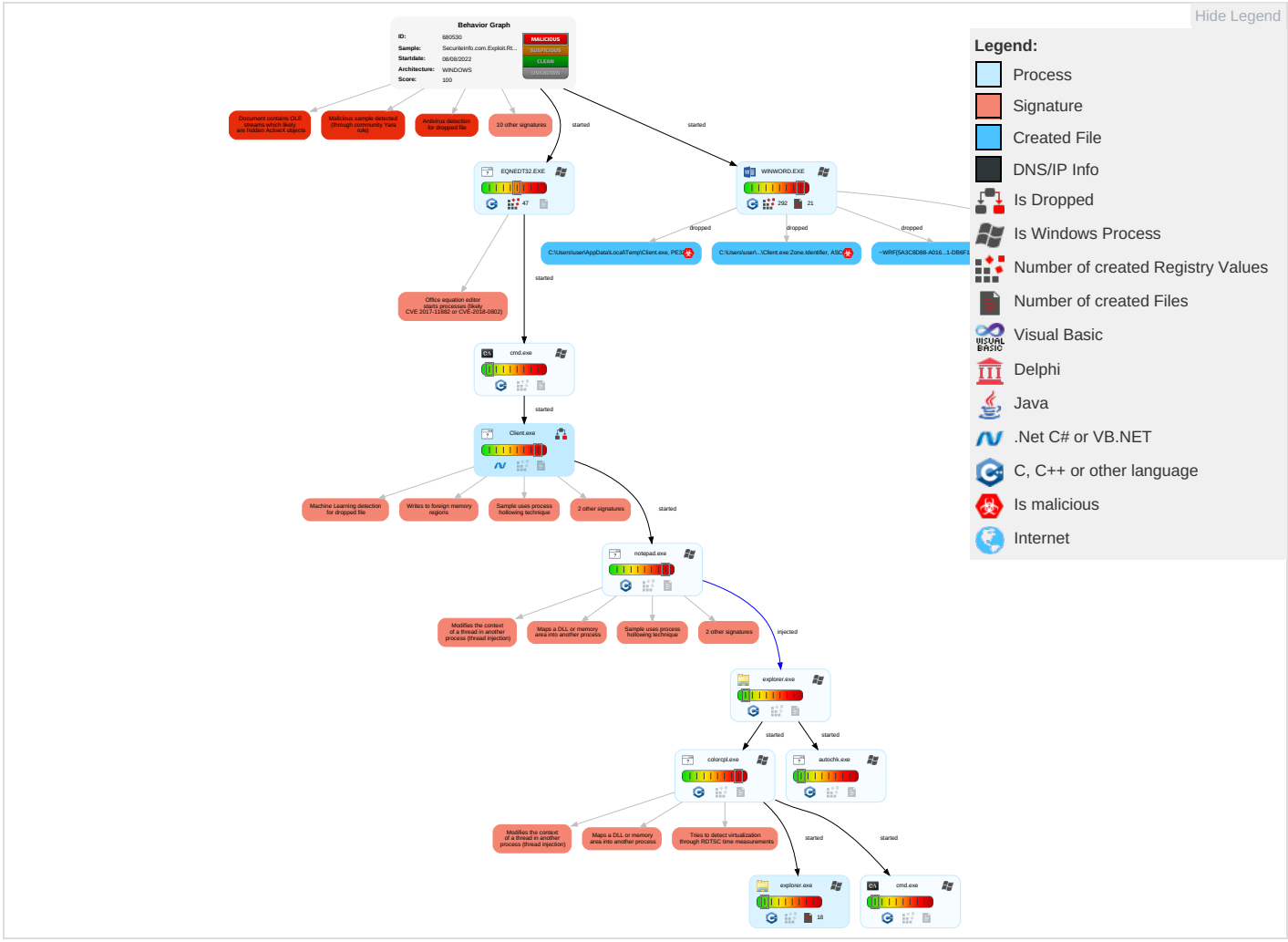
Yara detected FormBook

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 Command and Scripting Interpreter	1 DLL Side-Loading	7 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 3 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	4 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 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)	7 1 2 Process Injection	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	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

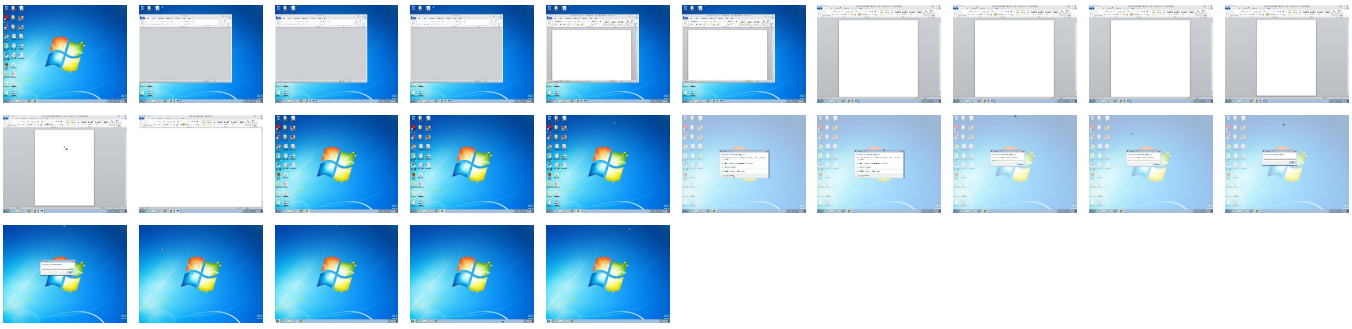
Behavior Graph

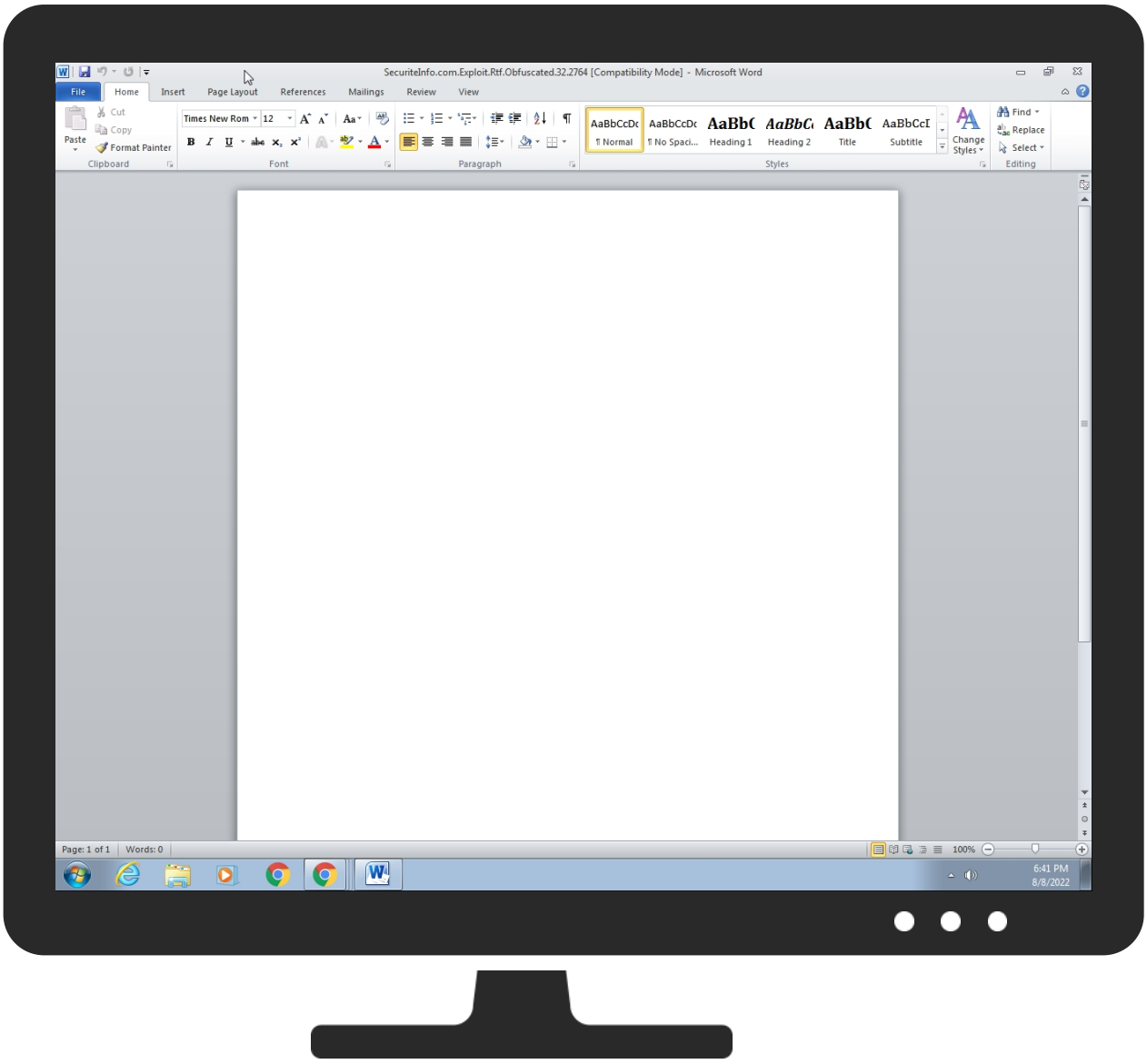


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{5A3C8D88-A016-4151-9911-DB6F195FA0DD}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Temp\Client.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.0.colorcpl.exe.490000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.0.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.notepad.exe.220000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.2.notepad.exe.310828.1.unpack	100%	Avira	TR/Dropper.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

Source	Detection	Scanner	Label	Link	Download
9.0.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.2.colorcpl.exe.490000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.2.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	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
www.kambilemuntupan.space/sy31/	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://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://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.kambilemuntupan.space/sy31/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 0000000A.00000000.10043349 86.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://investor.msn.com	explorer.exe, 0000000A.00000000.10043349 86.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 0000000A.00000000.10043349 86.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://wellformedweb.org/CommentAPI/	explorer.exe, 0000000A.00000000.96993651 8.00000000046D0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccl ean	explorer.exe, 00000010.00000000.11414061 51.00000000003F6000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 0010.00000000.1169666502.00000000003F600 0.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000010.00000002.1179532511.000 00000003F6000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 0000000A.00000000.96993651 8.00000000046D0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleanerq	explorer.exe, 0000000A.00000000.98851347 2.0000000002CBF000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1064634143.0000000002CBF000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.963611972.00000 00002CBF000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.1003285308.0000000002CBF000.000000 04.00000001.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner1SPS0	explorer.exe, 0000000A.00000000.98073595 7.0000000008611000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1010954444.0000000008611000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.997010696.00000 00008611000.00000004.00000001.00020000.0 0000000.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 0000000A.00000000.99057817 0.0000000003CF7000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	explorer.exe, 0000000A.00000000.10043349 86.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://treyresearch.net	explorer.exe, 0000000A.00000000.96993651 8.00000000046D0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	explorer.exe, 0000000A.00000000.99057817 0.0000000003CF7000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://java.sun.com	explorer.exe, 0000000A.00000000.98488825 7.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.952674805.0000000000335000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1062333301.00000 00000335000.00000004.00000020.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.1001709760.0000000000335000.000000 04.00000020.00020000.00000000.sdmp, explorer.exe, 00000010.00000000.1140645278.00000000003 7E000.00000004.00000020.00020000.0000000 0.sdmp, explorer.exe, 00000010.00000000. 1168478095.000000000037E000.00000004.000 00020.00020000.00000000.sdmp, explorer.exe, 00000010.00000002.1177864613.0000000 00037E000.00000004.00000020.00020000.000 00000.sdmp	false	• URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	explorer.exe, 0000000A.00000000.99057817 0.0000000003CF7000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	explorer.exe, 0000000A.00000000.95633297 9.0000000001DD0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 0000000A.00000000.98169693 1.0000000008807000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.981376298.000000000869E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.998141320.000000 000869E000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 0000000A.0000 0000.1011250334.000000000869E000.0000000 4.00000001.00020000.00000000.sdmp, explorer.exe, 00000010.00000003.1140594527.000000000293 5000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000010.00000000.1141406151. 00000000003F6000.00000004.00000020.00020 000.00000000.sdmp, explorer.exe, 0000001 0.00000000.1169666502.00000000003F6000.0 0000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000010.00000002.1179532 511.00000000003F6000.00000004.00000020.0 0020000.00000000.sdmp, explorer.exe, 000 00010.00000002.1184308439.0000000004BDF0 00.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000010.00000002.1180212786.00 000000028A0000.00000004.00000020.0002000 0.00000000.sdmp	false		high
http://www.piriform.com/ccleanerL	explorer.exe, 00000010.00000002.11802127 86.00000000028A0000.00000004.00000020.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	explorer.exe, 0000000A.00000000.10043349 86.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner	explorer.exe, 00000010.00000000.11428176 45.00000000028D5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://computername/printers/printername/.printer	explorer.exe, 0000000A.00000000.96993651 8.00000000046D0000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	explorer.exe, 0000000A.00000000.95633297 9.0000000001DD0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 0000000A.00000000.98488825 7.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.952674805.0000000000335000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1062333301.00000 00000335000.00000004.00000020.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.1001709760.0000000000335000.000000 04.00000020.00020000.00000000.sdmp, explorer.exe, 00000010.00000000.1140645278.00000000003 7E000.00000004.00000020.00020000.0000000 0.sdmp, explorer.exe, 00000010.00000000. 1168478095.000000000037E000.00000004.000 00020.00020000.00000000.sdmp, explorer.exe, 00000010.00000002.1177864613.0000000 00037E000.00000004.00000020.00020000.000 00000.sdmp	false		high
http://https://support.mozilla.org	explorer.exe, 0000000A.00000000.98488825 7.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.952674805.0000000000335000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1062333301.00000 00000335000.00000004.00000020.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.1001709760.0000000000335000.000000 04.00000020.00020000.00000000.sdmp, explorer.exe, 00000010.00000000.1140645278.00000000003 7E000.00000004.00000020.00020000.0000000 0.sdmp, explorer.exe, 00000010.00000000. 1168478095.000000000037E000.00000004.000 00020.00020000.00000000.sdmp, explorer.exe, 00000010.00000002.1177864613.0000000 00037E000.00000004.00000020.00020000.000 00000.sdmp	false		high
http://www.piriform.com/ccleanerv	explorer.exe, 0000000A.00000000.99170861 2.0000000004385000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1006533953.0000000004385000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1069727746.0000 000004385000.00000004.00000001.00020000. 00000000.sdmp, explorer.exe, 0000000A.00 000000.968708467.0000000004385000.000000 04.00000001.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Client.exe, 00000005.00000002.948805262. 0000000002251000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://servername/isapibackend.dll	explorer.exe, 0000000A.00000000.10082522 95.0000000006450000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680530
Start date and time: 08/08/202218:40:24	2022-08-08 18:40:24 +02:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 9m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.27077 (renamed file extension from 27077 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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winRTF@13/9@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 13% (good quality ratio 12%) • Quality average: 65.5% • Quality standard deviation: 30.5%
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
- Excluded IPs from analysis (whitelisted): 104.208.16.93
- Excluded domains from analysis (whitelisted): onedsblobprdcus07.centralus.cloudapp.azure.com, watson.microsoft.com, legacywatson.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly 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
18:41:15	API Interceptor	37x Sleep call for process: EQNEDT32.EXE modified
18:41:17	API Interceptor	181x Sleep call for process: Client.exe modified
18:41:40	API Interceptor	5x Sleep call for process: notepad.exe modified
18:42:14	API Interceptor	221x Sleep call for process: colorcpl.exe modified
18:43:06	API Interceptor	49x 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{5A3C8D88-A016-4151-9911-DB6F195FA0DD}.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):	993792
Entropy (8bit):	7.222485991107414
Encrypted:	false
SSDEEP:	12288:q1fPLY2Y841v3xqdanStZpGZh75x6OFMqnUDv2GTHPx2TZX5OHpCu9qvle:qhDY2d4kE1x+qeZTZAZJcpv9W
MD5:	4F21F03C3041A4441F3D7CB34F15BB5F
SHA1:	F7F6D3D57D0FE2E723D35534A5887214CE3B9BD8
SHA-256:	83D6D72D2C5140FC1C7CB6D6DBADA9B9421CE54E4E96DDBB099D9064956E02EA
SHA-512:	A970290CCC6CC397F91C49B98D49D0FE93AD9E29A23D28CF74F434E9904B7C6D0656417F792D1E04EA6FFFF7DB9F1ECE2158DF7028FC74DA7A6C323773B50BE
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{5A3C8D88-A016-4151-9911-DB6F195FA0DD}.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{5A3C8D88-A016-4151-9911-DB6F195FA0DD}.tmp, Author: ReversingLabs
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A951AE7E-D2D4-47F1-B4B4-2F2B249A12BF}.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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E3A4F74B-8D8B-4273-8507-885596050B2F}.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
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\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):	979456
Entropy (8bit):	7.255901249909526
Encrypted:	false
SSDEEP:	12288:t1fPLY2Y841v3xqdanStZpGZh75x6OFMqnUDv2GTHPx2TZX5OHpCu9qvle:thDY2d4kE1x+qeZTZAZJcpv9W
MD5:	599BB05227A88A5C83E36E05D67DA0EA
SHA1:	663EBDC243BDF990D2950A0BCAB08CF316BDFF50
SHA-256:	2D63CA0053F446B5531AA5703C136586CEC0635994FD5DEE51DF7FE51DF58EB4
SHA-512:	5E1826F4EB4BD831A02DD705E2DF1ED1C082BB7E7D4486F6A4F34E6323F2942448EC3D2C56F516AA9A65AF71A2F4411D5BDA4764656E3C7B9776C0DF44DB7AE1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b....."...0.....R.....@..... ....@.. ....@.....|...O.... .....`.....@.....H.....s.n=><v..F... ...H.....@....text...H.....L..... ..`.rsrc..... .....@..@.....@..... ..`.reloc.....`.....@..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:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E98
Malicious:	**true**
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.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=Tue Aug 9 00:41:01 2022, mtime=Tue Aug 9 00:41:01 2022, atime=Tue Aug 9 00:41:11 2022, length=2920194, window=hide
Category:	dropped
Size (bytes):	1199
Entropy (8bit):	4.594505916256018
Encrypted:	false
SSDEEP:	24:8S/XThO1VAaDHCn9UWJeFHCn9UkDv3qlu7D:8S/XT47hDHCnaWJGHCnaLl0D
MD5:	32B89312713DBA78D97CEC329D156889
SHA1:	2EB5385E7FB3E2B30519AC202BB0247ABBCBCD3E
SHA-256:	C1424ED0C28323E344068F84B6385C6A88FF87C7F4E640C6CCC8AB07C4BED7DD
SHA-512:	8E89FB9FF983A66B51B8D120D2CF0F51D68C4B82A7435B67CB39E0C720C575412BC3D99582889C925F489E27C3C5458CE06A97D5652A51C29E644C77195C61B
Malicious:	false
Preview:	L.....F.... .....,.....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...2.7.6.4...r.t.f.....-...8...[.....?J.....C:\Users\..#.....\\287400\Users.user\Desktop\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf.J.....\.....\.....\.....\.....\.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...2.7.6.4...r.t.f.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S

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):	146
Entropy (8bit):	4.9716806428490745
Encrypted:	false
SSDEEP:	3:bDuMJluscbcTLqjQWC0LXSdpFomxW9rbcTLqjQWC0LXSdpFov:bCVwTeS0LXSrFOrwTeS0LXSrFy
MD5:	E05B953212FAA9138D101E8B9D79F5A5
SHA1:	89690B0BA586C8B7F030B735BF88CFE1DB5DACD4
SHA-256:	6D24EEBBA9E66EB4B5E0090AC160DBD82B63AFB49568F91B15C129C05F764A8A
SHA-512:	C348EB6F5871255719AD9BE932052E7C5F746661E14CA6D426781CBCA3970F15922D934920C7C271F67A944869430FAB2655F0B8B3D1047AA8BE321B0A57633E
Malicious:	false
Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.LNK=0..[misc]..SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.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:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\user\Desktop\~$curiteInfo.com.Exploit.Rtf.Obfuscated.32.2764.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:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61

SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info

General

File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	4.7600452351752605
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2764.rtf
File size:	2920194
MD5:	a5b0c571197ee2931e12f11caf138eff
SHA1:	a4355fe45e321b99274f8000c5ac9c08f7146b28
SHA256:	00915bcbff87b2e195e1547df8e1944cadcdc6aa46beb130bd5a960dff01c7e3
SHA512:	eff4fadba11f02724628b950cfe815347c019759f2b40ea8ce4c9dcbf13964ac3fdf76230a2a685b0a6c68d33fff24fa3f43f026b365e0efb7a4cbf992834b6c
SSDEEP:	24576:0u0HN0y/U6FoR5bjoPL/GWEuwJpiGOR2QGBl0s5mp1BRX56XRsH9dBwK3UFHzZ:z
TLSH:	07D5A67071B535C6E26F0172429FBC59521738C3B3C62D88815DEAF62ED4B7A7B81A0E
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

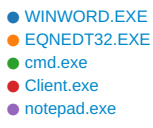
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000129Ah	2	embedded	Package	979623	Client.exe	C:\Path\Client.exe	C:\Path\Client.exe	no
1	001E86A2h	2	embedded	Equation.3	3072				no

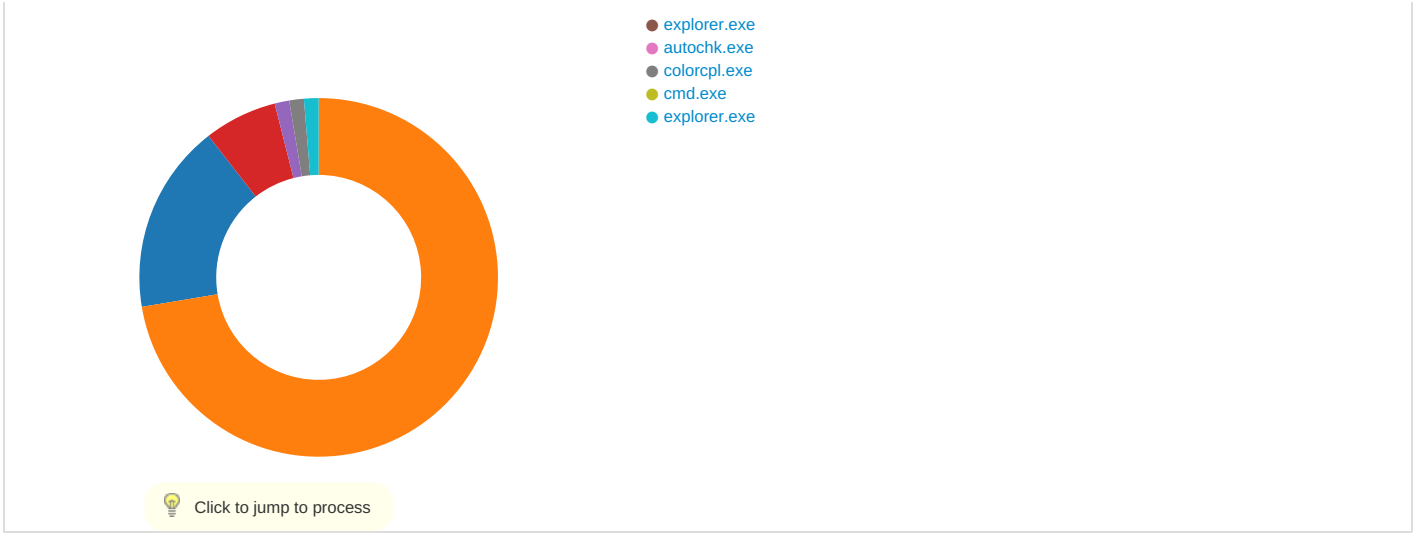
Network Behavior

No network behavior found

Statistics

Behavior





System Behavior

Analysis Process: WINWORD.EXE PID: 3024, Parent PID: 576

General

Target ID:	0
Start time:	18:41:12
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:	0x13fa00000
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: 1740, Parent PID: 576

General

Target ID:	2
Start time:	18:41:15
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: **972**, Parent PID: **1740**

General

Target ID:	3
Start time:	18:41:15
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:	0x4ac40000
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: **152**, Parent PID: **972**

General

Target ID:	5
Start time:	18:41:16
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:	0x1d0000
File size:	979456 bytes
MD5 hash:	599BB05227A88A5C83E36E05D67DA0EA
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: 00000005.00000002.956769759.0000000003276000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.956769759.0000000003276000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.956769759.0000000003276000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.956769759.0000000003276000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6DF57995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF57995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE6DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF5A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DE6DE2C	ReadFile

Analysis Process: notepad.exe PID: **280**, Parent PID: **1060**

General

Target ID:	9
Start time:	18:41:32
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\notepad.exe /Processid:{E9404046-8D8A-4DD0-8368-370A12D9C21C}
Imagebase:	0x2a0000
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: 00000009.00000000.946833187.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.946833187.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.946833187.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.946833187.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1020852335.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.1020852335.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1020852335.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1020852335.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.936817902.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.936817902.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.936817902.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.936817902.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.936384023.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.936384023.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.936384023.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.936384023.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.946015787.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.946015787.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.946015787.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.946015787.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1020404984.00000000001C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.1020404984.00000000001C0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1020404984.00000000001C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1020404984.00000000001C0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1020827183.00000000003D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.1020827183.00000000003D0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1020827183.00000000003D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1020827183.00000000003D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.946320961.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.946320961.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.946320961.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.946320961.0000000000400000.00000040.00000400.00020000.00000000.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	41A457	NtReadFile

Analysis Process: explorer.exe PID: **1860**, Parent PID: **280**

General

Target ID:	10
Start time:	18:41:41
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.00000000.1000544404.000000000B405000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000000.1000544404.000000000B405000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.1000544404.000000000B405000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.1000544404.000000000B405000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.1011962365.000000000B405000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000000.1011962365.000000000B405000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.1011962365.000000000B405000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.1011962365.000000000B405000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: autochk.exe PID: **1708**, Parent PID: **1860**

General

Target ID:	11
Start time:	18:42:09
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0xc80000
File size:	668160 bytes
MD5 hash:	F88A52EB62019D6A62FDD9E08034DBD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: colorcpl.exe PID: **2564**, Parent PID: **1860**

General

Target ID:	12
Start time:	18:42:10
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0x490000
File size:	86016 bytes
MD5 hash:	031183B7923637CBB3E99CBBE5E821CA
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: 0000000C.00000002.1179366947.0000000000270000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.1179366947.0000000000270000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.1179366947.0000000000270000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.1179366947.0000000000270000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.1180023035.0000000000430000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.1180023035.0000000000430000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.1180023035.0000000000430000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.1180023035.0000000000430000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.1177745038.00000000000E0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.1177745038.00000000000E0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.1177745038.00000000000E0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.1177745038.00000000000E0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	FA457	NtReadFile

Analysis Process: cmd.exe PID: **800**, Parent PID: **2564**

General

Target ID:	13
Start time:	18:42:15
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\SysWOW64\notepad.exe"
Imagebase:	0x49e10000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **968**, Parent PID: **1704**

General

Target ID:	16
Start time:	18:43:05
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe"
Imagebase:	0xffe80000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\User Account Pictures\user.bmp	unknown	49208	success or wait	1	FFE9B5A9	ReadFile

Registry Activities

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

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

Disassembly

No disassembly