ID: 635245
Sample Name: INVOICE.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:41:15
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

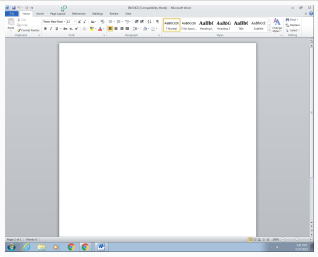
Windows Analysis Report

INVOICE.doc

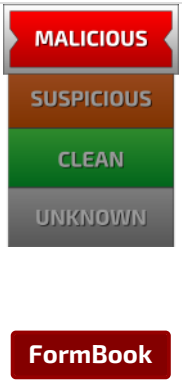
Overview

General Information

Sample Name:	INVOICE.doc
Analysis ID:	635245
MD5:	0ecb6ed891d173..
SHA1:	6867f37817db50..
SHA256:	f080b3ba979f854.
Tags:	doc
Infos:	



Detection



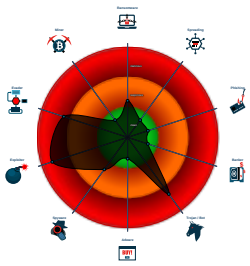
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Document exploit detected (drops P…
- Malicious sample detected (through…
- Document contains OLE streams w…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Office process drops PE file
- Writes to foreign memory regions

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2284 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1144 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - cmd.exe (PID: 2224 cmdline: CmD.exe /C %tmp%\Client.exe A C MD5: AD7B9C14083B52BC532FBA5948342B98)
    - Client.exe (PID: 2488 cmdline: C:\Users\user\AppData\Local\Temp\Client.exe A C MD5: 75C0471CCE805B589FDAF81D8D1D646C)
      - notepad.exe (PID: 2788 cmdline: C:\Windows\SysWOW64\notepad.exe MD5: A4F6DF0E33E644E802C8798ED94D80EA)
      - notepad.exe (PID: 1112 cmdline: C:\Windows\SysWOW64\notepad.exe MD5: A4F6DF0E33E644E802C8798ED94D80EA)
      - notepad.exe (PID: 1072 cmdline: C:\Windows\SysWOW64\notepad.exe MD5: A4F6DF0E33E644E802C8798ED94D80EA)
      - notepad.exe (PID: 1136 cmdline: C:\Windows\SysWOW64\notepad.exe MD5: A4F6DF0E33E644E802C8798ED94D80EA)
      - notepad.exe (PID: 2960 cmdline: C:\Windows\SysWOW64\notepad.exe MD5: A4F6DF0E33E644E802C8798ED94D80EA)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bense003.xyz/s3s3/"
  ],
  "decoy": [
    "tvielotus.com",
    "teesta.xyz",
    "talentrecruitor.com",
    "pamaungipb.com",
    "xn--90ahkh6a6b8b.site",
    "910carolina.com",
    "toyotaecoyouth-dev.com",
    "invetnables.com",
    "gdexc.com",
    "ssw168.com",
    "householdmould.com",
    "mqttradar.xyz",
    "t333c.com",
    "thepausestudio.com",
    "evershedsutherlands.com",
    "asbdataplus.com",
    "preddylilthingz.com",
    "jepwu.com",
    "tvlido.com",
    "artovus.com",
    "trainingmagazineme.com",
    "rettar.net",
    "underneathstardoll.com",
    "babipiko21.site",
    "getvpsdime.com",
    "accentsfurniture.com",
    "cutdowns.tech",
    "teklcin.online",
    "sunshareesg.com",
    "eventrewards.site",
    "lacomunaperu.com",
    "a-tavola.online",
    "gshund.com",
    "monsterflixer.com",
    "896851.com",
    "carpetlandcolortileflint.com",
    "filmproduction.management",
    "cherie-clinique.com",
    "medjoker.com",
    "grant-helpers.site",
    "sussdmortgages.com",
    "solaranlagen-forum.com",
    "freecustomsites.com",
    "h7578.com",
    "ideadly.com",
    "backend360.com",
    "podgorskidesign.com",
    "zilinsky.taxi",
    "ourelevatetribe.com",
    "thefitnesswardllc.com",
    "eficazindustrial.com",
    "thecovefishcamp.com",
    "niuxy.com",
    "myluxurypals.com",
    "clinicadentalvelinta.com",
    "dis99.com",
    "crosswealth.xyz",
    "itopjob.com",
    "oandbcleaningservices.com",
    "afri-solutions.com",
    "paradiseoe.com",
    "versionespublicas.com",
    "b2lonline.com",
    "usdcmeta.xyz"
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
INVOICE.doc	MAL_RTF_Embedded_OLE_PE	Detects a suspicious string often used in PE files in a hex encoded object stream	Florian Roth	• 0x177f:$a1: 546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f6465 • 0x16e3:$m1: 4d5a90000300000004000000ffff
INVOICE.doc	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x1269:$obj2: \objdata • 0x207214:$obj2: \objdata • 0x3e240c:$obj3: \objupdate • 0x8de:$obj4: \objemb • 0x206889:$obj4: \objemb

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E5C71654-C0CA-4182-8CA2-6F1C92DC7362}.tmp	rtf_cve2017_11882_ole	Attempts to identify the exploit CVE 2017 11882	John Davison	• 0xfbc00:$headers: 1C 00 00 00 02 00 9E C4 A9 00 00 00 00 00 00 00 C8 A7 5C 00 C4 EE 5B 00 00 00 00 00 03 01 01 03 0A • 0xfbc21:$font: 0A 01 08 5A 5A • 0xfbc52:$winexec: 12 0C 43 00
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E5C71654-C0CA-4182-8CA2-6F1C92DC7362}.tmp	EXP_potential_CVE_2017_11882	unknown	ReversingLabs	• 0x0:$docfilemagic: D0 CF 11 E0 A1 B1 1A E1 • 0xfbb00:$equation1: Equation Native • 0x920:$equation2: Microsoft Equation 3.0 • 0x2a0c:$exe: .exe • 0x2a1f:$exe: .exe • 0x2a3a:$exe: .exe • 0xfbc29:$exe: .exe • 0xfbc3d:$exe: .exe • 0xfbc52:$address: 12 0C 43 00

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.977766193.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.977766193.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.977766193.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000000.969790709.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000000.969790709.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.notepad.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
12.2.notepad.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
12.2.notepad.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C
8.2.notepad.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.2.notepad.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 100 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus detection for URL or domain
- 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

- 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

Anti Debugging

- Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion

- Writes to foreign memory regions
- Injects a PE file into a foreign processes

Stealing of Sensitive Information

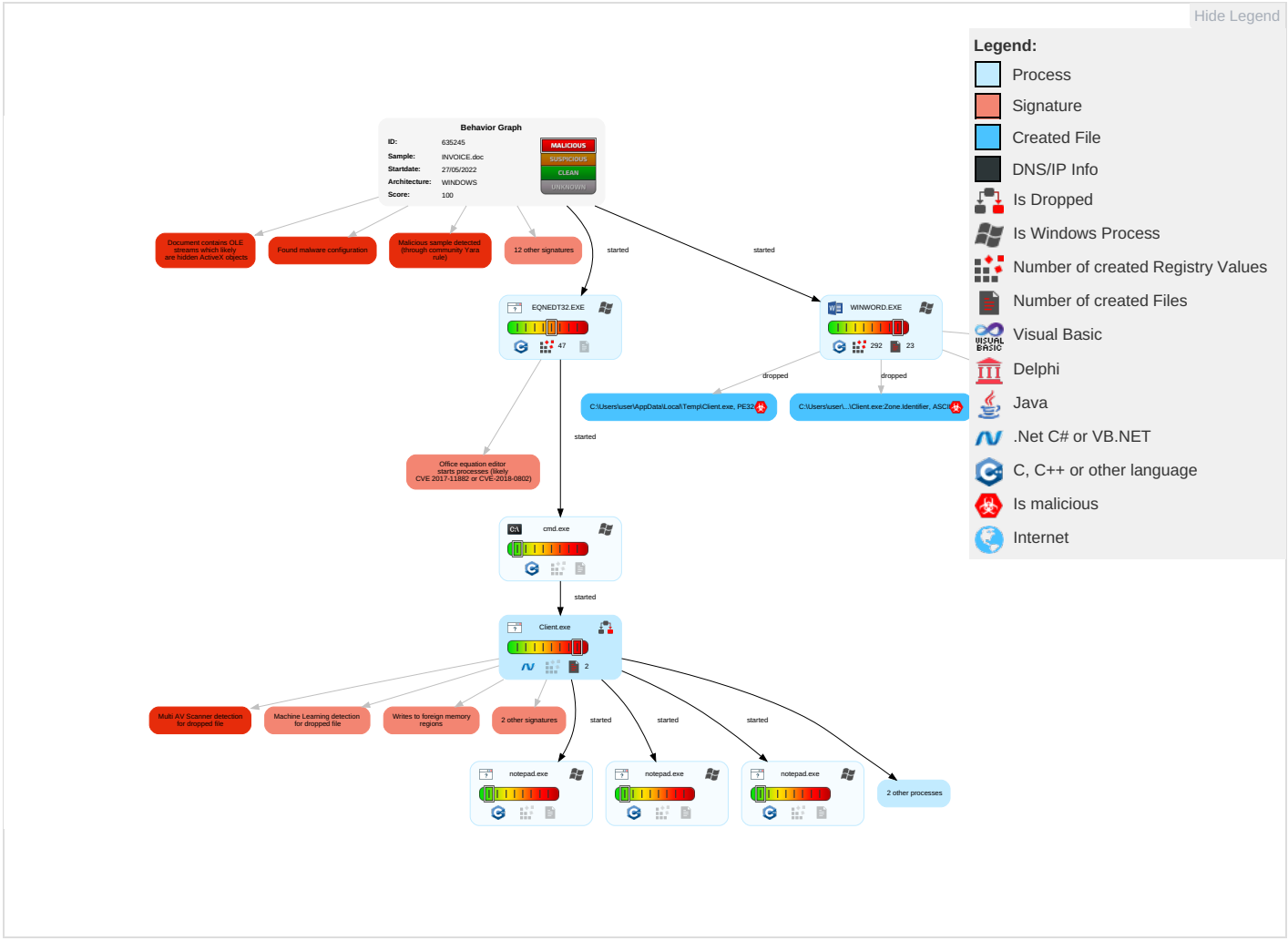
- Yara detected FormBook

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	4 Exploitation for Client Execution	1 DLL Side-Loading	2 1 1 Process Injection	1 Masquerading	OS Credential Dumping	2 1 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
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 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	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	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)	2 1 1 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	2 Obfuscated Files or Information	LSA Secrets	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	3 Software Packing	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	1 DLL Side-Loading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

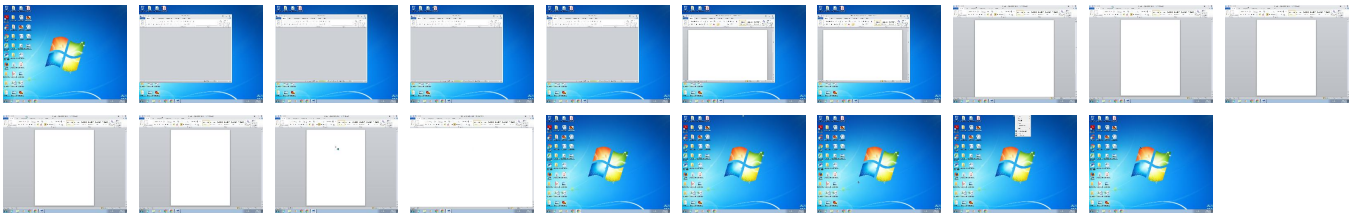
Behavior Graph

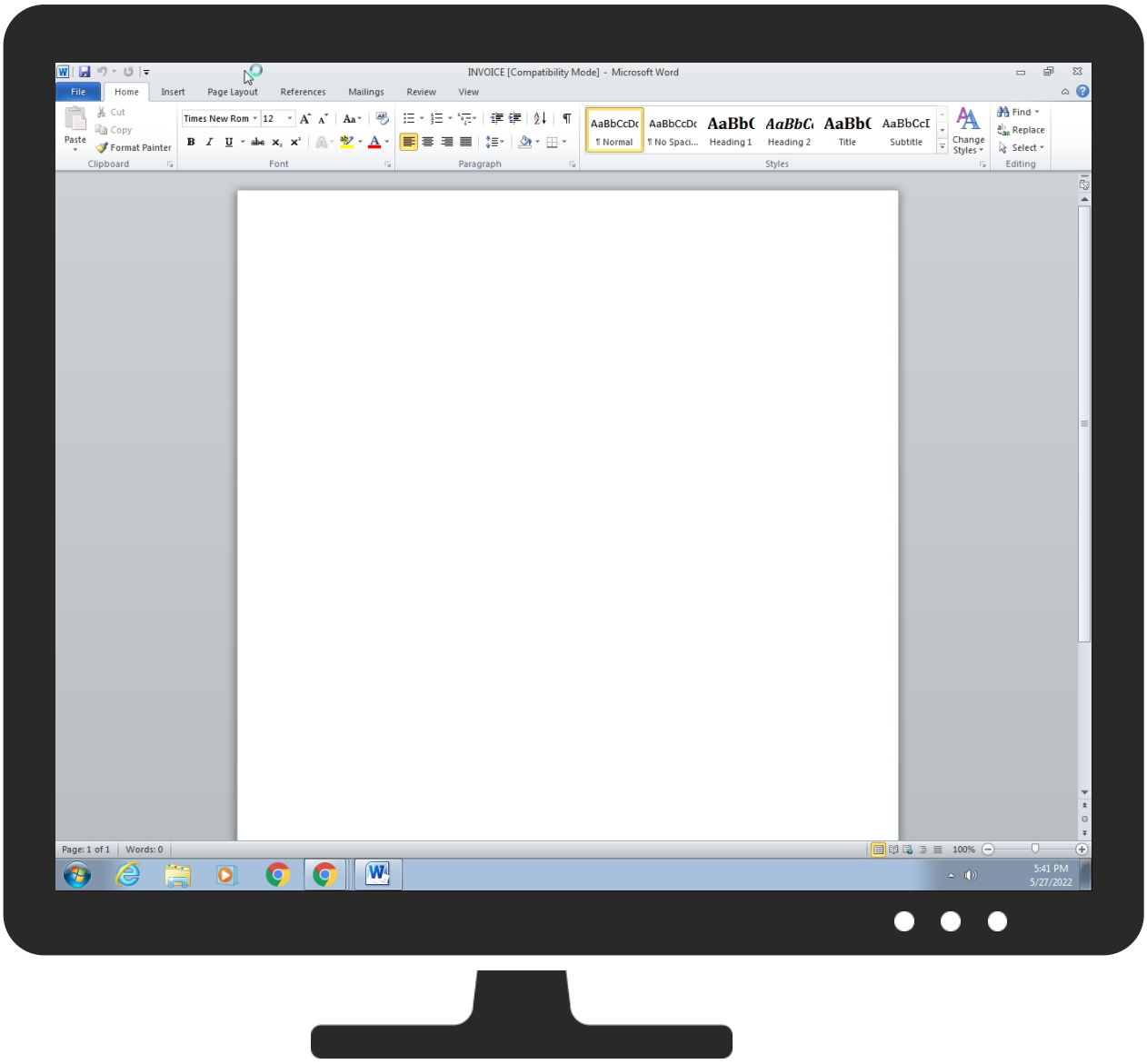


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
INVOICE.doc	50%	Virustotal		Browse
INVOICE.doc	20%	ReversingLabs	Document-RTF.Trojan.Injuke	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E5C71654-C0CA-4182-8CA2-6F1C92DC7362}.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	31%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Client.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.RealProtect	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.0.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.0.notepad.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.0.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.0.notepad.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.0.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.0.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.2.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.0.notepad.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.0.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.2.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.notepad.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.bense003.xyz/s3s3/	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.bense003.xyz/s3s3/	true	• Avira URL Cloud: phishing	low

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635245
Start date and time: 27/05/202217:41:15	2022-05-27 17:41:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE.doc
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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@16/9@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 13.8% (good quality ratio 13.1%) • Quality average: 59.2% • Quality standard deviation: 27.3%
HCA Information:	• Successful, ratio: 63% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • 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 size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:41:20	API Interceptor	34x Sleep call for process: EQNEDT32.EXE modified
17:41:22	API Interceptor	225x Sleep call for process: Client.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{E5C71654-C0CA-4182-8CA2-6F1C92DC7362}.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):	1033728
Entropy (8bit):	7.430455222200925
Encrypted:	false
SSDEEP:	12288:zM/Vjn7/MEaDBNAU+UY8WiUxjx0Kvd9cHGunMFrER0iONCXtykhWt7mxe4g:zM/VP/MXbL+fTFvMHGuOc0i4CXt5hWE
MD5:	23C4AC5F2EA3F3D19126836319E7D75A
SHA1:	4D307E0A330AF7350AF0A490D0D22B11AF7E2723
SHA-256:	65FC5F503844792A2FD68C477D56132EB8AC27AF8D92B7B5D98D7586BF40FECF
SHA-512:	C89A29CDF7C5BD36BBEF914FF258AC0B96BCB5B68F1CA846B64085BD0A074F37FCB8B320D73EDFE2914C56E4BFCF03AAB8245D351DEAD7BFAF9F14CFCFDD3101
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{E5C71654-C0CA-4182-8CA2-6F1C92DC7362}.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{E5C71654-C0CA-4182-8CA2-6F1C92DC7362}.tmp, Author: ReversingLabs
Antivirus:	• Antivirus: Avira, Detection: 100%
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{5683FAE1-8458-4065-875E-400E96F079D3}.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...O J..QJ..^J.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{BC3C4C95-52F5-42BB-8F60-EC57C3F97BE3}.tmp

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

C:\Users\user\AppData\Local\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):	1019392
Entropy (8bit):	7.463685655107809
Encrypted:	false
SSDEEP:	12288:/M/Vjn7/MEaDBNAU+UY8WiUxjx0Kvd9cHGunMFrER0iONCXtykhWt7mxe4g:/M/VP/MXbL+fTFvMHGuOc0i4CXt5hWE
MD5:	75C0471CCE805B589FDAF81D8D1D646C
SHA1:	28D5C23AB236A28376A64446EECC4B8068E71F51
SHA-256:	8C867636633BAB72230AB4F4123B1B37244A8325B40230947CDFD7EC3CC0C686
SHA-512:	2233A6BC864F0F2705010F2FDF688DB0E72A20A92C16711E63A06FBEE0D9C6D32E31AB70C93CEDA4B40D14D84EC045D65EDCDD97055B4C34DFBB6DE40019E 00
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 51%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Lg.b.....0..z..... ....@.. ....@.....O....@...}.....H.....VU3re.zH..... .....@....text....v.....x..... ..`.rsr c....}...@...~.....@..@..... ..`.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:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 98
Malicious:	**true**
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INVOICE.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 Mar 8 15:45:54 2022, mtime=Tue Mar 8 15:45:54 2022, atime=Fri May 27 23:41:14 2022, length=4073082, window=hide
Category:	dropped
Size (bytes):	997
Entropy (8bit):	4.579900792019912
Encrypted:	false
SSDEEP:	12:8zB3dGe0gXg/XAlCPCHaXBKBnB/xQpX+WxNXQai8TicvbI0rDEvJUDtZ3YilMMEA:8zB3dy/XTRKJIzNAtBemHJDv3q7Y7h
MD5:	24AE59D9E525D79955199E2607E082A9
SHA1:	BFE6EE00E329812712CA0B22858FBDDAF98F8573
SHA-256:	1F85C2A020C674E41B74B4A419CE011D5EA73929F4CBC46673EC67075B1018FE
SHA-512:	4F4A609D189DCBD5B0E4C7954BF64DC9A3D616D5D7EF06003457CF39FAE38E86E2D1C33235C7DE6BF426FA8C67845AD1F10CAC1D95AFB09A648404DE16A82E0
Malicious:	false
Preview:	L.....F.... .....v..3....v..3..M...+r..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.....hT....Desktop.d.....QK.XhT..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....^.2.z&>..T(. .INVOICE.doc.D.....hT..hT..*...r.....'.....I.N.V.O.I.C.E...d.o.c.....u.....-...8...[.....?J.....C:\Users\..#.....\\226546\Users.user\Desktop\INVOICE.doc."....\....\....\....\....\.D.e.s.k.t.o.p.\.I.N.V.O.I.C.E...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....226546.....D_....3N...W...9...N..... .....[D_....3N...W...9...N..... .....[....

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):	65
Entropy (8bit):	4.616856329393205
Encrypted:	false
SSDEEP:	3:bDuMJl0XXd64omX1KzqsXd64ov:bCP3izqA3y
MD5:	3360631D6A0AB8AFBC94014B8F902169
SHA1:	805E2351303FEB6AC86288558FC4D9E89F60DA9C
SHA-256:	2765D20F07A240269ADA61F9EB986C8AAB8B0054187EE7681F00EF2CEE35B37F
SHA-512:	6F4112B1F5FEB12142281B7E971A27EBC428D31C1F586F02933FC772DF47B0BEEED71C236614C2772F0403A1CA7E13A60429B64A408A7447F8703453C80BF4C2
Malicious:	false
Preview:	[folders]..Templates.LNK=0..INVOICE.LNK=0..[doc]..INVOICE.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):	2.4797606462020303
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyAI/ugXImW4eedln:vdsCkWtpIGgXvdl
MD5:	1674A1C7C99CD9FAADA789F5E2AEB335
SHA1:	26D9E81D5ED584A899A94D5EA8945A5AE3403F85
SHA-256:	BB5F0D32E0E1C8B6865FCE4AE1FC50E34CA954B89E771364A6BE6627F7C726B6
SHA-512:	B2225E8F93F06FFE32B4FDF987D5134BB06F1B0874509E1CC973FD4D30B0F1341CB1AE72FBE9C282A65794A130E2D9C8D4939B789492BC1BCC96394C5F03E02C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....12.....22.....@32.....32.....z.....p42.....x...

C:\Users\user\Desktop\~$NVOICE.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4797606462020303
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyAI/ugXImW4eedln:vdsCkWtpIGgXvdl

MD5:	1674A1C7C99CD9FAADA789F5E2AEB335
SHA1:	26D9E81D5ED584A899A94D5EA8945A5AE3403F85
SHA-256:	BB5F0D32E0E1C8B6865FCE4AE1FC50E34CA954B89E771364A6BE6627F7C726B6
SHA-512:	B2225E8F93F06FFE32B4FDF987D5134BB06F1B0874509E1CC973FD4D30B0F1341CB1AE72FBE9C282A65794A130E2D9C8D4939B789492BC1BCC96394C5F03E02C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....12.....22.....@32.....32.....z.....p42.....x...

Static File Info

General

File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	5.05599985084287
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	INVOICE.doc
File size:	4073082
MD5:	0ecb6ed891d173443fa3654c31e14320
SHA1:	6867f37817db501ce103813f791899f3cf1bc1e8
SHA256:	f080b3ba979f854761526f4bc6bd5b8210b48d5f91f15b1a1423849107775e11
SHA512:	608f95fa01b0ecfc45f81f8b1e56539f08aae01f5589e7ce98f150e6e6e580eed1e39910f0b39596bff68b1ce338f9d2cfb6727287ad644ec64bdf34be2e65ac
SSDEEP:	24576:Z+h5y9IA8yaw1fba/f84V6FXjhHavKVp7Ai4q0LD33bqJXCJIoYSUaJbjOpS/iqu:V
TLSH:	1616A431B13439D7C21F0435565FBD89430ABD83A3C66F8C518EFAF91EA69E7630690A
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

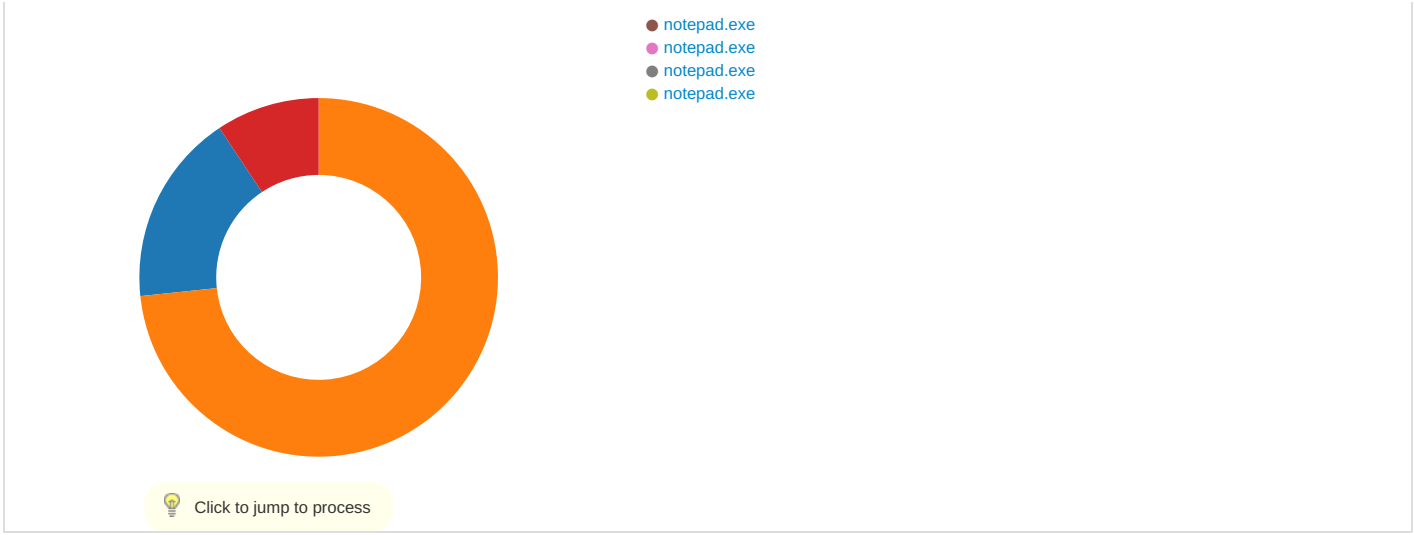
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000128Dh	2	embedded	Package	1019559	Client.exe	C:\Path\Client.exe	C:\Path\Client.exe	no
1	00207238h	2	embedded	Equation.3	3072				no

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **2284**, Parent PID: **576**

General

Target ID:	1
Start time:	17:41:16
Start date:	27/05/2022
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:	0x13f840000
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

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6C7CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6C7CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6C7CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6C7F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6C7F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6C7F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\704F0	success or wait	1	6C7F0648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\704F0	704F0	binary	04 00 00 00 EC 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00	success or wait	1	6C7F0648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 1A A1 17 BC 2B 72 D8 01 F0 04 07 00 F0 04 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000000F01FEC\Usage	ProductFiles	dword	1421541425	1421541426	success or wait	1	6C7F0648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000000F01FEC\Usage	ProductFiles	dword	1421541426	1421541427	success or wait	1	6C7F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\704F0	704F0	binary	04 00 00 00 EC 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 1A A1 17 BC 2B 72 D8 01 F0 04 07 00 F0 04 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 EC 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 04 07 00 F0 04 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C7F0648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: **1144**, Parent PID: **576**

General

Target ID:	2
Start time:	17:41:20
Start date:	27/05/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: **2224**, Parent PID: **1144**

General

Target ID:	3
Start time:	17:41:20
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	CmD.exe /C %tmp%\Client.exe A C
Imagebase:	0x4a540000
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: **2488**, Parent PID: **2224**

General

Target ID:	5
Start time:	17:41:21
Start date:	27/05/2022
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:	0x1340000
File size:	1019392 bytes
MD5 hash:	75C0471CCE805B589FDAF81D8D1D646C
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: 00000005.00000002.981449154.0000000003869000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.981449154.0000000003869000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.981449154.0000000003869000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, Metadefender, Browse • Detection: 51%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6DFF7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFF7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF0DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFFA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DF0DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFF7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFF7995	unknown

Analysis Process: notepad.exe PID: **2788**, Parent PID: **2488**

General

Target ID:	8
Start time:	17:41:45
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\notepad.exe
Imagebase:	0x830000
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: 00000008.00000000.962675676.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.962675676.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.962675676.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.963199556.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.963199556.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.963199556.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.963479345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.963479345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.963479345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Analysis Process: notepad.exe PID: **1112**, Parent PID: **2488**

General	
Target ID:	9
Start time:	17:41:46
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\notepad.exe
Imagebase:	0x830000
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: 00000009.00000002.966342475.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.966342475.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.966342475.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.965795915.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.965795915.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.965795915.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.966044835.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.966044835.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.966044835.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Analysis Process: notepad.exe PID: **1072**, Parent PID: **2488**

General	
Target ID:	10
Start time:	17:41:48
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\notepad.exe
Imagebase:	0x830000
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: 0000000A.00000000.969790709.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.969790709.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.969790709.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.972609635.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.972609635.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.972609635.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.973032461.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.973032461.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.973032461.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Analysis Process: notepad.exe PID: **1136**, Parent PID: **2488**

General

Target ID:	11
Start time:	17:41:51
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\notepad.exe
Imagebase:	0x830000
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: 0000000B.00000000.975022068.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.975022068.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.975022068.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.975431926.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.975431926.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.975431926.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.975260613.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.975260613.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.975260613.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: notepad.exe PID: **2960**, Parent PID: **2488**

General

Target ID:	12
Start time:	17:41:52
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\notepad.exe
Imagebase:	0x830000
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: 0000000C.00000002.977766193.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.977766193.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.977766193.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.977308196.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.977308196.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.977308196.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.977559635.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.977559635.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.977559635.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

Disassembly

No disassembly